



Instituto Politécnico de Coimbra
Instituto Superior de Contabilidade e Administração de Coimbra

Rita Cristina Rodrigues Carvalho

**A CONFIDENCIALIDADE DAS COMUNICAÇÕES
PRIVADAS DO TRABALHADOR:
[UM] DILEMA EMPRESARIAL.**

A Confidencialidade das Comunicações Privadas do Trabalhador: [Um] Dilema Empresarial.

Rita R. Carvalho

ISCAC | 2020

Coimbra, setembro de 2020



INSTITUTO POLITÉCNICO DE COIMBRA
INSTITUTO SUPERIOR DE CONTABILIDADE
E ADMINISTRAÇÃO DE COIMBRA

Rita Cristina Rodrigues Carvalho

**A Confidencialidade das Comunicações Privadas do
Trabalhador: [Um] Dilema Empresarial.**

Dissertação submetida ao Instituto Superior de Contabilidade e Administração de Coimbra, para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Solicitadoria, realizada sob a orientação do Professor Armando Ferreira Soares Veiga e coorientação da Professora Joana Filipa Brás.

Coimbra, setembro de 2020

TERMO DE RESPONSABILIDADE

Declaro ser a autora desta dissertação, que constitui um trabalho original e inédito, e que nunca foi submetido a outra instituição de ensino superior para obtenção de um grau académico ou outra habilitação. Atesto ainda que todas as citações estão devidamente identificadas e que tenho consciência de que o plágio constitui uma grave falta de ética, que poderá resultar na anulação da presente dissertação. Seguindo as normas institucionais do Instituto Politécnico de Coimbra e consequentemente do Instituto Superior de Contabilidade e Administração de Coimbra para a elaboração de uma dissertação, ter-se-á em conta na sua redação, a norma portuguesa ISO 405 (NP ISO 405) que transposta e harmoniza a norma internacional ISO 690:2010 na estrutura predefinida e estandardizada quanto às regras de formatação e citação.

PENSAMENTO

“Artigo 12.º

Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei.”

Declaração Universal dos Direitos Humanos

DEDICATÓRIA

Após uma longa caminhada, pontilhada por alguns obstáculos, dedico esta dissertação a todos que estiveram presentes nesta etapa da minha vida.

AGRADECIMENTOS

Ao Pedro, ao Miguel e à Bárbara.

Aos meus pais, porque sem eles não teria tido a oportunidade de realizar este trabalho.

Aos meus professores, pela partilha do conhecimento.

Aos meus colegas, que fizeram parte desta “luta”, especialmente *aos meus amigos* por estarem sempre disponíveis para dar a sua opinião crítica.

Ao meu orientador, Professor Armando Veiga, pelo apoio e conhecimento prestados durante a realização da dissertação.

À minha coorientadora, Professora Joana Brás, pelo conhecimento transmitido ao longo deste caminho.

RESUMO

A escolha do presente tema surge com a leitura de um acórdão do Tribunal Europeu dos Direitos Humanos, no qual, e no âmbito da primeira decisão, janeiro de 2016, as mensagens de caráter privado, enviadas por um trabalhador através de um aplicativo disponibilizado pelo empregador foram aceites como justa causa de despedimento.

Esta decisão potenciou a ideia de proceder a uma análise das garantias de proteção de um trabalhador, quando utiliza, o correio eletrónico, através de equipamentos disponibilizados pelo empregador, principalmente, os seus direitos de personalidade, os seus direitos fundamentais.

Com a entrada em vigor do Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, mais comumente designado por Regulamento Geral sobre a Proteção de Dados (RGPD), questionei-me sobre o porquê de uma decisão a favor do despedimento do trabalhador. Deste modo, considerei pertinente a concretização de uma investigação sobre os direitos do trabalhador no seio empresarial, bem como quais as medidas de proteção adicionais, que o RGPD pode trazer ao trabalhador enquanto titular de dados pessoais.

Tendo presente a evolução extraordinária das novas tecnologias de informação que são agora colocadas ao dispor do trabalhador pelas empresas, torna-se crucial o estudo deste tema tão atual.

Palavras-chave: correio eletrónico, regulamento, proteção de dados, acesso, trabalhador, empregador.

ABSTRACT

The choice of this theme comes with the reading of the application of the European Court of Human Rights, in which, and under the first decision, January 2016, private messages, sent by a worker through an application made available by the employer were accepted as a just cause of dismissal.

This decision has enhanced the idea of a need to analyse the guarantees of protection of a worker when using, email, through equipment made available by the employer, mainly their personality rights and fundamental rights.

With the Regulation (EU) 2016/679, by the European Parliament and the Council of 27 April 2016, most commonly referred to as the General Data Protection Regulation (GDPR), I questioned why a decision in favour of the dismissal of the worker. In this way, I considered it relevant to carry out an investigation concerning the rights of the worker within the business, as well as what additional protection measures, which the GDPR can bring to the worker as a personal data subject.

Bearing in mind the extraordinary evolution of new information technologies that are now put at the disposal of the worker by companies, it is crucial to study this issue so contemporary.

Keywords: email, regulation, data protection, access, worker, employer.

ÍNDICE GERAL

TERMO DE RESPONSABILIDADE.....	iii
PENSAMENTO.....	iv
DEDICATÓRIA	v
AGRADECIMENTOS	vi
RESUMO.....	vii
ABSTRACT.....	viii
ÍNDICE GERAL.....	ix
Lista de abreviaturas, acrónimos e siglas.....	xii
INTRODUÇÃO	1
CAPÍTULO I – Proteção dos dados pessoais: enquadramento	5
1. Considerações iniciais.....	5
1.1 Proteção no âmbito internacional e europeu	5
1.1.1 O direito à privacidade na Europa	7
1.1.1.1 A Convenção Europeia dos Direitos do Homem	7
1.1.2 A proteção de dados na Europa	8
1.1.2.1 A Carta dos Direitos Fundamentais da União Europeia.....	8
1.1.2.2 O Tratado sobre o Funcionamento da União Europeia	10
1.2 Proteção no quadro legislativo nacional	11
1.2.1 O direito à autodeterminação informativa	12
1.2.1.1 Tratamento informático dos dados pessoais.....	14
CAPÍTULO II – Os direitos <i>intuitu personae</i> do trabalhador	18
1. Breves Considerações	18
2. Direitos de personalidade do trabalhador vs Direito da empresa.....	19
2.1 Enquadramento legal.....	20

2.1.1	Normas legais: Constitucionais e Infraconstitucionais.....	21
2.1.1.1	Constituição da República Portuguesa	21
2.1.1.2	Os preceitos infraconstitucionais.....	28
CAPÍTULO III – As comunicações eletrónicas e a proteção de dados.....		45
1.	As novas tecnologias de informação e correspondente [ou não] relevância da violação da vida privada	45
1.1	Considerações iniciais	45
1.2	O RGPD e as relações laborais	46
1.2.1	Dados pessoais	47
1.2.1.1	Conceito e prazo de conservação	47
1.2.1.2	Tratamento: requisitos	51
1.2.1.3	Princípios inerentes ao tratamento.....	56
1.2.1.4	Responsabilidade pelo tratamento.....	56
1.3	Tratamento dados pessoais: contexto laboral.....	59
1.3.1	Privacy by Design and by default	60
1.4	<i>Profiling</i>	62
1.4.1	Definição de perfis: noção	62
1.5	As Avaliações de Impacto sobre a Proteção de dados	64
CAPÍTULO IV – As novas tecnologias informáticas e o trabalhador		68
1.	O uso das novas tecnologias de informação: internet e correio eletrónico.....	68
1.1	Para fins privados do trabalhador.....	68
1.1.1	O poder de controlo do empregador: problemas e limites.....	70
1.1.2	Caso paradigmático: Acórdão TEDH Barbulescu v Romania.....	73
1.2	Os meios de vigilância à distância	80
1.2.1	Correio eletrónico [ferramenta profissional e pessoal].....	81
1.2.1.1	O acesso às comunicações e sua divulgação	83

1.2.1.2	(I)licitude do despedimento pelo uso do correio eletrónico(?).....	84
1.2.2	Videovigilância: o que é?	86
1.2.2.1	Fonte de segurança ou fonte potencial de abusos?	86
1.2.2.2	Implementação e utilização de imagens	87
1.2.2.3	RGPD e a nova lei de execução na videovigilância	91
1.3	Videovigilância na relação laboral.....	92
1.3.1	A visualização de imagens e sua divulgação	92
CAPÍTULO V – A Autoridade de Controlo Nacional: CNPD.....		96
1.	A CNPD após publicação da Lei n.º 58/19, de 8 de agosto.....	96
CONCLUSÃO		99
REFERÊNCIAS BIBLIOGRÁFICAS		102
JURISPRUDÊNCIA		106
	Tribunal Europeu dos Direitos do Homem.....	106
	Supremo Tribunal de Justiça.....	106
	Tribunal da Relação de Coimbra	107
	Tribunal da Relação de Évora.....	107
	Tribunal da Relação de Guimarães	107
	Tribunal da Relação de Lisboa	108
	Tribunal da Relação do Porto	108
ARTIGOS ELETRÓNICOS.....		110
PÁGINAS ELETRÓNICAS.....		115

Lista de abreviaturas, acrónimos e siglas

Ac.	Acórdão
AIPD	Avaliações de Impacto sobre a Proteção de Dados
al.	Alínea
AR	Assembleia da República
art.	Artigo
CDFUE	Carta dos Direitos Fundamentais da União Europeia
CE	Comissão Europeia
CEDH	Convenção Europeia dos Direitos do Homem
Cfr.	Conforme
Cit.	Citação
CNPD	Comissão Nacional da Proteção de Dados
CP	Código Penal
CRP	Constituição da República Portuguesa
CT	Código do Trabalho
DL	Decreto-Lei
DUDH	Declaração Universal dos Direitos Humanos
EM	Estados Membros
EUA	Estados Unidos da América
GDPR	General Data Protection Regulation
GT29	Grupo de Trabalho do Artigo 29.º para a Proteção de Dados
n.º	Número
n.ºs	Numeros
p.	Página
pp.	Páginas

PIDCP	Pacto Internacional dos Direitos Cíveis e Políticos
RGPD	Regulamento Geral sobre a Proteção de Dados
Séc.	Século
ss	Seguintes
TEDH	Tribunal Europeu do Direitos do Homem
TFUE	Tratado sobre o Funcionamento da União Europeia
TJUE	Tribunal de Justiça da União Europeia
TUE	Tratado da União Europeia
STJ	Supremo Tribunal de Justiça
TRC	Tribunal da Relação de Coimbra
TRE	Tribunal da Relação de Évora
TRG	Tribunal da Relação de Guimarães
TRL	Tribunal da Relação de Lisboa
TRP	Tribunal da Relação do Porto
UE	União Europeia
WP	Working Party

INTRODUÇÃO

A evolução tecnológica e globalização vivenciada nos dias de hoje leva-nos a pensar que os trabalhadores, em matéria de proteção de dados, continuam numa posição fragilizada, ainda que modificações tenham ocorrido na legislação nacional.

É certo que a colocação à disposição do trabalhador de novas ferramentas de trabalho, conectadas em permanência, se traduzem num facilitismo a esse controlo e intromissão, pelo que nos perguntamos: quais as repercussões na relação laboral? Qual a liberdade do empregador no acesso ao conteúdo das mensagens de correio eletrónico? Pode o controlo ser realizado a todo o tempo? Quais as consequências na relação inerente ao contrato de trabalho¹ e à performance do trabalhador²?

Assim, importa ter presente que o trabalhador é uma pessoa e como tal, em nossa opinião, detentor de direitos *intuitu personae*. Direitos estes que se traduzem numa “manifestação da dignidade”³ do ser humano, e de acordo com JÚLIO GOMES, “não existe, por um lado, o trabalhador e, por outro, o cidadão”⁴. Assim se depreende que trabalhador e cidadão são um só, pelo que, assegurar que este detenha um adequado controlo da sua informação de “caráter pessoal”⁵ é deveras vital, assumindo, deste modo, uma grande importância para as garantias de proteção do trabalhador. Consequentemente, a violação de certos direitos constitui um atentado à pessoa do trabalhador e os abusos cometidos pelos empregadores levam a degradação da relação laboral. Logo, podemos perguntar: como se efetivam as garantias de proteção do trabalhador?

Tendo presente a problemática de fundo, comunicações privadas do trabalhador, importa para este estudo, refletir no que concerne à proteção de dados, levantando-se questões pertinentes quanto à proteção que os titulares de dados pessoais devem ter: o

¹ Que nos termos de art. 11.º do CT se traduz no contrato “pelo qual uma pessoa singular se obriga, mediante retribuição, a prestar a sua atividade a outra ou outras pessoas, no âmbito de organização e sob autoridade destas”. Sublinhado nosso, que pretende evidenciar que o trabalhador se encontra numa posição de subordinação.

² Cfr. Gomes, J. M. V. (2007). *In Direito do Trabalho, Relações Individuais de Trabalho, Vol. I*, Coimbra Editora, p. 265: diz-nos que: “existe uma assimetria de poder em regra presente na relação laboral”.

³ Vide Araújo, A. M. R. (2017). *In As transferências transatlânticas de dados pessoais*. Revista de Direitos Humanos e Democracia, ano 5, n.º 9, jan/jun, p. 203.

⁴ Gomes, J. M. V. (2007). *In Direito do Trabalho, (...)*, op. cit., p. 265.

⁵ Araújo, A. M. R. (2017). *In As transferências transatlânticas (...)*, op. cit., p. 203.

que pode mudar na relação de trabalho? Será necessário o aparecimento de um novo direito do trabalho? Ou será que com a aplicação efetiva, do Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, mais comumente designado por Regulamento Geral sobre a Proteção de Dados, e doravante designado por RGPD, pode reduzir os problemas de excesso de controlo pelo empregador sobre o trabalhador?

Consideramos que tendo sido concebido para servir as pessoas, a principal preocupação do tratamento de dados deve ser a sua proteção⁶ e esta deve ser conjugada com o exercício dos direitos fundamentais, respeitando sempre o princípio da proibição de excesso⁷. Temos assistido nas últimas décadas, a uma transformação sem igual da nossa sociedade porque esta vive sob o domínio das novas tecnologias criadas pelo homem⁸.

Destarte, este cenário de grande avanço tecnológico originou, ao nível da UE, alterações significativas em matéria de proteção de dados. Porém, constata-se que regulamentar o direito à privacidade, e a sua não violação, não foi previsto no RGPD. Em nossa opinião, esta situação pode potenciar a ocorrência da violação deste direito, pese embora, este se encontre legislado noutros diplomas como, e no caso de Portugal, na Constituição da República Portuguesa⁹, doravante CRP.

Desta situação, advém a necessidade de se aferir a violação do direito à vida privada para um momento ulterior, aquando da análise da licitude do tratamento, indo depender do julgamento de direitos conflitantes. É este o caso da relação laboral, na qual o direito do trabalhador à proteção dos seus dados pessoais, da vida privada, da sua correspondência [correio eletrónico], pode conflitar com o direito da empresa de gerir a

⁶ Segundo o exposto no considerando n.º 4 do RGPD existe a ideia de este não ser um direito absoluto, mas que deve ser tida em consideração a sua função na sociedade. Isto é, proteger os cidadãos, enquanto titulares de dados pessoais.

⁷ Vertido no art. 18.º da Constituição da República Portuguesa.

⁸ Rallo, A. (2018). *In Privacy and Freedom, European Data Protection Law Review*, n.º 4, 2, p. 150.

⁹ Nos termos do art. 26.º, n.º 1 da CRP: “A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação. (sublinhado nosso).

sua atividade empresarial¹⁰ e a exigência de execução do contrato de trabalho pelos trabalhadores.

A invasão das novas tecnologias na vida das empresas e, conseqüentemente, dos trabalhadores acarreta vantagens e riscos, designadamente, quanto aos direitos de personalidade, reduzindo ou tornando difusa a delimitação entre a vida profissional e a vida pessoal, acabando por culminar na invasão do trabalho na vida pessoal, “no domicílio do trabalhador”¹¹ e num maior controlo do empregador sobre o trabalhador, visto que, estas novas tecnologias “podem minar”¹² a privacidade do trabalhador.

Na dissertação, apresentamos, breves considerações iniciais, seguidas de um enquadramento legal internacional, europeu e nacional das normas que protegem os trabalhadores, enquanto titulares de dados pessoais. Posteriormente, estreitamos o estudo concentrando-o na problemática do uso do correio eletrónico e da videovigilância, analisando neste ponto as normas nacionais de proteção, abordando também o RGPD. Finalizamos, de forma breve, aludindo à Comissão Nacional de Proteção de Dados, daqui em diante CNPD, concretamente na questão da sua [nova] função.

Quanto ao procedimento metodológico a utilizar, este assenta no método sistemático e dedutivo de análise de normas supranacionais e nacionais, pela recolha de informação, designadamente, doutrina, legislação em vigor, artigos científicos, publicações, bem como jurisprudência nacional e europeia.

É perante este novo paradigma social, de trabalho com recurso a tecnologias de informação que as empresas devem tomar mais cuidado nos métodos usados para *controlarem*¹³ os seus trabalhadores. Considera-se que deve o legislador, perante as constantes violações de direitos dos trabalhadores, criar normas mais expressivas de sancionamento destas violações. Desta forma os trabalhadores podem sentir uma maior segurança no tratamento dos seus dados pessoais e, conseqüentemente, ter uma maior

¹⁰ Carvalho, P. M. (2013). In *Conferência Estado de direito e direitos fundamentais: A concretização dos direitos fundamentais pelos tribunais*. Julho, Assembleia da República, p. 42.

¹¹ Cfr. Carvalho, P. M. (2013). In *Conferência Estado de direito e direitos (...)*, op. cit., p. 42.

¹² *Idem*, p. 72.

¹³ Itálico nosso.

liberdade no consentir e no requer, v. g., o direito a serem informados e ao apagamento, sobre e dos seus dados.

CAPÍTULO I – Proteção dos dados pessoais: enquadramento

1. Considerações iniciais

O fenómeno da informática, o seu desenvolvimento e crescimento, operou no mundo uma verdadeira revolução nas relações pessoais, bem como nas relações profissionais. Hoje vivemos uma época de mudança dos hábitos comunicacionais que contribui para a transformação do desenvolvimento económico e social da nossa comunidade.

No seu desenvolvimento, a sociedade de informação, teve o contributo do computador, da internet e das comunicações eletrónicas que operaram uma revolução nos “métodos tradicionais para a organização, registo e utilização das informações”¹⁴.

Todas estas transformações, vistas como potenciadoras de menor proteção dos direitos dos titulares de dados pessoais, acabam por operar uma modificação no conceito de privacidade.

1.1 Proteção no âmbito internacional e europeu

Considerando a proteção de dados pessoais como outro meio de defesa da privacidade, gostaríamos de evidenciar que antes da existência de um direito à proteção de dados, nos dias de hoje¹⁵ efetivado pelo RGPD, a privacidade era já merecedora de tutela. Note-se que a *data protection*, enquanto regulamento, não veio substituir o, legalmente, constituído direito à privacidade, veio sim, e no nosso entendimento, reforçar a proteção em consequência direta das revoluções tecnológicas ocorridas nas últimas décadas do séc. XX e intensificadas no séc. XXI.

¹⁴ Cfr. Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores e as Novas Tecnologias de Informação e Comunicação: contributo para um estudo dos limites do poder de controlo electrónico do empregador*. Teses de doutoramento. s.l. Edições Almedina, p. 122.

¹⁵ Antes da criação do RGPD, a UE produziu a Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995.

O direito à privacidade teve a sua primeira enunciação na década de 40 do século passado^{16,17}. Mais tarde¹⁸ é aprovada a Declaração Universal dos Direitos Humanos [DUDH] que vem reconhecer um conjunto de direitos, “como é o caso do respeito pela privacidade”¹⁹.

Ainda que sem carácter vinculativo na UE, a DUDH, veio fomentar o início de um processo de tomada de consciência, na sociedade, no que aos direitos fundamentais concerne, em virtude da sua “grande força moral e política”²⁰, conforme secunda TERESA MOREIRA.

Ao postular, no art. 12.º da DUDH²¹ que não são permitidas ingerências na vida privada e que a correspondência goza de segredo, produziu-se um “precedente legislativo”²² que despoletou a criação de convenções internacionais com intuito, em nossa opinião, de reforçar a proteção dos direitos fundamentais²³.

Interessa notar que “os principais documentos de direito internacional”²⁴ que versam sobre a proteção dos direitos do homem não referem, expressamente, a proteção de dados pessoais, não obstante a proteção que garantem à privacidade. É por este motivo

¹⁶ Vide Declaração Americana dos Direitos do Homem, que no seu art. 5.º declara que “toda a pessoa tem direito à proteção da lei contra ataques abusivos à sua honra, reputação e vida privada e familiar”.

¹⁷ Nas palavras de Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit. p. 126.

¹⁸ A 10 de dezembro de 1948, em Paris.

¹⁹ Vide Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., p. 126.

²⁰ *Idem*, p. 127.

²¹ Que estatui: Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei.

²² Nas palavras de Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., p. 127.

²³ Tais como: Convenção Europeia dos Direitos do Homem (CEDH), art. 8.º: “Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária (...)”; Carta dos Direitos Fundamentais da União Europeia (CDFUE), art. 7.º: Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações; ou ainda o Pacto Internacional dos Direitos Cívicos e Políticos (PIDCP), art. 17.º: Ninguém será objeto de ingerências arbitrárias ou ilegais na sua vida privada, (...) ou na sua correspondência (...).

²⁴ Castro, C. S. (2005). *In Direito da Informática, Privacidade e Dados Pessoais*. Coimbra: Almedina, p. 39.

que se tem vindo a interpretar a proteção da privacidade como aglutinadora da proteção de dados pessoais.²⁵

1.1.1 O direito à privacidade na Europa

Em 1949, encontrava-se a Europa fragilizada após o término da II Guerra Mundial. Com o intuito de reforçar a proteção dos cidadãos foi criado o Conselho da Europa. Este visava a proteção dos direitos humanos e fundamentais, bem como a união entre “os diferentes estados europeus”^{26,27}. Tendo depois surgido outros dispositivos legais, sendo somente abordados os mais pertinentes para o âmbito do nosso estudo.

1.1.1.1 A Convenção Europeia dos Direitos do Homem

Do Conselho da Europa, surge, e nas palavras de TERESA MOREIRA²⁸, o documento mais importante: a Convenção Europeia dos Direitos do Homem (CEDH), criada com a finalidade de proteger direitos, até aí não eram valorizados, ou que não tinham proteção expressa e, por esse motivo alvo de constantes violações.

A CEDH, de acordo com TERESA MOREIRA²⁹, “pode considerar-se (...) o primeiro texto europeu” a consagrar o direito à privacidade. Com a CEDH definiram-se “garantias judiciais internacionais”³⁰ obtendo, deste modo, um lugar de destaque em relação a outros institutos de proteção dos direitos humanos nos estados que aceitaram a sua subscrição. Assim, a Convenção passa a deter caráter de obrigatoriedade. Ou seja, os estados que a implementam estão obrigados a respeitar o que ela estatui e a não permitir ingerências nem a violação dos direitos que protege.

O direito que determina o respeito pela privacidade tem consagração expressa no art. 8.º, n.º 1³¹ dispondo: “1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.”. Ademais, e em nossa opinião,

²⁵ No entendimento de Castro, C. S. (2005). *In Direito da Informática, Privacidade (...)*, op. cit., p. 39.

²⁶ Cfr. Estatuto do Conselho da Europa, de 05 de maio de 1949, art. 1.º, al. a), consultado em 26.12.2019, disponível em www.ministeriopublico.pt/instrumento/estatuto-do-conselho-da-europa-o.

²⁷ No início o Conselho da Europa era composto por 10 estados sendo, atualmente por 47.

²⁸ Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., p. 166.

²⁹ *Idem*, p. 166.

³⁰ *Ibidem*, p. 166.

³¹ Convenção Europeia dos Direitos do Homem.

esta norma vai mais além e reforça a restrição na intromissão, mesmo por parte das autoridades públicas, a estes direitos, quando determina no n.º 2 do art. 8.º: “Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei (...), seja necessária para a segurança (...) ou para a proteção dos direitos e das liberdades de terceiros”. Note-se, e assim secunda TERESA MOREIRA³², que o art. 8.º da CEDH tem também a vantagem, de associar o respeito pela vida privada ao segredo da correspondência, que no âmbito do presente estudo se associa ao correio eletrónico.

Assim, e como adiante tentaremos mostrar, a CEDH ao proteger a pessoa, enquanto cidadão, mira também a proteção do trabalhador, também ele um ser humano, que presta a uma atividade para um empregador.

1.1.2 A proteção de dados na Europa

A necessidade de proteção de dados advém de longa data³³. Em 1974, o Parlamento Europeu, elaborou um estudo no qual entendia ser pertinente a criação, rápida, de legislação europeia contributiva para “a uniformização das legislações”³⁴, dos estados membros, e para proteção dos cidadãos contra violações ou ingerências ocorridas pela via informática.

1.1.2.1 A Carta dos Direitos Fundamentais da União Europeia

Em 1981, através da Convenção 108, do Conselho da Europa, visou-se a proteção de dados³⁵ tendo como campo de aplicação “os ficheiros e tratamentos automatizados de

³² Cfr. Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., p. 166.

³³ Vide Pinheiro, A. S. (2015). *In Privacy e proteção de dados pessoais: a construção dogmática do direito à identidade informacional*. Tese de doutoramento. Lisboa: AAFDL- Associação Académica da Faculdade de Direito de Lisboa: “a discussão sobre a necessidade de aprovar um instrumento europeu de proteção de dados começou na década de 70”, p. 573.

³⁴ *Idem*, p. 573.

³⁵ Nos termos do art. 1.º, epígrafado de: Objectivos e finalidades: “ a presente convenção destina-se a garantir, no território de cada Parte, a todas as pessoas singulares, seja qual for a sua nacionalidade ou residência, o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal que lhes digam respeito («proteção dos dados»), consultado em: 26.12.2019, disponível em: <https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm>.

dados de carácter pessoal nos setores público e privados”³⁶. Na nossa opinião, este documento internacional aponta para a garantia do direito à liberdade informática ou direito à autodeterminação informacional³⁷ com o intuito de aumentar a proteção das pessoas, [e subentenda-se dos trabalhadores], dos seus direitos, enquanto utilizadores da informática e das tecnologias de comunicação.

No entanto, o direito à proteção de dados pessoais, só foi expressamente previsto com a aprovação da CDFUE^{38,39}, dispendo o art. 8.^o⁴⁰ sobre o direito à proteção de dados que deve ter um tratamento leal, para fins determinados e com o consentimento do titular dos dados ou outro fundamento legítimo previsto na lei, sendo que os titulares dos dados têm o direito de acesso aos dados objeto de tratamento e de solicitar a retificação quando entendam que os mesmos não estão corretos⁴¹.

Ainda que não se possa confundir o direito ao respeito pela vida privada e o direito à proteção de dados, eles acabam por se intersetar, sendo importante a correlação entre o art. 7.^o e art. 8.^o da CDFUE, porque “as raízes do direito à proteção de dados residem no

³⁶ Cf. art. 3.^o da Convenção n.^o 108, consultado em: 26.12.2019, disponível em: <https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm>.

³⁷ Direito à autodeterminação informacional que será desenvolvido mais adiante.

³⁸ Carta dos Direitos Fundamentais da União Europeia (CDFUE)

³⁹ Em 1992, a 7 de fevereiro, foi assinado em Maastricht o Tratado da União Europeia (TUE). Este tratado incorporou no direito originário, a jurisprudência criada pelo Tribunal de Justiça das Comunidades Europeias (TJCE). O TUE potenciou também “a conexão de três sistemas diferentes: o da UE, o do Conselho da Europa *ex vi* CEDH, da própria CEDH e da jurisprudência do Tribunal Europeu dos Direitos Humanos” (TEDH), nas palavras de Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., p. 192.

⁴⁰ Epigrafiado: Proteção de dados pessoais: “Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito. 2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.”

⁴¹ Cfr. Kranenborg, H. (2014). *In The EU Charter of Fundamental Rights, A commentary*. Edit Steve Peers et. Al., Hart Publishing, pp. 228 e 229.

direito à privacidade” de acordo com HERKE KRANENBORG⁴² e também TERESA COELHO⁴³.

A Carta foi formalmente adotada em Nice, em 07 dezembro de 2000, pelo Parlamento Europeu, pelo Conselho e pela Comissão⁴⁴, criando-se um documento para toda a Europa, com a aplicabilidade a englobar não só os cidadãos dos Estados Membros, mas também quem pela Europa passa.

1.1.2.2 O Tratado sobre o Funcionamento da União Europeia⁴⁵

Com a entrada em vigor do Tratado sobre o Funcionamento da União Europeia (TFUE), perfilha-se que “o art. 16.^o⁴⁶ é o preceito base da proteção de dados”⁴⁷, reconhecendo-se o seu n.º 1 como “o direito à proteção de dados”⁴⁸ pessoais, e atribuindo-se no n.º 2, à UE, as competências legislativas para versar sobre o tema “em todas as áreas da sua incumbência”⁴⁹.

Existe o entendimento que “o regime da proteção de dados”⁵⁰, nas palavras de LUÍS NETO GALVÃO⁵¹, “veio a ser constitucionalmente reforçado com a consagração do art. 16.^o do TFUE”⁵². Ademais, e pelo facto de se consubstanciar “pela primeira vez”⁵³

⁴² Kranenborg, H. (2014). In *The EU Charter of Fundamental Rights (...)*, op. cit.: “The right to privacy and the right to data protection are closely linked, but should not be seen as one and the same right”, p. 229.

⁴³ Moreira, T. A. C. (2010). In *A Privacidade dos Trabalhadores (...)*, op. cit., “Uma nota diferente em relação à Carta dos Direitos Fundamentais da União Europeia consiste no facto do conceito de vida privada referido abarcar a proteção de dados pessoais (...)” p. 200.

⁴⁴ A Carta tornou-se juridicamente vinculativa para a UE com a entrada em vigor do Tratado de Lisboa, em dezembro de 2009, tendo agora o mesmo valor jurídico que os Tratados da UE.

⁴⁵ Ou Tratado de Lisboa, porque foi assinado na cidade Lisboa pelos Estados Membros da UE, em 13 de dezembro de 2007, teve uma *vacatio legis* de 2 anos, entrando em vigor a 01 de dezembro de 2009.

⁴⁶ Nos termos do n.º 1 do art. 16.^o: “Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito.”

⁴⁷ Cfr. Araújo, A. M. R. (2017). In *As transferências transatlânticas (...)*, op. cit., p. 204.

⁴⁸ *Idem*, p. 204.

⁴⁹ *Ibidem*, p. 204.

⁵⁰ De acordo com Porto, M. L. e Anastácio. G. (2012). In *Tratado de Lisboa, Anotado e Comentado*. Coimbra. Edições Almedina, p. 252.

⁵¹ Vide Porto, M. L. e Anastácio. G. (2012). In *Tratado de Lisboa, (...)*, op. cit, p. 252.

⁵² *Idem*, p. 252.

⁵³ *Ibidem*, p. 252.

num pilar jurídico, “expressamente aplicável ao tratamento de dados pessoais (...) pelos Estados Membros”⁵⁴, traduz-se num avanço em relação ao regime anterior⁵⁵.

Encontramos o art. 16.º do TFUE integrado na Parte I intitulado “Os Princípios”, sob o título II – “Disposições de Aplicação Geral”, que consubstancia, deste modo, “um verdadeiro regime geral de proteção de dados”⁵⁶.

Quanto ao direito derivado, este compunha-se pela existência de uma Diretiva⁵⁷ relativa à proteção das pessoas singulares no que concerne ao tratamento de dados pessoais e à livre circulação desses dados, que vigorou até 25 de maio de 2018⁵⁸. Este documento cumpriu o papel de harmonizar as regras existentes nos vários ordenamentos jurídicos dos EM.

Destarte, com o novo quadro jurídico de proteção de dados, ocorre a revogação da Diretiva, mas não dos seus princípios e objetivos. Com a mudança e implementação do RGPD visa-se tão-somente, adaptar os princípios e objetivos, aos novos problemas que a evolução tecnológica e a globalização vieram trazer à UE e aos EM.

Na UE e com a CDFUE⁵⁹, contrariamente, ao que acontece em diplomas como a DUDH, PIDCP ou a CEDH, existe o reconhecimento do direito à proteção de dados e do direito à privacidade como direitos autónomos.

1.2 Proteção no quadro legislativo nacional

Desde que, em 1890, Warren e Brandeis definiram *The Right to Privacy*, como “*the right to be let alone*”⁶⁰, ocorreu uma grande transformação na forma como podem ser violados os assuntos pessoais. De acordo com TERESA MOREIRA, ideia que

⁵⁴ De acordo com Porto, M. L. e Anastácio. G. (2012). *In Tratado de Lisboa, (...)*, op. cit, p. 252.

⁵⁵ Do Tratado das Comunidades Europeias (TCE), art. 286º.

⁵⁶ Cfr. Porto, M. L. e Anastácio. G. (2012). *In Tratado de Lisboa, (...)*, op. cit, p. 253.

⁵⁷ Diretiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro, que necessitava de transposição para os ordenamentos jurídicos dos Estados Membros. Em Portugal a transposição ocorreu com a publicação da Lei n.º 67/98, de 26 de outubro.

⁵⁸ Data em que é substituída pelo RGPD com aplicação direta nos EM da UE.

⁵⁹ De acordo com art. 7.º da CDFUE: Respeito pela Vida privada e familiar e art. 8.º da CDFUE: Proteção de Dados Pessoais.

⁶⁰ Warren, S. D. & Brandeis, L. D. (1890) *In The Right to Privacy, Harvard Law Review*, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220 disponível em: <https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>;

também postulamos, não se pode estudar o direito à privacidade sem ter presente o conceito de dados pessoais e o direito à autodeterminação informativa⁶¹. Portugal foi um país pioneiro ao consagrar o direito à autodeterminação informativa, na CRP. Em que se traduz o este direito? Preconiza CATARINA CASTRO, que ele “nasce, (...), para garantir um direito à intimidade privada no que ao tratamento de dados pessoais”⁶² concerne.

1.2.1 O direito à autodeterminação informativa

Decorrente da rápida evolução tecnológica e do recurso à informática como meio de comunicação pessoal e profissional, houve a necessidade de legislar a temática da proteção de dados, porque nos dias de hoje é quase impossível delinear a fronteira que separa um e outro, bem como para se qualificar esta proteção como garantia do direito à privacidade⁶³ reforçando-se este último direito.

Tal como anteriormente referido, Portugal foi precursor ao estatuir, constitucionalmente, o direito à autodeterminação informativa. Segundo GLORIA FUSTER⁶⁴ Portugal foi o primeiro país a fazê-lo, ao nível Europeu.

⁶¹ Cfr. Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., p. 29.

⁶² Vide Castro, C. S. (2005). *In Direito da Informática, Privacidade (...)*, op. cit., p. 25.

⁶³ A reserva da vida privada encontra proteção legal, desde 1966, no ordenamento jurídico português – art. 70.º a 80.º do CC, cfr. Marques, G. e Martins, L. (2006). *In Direito da Informática, 2.ª edição refundida e atualizada*. Coimbra. Edições Almedina, p. 157; constitucionalmente encontra-se estatuída no art. 26.º, n.º 1 da CRP.

⁶⁴ Fuster, Gloria Gonzalez (2017). *In Law, Governance and Technology Series, Issues in Privacy and Data Protection, volume 16*. Springer International Publishing, “Historically, the first European Country to incorporate specific provisions on automated data processing in its fundamental law (...)” p. 66.

No ordenamento jurídico nacional, no art. 35.º da CRP⁶⁵, encontra-se “um direito especial de personalidade”⁶⁶ que visa proteger o cidadão relativamente ao uso da informática. Da sua leitura se depreende existir “um conjunto de direitos fundamentais”⁶⁷ que visam travar o tratamento da pessoa como “simples objeto de informações”⁶⁸, sem respeito pelos princípios básicos que lhe são inerentes. Entende-se que legislador português, e bem, terá previsto um abuso, por parte de terceiros, no uso das novas tecnologias de comunicação para aceder a informação pessoal, criando este preceito para proteger a pessoa, que usa a informática como meio comunicacional, tal como quando enviava uma simples carta.

Sem especificar, isto é, olhando globalmente para este preceito, verificamos que “consagra a proteção dos cidadãos”⁶⁹ quando esteja em vista o “tratamento de dados pessoais informatizados”⁷⁰.

De acordo com ALEXANDRE PINHEIRO⁷¹ “a identidade informacional” enquadra-se no núcleo dos direitos de personalidade, da proteção de dados pessoais. Para este autor, o “direito à identidade informacional”⁷² tem assento constitucional, não só

⁶⁵ Cfr. art. 35.º: “1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei. 2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente. 3. A informática não pode ser utilizada para 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. 4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei. 5. É proibida a atribuição de um número nacional único aos cidadãos. 6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional. 7. Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei”.

⁶⁶ De acordo com Castro, C. S. (2005). *In Direito da Informática, Privacidade (...)*, op. cit., p. 29.

⁶⁷ Cfr. Castro, C. S. (2005). *In Direito da Informática, Privacidade (...)*, op. cit., p. 33.

⁶⁸ Vide Canotilho, J. J. G. & Moreira, V. (2014). *In Constituição da República Anotada – Vol. I, 4ª edição*. Coimbra: Editora, p. 551.

⁶⁹ *Idem*, p. 550.

⁷⁰ Nas palavras de Neves, R. C. (2011). *In As ingerências nas comunicações electrónicas em processo penal*. 1.ª Edição, Coimbra: Coimbra Editora grupo Wolters Kluwer, p. 32.

⁷¹ Vide Pinheiro, A. S. (2015). *In Privacy e proteção de dados pessoais (...)*, op. cit., p. 818.

⁷² *Idem*, p. 818.

através do art. 35.º da CRP, mas, principalmente, do art. 26.º, n.º 1 da CRP que versa sobre a reserva da vida privada, revestindo desta forma “natureza de direito de personalidade”⁷³.

Com a consagração do direito à autodeterminação informativa pretende-se exercer a proteção da pessoa [na nossa opinião, nesta categoria enquadra-se o trabalhador, por ser detentor de direitos *intuitu personae*], quando pela via da informática ocorra: “recolha, armazenamento, utilização e transmissão dos seus dados pessoais”⁷⁴.

No entendimento de GOMES CANOTILHO e VITAL MOREIRA ⁷⁵, o crescimento e evolução das tecnologias de comunicação através de meios eletrónicos que deixam marcas digitais, v.g.: consulta de *sites* na internet, uso do correio eletrónico para trocas de mensagens e meios de vigilância, para o empregador [como forma de controlo], *inter alia*, como que obrigaram ao desenvolvimento de importantes garantias contra a violação dos dados pessoais informatizados.

1.2.1.1 Tratamento informático dos dados pessoais

Releva para o nosso estudo a abordagem à autodeterminação informativa, visto esta se consubstanciar na proteção da privacidade. Assim, no nosso entendimento, a proteção prevista no art. 35.º da CRP decompõe-se no: **a)** direito de acesso das pessoas aos registos informáticos; **b)** direito à retificação e atualização dos dados pessoais; **c)** direito à eliminação de dados pessoais que estejam errados⁷⁶. Pelo que, o aqui estatuído e aplicado nos dias de hoje ao tratamento de dados pessoais, comporta um reforço da proteção do cidadão quando conectado com o RGPD.

Detalhando neste ponto o art. 35.º da CRP, e principiando pelo vertido no seu n.º 1: “direito ao conhecimento dos dados pessoais”⁷⁷, entende-se que este será o mais básico dos direitos. Ou seja, para que o titular possa decidir em relação aos mesmos é necessário

⁷³ Assim secunda Pinheiro, A. S. (2015). *In Privacy e proteção de dados pessoais (...)*, op. cit., p. 818.

⁷⁴ Nas palavras de Neves, R. C. (2011). *In As ingerências nas comunicações (...)*, op. cit., pp. 57 e 58.

⁷⁵ Vide Canotilho, J. J. G. & Moreira, V. (2014). *In Constituição da (...)*, op. cit., p. 550.

⁷⁶ Sendo este também o entendimento de doutrinadores: Canotilho, J. J. G. & Moreira, V. (2014). *In Constituição da (...)*, op. cit., p. 551 e Castro, C. S. (2005). *In Direito da Informática, Privacidade (...)*, op. cit., pp. 34 e 35.

⁷⁷ Canotilho, J. J. G. & Moreira, V. (2014). *In Constituição da (...)*, op. cit., p. 551.

que tenha conhecimento – “habeas data”⁷⁸ que se pode traduzir no direito de o titular dos dados aceder a todas as informações sobre os mesmos.

Nesta medida, conforme GOMES CANOTILHO e VITAL MOREIRA⁷⁹ e CATARINA CASTRO⁸⁰, o direito à autodeterminação informativa subdivide-se noutros como o direito de acesso – que se impõe quer a entidades públicas como privadas. Ou seja, se o cidadão desejar consultar os seus dados, objeto de tratamento informatizado, tanto as entidades públicas como as privadas têm obrigação de conceder permissão de acesso⁸¹, porque permite ao titular dos dados perceber se o tratamento dos seus dados não foi desvirtuado⁸².

Conforme secunda BENJAMIM SILVA RODRIGUES⁸³, o direito à privacidade viu o seu âmbito arrastado à informática, designadamente à proteção de dados pessoais, por via do art. 35.º da CRP. Assim, importa notar o previsto no n.º 2 deste artigo, nele se dispõe que a lei deve definir o conceito de dados pessoais, criar condições para um tratamento automatizado e que a garantia de proteção deve ocorrer através de uma entidade administrativa independente⁸⁴.

Releva ainda para o objeto do nosso estudo o n.º 4 do art. 35.º da CRP, que proíbe o acesso a dados pessoais por terceiros, devendo a noção de terceiros ser totalmente abrangente, *i. e.*, “abranger toda as pessoas”⁸⁵. Deste modo, no seu âmbito encontra-se prevista a necessidade de proteção da vida privada, sendo este preceito muito relevante para “garantir o «right to be let alone»”⁸⁶. Note-se que é através deste direito que se

⁷⁸ Vide Neves, R. C. (2011). *In As ingerências nas comunicações (...)*, op. cit., p. 59.

⁷⁹ Canotilho, J. J. G. & Moreira, V. (2014). *In Constituição da (...)*, op. cit., p. 552.

⁸⁰ Castro, C. S. (2005). *In Direito da Informática, Privacidade (...)*, op. cit., p. 34.

⁸¹ *Idem*, p. 34.

⁸² Na nossa opinião, este é um dos problemas existentes nas relações laborais, visto que o trabalhador receia exercer em pleno os seus direitos com medo de represálias ou de tornar a relação laboral conflituosa.

⁸³ Rodrigues, B. S. (2009). *In Das Escutas Telefónicas À obtenção da prova (em ambiente) digital - Tomo II, 2ª Edição*, Coimbra: Editora, pp. 251 e 252.

⁸⁴ Seguindo a linha de pensamento de Castro, C. S. (2005). *In Direito da Informática, Privacidade (...)*, op. cit., p. 35: “o n.º 2 assume particular importância por nele se inscrever, desde a Revisão Constitucional de 1997, a previsão constitucional de uma autoridade independente cuja função primordial passará pela proteção de dados pessoais do cidadão”.

⁸⁵ Cfr. Canotilho, J. J. G. & Moreira, V. (2014). *In Constituição da (...)*, op. cit., p. 554.

⁸⁶ Castro, C. S. (2005). *In Direito da Informática, Privacidade (...)*, op. cit., p. 36.

impede o acesso a dados pessoais contidos em ficheiros de tratamento de dados, por terceiros.

In casu, consideramos o n.º 4 do art. 35.º da CRP, deveras vital para impedir que os dados cedidos pelo trabalhador ao empregador possam ser divulgados. De acordo com GOMES CANOTILHO e VITAL MOREIRA, os responsáveis pelo ficheiro de dados devem garantir o sigilo da informação⁸⁷, posição que também nós perfilhamos.

Do mesmo modo, entendemos, e outrossim CATARINA CASTRO que, não só o acesso é proibido, como também a divulgação, bem como o desvirtuamento para finalidades distintas da que “esteve na origem do tratamento”⁸⁸.

Porém, importa notar que é possível restringir esta proibição “nos casos excepcionais previstos na lei”⁸⁹. No entanto, a mesma deve obedecer ao princípio da proibição de excesso (n.º 2, do art. 18.º da CRP), pois as restrições só podem acontecer quando estritamente necessárias⁹⁰ para “defesa de direitos ou bens constitucionalmente protegidos”⁹¹

Pode assim dizer-se, e nas palavras de RITA NEVES, que o direito à autodeterminação informacional, tratado no art. 35.º da CRP, engloba nos dias de hoje um conjunto de outros direitos, como sejam: **a)** conhecer a finalidade do tratamento dos dados pessoais; **b)** proibir o acesso aos dados de terceiros; **c)** direito de acesso; **d)** direito de controlo; **e)** direito de conhecer os dados; **f)** direito à retificação; **g)** direito à eliminação; e **h)** direito à não divulgação dos dados⁹².

Ainda na temática da proteção de dados pessoais, existe o entendimento⁹³ que o art. 35.º da CRP é o principal “regulador da proteção da privacidade no que ao tratamento de dados pessoais” concerne. Porém, existem outros preceitos constitucionais que

⁸⁷ Cfr. Canotilho, J. J. G. & Moreira, V. (2014). *In Constituição da (...)*, op. cit., p. 554.

⁸⁸ Vide Castro, C. S. (2005). *In Direito da Informática, Privacidade (...)*, op. cit., p. 36.

⁸⁹ De acordo com o n.º 4, do art. 35.º da CRP, *in fine*.

⁹⁰ Veja-se Canotilho, J. J. G. & Moreira, V. (2014). *In Constituição da (...)*, op. cit., p. 555.

⁹¹ *Idem*, p. 555.

⁹² Neves, R. C. (2011). *In As ingerências nas comunicações (...)*, op. cit., p. 58.

⁹³ Cfr. Castro, C. S. (2005). *In Direito da Informática, Privacidade (...)*, op. cit., p. 39.

assumem um papel preponderante e que juntos formam um núcleo forte⁹⁴ da proteção da privacidade quanto aos dados pessoais, seu tratamento, a saber: art. 26.º, n.º 1 da CRP⁹⁵; art. 34.º, n.º 1 e n.º 4 da CRP⁹⁶; art. 32.º, n.º 8 da CRP⁹⁷ e o art. 37.º da CRP⁹⁸.

Em suma, considera-se que a proteção de dados pessoais comporta uma dimensão da proteção da privacidade das pessoas. No mundo digital de hoje, assume especial relevância o direito à autodeterminação informativa, posição sustentada por BENJAMIM SILVA RODRIGUES⁹⁹, pois este direito confere ao titular dos dados exercer um controlo sobre os dados que lhe sejam inerentes, e conseqüentemente, proteger aspetos da sua vida privada (nos termos do n.º 4 do art. 35.º da CRP) pelo exercício do direito «to be let alone» ao proibir o acesso por terceiros.

⁹⁴ Veja-se Castro, C. S. (2005). *In Direito da Informática, Privacidade (...)*, op. cit., p. 39 e Rodrigues, B. S. (2009). *In Das Escutas Telefónicas À obtenção (...)* Tomo II, op. cit., p. 271.

⁹⁵ “A todos são reconhecidos os direitos (...), à reserva da intimidade da vida privada (...)”, de acordo com Canotilho, J. J. G. & Moreira, V. (2014). *In Constituição da (...)*, op. cit., p. 467, este direito analisa-se através de dois direitos menores: impedir o acesso de estranhos e não divulgação da informação.

⁹⁶ “O (...) sigilo da correspondência e dos outros meios de comunicação privada são invioláveis”, proibindo a ingerência das autoridades públicas e privadas (...) nas telecomunicações e nos demais meios de comunicação” [correio eletrónico, perspetiva que interessa, *in casu*].

⁹⁷ No âmbito das garantias em processo criminal, “São nulas todas as provas obtidas mediante (...), abusiva intromissão na vida privada, (...), na correspondência ou nas telecomunicações”.

⁹⁸ “Todos têm o direito de exprimir e divulgar livremente o seu pensamento pela palavra, (...) por qualquer outro meio, bem como o direito de informar, de se informar e de ser informados, sem impedimentos nem discriminações”.

⁹⁹ Cfr. Rodrigues, B. S. (2009). *In Das Escutas Telefónicas À obtenção (...)* Tomo II, op. cit., quando nos diz que “Existe um verdadeiro poder de controlo e disposição sobre os dados de carácter pessoal” p. 255.

CAPÍTULO II – Os direitos *intuitu personae* do trabalhador

1. Breves Considerações

As novas tecnologias¹⁰⁰, tal como anteriormente notado, vieram transformar a sociedade, e bem assim, também o Direito sentiu necessidade de se adaptar na medida em que este só pode ser explicado quando “inserido na ordem social”¹⁰¹.

Neste sentido é muito importante que se conheça a “sociedade de informação”¹⁰² para que possa ser entendido o direito à privacidade num mundo digital¹⁰³ como este no qual nos encontramos.

Nos dias de hoje, a grande questão relacionada com a privacidade, na “vertente informacional”¹⁰⁴, está na proteção dos dados pessoais dos seus utilizadores. Este dilema coloca-se a toda a sociedade, no seu conjunto, importando para este estudo, especificamente, relações laborais, que foram invadidas por problemas ligados ao uso de aplicativos digitais, colocados ao dispor do trabalhador pelo empregador. É, assim, nesta medida que se “justifica a intervenção do direito”¹⁰⁵, bem como dos direitos fundamentais previstos na Constituição ou em legislação infraconstitucional.

¹⁰⁰ A utilização da informática despoletou o surgimento de um novo direito: o direito à *privacy*. Nas palavras de CATARINA CASTRO *In Direito da Informática, Privacidade (...)*, op. cit., p. 17,

“foi autonomizado pela primeira vez em 1890” nos EUA com a publicação na “Harvard Law Review, um artigo sob o título “The Right to Privacy”. Este artigo redigido para defesa do “right to be let alone” visava dirimir as ingerências na vida privada dos seus autores. Os tribunais americanos, após a publicação deste artigo, foram levados a produzir decisões quanto a esta matéria em variadíssimos casos. É importante tomar em consideração o direito à privacidade, porque a dependência que existe hoje em relação às novas tecnologias de informação como que nos “transformou em pessoas eletrónicas”. De relevar, que inclusive enquanto trabalhadores, numa empresa, se coloca este dilema da privacidade e do tratamento de dados, bem como da necessidade de segurança dos mesmos. Vide Castro, C. S. (2005). *In Direito da Informática, Privacidade (...)*, op. cit., p. 20: “No emprego a entidade patronal conhece informação nossa (...) e é mesmo obrigada a transmiti-la a outras entidades – v.g., para efeitos fiscais (...). A nossa entrada no emprego foi controlada através de um registo eletrónico de dados. (...) a nossa entidade patronal conhece os nossos movimentos espaço-temporais (...). No exercício das nossas tarefas, ou não..., (...) enviámos e recebemos mensagens de correio eletrónico (...)”.

¹⁰¹ Veja-se Pinheiro, A. S. (2015). *In Privacy e proteção de dados pessoais (...)*, op. cit., p. 103.

¹⁰² *Idem*, p. 104.

¹⁰³ A utilização da informática

¹⁰⁴ Pinheiro, A. S. (2015). *In Privacy e proteção de dados pessoais (...)*, op. cit., p. 104.

¹⁰⁵ *Idem*, p. 104.

Conforme postula ALEXANDRE SOUSA PINHEIRO¹⁰⁶ “o direito, por meio de instrumentos como os direitos de personalidade, da proteção da vida privada, e (...), por meio da proteção de dados pessoais” cimentou um trabalho vital com o intuito de centralizar na pessoa, a proteção dos seus dados pessoais, *i. e.*, a pessoa é sujeito logo titular de dados pessoais¹⁰⁷.

Ponderado tudo o anteriormente exposto, e porque devemos entender a proteção como garantia da pessoa que é titular de dados, compreendemos tal como ALEXANDRE SOUSA PINHEIRO¹⁰⁸ que a proteção de dados deve ser qualificada como um direito *intuitu personae*, porquanto exerce proteção sobre um “bem da personalidade”¹⁰⁹.

2. Direitos de personalidade do trabalhador vs Direito da empresa

Considerando a relação subjacente num contrato de trabalho, relação de subordinação do trabalhador ao empregador, constatamos ser possível a existência da colisão de direitos, concretamente, os direitos do trabalhador e os direitos da empresa.

Como se sabe, e de acordo com JOÃO LEAL AMADO¹¹⁰ na relação laboral, o trabalhador “surge como sujeito juridicamente subordinado e adstrito”¹¹¹, *v. g.*, do dever de obediência em relação às diretivas emanadas pelo empregador que detém uma “posição de domínio”¹¹² decompondo-se em três poderes, a saber: diretivo, regulamentar e disciplinar¹¹³.

Entendemos que quando uma empresa contrata um trabalhador recebe “também um ser humano”¹¹⁴. Assim, tomando em consideração esta afirmação, o trabalhador não

¹⁰⁶ Pinheiro, A. S. (2015). *In Privacy e proteção de dados pessoais (...)*, op. cit., p. 105.

¹⁰⁷ *Idem*, p. 105.

¹⁰⁸ Cfr. Pinheiro, A. S. (2015). *In Privacy e proteção de dados pessoais (...)*, op. cit., p. 803.

¹⁰⁹ *Idem*, p. 803.

¹¹⁰ *Vide* Amado, J. L. (2019). *In Contrato de trabalho: noções básicas*. Coimbra: Edições Almedina, p. 203.

¹¹¹ *Idem*, p. 203.

¹¹² *Ibidem*, p. 203.

¹¹³ Diretivo: enquanto poder de direção e que consiste na capacidade de emitir ordens, instruções ou orientações; disciplinar: faculdade de sancionar o trabalhador.

¹¹⁴ Assim nos diz Amado, J. L. (2019). *In Contrato de trabalho (...)*, op. cit., p. 209: “(...) o famoso empresário Henry Ford queixou-se que, ao contratar um par de mãos, (...)”.

pode ser uma pessoa que se limita a obedecer, cegamente^{115,116}, às instruções transmitidas pelo empregador, ele é acima de tudo “uma pessoa e um cidadão”¹¹⁷.

Por conseguinte, talvez se deva questionar: pode o empregador controlar, sem regra nem medida, um seu trabalhador? Não deverá ele ser visto como detentor de direitos de personalidade? Tem o trabalhador direito à privacidade, por exemplo, quando utiliza o correio eletrónico da empresa? Goza o trabalhador do direito à confidencialidade das suas mensagens, enviadas e/ou recebidas, através do correio eletrónico da empresa? E se for através de outros aplicativos?¹¹⁸ Pode o trabalhador expressar livremente o seu pensamento, a sua opinião? Dentro da empresa ou [só] fora dela? Deve o empregador utilizar a videovigilância no local de trabalho com vista à fiscalização da prestação de trabalho?

Os quesitos supra enunciados permitem a constatação da existência de um conflito de direitos, não dos “direitos enquanto trabalhadores (...) mas os seus enquanto pessoa e cidadão”¹¹⁹.

Posto isto, como pode ser alcançado o “desejado ponto de equilíbrio”¹²⁰ ?

2.1 Enquadramento legal

Os direitos de personalidade do trabalhador, antes de expressamente consagrados, no Código do Trabalho, já tinham proteção no ordenamento jurídico nacional, seja por via do previsto no n.º 1 do art. 16.º da CRP¹²¹, denominado princípio da cláusula aberta, que atribui aos diplomas análogos à CRP o mesmo âmbito de proteção que o estatuído

¹¹⁵ Como se não fosse detentor de pensamentos, emoções, sentimentos...

¹¹⁶ Cfr. expressa Amado, J. L. (2019). *In Contrato de trabalho (...)*, op. ct., “alguém que se dedica a cumprir escrupulosamente as múltiplas obrigações emergentes do contrato de trabalho”, p. 209.

¹¹⁷ *Idem*, p. 209.

¹¹⁸ V.g. *Messenger, Skype, WhatSapp, LinkedIn*, entre outros.

¹¹⁹ Cfr. Amado, J. L. (2019). *In Contrato de trabalho (...)*, op. ct., p. 211.

¹²⁰ *Idem*, p. 212.

¹²¹ Nos termos do art. 16.º, n.º 1 da CRP: “Os direitos fundamentais consagrados na Constituição não excluem quaisquer outros constantes das leis e das regras aplicáveis de direito internacional”.

pela mesma, quer através do art. 18.º da Lei Fundamental, determinando esta um reconhecimento de eficácia dos direitos fundamentais nas relações entre particulares¹²².

Conforme nos transmite GUILHERME DRAY¹²³, “os direitos de personalidade envolvem, v.g., a liberdade de expressão e de opinião (...), o direito à reserva da intimidade da vida privada (...), bem como a criação de regras sobre o acesso a mensagens de correio eletrónico (...)”, que para nós, abrangem também a implementação da videovigilância no local de trabalho.

De acordo com PEDRO PAIS DE VASCONCELOS¹²⁴, “a personalidade é uma qualidade: a qualidade de ser pessoa”. Neste sentido, e na nossa perspetiva, esse é um dos motivos pelos quais importa proteger os direitos de personalidade do trabalhador, principalmente, o respeito pela dignidade da pessoa.

2.1.1 Normas legais: Constitucionais e Infraconstitucionais

2.1.1.1 Constituição da República Portuguesa

Constatamos, bem como TERESA MOREIRA¹²⁵, que no ordenamento jurídico português, o direito à privacidade do trabalhador, “o conceito de privacidade (...) assenta na ideia de dignidade da pessoa humana”. Assim, este direito, para ALEXANDRE SOUSA PINHEIRO, é também muito importante para a criação do direito à proteção de dados^{126,127}.

¹²² Cfr. Lopes, S. (2019). *In Direitos Fundamentais e de Personalidade do Trabalhador*, 3ª edição, Centro De Estudos Judiciários (CEJ), Consultado em 23.11.2019, Disponível em http://www.cej.mj.pt/cej/recursos/ebooks/trabalho/eb_DireitoPersonalidade2019.pdf?id=9&username=guest, p. 27.

¹²³ Vide Dray, G. (2019). *In Direitos Fundamentais e de Personalidade do Trabalhador*, 3ª edição, Centro De Estudos Judiciários (CEJ), Jurisdição do Trabalho e da Empresa, consultado em 23.11.2019, disponível em: http://www.cej.mj.pt/cej/recursos/ebooks/trabalho/eb_DireitoPersonalidade2019.pdf?id=9&username=guest, p. 69.

¹²⁴ Vide Vasconcelos, P. P. (2017). *In Direito de Personalidade*. Coimbra. Edições Almedina, p. 5.

¹²⁵ Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., p. 29.

¹²⁶ Vide Pinheiro, A. S. (2015). *In Privacy e proteção de dados pessoais (...)*, op. cit., p. 823. Este autor postula que a proteção de dados visa proteger “o desrespeito por elementares regras de igualdade entre os homens” promovendo de modo idêntico o respeito pela pessoa.

¹²⁷ Na nossa opinião e de acordo com o já defendido, a proteção de dados é a proteção da privacidade, fazendo todo o sentido que a proteção de dados tenha em vista, outrossim, a dignidade da pessoa humana. Ou seja, se a proteção de dados e a privacidade caminham juntas então faz todo o sentido que assentem na

a) Dignidade da pessoa Humana

O direito à dignidade da pessoa humana conecta-se com o direito à privacidade, neste sentido, postulam PEDRO PAIS DE VASCONCELO¹²⁸ e TERESA MOREIRA¹²⁹ donde se conclui que o direito à privacidade é inerente à pessoa¹³⁰, e deve ser “sempre entendido como a regra e não a exceção”¹³¹. Uma vez que a proteção da privacidade tem assento constitucional, pode considerar-se como direito fundamental. No entanto, não se restringe à lei fundamental, expande-se a outros ramos do direito, desde o laboral ao penal, bem como ao civil¹³².

Conforme nos transmite GOMES CANOTILHO e VITAL MOREIRA¹³³ um dos pilares da República é a dignidade da pessoa humana, vertido no art. 1.º da CRP: “Portugal é uma República (...), baseada na dignidade da pessoa humana”¹³⁴. Os autores JORGE MIRANDA e RUI MEDEIROS¹³⁵ consideram este princípio “um prius”.

Ora, quando se estabelece, logo, no art. 1.º da CRP que a base da República é a dignidade da pessoa humana, então a pessoa é colocada acima da “organização política”¹³⁶. Neste pressuposto questiona-se se no âmbito laboral [entendendo-se a

ideia de promover/proteger a dignidade da pessoa humana. Todavia questionamos: como será o futuro? Tendo presente a evolução tecnológica e o desenvolvimento da Inteligência Artificial (IA), com vista à substituição, do ser humano no desempenho de muitas tarefas, manter-se-á, este princípio assim ou terá de sofrer uma mutação? Uma adaptação?

¹²⁸ Cfr. Vasconcelos, P. P. (2017). *In Direito de Personalidade*. Op. cit., p. 79: “a dignidade da pessoa exige que seja reconhecido um espaço de privacidade (...)”, the right to be let alone. É, de certo modo, o direito a ser deixado em paz.

¹²⁹ Neste sentido também Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., p. 262: “o direito à privacidade assenta na ideia da dignidade da pessoa humana”.

¹³⁰ Pois assenta na pessoa concreta, na vida real e quotidiana e não num ser ideal e abstrato, conforme nos transmitem Canotilho, J. J. G. & Moreira, V. (2014). *In Constituição da (...)*, op. cit., p. 199 e Miranda, J. & Medeiros, R. (2010). *In Constituição Portuguesa Anotada, Tomo I, 2ª edição revista, atualizada e ampliada, art.º 1.º a 79.º*. Coimbra: Editor Wolters Kluwer Portugal sob a marca Coimbra Editora, p. 81, sendo também esta a posição de Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., pp. 272 e 273.

¹³¹ Cfr. Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., p. 263.

¹³² *Idem*, p. 263.

¹³³ Cfr. Canotilho, J. J. G. & Moreira, V. (2014). *In Constituição da (...)*, op. cit., p. 198.

¹³⁴ De acordo com art. 1.º da CRP.

¹³⁵ Miranda, J. & Medeiros, R. (2010). *In Constituição Portuguesa Anotada, (...)*, op. cit., p. 77.

¹³⁶ Vide Canotilho, J. J. G. & Moreira, V. (2014). *In Constituição da (...)*, op. cit., p. 198.

empresa como uma organização] deve igualmente colocar-se o trabalhador em primeiro e depois a empresa?¹³⁷.

Importa ainda notar que a dignidade da pessoa humana está também na base da concretização de outros direitos, v.g., direito ao desenvolvimento da personalidade e promove o direito à igualdade (art. 13.º da CRP) ao proibir a discriminação de qualquer forma.

b) Direito à reserva sobre a intimidade da vida privada

Unido à dignidade encontra-se o direito à reserva sobre a intimidade da vida privada¹³⁸. Este direito encontra consagração na lei fundamental, no n.º 1 do art. 26.º onde são reconhecidos os direitos pessoais: “a todos são reconhecidos os direitos (...) à reserva da intimidade da vida privada”, que conforme secundam GOMES CANOTILHO e VITAL MOREIRA se analisa em dois direitos menores: não acesso, por terceiros, a informação sobre a vida privada e se acedidas que não sejam divulgadas¹³⁹. Neste sentido, atento o defendido por ISA ANTÓNIO¹⁴⁰ importa “trazer à colação”, o vertido no n.º 2 do art. 26.º da CRP¹⁴¹, pois este preceito determina que a “lei estabelecerá as garantias efetivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informação relativas às pessoas”.

¹³⁷ No nosso entendimento sim, desde que, considerando o respeito pelo não excesso de abusos pelo trabalhador, pois não existe liberdade absoluta. Ou seja, ao colocar-se o trabalhador acima da organização, não se quer com isto dizer que ele pode tudo. Muito pelo contrário, queremos transmitir que a empresa é que não pode tudo. O ideal é ambos serem colocados ao mesmo nível, porque um depende do outro, existe uma corresponsabilidade, pois a empresa sem o trabalhador pode não conseguir prosseguir a sua atividade, o seu fim económico. E por outro lado, o trabalhador pode ficar sem o seu retorno financeiro, a sua compensação pela atividade prestada.

¹³⁸ “o art. 26.º da CRP constitui expressão direta do postulado básico da dignidade humana que a constituição consagra, nas palavras de Miranda, J. & Medeiros, R. (2010). *In Constituição Portuguesa Anotada, (...)*, op. cit., p. 607.

¹³⁹ Cfr. Canotilho, J. J. G. & Moreira, V. (2014). *In Constituição da (...)*, op. cit., p. 467.

¹⁴⁰ Veja-se António, I. (2016). *In O Direito Fundamental do Trabalhador à confidencialidade das Comunicações Eletrónicas no Contexto Laboral e o Despedimento Com Justa Causa (?)*. *In Transformações recentes do Direito do Trabalho Ibérico*, Livro Razão, CIJE – Centro de Investigação Jurídico Económica, Faculdade de Direito do Porto; Consultado em 23.11.2019, Disponível em https://sigarra.up.pt/fdup/pt/web_gessi_docs.download_file?p_name=F1854330697/Livro_Razao.pdf, p. 13.

¹⁴¹ Nos termos do n.º 2 do art. 26.º da CRP.

De acordo com TERESA MOREIRA¹⁴² “em abstrato, o conteúdo da noção de vida privada engloba a informação a ela respeitante e à identidade da pessoa: (...) as comunicações por correspondência (...) com suporte digital”, assim, entendemos que se o empregador fizer uso do seu poder de controlo, guardando, acedendo e fazendo uso de mensagens privadas do trabalhador, enviadas e/ou recebidas, nos equipamentos eletrónicos disponibilizados pelo empregador estará a conflitar com o preceito constitucional postulado no art. 26.º da CRP¹⁴³.

Ademais, e considerando o vertido no n.º 8, do art. 32.º da CRP, “são nulas todas as provas obtidas mediante (...) abusiva intromissão na vida privada, (...), na correspondência ou nas telecomunicações, sendo esta uma garantia no âmbito do processo criminal”¹⁴⁴, encontrando “os interesses do processo criminal”¹⁴⁵ limites no princípio da dignidade da pessoa humana, pelo que se consubstancia num dos motivos da nulidade das provas obtidas por violação do acima enunciado.

c) Violação da Correspondência

Correlacionado com a reserva da vida privada está o sigilo da correspondência e dos outros meios de comunicação privada¹⁴⁶. Este preceito tem tutela constitucional, prevista no art. 34.º da CRP dispendo no sentido de a correspondência ser inviolável. Por outras palavras, a correspondência e os outros meios de comunicação privada, gozam do direito ao sigilo e são invioláveis, nos termos do n.º 1 do art. 34.º da CRP¹⁴⁷.

Segundo GOMES CANOTILHO e VITAL MOREIRA¹⁴⁸ o direito ao sigilo da correspondência abarca, de igual modo, as mensagens transmitidas pelo uso das

¹⁴² Cfr. Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., pp. 280 a 282.

¹⁴³ Neste sentido vão também Canotilho, J. J. G. & Moreira, V. (2014). *In Constituição da (...)*, op. cit., p. 471, quando dizem: “o n.º 2 (...) vincula o legislador, obrigando-o a estabelecer garantias” contra intrusões abusivas, tratando-se deste modo “de uma garantia concreta do direito à reserva da intimidade da vida privada” e que vincula entidades públicas e privadas.

¹⁴⁴ Cfr. n.º 8 do art. 32.º da CRP.

¹⁴⁵ Cfr. Canotilho, J. J. G. & Moreira, V. (2014). *In Constituição da (...)*, op. cit., p. 524.

¹⁴⁶ Por exemplo: Messenger, whatSapp.

¹⁴⁷ Cfr. n.º 1 do art. 34.º da CRP: “(...) o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis”.

¹⁴⁸ Cfr. Canotilho, J. J. G. & Moreira, V. (2014). *In Constituição da (...)*, op. cit., p. 544. No mesmo sentido Miranda, J. & Medeiros, R. (2010). *In Constituição Portuguesa Anotada, (...)*, op. cit., p. 773, no entanto estes autores advertem que devem os utilizadores ter atenção, principalmente, “aqueles que têm como

telecomunicações¹⁴⁹, pelo que, ao legislar “e todos os outros meios de comunicação privada” somos do entendimento que abarca todo o tipo de correspondência, v.g., o email.

O legislador português estatui que é proibida toda a ingerência das autoridades públicas¹⁵⁰ na correspondência, nas telecomunicações e nos demais meios de comunicação (...) ¹⁵¹. Neste seguimento, a confidencialidade das mensagens [correio eletrónico]¹⁵² “constituem um regime especial de tutela do direito à reserva da intimidade da vida privada”¹⁵³, proibindo toda a intromissão ao conteúdo das mensagens, pelo que deve o art. 34.º da CRP ser cumulado com o n.º 4 do art. 35.º da CRP que versa sobre a proibição de acesso aos dados pessoais por terceiros.

Queremos ainda notar que os limites da inviolabilidade são definidos pelo texto constitucional, estabelecendo os n.ºs 2, 3 e 4 do art. 34.º da CRP um conjunto de “violações admissíveis”¹⁵⁴. A possibilidade de restrição deste direito é aceitável quando perante “uma situação de estado de sítio ou emergência”¹⁵⁵, assim se entende que a restrição de direitos fundamentais é possível, em casos excepcionais, pelo que concluímos que não são um direito absoluto, pois se o fossem, como é o caso do direito à vida, a inviolabilidade seria total¹⁵⁶.

suporte a internet”, entenda-se o correio eletrónico, na medida em que para garantir o sigilo é necessário um cuidado superior, porque existe uma maior facilidade de acesso e divulgação por outros, inclusive pelo empregador. Coloca-se a dúvida, e considerando os avanços tecnológicos e o uso cada vez maior da informática, se não devem estes meios de comunicação merecer uma tutela constitucional mais vinculada.

¹⁴⁹ Vide Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., p. 291.

¹⁵⁰ Consideramos que esta inviolabilidade deve compreender também o acesso ilícito por terceiros, *i.e.*, sem autorização, ao conteúdo das mensagens. Ademais pensamos que, não obstante o n.º 4 referir somente entidades públicas, também as privadas estão proibidas de aceder, e bem assim preconiza Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., p. 291. Também Canotilho, J. J. G. & Moreira, V. (2014). *In Constituição da (...)*, op. cit., pp. 544 e 545, quanto mais não seja pelo vertido no n.º 1, do art. 18.º da CRP que vincula as entidades privadas ao respeito pelos direitos fundamentais, entendimento também postulado por Canotilho, J. J. G. & Moreira, V. (2014). *In Constituição da (...)*, op. cit., p. 545.

¹⁵¹ Cfr. n.º 4 do art. 34.º CRP.

¹⁵² Cfr. secunda Canotilho, J. J. G. & Moreira, V. (2014). *In Constituição da (...)*, op. cit., p. 544.

¹⁵³ Miranda, J. & Medeiros, R. (2010). *In Constituição Portuguesa Anotada, (...)*, op. cit., p. 756.

¹⁵⁴ *Idem*, p. 757.

¹⁵⁵ *Ibidem*, p. 757.

¹⁵⁶ Assim defendem Miranda, J. & Medeiros, R. (2010). *In Constituição Portuguesa Anotada, (...)*, op. cit., p. 757.

d) Privacidade vs Liberdade de expressão

Poderá a privacidade colocar em perigo a liberdade de expressão?

Nas palavras de TERESA MOREIRA¹⁵⁷ “o direito à liberdade das comunicações (...) de comunicar quando, como, com quem, e o que se quiser” consubstancia o direito à reserva da vida privada. Ou seja, se o trabalhador confiar que não vão ser violadas as suas comunicações: acedidas e divulgadas, vai transmitir as suas opiniões, pensamentos, ideologias sem receios.

Ora, se não é garantida a privacidade [a proteção de dados] pode a liberdade de expressão ser colocada em perigo, pois a pessoa vai *medir* tudo aquilo que quer transmitir, com medo, logo sem liberdade.

Conforme o texto da lei fundamental, n.º 1 do art. 37.^o¹⁵⁸ “todos têm o direito de exprimir e divulgar livremente o seu pensamento pela palavra, (...) ou por qualquer outro meio¹⁵⁹, bem como o direito de informar, de se informar e de ser informados, sem impedimentos nem discriminações”. De acordo com GOMES CANOTILHO e VITAL MOREIRA, o art. 37.º da CRP “regula as liberdades e direitos de expressão e informação”¹⁶⁰, que no nosso prisma, abarcam também o trabalhador, pois este é pessoa e cidadão e, como tal, merecedor desta tutela.

Comportando este preceito o direito de expressão e o de informação existe o entendimento que estes dois direitos são de difícil delimitação, não obstante, considera-se que a mesma se centra na “distinção comum entre (...) a expressão de ideias ou opiniões e (...) a recolha e transmissão de informações”.¹⁶¹ Ou seja, e transpondo para o

¹⁵⁷ De acordo com o exposto por Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., p. 290.

¹⁵⁸ Nos termos do n.º 1 do art. 37.º da CRP.

¹⁵⁹ Segundo Miranda, J. & Medeiros, R. (2010). *In Constituição Portuguesa Anotada, (...)*, op. cit., p. 847, não é porque a CRP determina o direito de todos se exprimirem e divulgarem o pensamento por qualquer meio que existe uma “incondicionada e livre utilização de todos os meios” sendo importante diferenciá-los, pelo que estes autores qualificam o uso do correio eletrónico na categoria de meios de acesso condicionado e utilização livre. Canotilho, J. J. G. & Moreira, V. (2014). *In Constituição da (...)*, op. cit., p.572, entendem que estes outros meios englobam “as novas formas de expressão.

¹⁶⁰ Canotilho, J. J. G. & Moreira, V. (2014). *In Constituição da (...)*, op. cit., p.571. e também Miranda, J. & Medeiros, R. (2010). *In Constituição Portuguesa Anotada, (...)*, op. cit., p. 847.

¹⁶¹ Canotilho, J. J. G. & Moreira, V. (2014). *In Constituição da (...)*, op. cit., p. 572.

âmbito do nosso estudo, um trabalhador tem o direito a expor a suas ideias, sem medos, nem receios, mantendo a expectativa de privacidade, de que não existirão acessos indevidos nem transmissão a terceiros, bem como se espera que estas não sejam desvirtuadas, *i.e.*, utilizadas para fins distintos¹⁶².

Com o “direito de expressão”¹⁶³ vem a liberdade de expressão, *i.e.*, com este direito não pode haver impedimento à expressão, à divulgação de ideias/opiniões¹⁶⁴. Segundo JORGE MIRANDA e RUI MEDEIROS¹⁶⁵, o âmbito de proteção da liberdade de expressão está: no direito de não ser impedido de divulgar opiniões pelos meios que se tenham disponíveis, pois a criação de impedimentos pode restringir o princípio da dignidade humana¹⁶⁶ e o desenvolvimento da personalidade^{167,168}.

Relativamente ao direito de informação, e conforme JORGE MIRANDA e RUI MEDEIROS¹⁶⁹ esta é uma “figura recente”, que comporta uma dimensão tripla: **a)** direito de informação¹⁷⁰, **b)** direito de se informar¹⁷¹ e **c)** o direito de ser informado¹⁷². Tal como se verifica no n.º 1, *in fine*, do art. 37.º da CRP, os direitos de expressão e informação não podem estar sujeitos a impedimentos nem ser discriminados. Não deve haver censura, aplicando-se esta proibição de censura também às empresas¹⁷³.

¹⁶² Importa referir que a liberdade de expressão pode ser exercida através do direito de expor verbalmente uma ideia/opinião, mas pode também ser pelo não expor. Ou seja, “revestir forma de silêncio” não devendo o trabalhador ser obrigado a emitir uma quando, por exemplo, com ela não concorda, cfr. Canotilho, J. J. G. & Moreira, V. (2014). *In Constituição da (...)*, op. cit., p. 572.

¹⁶³ *Idem*, p. 572.

¹⁶⁴ *Ibidem*, p. 572.

¹⁶⁵ Miranda, J. & Medeiros, R. (2010). *In Constituição Portuguesa Anotada, (...)*, op. cit., p. 849.

¹⁶⁶ Nos termos do art. 1.º da CRP.

¹⁶⁷ De acordo com o vertido no art. 26.º da CRP

¹⁶⁸ Vide Miranda, J. & Medeiros, R. (2010). *In Constituição Portuguesa Anotada, (...)*, op. cit., p. 848.

¹⁶⁹ *Idem*, p. 852.

¹⁷⁰ Cfr. Canotilho, J. J. G. & Moreira, V. (2014). *In Constituição da (...)*, op. cit., p. 573: consiste “na liberdade de transmitir” informação a outros destinatários, sem impedimentos, *v.g.*, emitir uma ideia produtiva para melhorar o funcionamento da empresa onde labora.

¹⁷¹ *Idem*, p. 573: tem por objeto “a liberdade de recolha de informação”, por exemplo, solicitar ao empregador informação sobre os dados que foram inicialmente recolhidos e que são objeto de tratamento.

¹⁷² *Ibidem*, p. 573: “direito a ser mantido adequadamente informado”, sempre que o empregador use os dados para fim diferente deve informar, bem como sempre que ocorram mudanças de procedimentos deve também informar o trabalhador.

¹⁷³ Assim secundam: Canotilho, J. J. G. & Moreira, V. (2014). *In Constituição da (...)*, op. cit., p. 574.

Por fim, referir ainda que o n.º 4 do art. 37.º da lei fundamental¹⁷⁴ contempla o direito de resposta e retificação¹⁷⁵. Estes dois direitos podem ser exercidos, por exemplo, quando ocorra a emissão de informações não verdadeiras¹⁷⁶ ou incorretas, como meio de defesa, para requerer uma retificação¹⁷⁷. Ademais, o recurso a estes direitos, poder ser executado “em meio eletrónico”, pois a utilização dos meios eletrónicos é atualmente praticada em grande escala quando se emitem ou recebem mensagens via correio eletrónico, *chats, blogs, inter alia*¹⁷⁸.

2.1.1.2 Os preceitos infraconstitucionais

O direito à privacidade e à proteção de dados são direitos que se encontram ligados ao trabalhador, porque e tal como nos transmite JÚLIO GOMES, ele é antes de tudo uma pessoa, é “simultaneamente cidadão e trabalhador”¹⁷⁹. Também TERESA MOREIRA detém este entendimento, quando diz que o direito à privacidade está conectado à “dignidade do trabalhador enquanto pessoa”^{180,181}, sendo por esta razão que a consagração desta proteção nas leis laborais é deveras importante.

Com a introdução das tecnologias de comunicação no seio laboral, seja para comunicar [ou para controlar a prestação laboral], potenciam-se “mais e maiores invasões”¹⁸² na privacidade do trabalhador, logo na proteção dos seus dados.

¹⁷⁴ Nos termos no art. 37.º, n.º 4 da CRP: “a todas as pessoas, singulares ou coletivas, é assegurado, em condições de igualdade e eficácia, o direito de resposta e de retificação, bem como o direito a indemnização pelos danos sofridos”.

¹⁷⁵ Vide Canotilho, J. J. G. & Moreira, V. (2014). *In Constituição da (...)*, op. cit., p. 574.

¹⁷⁶ Assim defende Miranda, J. & Medeiros, R. (2010). *In Constituição Portuguesa Anotada, (...)*, op. cit., p. 858.

¹⁷⁷ Cfr. Canotilho, J. J. G. & Moreira, V. (2014). *In Constituição da (...)*, op. cit., pp. 575 e 576.

¹⁷⁸ *Idem*, p. 576.

¹⁷⁹ Cfr. Gomes, J. M. V. (2007). *In Direito do Trabalho, (...)*, op. cit., p. 265.

¹⁸⁰ Vide Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., p. 30.

¹⁸¹ E ainda Festas, D. O. (2004). *In O direito à reserva da intimidade da vida privada do trabalhador no Código do Trabalho. Revista da Ordem dos Advogados, ano 64, Vol. I/II*, Consultado em 17.03.2019, Disponível em: <https://portal.oa.pt/comunicacao/publicacoes/revista/ano-2004/ano-64-vol-i-ii-nov-2004/artigos-doutrinais/david-de-oliveira-festas-o-direito-a-reserva-da-intimidade-da-vida-privada-do-trabalhador-no-codigo-do-trabalho-star/>, p. 3.: “a relevância do direito à reserva da vida privada do trabalhador é manifesta e resulta da consideração do trabalhador como uma pessoa”.

¹⁸² *Idem*, p. 3.

Todavia, de que forma pode ser concretizado este direito, considerando a relação de desequilíbrio que existe entre o empregador e o trabalhador?

Tal como antedito, a relação de trabalho significa para o trabalhador uma “compressão dos seus direitos enquanto indivíduo”¹⁸³, pois o trabalhador fica numa posição de sujeição¹⁸⁴. Deste modo, a previsão expressa de normas que visam a proteção de direitos de personalidade no Código do Trabalho, doravante CT¹⁸⁵, vieram demonstrar a preocupação do legislador com os riscos que existem “para a pessoa do trabalhador”¹⁸⁶.

Porém, pensamos que o legislador pode em alterações futuras considerar, as peculiares características inerentes à relação laboral¹⁸⁷ no sentido de as melhorar, pois a hipótese da sua violação, pelas inúmeras exceções previstas, pode limitar muitos o exercício destes direitos¹⁸⁸.

A. Proteção dos direitos personalidade no Código do Trabalho

O CT português¹⁸⁹ regulamenta os direitos de personalidade nos arts. 14.º a 22.º, sendo esta uma inovação no ordenamento laboral nacional. Tendo presente o objeto do nosso estudo, abordaremos aqueles que nos parecem mais pertinentes¹⁹⁰ na determinação do âmbito de proteção dos direitos dos trabalhadores, concretamente na questão

¹⁸³ Cfr. Lopes, S. (2019). *In Direitos Fundamentais e de Personalidade (...)*, op. cit., p. 25.

¹⁸⁴ Abrantes, J. J. (2008). *In Algumas notas sobre o direito do trabalhador à reserva da vida privada. Estudos comemorativos dos 10 anos da Faculdade de Direito da Universidade Nova de Lisboa*. Coimbra: Almedina. Vol. 2, p. 243.

¹⁸⁵ O CT de 2003, pela aprovação da Lei n.º 99/2003, de 27 de agosto, passou a incluir um capítulo dedicado aos direitos de personalidade do trabalhador, e com a revisão de 2009, pela Lei n.º 7/2009, de 12 de fevereiro, passam a constar nos arts 14.º a 22.º. A inovação consagrada, no CT, não significa que antes estes direitos não tinham proteção. De facto, os mesmos, e tal como já referimos, tinham tutela constitucional, *ex vi* art. 18.º CRP, cfr. Abrantes, J. J. (2008). *In Algumas notas sobre o direito do trabalhador (...)*, op. cit., p. 244, bem como civil (art. 70.º e ss do CC).

¹⁸⁶ Vide Gomes, J. M. V. (2007). *In Direito do Trabalho, (...)*, op. cit., p. 268.

¹⁸⁷ Consideramos que as novas leis de proteção de dados que têm vindo a ser promulgadas podem trazer vantagens de proteção aos trabalhadores, não obstante, uma regulamentação mais vinculada no CT para dirimir os problemas de violação dos direitos dos trabalhadores.

¹⁸⁸ Assim nos diz: Abrantes, J. J. (2008). *In Algumas notas sobre o direito do trabalhador (...)*, op. cit, p. 243.

¹⁸⁹ De 2003, substituído pelo de 2009, Lei n.º 7/2009, de 12 de fevereiro e revisto.

¹⁹⁰ A saber liberdade de expressão – art. 14.º do CT; reserva da intimidade da vida privada – art. 16.º do CT; proteção de dados pessoais – art. 17.º do CT; meios de vigilância à distância – art. 20.º e sua utilização – art. 21.º e a confidencialidade de mensagens e de acesso a informação – art. 22.º.

relacionada com a confidencialidade das mensagens privadas, pois este conjunto de normas visam a proteção dos direitos de personalidade¹⁹¹.

I. Liberdade de expressão – art. 14.º do CT

O direito à liberdade de expressão, no âmbito da empresa, encontra-se vertido no art. 14.º do CT. Este consubstancia o direito dos trabalhadores se expressarem, neste sentido os regulamentos que possam existir na empresa não devem ser limitadores do exercício da liberdade de expressão¹⁹².

No entendimento de JÚLIO GOMES¹⁹³, durante muitos anos não foi reconhecido, ao trabalhador, o direito a expressar-se livremente. Todavia, atualmente é impossível negar a existência deste direito, que vem determinar na esfera do trabalhador, a liberdade de expressão e opinião, *inside de company and outside*¹⁹⁴.

Subsiste a ideia de que o preceito é inerente a ambas as partes. Ou seja, ambas gozam do direito à liberdade de expressão e opinião. No entanto, e porque o trabalhador é subordinado do empregador, no entendimento de PAULA QUINTAS e HELDER QUINTAS¹⁹⁵ “o destinatário principal é o trabalhador”, pois ele necessita de liberdade para se desenvolver, podendo esta ser colocada em perigo quando o empregador monitorize a prestação da atividade do trabalhador¹⁹⁶.

O direito à liberdade de expressão e de opinião “constitui uma condição necessária à tutela da dignidade do trabalhador”^{197,198}. Assim, ele não deve ser impedido ou mesmo

¹⁹¹ Vide Dray, G. (2019). *In Direitos Fundamentais e de Personalidade (...)*, op. cit., p. 69.

¹⁹² Vide Leitão, L. M. T. M. (2019). *In Direito do trabalho, 6ª edição*. Coimbra: Edições Almedina, p. 152.

¹⁹³ Gomes, J. M. V. (2007). *In Direito do Trabalho, (...)*, op. cit., p. 272.

¹⁹⁴ *Idem*, pp. 272 e 273, sendo o inglês nosso. Neste sentido veja-se o Ac. do STJ, proc. n.º 296/17.9T8FAR.E1.S1, de 06 de março de 2019, relator: MJD Leones Dantas, consultado em 04/01/2020, disponível em https://www.stj.pt/wp-content/uploads/2019/06/sum_acor_social_marco_2019.pdf: “o trabalhador goza tanto no âmbito da empresa como fora dela do direito de liberdade de expressão (...)”.

¹⁹⁵ Quintas, P. & Quintas, H. (2016). *In Código do Trabalho Anotado e Comentado” 4ª edição*, s.l.: Editora: Almedina, p. 91.

¹⁹⁶ Cfr. Quintas, P. & Quintas, H. (2016). *In Código do Trabalho Anotado (...)*, op. cit., p. 91.

¹⁹⁷ Veja-se Lopes, S. (2019). *In Direitos Fundamentais e de Personalidade (...)*, op. cit., p. 28.

¹⁹⁸ Esta tutela, nos termos do art. 24.º da Lei n.º 58/2019, de 8 de agosto, consultada em: 04.11.2019, disponível em:

http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=3118A0002&nid=3118&tabela=leis&pagina=1&ficha=1&so_miolo=&nverso=, pode ser vista à luz da proteção de dados, porque o empregador deve respeitar, no exercício da liberdade de informação, quando comporte dados pessoais do trabalhador o

“proibido de manter conversas”¹⁹⁹ ainda que sobre temáticas sociais²⁰⁰, no seu local de trabalho, pois estas servem muitas vezes como momento de decompressão, para um posterior rendimento mais positivo e motivado da sua prestação de trabalho.

Outrossim, existe liberdade de expressão quando o trabalhador emite opiniões dissidentes das do empregador. Estas devem ser encaradas, pelo empregador, numa vertente positiva, potenciadora do desenvolvimento do trabalhador, do seu pensamento. No entanto, é importante perceber até onde pode ir a emissão de opiniões, pelo trabalhador, para evitar perturbações no ambiente de trabalho, e consequências negativas²⁰¹.

De acordo com MENEZES LEITÃO²⁰², o art. 14.º do CT estabelece dois limites ao direito de exercer a liberdade de expressão: respeitar o direito de personalidade dos colegas e o “normal funcionamento da empresa”²⁰³.

Pela análise doutrinária, constata-se que as empresas só consideram este direito para aferir abusos dos trabalhadores invocando-o, por exemplo, como “justa causa de despedimento”²⁰⁴ ou outra medida sancionatória – suspensão do contrato de trabalho com perda de retribuição e antiguidade. Também na jurisprudência encontramos referência a

previsto no n.º 1 do art. 9.º do RGPD, respeitando o princípio da dignidade da pessoa humana. Por conseguinte não é legítimo que o empregador, somente porque tem direito à liberdade de expressão, divulgue moradas ou contactos telefónicos, exceto se forem do conhecimento geral.

¹⁹⁹ *Idem*, p. 28.

²⁰⁰ No Ac. do TRL Processo n.º 24163/09.0T2SNT.L1-4 de 07 de março de 2012. Relator: MJD José Eduardo Sapateiro, consultado em 22.10.2018, disponível em <http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/109499c90995e66d802579bf0050cfa4?OpenDocument>, constata-se que “uma das vertentes em que se desdobra o direito” da liberdade expressão e opinião é aquele que normalmente se define no decorrer de uma conversa privada.

²⁰¹ Gomes, J. M. V. (2007). *In Direito do Trabalho*, (...), op. cit., p. 274.

²⁰² Leitão, L. M. T. M. (2019). *In Direito do trabalho* (...), op. cit., p. 152.

²⁰³ *Idem*, p. 152.

Atente-se ao disposto no ac. do TRP processo n.º 276/13.3TTSTS.P1, de 15.02.2016. Relator: MJD Jorge Loureiro, consultado em: 05.11.2019, disponível em: <https://dre.pt/web/guest/pesquisa/-/search/104284775/details/maximized?perPage=100&sort=whenSearchable&sortOrder=DESC&q=valor%2Fen%2Fen>. Este dispõe que “o direito à liberdade de expressão por parte dos trabalhadores não é absoluto, devendo harmonizar-se” com os direitos da empresa, encontrando-se deste modo limitado também “pelo dever de respeito, urbanidade e probidade”.

²⁰⁴ Vide Gomes, J. M. V. (2007). *In Direito do Trabalho*, (...), op. cit., p. 275.

esta questão, neste sentido veja-se uma decisão proferida pelo Tribunal da Relação do Porto²⁰⁵.

Concomitantemente, quando o trabalhador utiliza as tecnologias de comunicação laborais, exercita o direito à liberdade de expressão. Todavia, é importante tomar em atenção que fora do local de trabalho, o trabalhador, dispõe de uma liberdade mais ampla. Pese embora a sensação de maior liberdade, ela deve ser exercida com cuidado pois “não é ilimitada”²⁰⁶, onde os comentários pejorativos ou difamadores contra o empregador devem ser evitados.

O art. 14.º do CT pode, ainda, ser interpretado numa perspetiva diferente, pois o direito à liberdade de expressão pode ser consequência necessária do exercício do direito de defesa quando perante sanções aplicadas pelo empregador²⁰⁷, concedendo ao trabalhador o direito de defesa para contestar uma decisão do empregador.

Relativamente ao RGPD e ao facto de estatuir sobre a liberdade de expressão, a questão vem legislada no art. 85.º²⁰⁸ delegando-se para o EM²⁰⁹, por divergências consensuais, a regulamentação, conciliação das normas que regem a liberdade de expressão e de informação com o direito à proteção de dados²¹⁰, tendo em Portugal ocorrido com a publicação da Lei n.º 58/19, de 8 de agosto²¹¹.

²⁰⁵ TRP, Processo n.º 68/14.2TTMTS.P1, de 01 de fevereiro de 2016. Relatora: MJD Fernanda Soares, consultado em: 05.11.2019, disponível em: <https://dre.pt/pesquisa-avancada/-/asearch/104279975/details/maximized?emissor=Tribunal+da+Rela%C3%A7%C3%A3o+do+Porto&perPage=100&types=JURISPRUDENCIA&search=Pesquisar>: “A mensagem de correio eletrónico remetida por um trabalhador (...) a dois trabalhadores dessa empresa, com conhecimento para a Comissão de Trabalhadores da mesma empresa e para 47 outros trabalhadores (...) não consubstancia, objetivamente, qualquer violação dos deveres de respeito, de urbanidade por parte desse trabalhador para com a sua entidade empregadora (...) na medida em que traduz, tão só, o exercício do direito de liberdade de expressão (...)”.

²⁰⁶ Conforme secunda Gomes, J. M. V. (2007). *In Direito do Trabalho*, (...), op. cit., p. 279.

²⁰⁷ De acordo com Quintas, P. & Quintas, H. (2016). *In Código do Trabalho Anotado* (...), op. cit, p. 92.

²⁰⁸ Veja-se o art. 85.º, n.º 1 do RGPD.

²⁰⁹ Vide Pinheiro, A. S. (Coord.) (2018). *In Comentário ao Regulamento Geral de Proteção de Dados*, s.l.: Edições Almedina, p. 651.

²¹⁰ *Idem*, no considerando 153, p. 651.

²¹¹ O art. 24.º dispõe: “1 - A proteção de dados pessoais, nos termos do RGPD e da presente lei, não prejudica o exercício da liberdade de expressão, informação (...). 2 - O exercício da liberdade de informação, especialmente quando revele dados pessoais previstos no n.º 1 do artigo 9.º do RGPD e no artigo 17.º da presente lei, deve respeitar o princípio da dignidade da pessoa humana previsto na Constituição da República Portuguesa, bem como os direitos de personalidade nela e na legislação nacional

II. Reserva da intimidade da vida privada – art. 16.º do CT

Dando continuidade à análise dos preceitos laborais, MENEZES LEITÃO postula que “a tutela da personalidade abrange especificamente a imposição de reserva sobre a intimidade da vida privada”^{212,213}. O que significa que existe proteção sobre os dados pessoais, privados do trabalhador.

À luz do preceituado por PAULA QUINTAS e HELDER QUINTAS, a lei não estipula um conceito²¹⁴ sobre o que é vida privada. Todavia, o legislador nacional vai beber à teoria alemã das três esferas – *Sphärentheorie* – para concluir que este direito engloba uma esfera pública²¹⁵, uma privada²¹⁶ e uma íntima²¹⁷.

Convém notar que o vertido no art. 16.º do CT, não é absoluto, podendo ser derogado quando o empregador ateste ser “essencial para o funcionamento da empresa”²¹⁸, v.g., monitorizar a utilização das ferramentas informáticas. Todavia, é importante que o empregador entenda que “a proteção conferida à reserva da intimidade

consagrados. (...) 4 - O exercício da liberdade de expressão não legitima a divulgação de dados pessoais como moradas e contactos, à exceção daqueles que sejam de conhecimento generalizado.”

²¹² Conforme expõe Leitão, L. M. T. M. (2019). In *Direito do trabalho (...)*, op. cit., p. 160.

²¹³ Jurisprudencialmente, o ac. do TRL processo n.º 23019/16.5T8LSB.L1-8, de 23 de fevereiro de 2017. Relator: MJD Isoleta Almeida Costa, consultado em: 04.11.2019, disponível em: <http://www.dgsi.pt/jtrl.nsf/-/26988FB6EF65C551802580DF0034F791>: a vida íntima e privada da pessoa “abrange a identidade, isto é, o nome, a fotografia, (...), a situação financeira, fiscal (...)”.

²¹⁴ Porém o “TC considera o conceito de «vida privada» como o *direito de cada um ver protegido o espaço interior da pessoa ou do seu lar contra intromissões alheias, ou seja, o direito a um espaço própria inviolável, onde ninguém deve poder penetrar sem autorização do respetivo titular*” (Ac. n.º 182/92, pub. no DR, II série, de 24.07.92” Quintas, P. & Quintas, H. (2016). In *Código do Trabalho Anotado (...)*, op. cit, p. 96.

²¹⁵ Nas palavras de Leitão, L. M. T. M. (2019). In *Direito do trabalho (...)*, op. cit., p. 161: relaciona-se com situações que podem ser do conhecimento público, “livremente divulgadas”.

²¹⁶ *Idem*, p. 161: esta esfera prevê uma proteção relativa, pois quando perante uma emergência ou conflito com interesses superiores a proteção pode cair.

Jurisprudencialmente: o ac. do TRL processo n.º 15070/18.T8LSB.L1-4, de 11 de julho de 2019. Relator: Filomena Manso, consultado em 05.11.2019, disponível em: <http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/974eaa48f5719bc3802584390032b39f?OpenDocument>: Os actos da vida privada do trabalhador não podem ser valorados em si mesmo, mas apenas nos reflexos que estes possam ter na estrutura empresarial ou na relação de confiança entre trabalhador e empregador. A mensagem que uma trabalhadora (...), via facebook, por chat, (...), fora do tempo e do local de trabalho, a respeito de assuntos pessoais, é um acto da vida privada da trabalhadora”.

²¹⁷ *Ibidem*, p. 161: abrange os dados íntimos, os que se conectam com a vida familiar, escolhas políticas, orientação sexual, sendo em princípio absoluta. Neste campo, releva ter em consideração o RGPD, no n.º 1 do art. 9.º, que versa sobre o tratamento de dados pessoais sensíveis, íntimos.

²¹⁸ Veja-se Leitão, L. M. T. M. (2019). In *Direito do trabalho (...)*, op. cit., p. 162.

da vida privada”²¹⁹ abarca quer o acesso, quer a divulgação, devendo envidar todos os esforços para garantir esta proteção, e informar o trabalhador sobre a possibilidade de acesso, bem como solicitar o seu consentimento, para aceder e/ou divulgar. Neste sentido, e porque existe uma maior dificuldade em separar a vida profissional da vida pessoal, o empregador deve perceber que a “pessoa do trabalhador tem de ser protegida na sua integridade”²²⁰ – tanto dentro como fora da empresa.

O direito à reserva da intimidade da vida privada “marca e influencia”²²¹ o regime da proteção de dados, da confidencialidade de mensagens e de acesso a informação, bem como o da videovigilância, temáticas que serão abordadas em seguida. Ainda assim, e de acordo com a doutrina, quando é violada a confidencialidade das mensagens, o regime colocado em causa é o da confidencialidade da correspondência e cumulativamente o da reserva da vida privada²²².

III. A proteção de dados pessoais – art. 17.º do CT

A rápida evolução da informática no mundo laboral, “teve um impacto”²²³ muito significativo no que se veio a denominar por intimidade informática ou autodeterminação informativa. Neste sentido, e pela análise do art. 17.º do CT²²⁴, reconhece-se que este preceito, cuida “do alcance, sentido e limites do direito à informação”²²⁵ que é concedido

²¹⁹ No entendimento de Lopes, S. (2019). *In Direitos Fundamentais e de Personalidade (...)*, op. cit., p. 31.

²²⁰ Vide Dray, G. (2019). *In Direitos Fundamentais e de Personalidade (...)*, op. cit., p. 73.

²²¹ *Idem*, p. 74.

²²² *Ibidem*, p. 74.

²²³ Vide Gomes, J. M. V. (2007). *In Direito do Trabalho, (...)*, op. cit., p. 353.

²²⁴ Art. 17.º do CT: “1 - O empregador não pode exigir a candidato a emprego ou a trabalhador que preste informações relativas: a) À sua vida privada, salvo quando estas sejam estritamente necessárias e relevantes para avaliar da respectiva aptidão no que respeita à execução do contrato de trabalho e seja fornecida por escrito a respectiva fundamentação; b) À sua saúde ou estado de gravidez, salvo quando particulares exigências inerentes à natureza da actividade profissional o justifiquem e seja fornecida por escrito a respectiva fundamentação. 2 - As informações previstas na alínea b) do número anterior são prestadas a médico, que só pode comunicar ao empregador se o trabalhador está ou não apto a desempenhar a actividade. 3 - O candidato a emprego ou o trabalhador que haja fornecido informações de índole pessoal goza do direito ao controlo dos respectivos dados pessoais, podendo tomar conhecimento do seu teor e dos fins a que se destinam, bem como exigir a sua rectificação e actualização. 4 - 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. 5 - Constitui contra-ordenação muito grave a violação do disposto nos n.ºs 1 ou 2.

²²⁵ De acordo com Quintas, P. & Quintas, H. (2016). *In Código do Trabalho Anotado (...)*, op. cit., p. 95.

ao empregador. Por outras palavras, versa sobre até onde pode ir a recolha de dados pelo empregador, elencando quais as áreas que lhe estão vedadas, nas quais não pode exigir informação ao trabalhador.

O preceituado no art. 17.º do CT encontra-se ligado à privacidade do trabalhador. Conforme nos transmite MENEZES LEITÃO²²⁶, se os dados recolhidos, no âmbito do contrato de trabalho, disserem respeito à esfera pública então, ela é permitida, porém poderá ser proibida se estiver em causa informação relacionada com esfera íntima e privada do trabalhador. Quanto à esfera privada²²⁷, a al. a), do n.º 1 do art. 17.º determina que é proibida a recolha, pelo empregador, de informação inerente à vida privada do trabalhador, exceto se esta for pertinente para aferir a aptidão do trabalhador²²⁸, devendo tal pedido ser fundamentado por escrito, mediante o consentimento do trabalhador^{229,230}. Na al. b), do n.º 1 do art. 17.º do CT^{231,232} determina-se uma proibição quanto à exigência de informação relativa a dados sensíveis²³³ [esfera íntima].

²²⁶ Leitão, L. M. T. M. (2019). *In Direito do trabalho (...)*, op. cit., p. 163.

²²⁷ O Ac. do TRG processo n.º 15/11.3TTVRL.G1, de 11 de junho de 2015. Relator: MJD Antero Veiga diz-nos que “os dados pessoais relativos à esfera privada não são, por regra, acessíveis sem prévia autorização do titular”, estando alguns desses dados, sujeitos a proteção especial, consultado em 15.03.2019, disponível em: <http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/602f7d06304fc8bc80257eb20036e5fe?OpenDocument>

²²⁸ Vide Leitão, L. M. T. M. (2019). *In Direito do trabalho (...)*, op. cit., p. 163 e Quintas, P. & Quintas, H. (2016). *In Código do Trabalho Anotado (...)*, op. cit., p. 99.

²²⁹ Assim expõe Festas, D. O. (2004). *In O direito à reserva da intimidade (...)*, op. cit., p. 13.

²³⁰ Porém, e porque o tratamento de dados só é lícito quando cumpra certos requisitos [art. 6.º do RGPD], será na relação laboral sempre legitimado pela execução de um contrato? Ou existe consentimento do trabalhador, nos termos do n.º 11 do art. 4.º do RGPD 11): “Consentimento» do titular dos dados, uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento”. Em nossa opinião não existe um consentimento com as características supra enunciadas. Também neste sentido postula Gomes, J. M. V. (2007). *In Direito do Trabalho, (...)*, op. cit., p. 354 quando diz: “não parece adequado considerar” no contrato de trabalho “o consentimento do trabalhador considerando como constituindo sempre causa de justificação do tratamento dos seus dados”.

²³¹ Veja-se Leitão, L. M. T. M. (2019). *In Direito do trabalho (...)*, op. cit., p. 163 e Quintas, P. & Quintas, H. (2016). *In Código do Trabalho Anotado (...)*, op. cit., p. 100.

²³² Releva notar que esta recolha de informação pelo empregador deve respeitar o princípio da proporcionalidade *lato sensu*, nas suas três dimensões: necessidade, adequação e proporcionalidade *strictu sensu*, cfr. n.º 2 do art. 18.º da CRP.

²³³ Sendo um dos dados relativos à saúde, defende-se que a informação que for recolhida não deve servir para justificar a não celebração de um contrato ou como justa causa de despedimento. A recolha pode ser

O art. 17.º do CT protege os dados pessoais quando na recolha e no tratamento – cfr. n.º 4 e n.º 5 do citado artigo²³⁴. Ademais, o n.º 4 do art. 17.º do CT declara que: “os ficheiros e acessos informáticos utilizados pelo empregador para tratamento de dados pessoais (...) do trabalhador ficam sujeitos à legislação em vigor relativa à proteção de dados pessoais”. Pelo que, deve este ser cumulado com os diplomas que regulam a matéria da proteção de dados em vigor no ordenamento nacional: RGPD e a Lei n.º 58/2019, de 8 de agosto que o executa em Portugal.

Todavia, constatamos que nem o CT, nem a Lei de execução do RGPD, consagram expressamente como pode ser também utilizado o requisito do consentimento pelo trabalhador. Por conseguinte, e porque não existe um consentimento dado de forma livre pelo trabalhador, que tem receio em dissentir, este acaba numa posição de maior fragilidade²³⁵.

Perante o exposto, e no nosso prisma, verificamos que a proteção de dados pessoais do trabalhador acaba por resultar num conflito de direitos [entre direito do trabalhador à privacidade e o direito da empresa]²³⁶.

IV. Os meios de vigilância à distância e sua utilização – arts. 20.º e 21.º do CT

A previsão legal, no CT sobre os meios de vigilância à distância encontra-se no art. 20.º consagrando-se numa novidade no ordenamento jurídico nacional²³⁷, potenciada

relevante quando para determinar qual o melhor local para o colaborador prestar a sua atividade sem colocar em risco a sua saúde ou a atividade empresarial.

²³⁴ Este é um entendimento defendido por Leitão, L. M. T. M. (2019). *In Direito do trabalho (...)*, op. cit., pp. 164 e 165, Quintas, P. & Quintas, H. (2016). *In Código do Trabalho Anotado (...)*, op. cit., pp. 100 a 102 e Festas, D. O. (2004). *In O direito à reserva da intimidade (...)*, op. cit., p. 13.

²³⁵ Em nossa opinião, o consentimento merece um cuidado especial pelo legislador, em matéria laboral, devendo ser consagrado numa norma expressa que conceda liberdade ao trabalhador para dar o seu consentimento ou não. A não existência de tal norma coloca em perigo o princípio da liberdade de expressão e consequentemente da dignidade da pessoa humana. Esta parece ser também a opinião de Leitão, L. M. T. M. (2019). *In Direito do trabalho (...)*, op. cit., p. 164, que entende que a proteção de dados [RGPD], “aplicável no âmbito das relações laborais”, não pode ser tão ambígua.

²³⁶ Também neste sentido caminha Festas, D. O. (2004). *In O direito à reserva da intimidade (...)*, op. cit., p. 13.

²³⁷ Veja-se Festas, D. O. (2004). *In O direito à reserva da intimidade (...)*, op. cit., p. 18.

pela crescente introdução das novas tecnologias de comunicação no mundo laboral, trazendo consigo perigos para o trabalhador²³⁸.

Este preceito trata a questão de o empregador ter a possibilidade de utilizar os meios de vigilância à distância no local de trabalho²³⁹ para controlar a prestação da atividade do trabalhador. Nos termos do n.º 1 do art. 20.º do CT, os meios de vigilância à distância não podem ser usados com a finalidade de controlo, não sendo “lícito o recurso a vigilância secreta”²⁴⁰. Contudo, existirá licitude na utilização destes meios quando esteja em causa “proteção e segurança de pessoas e bens” ou quando particulares exigências inerentes à natureza da atividade o justifiquem”^{241, 242} sempre mediante autorização da CNPD que verificará se o princípio da proporcionalidade foi atendido.

Ademais, e na medida que a vigilância secreta é proibida, vem o n.º 3 do art. 20.º do CT determinar que deve o trabalhador ser informado sobre a existência e finalidade dos meios, nomeadamente, através da afixação de dizeres: “«Este local encontra-se sob vigilância de um circuito fechado de televisão» ou «Este local encontra-se sob vigilância de um circuito fechado de televisão, procedendo-se à gravação de imagem e som», seguido de símbolo identificativo”²⁴³.

Para MENEZES LEITÃO a proibição vertida no n.º 1 do art. 20.º do CT “abrange quaisquer meios de vigilância à distância”²⁴⁴ que tenham como finalidade controlar o

²³⁸ *Idem*, pp. 18 e 19. Para este Autor, neste preceito “está subjacente uma colisão de direitos e interesses” que se traduz, pelo poder de direção que assiste o empregador: “vigiar e controlar” a atividade do trabalhador e o uso que “este último dá aos instrumentos laborais”, por outro lado, temos o trabalhador que possui o direito à reserva da intimidade da vida privada e que o poderá ver ser violado.

²³⁹ Meios estes, na nossa opinião, podem ir desde o computador até uma câmara de vídeo ou mesmo um telemóvel.

²⁴⁰ Lopes, S. (2014). *In Direitos Fundamentais e de Personalidade do Trabalhador, 2ª edição*, Centro De Estudos Judiciários (CEJ), Consultado em 06.07.2019, Disponível em http://www.cej.mj.pt/cej/recursos/ebooks/trabalho/eb_DireitoPersonalidade2019.pdf?id=9&username=guest, p. 37 e também neste sentido Gomes, J. M. V. (2007). *In Direito do Trabalho, (...)*, op. cit., p. 323: “a gravação oculta parece-nos claramente proibida”.

²⁴¹ Cfr. n.º 2 do art. 20.º do CT: “A utilização de equipamento referido no número anterior é lícita sempre que tenha por finalidade a proteção e segurança de pessoas e bens ou quando particulares exigências inerentes à natureza da actividade o justifiquem”

²⁴² Vide Festas, D. O. (2004). *In O direito à reserva da intimidade (...)*, op. cit., p. 19 e exemplificado por Lopes, S. (2014). *In Direitos Fundamentais e de (...)*, op. cit., p.38.

²⁴³ Nos termos do n.º 3 do art. 20.º do CT.

²⁴⁴ Cfr. Leitão, L. M. T. M. (2019). *In Direito do trabalho (...)*, op. cit., p. 172.

desempenho do trabalhador, com a conseqüente violação dos seus direitos de personalidade²⁴⁵. Neste sentido, traz o art. 20.º do CT a debate um conjunto de questões pertinentes: i) pode o empregador controlar, *ad eternum* o trabalhador? ii) quais as finalidades concretas admissíveis para autorizar a implementação destes meios?

De acordo com o art. 21.º do CT compete à CNPD analisar os pedidos de implementação de sistemas de videovigilância e autorizá-los²⁴⁶, com respeito pelo princípio da proibição de excesso e seus subprincípios: necessidade, adequação e proporcionalidade – n.º 2 do art. 21.º do CT. Relevar, que antes de submetido à CNPD deve ser analisado pela comissão de trabalhadores que emitirá um parecer para acompanhamento do pedido a submeter à CNPD – n.º 4 do art. 21.º do CT^{247,248}.

²⁴⁵ *Idem*, p. 172. Veja-se também o ac. do TRP processo n.º 6909/16.2T8PRT.P1, de 26 de junho de 2017. Relator: MJD Jerónimo Freitas, consultado em 05.01.2020, disponível em: <http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/213e51a9c28137de80258169003b373d?OpenDocument>: “É de aceitar as imagens captadas por sistema de videovigilância como meio de prova em processo disciplinar e na subsequente ação judicial em que se discuta a aplicação de sanção disciplinar, mormente o despedimento, **desde que sejam observados os pressupostos que decorrem da legislação sobre a proteção de dados e concomitantemente se conclua que a finalidade da sua colocação não foi exclusivamente a de controlar o desempenho profissional do trabalhador**. Num quadro circunstancial assim apurado, o trabalhador não merece – nem a lei lhe confere - maior proteção do que aquela que é conferida aos demais cidadãos e, logo, o meio de prova é lícito e admissível.

IV - Concluindo-se que foram observados os pressupostos que decorrem da legislação sobre a proteção de dados no que respeita à autorização do sistema de videovigilância, que nem a sua colocação nem as imagens captadas visam exclusivamente controlar o desempenho profissional dos trabalhadores e que a autora tinha conhecimento da existência do sistema de videovigilância e, logo, que estariam a ser captadas imagens (...). Sublinhado nosso.

²⁴⁶ Neste sentido o ac. do TRE processo n.º 244/17.6T8PTM.E1, de 06 de dezembro de 2017. Relator: MJD Moisés Silva, consultado em 05.01.2020, disponível em: <http://www.dgsi.pt/jtre.nsf/-/DC3C8C21D1195564802581FD003421B6>: “As imagens captadas pelo sistema de videovigilância, **nos termos da autorização concedida pela CNPD**, são proibidas se tiverem por finalidade controlar o trabalhador e a sua prestação, mas são admitidas se tiverem por fim proteger os bens e as pessoas(...)” – sublinhado nosso, e o ac. do TRC processo n.º 359/13.0TTFIG-A.C1, de 06 de fevereiro de 2015. Relator: MJD Azevedo Mendes, consultado em 15.03.2019, disponível em, <http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/fe545bb508b68e6980257dee004bf0bd?OpenDocument>.

²⁴⁷ Cfr. Leitão, L. M. T. M. (2019). *In Direito do trabalho (...)*, op. cit., pp. 172 e 173.

²⁴⁸ Na nossa opinião, convém notar que cumpridas as formalidades subjacentes à implementação de sistemas de vigilância à distância, o trabalhador quando tenha conhecimento da utilização destes meios deve resguardar a sua privacidade, pois a informação captada/recolhida, pode ser usada em sede de processo disciplinar. A título ilustrativo veja-se o ac. do TRP processo n.º 159/18.0T8PNF-A. P1, de 07 de dezembro de 2018. Relator Domingos Morais, consultado em 15.03.2019, disponível em, <http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/cc2a4b78e8ec279d8025839800517f79?>

V. A confidencialidade de mensagens e de acesso a informação – art. 22.º do CT

No âmbito laboral, existe a problemática de se saber quais as mensagens que gozam do direito à confidencialidade, isto porque o art. 22.º do CT apenas diz que o trabalhador goza do direito de reserva e confidencialidade relativamente ao conteúdo das mensagens de “natureza pessoal e de acesso à informação de carácter não profissional”²⁴⁹ que envie, receba ou consulte, nomeadamente através do correio eletrónico”^{250,251}.

De acordo com PAULA QUINTAS e HELDER QUINTAS, “este direito possui natureza absoluta”²⁵² devendo o empregador respeitá-lo. Todavia, esta natureza absoluta abarca todas as mensagens? Ou seja, as de natureza pessoal e as não profissionais? De acordo com estes autores, sim²⁵³.

Pese embora o preceito estabelecer o direito à confidencialidade, vem o n.º 2 do art. 22.º do CT, dizer que ainda assim pode o empregador regulamentar a forma de utilização dos meios de comunicação²⁵⁴. Ora, ao regulamentar, v.g., regulamento interno, pode nele definir o que pode ou não ser consultado na internet, pode estipular a

[OpenDocument](#). Donde se conclui que o direito à privacidade e à proteção de dados pessoais, não são absolutos, porque podem ser derogados e utilizados, daí que o trabalhador deva também atuar com cuidado.
²⁴⁹ Segundo Festas, D. O. (2004). *In O direito à reserva da intimidade (...)*, op. cit., pp. 21 e 22, são três os tipos de mensagens (profissionais, de natureza pessoal e de “carácter não profissional”) nas de natureza pessoal as “que poderão dizer respeito à esfera íntima ou privada” as não profissionais, nestas “incluem-se (...) as mensagens de carácter publicitário, informativo” que em nada de se relacionem com a vida privada do trabalhador.

²⁵⁰ Cfr n.º 1 do art. 22.º do CT.

²⁵¹ Cremos que o legislador quando diz “nomeadamente através de correio eletrónico” determina que a confidencialidade das mensagens pode existir noutros aplicativos, como seja o Messenger ou o WhatsApp, não restringe, sendo um este um mero exemplo, não é taxativo. Também Lopes, S. (2014). *In Direitos Fundamentais e de (...)*, op. cit., p.41, assim o entende quando chama a atenção para o facto de ter o legislador deixado em aberto a inclusão de outros meios eletrónicos.

Neste ponto, notar que o trabalhador deve ter um cuidado acrescido com o instrumento de trabalho que usa para enviar/receber mensagens, pois se este for de uso partilhado, a natureza pessoal das mensagens pode não existir, veja-se o ac. do TRL processo n.º 2330/16.0T8LSB-4, de 25 de janeiro de 2017. Relator: MJD Leopoldo Soares, consultado em 04.11.2019, disponível em: <http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/a2a6b4fcf4d104af802580cd00373bc7?OpenDocument>.

²⁵² Quintas, P. & Quintas, H. (2016). *In Código do Trabalho Anotado (...)*, op. cit., p. 113.

²⁵³ *Idem*, p. 113.

²⁵⁴ Vide Dray, G. (2019). *In Direitos Fundamentais e de Personalidade (...)*, op. cit., p. 76.

monitorização de mensagens, bem como determinar os tempos de utilização e ainda proibir o acesso quando os fins não sejam profissionais²⁵⁵.

Caso o empregador disponibilize os meios sem regulamentar a utilização, o acesso ao conteúdo dos emails, mesmo que marcados como não pessoais, fica interdito ao empregador²⁵⁶. Pelo que, regulamentada que esteja a utilização para fins pessoais, o acesso pelo empregador fica, outrossim, proibido, e bem assim a divulgação, quer das mensagens de natureza pessoal quer as de natureza extraprofissional. Neste ponto, duas perguntas se colocam: o que é pessoal e o que é extraprofissional? Como pode o empregador saber a natureza da mensagem sem antes a abrir?

À primeira questão, DAVID FESTAS, responde dizendo que se as mensagens são de natureza pessoal o trabalhador tem o direito ao sigilo da correspondência pois está em causa a reserva da vida privada²⁵⁷. O mesmo autor diz que as mensagens de natureza extraprofissional podem englobar: a marcação de uma viagem²⁵⁸, não existindo nesta uma reserva da vida privada. Porém, em nosso entendimento existe o direito ao sigilo da correspondência, deste modo, não devem ser acedidas e muito menos divulgadas²⁵⁹.

Quanto à segunda questão, para tentar a aceder às mensagens é necessário que o empregador controle os meios eletrónicos onde as mesmas são difundidas, existindo uma maioria que defende ser “ilícito o controlo permanente”^{260,261}.

²⁵⁵ Lopes, S. (2014). *In Direitos Fundamentais e de (...)*, op. cit., p.40. Porém, na nossa opinião, uma proibição total pode ser contraproducente.

²⁵⁶ Para esta situação alerta-nos o ac. do TRP processo n.º 208/14.1TTVFR-D.P1, de 15 de dezembro de 2016. Relatora: MJD Paula Leal de Carvalho, consultado em 11.10.2018, disponível em, <http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/df89d957d1942212802580a70058cc70?OpenDocument>

²⁵⁷ Festas, D. O. (2004). *In O direito à reserva da intimidade (...)*, op. cit., p. 21. Por exemplo, uma mensagem que o trabalhador envie para o filho.

²⁵⁸ *Idem*, p. 22.

²⁵⁹ Outrossim, Dray, G. (2019). *In Direitos Fundamentais e de Personalidade (...)*, op. cit., p. 76, assim o entende quando diz: “são proscritas ao empregador intrusões ao conteúdo das mensagens de natureza não profissional”.

²⁶⁰ Lopes, S. (2014). *In Direitos Fundamentais e de (...)*, op. cit., p.41.

²⁶¹ Uma solução é, a previsão no regulamento da empresa, que as mensagens não profissionais sejam marcadas como tal, v.g., personal ou private, não devendo, o trabalhador, fazer um uso abusivo deste tipo de comunicação no local e no tempo de trabalho, para não prejudicar a prestação da sua atividade não criando, destarte, conflitos com o empregador.

Secunda GUILHERME DRAY²⁶², a impossibilidade de o empregador não poder aceder às mensagens de natureza pessoal do trabalhador. Todavia, quando, e por especial, razões seja necessária a visualização esta deve ocorrer na presença do trabalhador, de um responsável do sindicato ou da comissão de trabalhadores. Porém, a visualização nunca deve ser do conteúdo, mas só de dados que não afetem a privacidade do trabalhador²⁶³.

Posto isto, referir que o incumprimento de ambas as partes [trabalhador: regra de utilização, e do empregador: violação do direito reserva vida privada] produz sanções. Para o trabalhador há uma infração disciplinar, já o empregador incorre em responsabilidade contraordenacional²⁶⁴.

Não só a doutrina, mas também a jurisprudência, vão no sentido de considerar o acesso e divulgação como violação do direito à reserva da vida privada e confidencialidade das mensagens, ou seja, do sigilo da correspondência²⁶⁵.

B. Proteção penal

Já antes referido, o código penal também tutela a proteção da reserva sobre a vida privada e a violação da correspondência. Ou seja, consubstancia um ilícito criminal o

²⁶² Vide Dray, G. (2019). *In Direitos Fundamentais e de Personalidade (...)*, op. cit., pp. 76 e 77.

²⁶³ Veja-se o ac. do TRE processo n.º 747/18.5T8PTM.E1, de 28 de março de 2019. Relator: MJD Paula d Paço, consultado em 15.01.2020, disponível em: <http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/55801c7296f02f54802583d90052c54c?OpenDocument&Highlight=0.whatsapp>, vem firmar a posição que o conteúdo da “mensagens emitidas pelo trabalhador (...) não poderiam ser utilizadas em sede de procedimento disciplinar, por se tratarem de comunicações pessoais e privadas” havendo nesta medida violação do direito fundamental de reserva da intimidade da vida privada e da “tutela legal e constitucional da confidencialidade da mensagem pessoal”, leia-se correspondência.

²⁶⁴ De acordo com Dray, G. (2019). *In Direitos Fundamentais e de Personalidade (...)*, op. cit., p. 77 e Festas, D. O. (2004). *In O direito à reserva da intimidade (...)*, op. cit., pp. 24 e 25.

²⁶⁵ A título ilustrativo:

Ac. do STJ processo n.º 07S043, de 05 de julho de 2017. Relator: MJD Mário Pereira, consultado em 17.01.2020, disponível em: <http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/54d3c9f0041a33d58025735900331cc3>.

Ac. do TRL processo n.º 2970/07.4, de 05 de junho de 2008. Relator: MJD Leopoldo Soares, consultado em 04.11.2019, disponível em: <http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/6c195267c4ce32e480257474003464f7?OpenDocument>.

Ac. do TRP processo n.º 208/14.1TTVFR-D. P1, de 15 de dezembro de 2016. Relatora: MJD Paula Leal de Carvalho, consultado em 11.10.2018, disponível em: <http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/df89d957d1942212802580a70058cc70?OpenDocument>.

desrespeito dos dois direitos mencionados. O direito à reserva da intimidade tem, na opinião de M.^a ANGELES RUÉDA MARTINS proteção penal em três vertentes: quando seja colocado em causa o direito de personalidade da reserva da vida privada; porque é merecedor de confidencialidade; e quando perante a proteção de dados, consequência das novas formas de comunicação e das novas tecnologias de informação²⁶⁶.

Segundo alguma doutrina, estas novas tecnologias de informação e comunicação despoletaram a necessidade de se estudarem outras áreas do direito, criando espaço para o aparecimento de outros ramos do direito²⁶⁷: “direito das telecomunicações ou direito das comunicações eletrónicas”.

Deste modo, basta olharmos para o Direito Penal para constatar que “surgiram novas incriminações”²⁶⁸, culminando numa necessária atualização do direito penal para conseguir a garantia da proteção das comunicações realizadas por meio informático. Ou seja, já existia, no ordenamento jurídico nacional a proteção da vida privada e da correspondência, mas que se limitava aos tradicionais meios de comunicação²⁶⁹. Com a explosão tecnológica que se estendeu também ao meio laboral, com as empresas a fazerem uso destas tecnologias, criou-se a necessidade de salvaguarda dos utilizadores destas tecnologias²⁷⁰.

Destarte, o art. 194.^o²⁷¹ do Código Penal, doravante CP, vem determinar que incorre num crime quem violar a correspondência ou a telecomunicação. Este crime pode

²⁶⁶ Rueda Martín, M. Á. (2004). *In Protección penal de la intimidad personal e informática: los delitos de descubrimiento y revelación de secretos de los artículos 197 y 198 del código penal*. Barcelona: Atelier, pp. 28 e 29.

²⁶⁷ No entendimento de Neves, R. C. (2011). *In As ingerências nas comunicações (...)*, op. cit., p. 19.

²⁶⁸ Cfr. Neves, R. C. (2011). *In As ingerências nas comunicações (...)*, op. cit., p. 21.

²⁶⁹ Entenda-se, as denominadas cartas enviadas por correio.

²⁷⁰ Vide Neves, R. C. (2011). *In As ingerências nas comunicações (...)*, op. cit., p. 23.

²⁷¹ Veja-se art. 194.^o do CP: “1 - Quem, sem consentimento, abrir encomenda, carta ou qualquer outro escrito que se encontre fechado e lhe não seja dirigido, ou tomar conhecimento, por processos técnicos, do seu conteúdo, ou impedir, por qualquer modo, que seja recebido pelo destinatário, é punido com pena de prisão até 1 ano ou com pena de multa até 240 dias. 2 - Na mesma pena incorre quem, sem consentimento, se intrometer no conteúdo de telecomunicação ou dele tomar conhecimento. 3 - Quem, sem consentimento, divulgar o conteúdo de cartas, encomendas, escritos fechados, ou telecomunicações a que se referem os números anteriores, é punido com pena de prisão até 1 ano ou com pena de multa até 240 dias.”

compreender “seis modalidades distintas de conduta”^{272,273}. Contudo, tendo presente o âmbito do nosso estudo vamos dar ênfase às modalidades relacionadas com as telecomunicações: “intrometer-se no conteúdo de telecomunicação ou dele tomar conhecimento”²⁷⁴ e concluir que quem desrespeitar o direito à confidencialidade das mensagens incorre na prática de um crime estatuído e punido pelo citado artigo do CP.

Segundo PAULO PINTO DE ALBUQUERQUE²⁷⁵ “a intromissão no conteúdo da telecomunicação consubstancia uma interferência, uma perturbação” de modo que “comete um só crime o agente que divulga, sem consentimento do autor, o conteúdo (...)”²⁷⁶.

Na nossa opinião, o art. 193.º do CP traduz-se num meio efetivo de proteção do trabalhador, porque o empregador não pode violar, por meio informático, a proteção de dados. Por outras palavras, um empregador que crie, mantenha ou utilize ficheiros de dados que comportam informação referente a dados pessoais, pode incorrer em devassa por meio informático quando não detenha a devida autorização²⁷⁷ de acordo com o vertido no art. 193.º do CP²⁷⁸.

Conforme secunda FIGUEIREDO DIAS²⁷⁹ visa-se “garantir a interdição absoluta, constitucionalmente imposta, do tratamento informático de um conjunto de dados pessoais”. Neste preceito, art. 193.º do CP, e nas palavras de PAULO PINTO DE

²⁷² Assim postula Dias, J. de F. (1999). *In Comentário Conimbricense do Código Penal, Parte Especial, Tomo I, arts. 131.º a 201.º*. Coimbra Editora, pp. 760 e ss, comentário do art. 194.º realizado por Manuel da Costa Andrade.

²⁷³ Para mais detalhe ver Dias, J. de F. (1999). *In Comentário Conimbricense (...)*, op. cit., pp. 760 e ss.

²⁷⁴ *Idem*, p. 762.

²⁷⁵ Cfr. Albuquerque, P. P. (2008). *In Comentário do Código Penal à Luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem*. Lisboa: Universidade Católica Editora, pp. 527 e ss.

²⁷⁶ *Idem*, p. 529.

²⁷⁷ Emitida pela CNPD.

²⁷⁸ Cfr. art. 193.º do CP: “1 - Quem criar, manter ou utilizar ficheiro automatizado de dados individualmente identificáveis e referentes a convicções políticas, religiosas ou filosóficas, à filiação partidária ou sindical, à vida privada, ou a origem étnica, é punido com pena de prisão até 2 anos ou com pena de multa até 240 dias. 2 - A tentativa é punível”.

²⁷⁹ Vide Dias, J. de F. (1999). *In Comentário Conimbricense (...)*, op. cit., pp. 744.

ALBUQUERQUE²⁸⁰, “o bem jurídico protegido (...) é a autodeterminação informacional de cada pessoa” que seja tratada informaticamente e sem o devido consentimento.

Perante o exposto subsistem dúvidas: pode um empregador ou uma empresa ser sancionada criminalmente? Não o podendo ser enquanto pessoa coletiva pode sê-lo na qualidade de representante da sociedade, o gerente ou o Administrador? Assim, será o Administrador ou um trabalhador, indicado para o efeito, constituído arguido respondendo em sede de procedimento criminal? No âmbito da proteção de dados poderá essa responsabilidade recair sobre a figura do responsável pelo tratamento de dados? Como fica a posição deste trabalhador?

Após algum estudo, não se vislumbram respostas, na lei para estas questões. Ora sendo um trabalhador da empresa, e não uma entidade externa, a exercer o cargo de responsável pelo tratamento de dados, estamos em crer que a posição deste trabalhador é deveras frágil, devendo esta situação ser, *qui sapit*, acautelada na lei.

²⁸⁰ Cfr. Albuquerque, P. P. (2008). *In Comentário do Código Penal (...)*, op. cit., pp. 523.

CAPÍTULO III – As comunicações eletrónicas e a proteção de dados

1. As novas tecnologias de informação e correspondente [ou não] relevância da violação da vida privada

1.1 Considerações iniciais

O crescente uso das tecnologias de informação e comunicação transformou a privacidade. Hoje, se assim se quiser tudo pode ser público e facilmente acessado. Segundo ALEXANDRE PINHEIRO²⁸¹ “o clima sociocultural” no qual se vive “não favorece nem a *privacy*, nem a proteção de dados. Estranha-as”.

O mesmo sucede com o trabalhador. Este tem acesso a dispositivos, fornecidos pela empresa, eventualmente, para facilitar a forma de trabalho, no entanto o trabalhador tem de ter em mente que esta é uma situação que pode ter um reverso. Ora, se por um lado lhe facilita a forma de trabalho, pois não o obriga a estar preso, num escritório²⁸², para prestar a sua atividade, por outro ao levar consigo estes dispositivos, pode estar a colocar em risco a sua privacidade. Daqui decorre a existência de uma grande “flexibilidade das relações laborais que tem de ser aceite como uma via de dois sentidos”²⁸³.

Esta flexibilidade vai produzir efeitos na delimitação entre a fronteira do que é pessoal e do que é profissional, pelo que se defende, a existência de uma aceitável “qualidade de vida profissional”²⁸⁴ sendo a privacidade um dos seus principais elementos, posição sustentada por TERESA MOREIRA.

O modo de trabalho ficou mais facilitado pelo uso de novas formas de comunicação, “principalmente a internet e o *email*”²⁸⁵ adquiridas pelo empregador e disponibilizadas ao trabalhador. Com o recurso à utilização das tecnologias de informação e comunicação modernas, coloca-se em perigo a privacidade do trabalhador, todavia elas

²⁸¹ Vide Pinheiro, A. S. (2015). *In Privacy e proteção de dados pessoais (...)*, op. cit., p. 107.

²⁸² Cfr. Marques, G. e Martins, L. (2006). *In Direito da Informática (...)*, op. cit., p. 53., indicam mesmo esta transformação quando dizem que “as mudanças nos métodos de trabalho são já visíveis” pois hoje pode trabalhar-se, desde logo, a partir de casa “teletrabalho”.

²⁸³ Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., p. 626.

²⁸⁴ *Idem*, p. 627.

²⁸⁵ Veja-se Moreira, T. A. C. (2010). *In A privacidade dos trabalhadores e o controlo eletrónico da utilização da Internet*, Questões Laborais, p. 23

potenciam uma maior fluidez nas comunicações, com a consequente poupança de “tempo e custos”²⁸⁶. Concomitantemente se percebe que o computador assume um papel preponderante como meio comunicacional²⁸⁷, inclusive, fora do contexto laboral, pelo trabalhador. O facto dos meios de comunicação se poderem deslocar com o trabalhador consubstanciam um perigo para a privacidade, bem como para o “exercício das liberdades”²⁸⁸.

Porém, é impensável, trabalharmos hoje, sem recurso às tecnologias de informação, seja através do computador ou de outro dispositivo. Neste sentido, importa proteger a privacidade dos seus utilizadores, os seus dados, porquanto a informação transmitida, acedida pelo empregador encontra-se protegida pelo art.º 35.º da CRP²⁸⁹.

1.2 O RGPD e as relações laborais

O uso das tecnologias de informação e comunicação pelos trabalhadores acabam por comportar um tratamento de informação que obriga ao necessário respeito pelo RGPD pois podemos estar perante dados pessoais. Assim, toda a ação que seja praticada com recurso ao uso das tecnologias informáticas [consulta de sites, envio de mensagens] abrange informação pessoal dos seus utilizadores²⁹⁰. Posto isto, consideramos que devem ser atendidos os princípios fundamentais que tutelam a proteção de dados pessoais, previstos no RGPD.

Todavia, temos constatado que a proteção de dados, no âmbito laboral, assenta numa posição jurídica complexa pois a licitude do tratamento de dados raramente ou nunca assenta num dos requisitos²⁹¹. Conforme secunda ALEXANDRE PINHEIRO, o

²⁸⁶ *Idem*, p. 25

²⁸⁷ Marques, G. e Martins, L. (2006). *In Direito da Informática (...)*, op. cit., p. 36, de acordo com os autores, nos dias de hoje a sociedade de informação depende do uso do computador para tudo.

²⁸⁸ Cfr. Pinheiro, A. S. (2015). *In Privacy e proteção de dados pessoais (...)*, op. cit., p. 803. Para o autor, “a proteção de dados deve ser qualificada como um direito de personalidade” pois protege os titulares - as pessoas [trabalhadores], posição que também nós defendemos.

²⁸⁹ Vide Moreira, T. A. C. (2010). *In A privacidade dos trabalhadores e o controlo eletrónico da utilização da Internet*. Questões Laborais. Coimbra, n.º 35/36, p. 58, e Pinheiro, A. S. (2015). *In Privacy e proteção de dados pessoais (...)*, op. cit., p. 830.

²⁹⁰ De acordo com Moreira, T. A. C. (2010). *In A privacidade dos trabalhadores e o controlo (...)*, op. cit., p. 62.

²⁹¹ Referimo-nos ao requisito: consentimento.

consentimento como fonte de legitimidade é, porém, superado por razões contratuais, para cumprimento de obrigações legais”²⁹², destarte, o trabalhador dificilmente dará – consentimento - pois o empregador recorre aos outros meios lícitos para regularizar o tratamento que necessita fazer²⁹³, criando esta realidade um dilema que se considera interessante estudar, quem sabe para produzir uma alteração e chegar-se à possibilidade de recorrer ao consentimento como fundamento de licitude em contexto laboral.

1.2.1 Dados pessoais

1.2.1.1 Conceito e prazo de conservação

O conceito de dados pessoais, encontra-se vertido no n.º 1 do art. 4.º do RGPD, sendo: “dados pessoais, informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»)”²⁹⁴. De acordo com o *Working Party*, doravante WP, do *article 29.º*, no Parecer 4/2007²⁹⁵, o conceito vertido na Diretiva 95/46/CE, continha uma noção ampla de dados pessoais. Verifica-se, ao analisar a definição vertida na Diretiva e a do RGPD, que esta se mantém ampla, em nosso entendimento, para englobar todos os tipos de informações²⁹⁶, mas também, para “proteger o direitos e liberdades fundamentais das pessoas, nomeadamente o seu direito à vida privada, no que toca ao tratamento de dados pessoais”²⁹⁷.

Outrossim, da leitura do considerando (26) se aprende que o conceito é lato, pelo que aplicar-se-á a qualquer informação relativa a uma pessoa singular²⁹⁸. A análise do

²⁹² Conforme expõe Pinheiro, A. S. (2015). *In Privacy e proteção de dados pessoais (...)*, op. cit., p. 809.

²⁹³ Em nosso entendimento, o consentimento é o meio mais fiel de aceitar o tratamento de dados, pois dá ao trabalhador informação que lhe permite tomar uma decisão, pois é-lhe dado a conhecer a finalidade para a qual foi recolhido um dado. Desta forma ele tem uma visão clara e decide com maior facilidade e conhecimento.

²⁹⁴ Cfr. n.º 1 do art. 4.º do RGPD, disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN>.

²⁹⁵ Sobre o conceito de dados pessoais, consultado em: 06.10.2019, disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_pt.pdf.

²⁹⁶ Vide Pinheiro, A. S. (Coord.) (2018). *In Comentário ao Regulamento (...)*, op. cit, p. 121, onde são dados exemplos sobre o que pode ser um identificador.

²⁹⁷ Cfr. Parecer 4/2007, sobre o conceito de dados pessoais – wp136 consultado em: 06.10.2019, disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_pt.pdf.

²⁹⁸ De acordo com considerando (26) do RGPD disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN>.

conceito, realizada pelo WP do Article 29.º, decompõe-se em quatro pilares, a saber: “informação”, “relativa a”, “identificada ou identificável” e “pessoa singular”²⁹⁹. Pela leitura do considerando (30)³⁰⁰ do RGPD, concluímos que uma pessoa pode ser identificada ou torna-se identificável, não só através do nome ou do número de telefone, mas também através de identificadores eletrónicos³⁰¹.

Destarte, se apreende que a informática veio revolucionar os métodos “tradicionais de organização, registo e utilização da informática”³⁰², porque à distância de um clique a informação fica acessível, disponível para quem quiser fazer uso dela, tornando-se essencial conectar a proteção de dados com a privacidade, tendo este último conceito de sofrer uma alteração, para se adaptar e abarcar a nova realidade vivida na era da informática³⁰³, pois até o IP (*Internet Protocol*) se enquadra no conceito de dados pessoais.

No âmbito da relação laboral, e de acordo com AMADEU GUERRA³⁰⁴, os dados que a entidade empregadora pode recolher prendem-se com os necessários para “aférir a capacidade jurídica (...) à celebração de um contrato de trabalho: idade e habilitações literárias”. Além destes, outros, quando adequados e pertinentes podem ser solicitados, é o caso: a) da residência do trabalhador; b) contacto; c) aptidões que possam ser úteis ao desempenho da sua atividade, *inter alia*^{305,306}.

Uma dúvida que consideramos importante assinalar relaciona-se com o endereço de *email* atribuído ao trabalhador. Ou seja, quando uma empresa define como endereço eletrónico, v.g., rita.rodrigues@empresa.pt, está a criar um endereço pessoal? Que

²⁹⁹ Cfr. Parecer 4/2007, sobre o conceito de dados pessoais – wp136 consultado em: 06.10.2019, disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion_recommendation/files/2007/wp136_pt.pdf.

³⁰⁰ De acordo com considerando (30) do RGPD disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN>.

³⁰¹ Por conseguinte, um trabalhador, ao qual é atribuído um computador, pode ser identificado ou tornar-se identificável pelo seu endereço de IP (*Internet Protocol*).

³⁰² Nas palavras de Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit. p. 122.

³⁰³ *Idem*, p. 123.

³⁰⁴ Guerra, A. (2004). *In A privacidade no local de trabalho: as novas tecnologias e o controlo dos trabalhadores através de sistemas automatizados: as alterações do código do trabalho*. Coimbra: Almedina, p. 159.

³⁰⁵ Guerra, A. (2004). *In A privacidade no local de trabalho: as novas tecnologias (...)*, op. cit., p. 159.

³⁰⁶ V.g. conhecimentos informáticos, linguísticos, carta de condução, formação, *inter alia*.

identifica ou pode identificar um trabalhador? E quando transmitido a terceiros concede a informação sobre um dado pessoal³⁰⁷? Entendemos que existem outras formas de criação de endereços eletrónicos menos identificativos, onde não conste o nome, usando iniciais ou números mecanográficos, por exemplo: 100055562@empresa.pt, e defendemos que deve esta forma de atribuição de um endereço constar do regulamento interno das empresas com a devida comunicação ao trabalhador.

Outra matéria que consideramos pertinente é o prazo de conservação dos dados pessoais. Com a Lei n.º 67/98, de 26 de outubro, na al. b) do n.º 1 do art.º 5.º, os dados, no decurso do processo de contratação, eram recolhidos com a finalidade de organizar e suportar o processo de seleção. Se a contratação avançasse os dados eram aproveitados e encaminhados para o departamento de gestão de pessoal³⁰⁸. Não havendo contratação então eram apagados³⁰⁹.

Porém, da leitura da lei de execução do RGPD, concluímos que, não foi definido expressamente nenhum prazo de conservação, mantendo-se em abstrato. Ou seja, o prazo será aquele que se revele necessário para a prossecução da finalidade, conforme n.º 1 do art.º 21 da Lei n.º 58/2019, de 8 de agosto. Porém, e de acordo com a al. a), do n.º 2 do art. 13.º do RGPD deve o prazo ser comunicado ou explicitado.

Tendo presente o facto que o prazo de conservação se encontra intrinsecamente ligado às finalidades, é assim “fundamental que sejam especificadas com rigor as finalidades”³¹⁰, bem como as “mesmas sejam do conhecimento dos titulares dos dados”³¹¹. Só deste modo são garantidas as devidas condições para uma adequada intervenção, pelos titulares, na conservação dos dados. Estatui o n.º 4 do art. 21.º da Lei n.º 58/2019, de 8 de agosto, que após cessar a finalidade que motivou o tratamento, o responsável pelo tratamento deve proceder à sua destruição ou anonimização.

³⁰⁷ O nome, um IP, de acordo com n.º 1 do art. 4.º do RGPD.

³⁰⁸ Neste caso, não existia um pedido de consentimento ao trabalhador? Enquadrar-se-á na al. b) do n.º 1 do art.º 6.º do RGPD? Na nossa opinião, ainda que não seja pedido o consentimento do trabalhador, devia pelo menos ser informado sobre a transmissão dos dados.

³⁰⁹ Veja-se Guerra, A. (2004). *In A privacidade no local de trabalho: as novas tecnologias (...)*, op. cit., p. 169.

³¹⁰ *Idem*, p. 169.

³¹¹ *Ibidem*, p. 169.

O aqui vertido refere-se ao novo direito que o RGPD trouxe para o titular dos dados, a possibilidade de apagamento dos dados, de ser esquecido – art. 17.º do RGPD³¹²,³¹³. Pelo vertido no n.º 1 do art. 17.º do RGPD, os titulares têm o direito de solicitar o apagamento, que deve ser atendido com a maior brevidade possível pelo responsável ou pelo subcontratante³¹⁴ com fundamento num dos motivos apresentados nas alíneas do n.º 1. O direito ao esquecimento, bem como o direito de informação, são no entendimento de CATARINA CASTRO³¹⁵, alguns direitos que assistem aos titulares dos dados. Porém, quando cessa a relação laboral, o trabalhador pode solicitar o apagamento ou ele é, automaticamente, promovido pelo responsável pelo tratamento?

Entendemos que, para proteção do trabalhador e garantia efetiva deste direito, deveria constar na lei de execução do RGPD, *qui sabit* no art. 28.º a informação sobre o direito ao apagamento dos dados pessoais. Ou então no art. 21.º, estipular que os dados são conservados pelo tempo que vigora a relação contratual sendo os mesmos destruídos quando esta finde, efetivando-se o conhecimento através de notificação conjunta à autoridade de controlo e ao trabalhador, tornando-se, assim, num procedimento transparente.

³¹² Cfr. art. 17.º do RGPD: 1. O titular 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 (...).

³¹³ Questionamos: no âmbito da relação laboral, este direito pode ser plenamente exercido pelo titular? Não o sendo, é limitado, há uma restrição pelo tipo de relação existente entre o titular dos dados e o responsável pelo tratamento dos mesmos? Será esta limitação admissível? Consideramos que não, mas ponderando a posição do trabalhador ela é aceitável, devendo, no entanto, ser modificada.

³¹⁴ Vide Pinheiro, A. S. (Coord.) (2018). *In Comentário ao Regulamento (...)*, op. cit., p. 367

³¹⁵ Castro, C. S. (2005). *In Direito da Informática, Privacidade (...)*, op. cit., p. 240, para a autora “le droit a l’oubli” determina que os dados sejam somente conservados pelo prazo estritamente necessário para a “prosseção das finalidades da recolha” é por este motivo que a existência do direito, à autodeterminação informativa está intrinsecamente ligado ao prazo de conservação dos dados pessoais.

1.2.1.2 Tratamento: requisitos

Considerando que as tecnologias informáticas, foram criadas pelo homem e usadas por ele, importa realçar, tal como o faz TERESA MOREIRA³¹⁶ que o seu uso potencia a necessidade de proteção³¹⁷.

De acordo com TERESA MOREIRA³¹⁸, o tratamento lícito é requisito *sine qua non*³¹⁹ para se estar perante dados pessoais, não bastando que se “opere a subsunção legal”³²⁰. Assim, questiona-se: o que deve ser entendido por tratamento? Nos termos do vertido no n.º 2 do art. 4.º do RGPD³²¹, uma operação ou um conjunto delas, realizadas sobre dados pessoais, quer por meios automatizados ou não automatizados, designadamente: recolha, registo, organização, conservação, comportam o denominado tratamento de dados pessoais. Ou seja, todas as operações efetuadas com os dados pessoais de um titular [trabalhador], inclusive apagá-los ou limitá-los, é tratamento. Este é um conceito deveras fundamental pois transmite a real dimensão do que pode ser feito com a informação inerente ao trabalhador.

Como se processa um tratamento lícito?

Secunda CATARINA CASTRO ser essencial a verificação de uma condição de legitimidade para que exista um tratamento devidamente fundamentado, pelo que a licitude do tratamento de dados pessoais sustenta-se através dos requisitos vertidos nas als. a) a f) do art. 6.º do RGPD.

³¹⁶ Assim expõe Moreira, T. A. C. (2010). *In A privacidade dos trabalhadores e o controlo (...)*, op. cit., p. 24.

³¹⁷ De acordo com Castro, C. S. (2005). *In Direito da Informática, Privacidade (...)*, op. cit., p. 64: “a criação e manutenção de um conjunto de dados pessoais, pelos perigos que pode constituir para os titulares dos dados, é uma tarefa de responsabilidade.

³¹⁸ Moreira, T. A. C. (2010). *In A privacidade dos trabalhadores e o controlo (...)*, op. cit., p. 35.

³¹⁹ Essencial, de acordo com Infopédia, consultado em: 15.02.2020, disponível em: <https://www.infopedia.pt/dicionarios/lingua-portuguesa/sine+qua+non>.

³²⁰ Veja-se Moreira, T. A. C. (2010). *In A privacidade dos trabalhadores e o controlo (...)*, op. cit., p. 35.

³²¹ «Tratamento», uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

A. Legitimidade para tratamento de dados pessoais dos trabalhadores

A legitimidade para se tratar dados pessoais surge, desde logo, no elenco do art. 6.º do RGPD. Neste preceito, determina-se, na al. a), que o tratamento só é lícito se e na medida em que se verifique pelo menos o facto de titular dos dados ter dado **o seu consentimento**³²² para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas. O n.º 11 do art. 4.º do RGPD define-o como: **uma manifestação de vontade, livre, específica, informada e explícita**³²³, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento³²⁴. Por conseguinte, verifica-se que a manifestação de vontade, clara, positiva e inequívoca³²⁵, deve estar presente, e deste modo, a liberdade para consentir implica “uma escolha real”³²⁶ feita pelos titulares.

O consentimento não pode ser genérico, tem de estar ligado a uma finalidade concreta, pois assim permite ao titular dos dados saber qual a informação que está a ser tratada e para que fim³²⁷.

A Diretiva 95/46/CE, de 24 de outubro de 1995, não exigia uma demonstração sobre como tinha sido obtido o consentimento. Uma das mudanças operadas pelo RGPD centra-se exatamente neste ponto, vindo o n.º 2 do art. 5.º determinar que os responsáveis pelo tratamento tenham, não só de verificar o cumprimento dos princípios como também a capacidade de comprovar e demonstrar que o consentimento foi obtido lícita e

³²² Sublinhado nosso.

³²³ Sublinhado nosso.

³²⁴ A noção em inglês é ligeiramente diferente: “*consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*”, de acordo com Mota, J. (2018). *In O consentimento no Regulamento (...)*, op. cit., p. 6.

³²⁵ Atente-se ao considerando (32) do RGPD.

³²⁶ Vide Mota, J. (2018). *In O consentimento no Regulamento (...)*, op. cit., p. 6.

³²⁷ De acordo com o Parecer 15/2011, sobre consentimento do Grupo de Trabalho do Artigo 29.º (2011). Orientações sobre o consentimento. WP187, consultado em: 25.01.2020, disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf.

validamente^{328,329}. No RGPD temos, nos considerandos, importante *guidelines* para perceber o que pode ou não ser aceite³³⁰ e como se pode ou não operar o consentimento.

Relativamente ao consentimento, que em nossa opinião é o mais relevante, notar que nas relações laborais é de difícil aplicabilidade. Questionamo-nos: haverá consentimento livre e individualmente dado pelo trabalhador?

Esta é uma questão vital, na nossa opinião, e outrossim na de TERESA MOREIRA, pois também para a autora subsistem dúvidas, nomeadamente: na relação laboral o consentimento, quando prestado, é livre e esclarecido? Existirão vícios na formação da vontade? Considerando-se as especiais características da relação Trabalhador/Empregador, não deveriam ter sido adotadas medidas mais específicas na legislação laboral? Como se processa este consentimento?³³¹

A doutrinadora, vem defender que “o consentimento do titular dos dados, livre e individualmente concedido, é considerado como um dos elementos centrais do direito à autodeterminação informativa”, podendo a recolha, sem consentimento, causar graves perigos na sua privacidade³³². No entanto, é difícil a aceitação desta ideia pelo Direito do Trabalho, quanto ao consentimento do titular dos dados, ou seja, do trabalhador.

No nosso entendimento, o consentimento não é utilizado no âmbito das relações laborais porque dificilmente ele será “dado de livre vontade se o titular dos dados não dispuser de uma escolha verdadeira, sem restrições ou não puder recusar nem retirar o

³²⁸ Mota, J. (2018). *In O consentimento no Regulamento (...)*, op. cit., p. 7.

³²⁹ Considerando (42): “Sempre que o tratamento for realizado com base no consentimento do titular dos dados, o responsável pelo tratamento deverá poder demonstrar que o titular deu o seu consentimento à operação de tratamento dos dados. Em especial, no contexto de uma declaração escrita relativa a outra matéria, deverão existir as devidas garantias de que o titular dos dados está plenamente ciente do consentimento dado e do seu alcance”.

³³⁰ Veja-se o considerando (32): O consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrónico, ou uma declaração oral”, podendo este operar-se através de uma simples consulta num sítio da *web*. No considerando (43) é transmitida a existência de uma presunção quanto ao consentimento, que pode não ser livre se não for individualizado. Isto é, para cada finalidade um consentimento.

³³¹ Veja-se Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., p. 36.

³³² *Idem*, p. 476.

consentimento sem ser prejudicado”³³³, ficando, “relegado para um segundo plano”³³⁴. O WP259 tem este mesmo entendimento, consubstanciando esta ideia no seu parecer quando diz: “atendendo à dependência que resulta da relação empregador/trabalhador, é improvável que o titular dos dados possa recusar ao seu empregador o consentimento para o tratamento dos dados sem que haja medo ou risco real de consequências negativas decorrentes da recusa. É improvável que um trabalhador responda livremente ao pedido de consentimento do empregador (...)”³³⁵. Deste modo, bastará, e porque a relação jurídica se baseia quase sempre num contrato de trabalho, recorrer-se aos fundamentos: execução do contrato ou obrigações legais para que o tratamento seja lícito³³⁶.

Porém, ao utilizarem-se estes fundamentos dá-se o caso de o trabalhador não ter um conhecimento real sobre quais os dados objeto de tratamento e para que finalidades. Compreende-se que, se as empresas recorressem ao requisito – consentimento - poderiam ver recusada a recolha de determinados dados, v.g. impressão digital, ou então o consentimento seria obtido mediante imposição do empregador. Por conseguinte, e de acordo com *Opinion 2/2017 on data processing at work*, o *Working Party of article 29.º*, é “muito improvável que o consentimento possa constituir uma base jurídica para o tratamento de dados no local de trabalho, a menos que os empregados possam recusar, sem consequências adversas”^{337,338}.

No entanto, em nossa opinião, uma mudança legislativa mais vinculativa poderia ter sido tentada, quando estava em debate a Lei n.º 58/19, de 08 de agosto. Esta deveria ter sido no sentido de criar condições para tornar o consentimento admissível, nas relações

³³³ Considerando (42) *in fine*.

³³⁴ Cfr. Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., p. 480.

³³⁵ Vide Grupo de Trabalho do Artigo 29.º (2018). *Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679*. WP259 rev.01., consultado em 01.02.2020, disponível em: https://www.cnpd.pt/bin/rgpd/docs/wp259rev0.1_PT.pdf, p. 7.

³³⁶ Grupo de Trabalho do Artigo 29.º (2017). *Opinion 2/2017 on data processing at work*. WP249, consultado em: 06.10.2019, disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169.

³³⁷ *Idem*, p. 4

³³⁸ O GT do art. 29.º, no Parecer 2/2017, vem confirmar que o consentimento nunca será válido quando obtido de forma coerciva. Ou seja, se o empregador o pedir e o trabalhador consentir, poderá ser pelo facto de este estar numa posição de subordinação em relação ao empregador.

laborais, pois defendemos ser o fundamento de licitude mais importante e que melhor dá a saber, ao titular dos dados, as finalidades do tratamento.

Não tendo esta mudança ocorrido, dúvidas interpretativas se levantam ou se mantêm, sobre o recurso permanente aos fundamentos constantes da al. b), do n.º 1, do art. 6.º do RGPD. Porém, para MENEZES LEITÃO esta parece uma “permissão implícita no art. 17.º do CT”³³⁹. Ou seja, sendo os dados tratados ao abrigo da execução do contrato de trabalho não há conflitos entre o disposto no art. 17.º do CT e o Regulamento³⁴⁰, logo não há necessidade de recurso ao fundamento: consentimento. O n.º 1 do art. 28.º da Lei que executa o RGPD em Portugal, vem confirmar este entendimento quando, amplamente, diz que o “empregador pode tratar os dados pessoais dos seus trabalhadores para as finalidades e com os limites definidos no CT (...)”.

A nova lei, no n.º 3 do art. 28.º, define as condições para que o consentimento seja requisito de legitimidade do tratamento dos seus dados pessoais. No entanto, e por restringir à existência de uma norma legal³⁴¹, constatamos que se este já não era usado, agora, mais reforçada ficou a opção de não recurso ao consentimento. Por conseguinte, os empregadores não vão socorrer-se deste quesito de licitude.

A nosso ver, o RGPD, já não era vantajoso para os trabalhadores e a AR, teve uma oportunidade de modificar a forma como o trabalhador é encarado enquanto titular de dados. Todavia, optou por dar ainda mais poder ao empregador mantendo o trabalhador numa posição de fragilidade.

Ainda assim, e segundo MENEZES LEITÃO³⁴², a empresa deve cumprir com os princípios inerentes ao tratamento e proteção de dados pessoais³⁴³: finalidade, informação e transparência no tratamento.

³³⁹ Conforme expõe Leitão, L. M. T. M. (2019). *In Direito do trabalho (...)*, op. cit., p. 165.

³⁴⁰ Ademais, e porque o regulamento dispõe que basta um dos fundamentos constantes do art. 6.º, necessidade não há de recurso ou de tentativas de melhoramento do uso do consentimento.

³⁴¹ Entendimento postulado pela CNPD. *In Deliberação 2019/494*, consultado em 06.03.2020, disponível em https://www.cnpd.pt/home/decisooes/Delib/DEL_2019_494.pdf, p. 5v.

³⁴² Vide Leitão, L. M. T. M. (2019). *In Direito do trabalho (...)*, op. cit., p. 166.

³⁴³ Secundado também, esta posição, pelo GT do art. 29.º, *Opinion 2/2017 on data processing at work - wp249*, consultado em: 06.10.2019, disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169, p. 4.

1.2.1.3 Princípios inerentes ao tratamento

No art. 5.º do RGPD encontramos postulados os princípios relativos ao tratamento de dados pessoais. Por conseguinte, os dados pessoais só devem ser tratados quando exista licitude, lealdade, transparência e finalidades concretas, sempre com respeito pelo princípio da proporcionalidade, ou seja, quando adequados, pertinentes e limitados ao estritamente necessário. Ademais, estes dados devem, igualmente, ser exatos e atualizados sempre que necessário, e conservados somente pelo período estritamente necessário, bem como tratados com a devida segurança para evitar violações.

A doutrina considera que o princípio da finalidade é a trave-mestra do regime jurídico da proteção de dados pessoais³⁴⁴, pois é através do respeito por este princípio que se verifica a existência de legitimidade para recolher a informação. Ou seja, se ele é útil ao fim a que se destina, servindo para verificação de incompatibilidades. Além disso, e porque este princípio se encontra aliado ao princípio da necessidade, quando os dados deixem de ser necessários devem ser apagados. Destarte, o princípio da finalidade encontra-se balizado pelo da proporcionalidade *lato sensu*³⁴⁵.

Não obstante a atribuição de destaque ao princípio supramencionado outros mais devem ser observados para garantir a efetiva proteção dos dados pessoais³⁴⁶.

1.2.1.4 Responsabilidade pelo tratamento

O tratamento e cumprimento dos requisitos inerentes aos dados pessoais importa em responsabilidade, devendo a atividade de averiguação ser promovida por um responsável, que aplica as medidas técnicas e organizativas adequadas a assegurar e poder comprovar que o tratamento é realizado com respeito pelo vertido no Regulamento³⁴⁷.

³⁴⁴ Cfr. Pinheiro, A. S. (Coord.) (2018). *In Comentário ao Regulamento (...)*, op. cit, p. 207; Moreira, T. A. C. (2010). *In A privacidade dos trabalhadores e o controlo (...)*, op. cit., p. 64 e Pinheiro, A. S. (2015). *In Privacy e proteção de dados pessoais (...)*, op. cit., p. 806.

³⁴⁵ Veja-se Pinheiro, A. S. (2015). *In Privacy e proteção de dados pessoais (...)*, op. cit., p. 806.

³⁴⁶ Princípio da lealdade, intimamente relacionado com o tratamento de dados pessoais assente numa relação de equilíbrio entre os responsáveis pelo tratamento e o titular dos dados; ou o princípio da minimização dos dados: estes devem ser adequados, pertinentes e necessários, recolhido só para uma finalidade, *inter alia*. Para mais desenvolvimento veja-se Pinheiro, A. S. (Coord.) (2018). *In Comentário ao Regulamento (...)*, op. cit, pp. 205 a 212.

³⁴⁷ Nos termos do art. 24.º do RGPD.

Alerta-nos CARLOS GONÇALVES³⁴⁸ para o cuidado acrescido que deve existir quando os dados forem de maior sensibilidade, tendo as medidas de ser adequadas ao tipo de dados tratados. Outra função do responsável é a de revisão e atualização das medidas de acordo com as necessidades e finalidades, aferindo se as mesmas ainda se mantêm atuais para evitar o desvirtuamento e conseqüente desrespeito.

O responsável deve conservar um registo de todas as atividades de tratamento que estejam sob a sua responsabilidade – art. 30.º do RGPD, para comprovar a observância do disposto no RGPD³⁴⁹. Ademais, o responsável pelo tratamento coopera com a autoridade de controlo, a pedido dela, na prossecução das suas atividades³⁵⁰.

A segurança dos dados pessoais, do tratamento, enquadra-se no âmbito das funções do responsável pelo tratamento que aplica as já mencionadas medidas técnicas e organizativas, mediante o que for mais pertinente, nos termos do previsto no art. 32.º do RGPD³⁵¹. Assim, assume grande relevância, a função de notificação da violação dos dados pessoais à autoridade de controlo³⁵², que deve ocorrer nos termos do disposto no art. 55º do RGPD, sem demora injustificada, e, sempre que possível, até 72 horas após o conhecimento da mesma. Caso o prazo de 72 horas não seja cumprido deve então ser acompanhado do devido justificativo³⁵³. Atente-se que se a violação comportar também um risco para os direitos e liberdades das pessoas singulares, de acordo com o art. 34.º do

³⁴⁸ No comentário ao RGPD, veja-se Pinheiro, A. S. (Coord.) (2018). *In Comentário ao Regulamento (...)*, op. cit, pp. 396 e 397.

³⁴⁹ Veja-se o considerando (82) do RGPD.

³⁵⁰ De acordo com o vertido no art. 31.º do RGPD. Note-se, e de acordo com CARLOS GONÇALVES, em Pinheiro, A. S. (Coord.) (2018). *In Comentário ao Regulamento (...)*, op. cit, p. 448, que a obrigação de cooperação com a autoridade de controlo depende de uma primeira iniciativa desta. Ou seja, a Autoridade de Controlo tem de encetar o primeiro contacto com o responsável e formula o pedido de cooperação.

³⁵¹ Art. 32.º do RGPD: “Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado (...)”.

³⁵² Em Portugal: Comissão Nacional de Proteção de Dados – CNPD.

³⁵³ Para maior desenvolvimento veja-se Pinheiro, A. S. (Coord.) (2018). *In Comentário ao Regulamento (...)*, op. cit, p. 453.

RGPD, é necessária uma comunicação ao titular dos dados sem demora injustificada, para que este, e conforme considerando (86) tome as devidas precauções³⁵⁴.

A designação de um encarregado de proteção de dados pode ocorrer, pelo responsável quando o tratamento for efetuado por uma autoridade ou organismo público; quando envolva operações de tratamento em grande escala, conforme art. 37.º do RGPD. Notar que o n.º 6 do referido artigo determina que o encarregado pode ser um elemento do pessoal da entidade responsável ou exercer as funções com base num contrato de prestação de serviços. Quanto às suas funções elas encontram-se elencadas no art. 39.º do RGPD³⁵⁵.

No mundo empresarial, “a empresa torna-se responsável pela segurança”³⁵⁶ dos dados, pois é ela que procede à recolha dos dados de acordo com as finalidades. Esta recolha implica o dever de informar o titular sobre quem é o responsável pelo tratamento, sobre o prazo de conservação dos dados, a possibilidade de pedir o dissentimento, de solicitar esclarecimentos junto da CNPD ou de requer o acesso e/ou retificação dos dados. O responsável ao agir com diligência e probidade desempenha as suas funções e cumpre com os princípios da transparência e da informação, vertidos nos arts 12.º e 13.º do RGPD³⁵⁷.

Todavia, a empresa se não agir em conformidade com o dever de segurança será responsável perante o trabalhador, nos termos do art. 33.º da Lei n.º 58/2019, de 8 de agosto, podendo ser aplicadas sanções contraordenacionais de acordo com o exposto nos arts. 37.º a 45.º da referida lei.

³⁵⁴ Pinheiro, A. S. (Coord.) (2018). *In Comentário ao Regulamento (...)*, op. cit, pp. 456 e 457, desenvolve mais aprofundadamente este tema.

³⁵⁵ Na medida em que é concedido ao legislador do EM o poder de legislar sobre algumas matérias vertidas no Regulamento, Portugal fê-lo na Lei n.º 58/2019, de 8 de agosto, no capítulo III. Nele encontram-se as disposições relativas à figura do encarregado de proteção de dados, nos arts. 9.º a 13.º.

³⁵⁶ Assim nos transmite Leitão, L. M. T. M. (2019). *In Direito do trabalho (...)*, op. cit., p. 166.

³⁵⁷ O GT do art. 29.º entende que os trabalhadores devem ser informados sobre qualquer monitorização que exista, sobre as finalidades, para garantia de um tratamento justo, porque com as novas tecnologias, a transparência é deveras importante considerando a rapidez com que a informação circula e pode ser acedida.

1.3 Tratamento dados pessoais: contexto laboral

O capítulo X do RGPD atribui no art. 88.º, aos EM a possibilidade de definirem, nos seus ordenamentos jurídicos, em convenções coletivas e/ou em normas mais específicas a garantia de defesa dos direitos e liberdades quanto ao tratamento de dados pessoais dos trabalhadores no contexto laboral e para efeitos diversos³⁵⁸ devendo ser aplicadas medidas adequadas e específicas com vista a salvaguardar a dignidade e os direitos fundamentais do titular dos dados. Todas estas medidas devem tomar especial atenção quanto à transparência do tratamento e transferência de dados num grupo empresarial.

De acordo com o n.º 1 do art. 2.º do RGPD, o regulamento aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, “bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados”. De igual modo, o n.º 1 do art. 2.º da Lei n.º 58/2019, de 8 de agosto, determina a aplicabilidade “aos tratamentos de dados pessoais realizados no território nacional, independentemente, da natureza pública ou privada do responsável pelo tratamento (...)”.

Do supra exposto se conclui que deve aplicar-se o RGPD quando o empregador crie ou mantenha bases de dados organizadas relativas aos dados dos seus trabalhadores, independentemente da natureza dos mesmos³⁵⁹. Portanto, com a criação de bases de dados estamos perante um tratamento automatizado, pelo que no âmbito de aplicação do RGPD pressupõem-se também os ficheiros³⁶⁰ de dados pessoais³⁶¹. Neste sentido, é importante

³⁵⁸ Cfr. n.º 1 do art. 88.º da RGPD: “(...) 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”.

³⁵⁹ Vide Leitão, L. M. T. M. (2019). *In Direito do trabalho (...)*, op. cit., pp. 164 e 165.

³⁶⁰ Nos termos do n.º 6 do art. 4.º do RGPD: qualquer conjunto estruturado de dados pessoais, acessível segundo critérios específicos, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico.

³⁶¹ De acordo com Pinheiro, A. S. (Coord.) (2018). *In Comentário ao Regulamento (...)*, op. cit, pp. 101 e 102.

que a empresa informe os trabalhadores sobre os dados tratados e quais as finalidades para as quais estes foram recolhidos.

Por conseguinte, os requisitos relacionados com a transparência e informação vertidos nos arts 12.º e 13.º do RGPD aplicam-se ao tratamento de dados no local de trabalho. Deste modo, os trabalhadores devem ser informados sobre a existência de um qualquer tipo de monitorização³⁶², das finalidades bem como outras informações pertinentes para garantia de um tratamento justo.

Nos termos do art. 22.º do RGPD existe o reconhecimento que o titular dos dados tem o direito “de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar”.

Com o Regulamento foram incluídos e reforçados requisitos, introduzindo novas obrigações aos responsáveis pelo tratamento, incluindo-se neste âmbito os empregadores³⁶³.

1.3.1 Privacy by Design and by default

Considerando a facilidade com que podem ser captados, armazenados e transmitidos todos os tipos de dados, é importante a adoção de medidas que garantam a segurança dos mesmos³⁶⁴, sendo necessário que o responsável pelo tratamento aplique as medidas técnicas e organizativas adequadas garantindo e comprovando um tratamento lícito³⁶⁵. Porém, a adoção das técnicas mais avançadas, que melhor desempenhem este papel comportam custos, avultados em muitos casos. Assim, e tomando em consideração o disposto no art. 25.º do RGPD³⁶⁶ deve o responsável pelo tratamento aplicar “a proteção

³⁶² Correio eletrónico, geolocalização, videovigilância, *inter alia*.

³⁶³ Veja-se o trabalho desenvolvido pelo GT do art. 29.º, *Opinion 2/2017 on data processing at work - wp249*, consultado em: 06.10.2019, disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169.

³⁶⁴ Vide Moreira, T. A. C. (2010). *In A privacidade dos trabalhadores e o controlo (...)*, op. cit., p. 23.

³⁶⁵ Assim estatui o n.º 1 do art. 24.º do RGPD.

³⁶⁶ Cfr. n.º 1 do art. 25.º do RGPD: “Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares (...)”.

de dados desde a conceção e por defeito”^{367,368}. No contexto laboral, quando uma empresa entrega um computador, um telemóvel ou uma viatura, deve também desenvolver mais esforços para garantir a privacidade, sendo o menos invasivo possível e verificando a menor quantidade de informação [princípio da minimização dos dados].

De acordo com ANN CAVOUKIAN³⁶⁹, a *privacy by design* deve ser proactiva e não reativa, preventiva e não remediadora. Ou seja, devem criar-se condições de proteção, antecipando e prevendo o respeito pela privacidade antes de ocorrer uma violação para depois não ser necessária a aplicação de medidas reativas a essa violação. A *privacy by design* não deve esperar que aconteça a violação, o seu objetivo é evitar o risco de ocorrência de uma violação, pelo que deve abarcar medidas protetoras, preventivas da privacidade.

Quando a empresa [enquanto responsável pelo tratamento] toma uma decisão “sobre as medidas técnicas e organizativas, *a priori*, aquando da conceção” está a materializar a *Privacy by Design*, enquanto princípio da proteção de dados, consagrado no n.º 1 do art. 25.º do RGPD³⁷⁰.

No n.º 2 do referido artigo, encontramos postulado o princípio da *Data Protection by Default* (por defeito), este determina que a recolha e o tratamento devem restringir-se ao mínimo necessário para as finalidades do tratamento pretendido, pelo que não deve ser violado o princípio da proibição de excesso. Ou seja, quando exceda o necessário e adequado há violação, logo é proibida tal ação³⁷¹.

³⁶⁷ De acordo com WP 249, *Opinion 2/2017 on data processing at work* - wp249, consultado em: 06.10.2019, disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169, p. 10.

³⁶⁸ Ou seja, desde que decida ou que verifique que vai necessitar efetuar um tratamento de dados e antes de iniciar (desde a conceção), bem como sempre que o realizar (por defeito).

³⁶⁹ Cavoukian, A (2011). *In Privacy by Design The 7 Foundational Principles*, consultado em 07.02.2020, disponível em: <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>.

³⁷⁰ Vide Pinheiro, A. S. (Coord.) (2018). *In Comentário ao Regulamento (...)*, op. cit, p. 401.

³⁷¹ Cfr. Pinheiro, A. S. (Coord.) (2018). *In Comentário ao Regulamento (...)*, op. cit, pp. 405 e 406.

1.4 Profiling

As novas tecnologias, criadas e usadas pelo homem, permitem a captura de informações que fica armazenada *online*, e que pode ser qualificada como uma *digital library* acessível a consulta pelos mais diversos utilizadores da *internet*.

O que é *Profiling*?

Desde a implementação da Diretiva 95/46/CE, que ocorreram transformações significativas no mundo digital. Tais transformações possibilitaram aos responsáveis pelo tratamento de dados pessoais aglutinar dados pessoais dos utilizadores das tecnologias de informação. Deste modo, e porque a informação fica na rede virtual é facilitada a criação de “perfis comportamentais”³⁷².

Destarte, uma tradução aceitável para *profiling* é: definição de perfis.

1.4.1 Definição de perfis: noção

Nos termos do n.º 4 do art. 4.º do RGPD, *profiling* ou definição de perfis é “qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente, para analisar ou prever aspetos relacionados com o seu desempenho profissional, (...), preferências pessoais, interesses, (...), comportamentos, localizações ou deslocações”³⁷³.

A definição de perfis deve obedecer a determinados princípios da proteção de dados. Assim, os responsáveis pelo tratamento [empregador] deve ter em conta, que este tratamento deve ser lícito, leal e transparente; limitado às finalidades adequadas e necessárias; limitado ao mínimo; exato e atento ao prazo de conservação dos dados.

A noção de *profiling* assenta em dois elementos essenciais: a existência de tratamento automatizado de dados e o seu uso servir para avaliar aspetos pessoais, assim se entende não existir definição de perfis se não existir um tratamento de dados automatizado³⁷⁴.

³⁷² Fazendeiro, A. (2018). *In Regulamento Geral sobre a Proteção de Dados Algumas notas sobre o RGPD*, 3.ª Edição. s.l. Edições Almedina, p. 52.

³⁷³ Vide Fazendeiro, A. (2018). *In Regulamento Geral sobre a Proteção (...)*, op. cit., p. 52.

³⁷⁴ Cfr. Fazendeiro, A. (2018). *In Regulamento Geral sobre a Proteção (...)*, op. cit., p. 52.

Ao utilizarmos os meios sociais, deixamos uma pegada digital. As empresas, “através da existência de perfis nos meios sociais”³⁷⁵ conseguem, se assim o desejarem, obter a capacidade técnica de verificação dos mesmos, e deste modo, acabam por obter dados dos seus empregados, pois têm meios para recolher informação sobre aspetos pessoais, comportamentais culminado numa “captação de dados (...) relativos à vida privada e familiar dos empregados”^{376,377}.

De acordo com o Parecer 2/2017 do GT do artigo 29.º, uma verificação do histórico laboral de um empregado, através dos perfis existentes nas redes sociais³⁷⁸ deve ser concreta com os fins a que se destina. Com o intuito de garantia de um tratamento equitativo e transparente no *profiling*, o considerando (71) refere que o responsável pelo tratamento deverá implementar medidas técnicas e organizativas que possam reduzir a ocorrência de erros que conduzam a potenciais riscos para os direitos dos titulares³⁷⁹. Desta forma, visa-se dirimir “efeitos discriminatórios”³⁸⁰ contra os empregados, seja pelas suas crenças ou pela orientação sexual, *inter alia*.

Ademais, o considerando (71) alerta, de igual modo, para o facto de só se poder avançar para uma definição de perfis automatizada em casos muito específicos, *v.g.*, quando se baseie em categorias especiais de dados pessoais. Por conseguinte, este tratamento “deverá ser acompanhado das garantias adequadas”³⁸¹, por exemplo, oposição ao tratamento, que deverá incluir informação específica³⁸². Atente-se que para respeitar o princípio da transparência, “o titular dos dados deverá também ser informado da definição de perfis e das consequências que daí advêm”³⁸³. Assim, quando informado³⁸⁴, o titular

³⁷⁵ Vide WP 249, *Opinion 2/2017 on data processing at work - wp249*, consultado em: 06.10.2019, disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169, p. 17.

³⁷⁶ *Idem*, p. 15.

³⁷⁷ Veja-se também WP251rev01 (redação de 2018). *Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679*, consultado em: 07.02.2020, disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053, p. 8.

³⁷⁸ *V.g. LinkedIn*.

³⁷⁹ Cfr. Pinheiro, A. S. (Coord.) (2018). *In Comentário ao Regulamento (...)*, op. cit, p. 56.

³⁸⁰ *Idem*, p. 56.

³⁸¹ Cfr. art. 21.º do RGPD.

³⁸² Nos termos do n.º 2 do art. 13.º do RGPD.

³⁸³ Cfr. Considerando (60) do RGPD.

³⁸⁴ Nos termos dos arts 13.º e 14.º do RGPD.

adquire a possibilidade de manifestar a sua vontade, e de obter uma explicação sobre a decisão tomada, bem como de a contestar³⁸⁵.

O WP249 chama a atenção para o facto de o empregado não ter a obrigação de usar um perfil, nas redes sociais, fornecido pelo empregador³⁸⁶ “mesmo quando tal seja especificamente previsto à luz das suas tarefas”³⁸⁷. Deste modo, deve o empregador dar opção ao empregado de escolha de um “perfil «não laboral», devendo tal opção ficar estabelecido no contrato para que não ocorram conflitos como o que sucedeu no caso *Barbulescu v Romania*³⁸⁸.

Relativamente à Lei n.º 58/2019, de 8 de agosto, nada se diz sobre a questão do *profiling*, pelo que, se existir um conflito que envolva a definição de perfis, o titular dos dados deve fazer uso da *legis* vertida no RGPD, recorrendo à CNPD, entidade administrativa com legitimidade, de acordo com o art. 26 do citado diploma³⁸⁹.

Notar que quando exista tratamento de dados potenciador de riscos para o titular dos dados, exige-se que o responsável pelo tratamento realize uma avaliação de impacto sobre a proteção de dados.

1.5 As Avaliações de Impacto sobre a Proteção de dados

De acordo com WP251, “uma AIPD³⁹⁰ pode revelar-se”³⁹¹ muito útil para os responsáveis, sempre que estes tenham dúvidas se através do *profiling*, subsistam ou não riscos para os titulares de dados.

³⁸⁵ Cfr. Pinheiro, A. S. (Coord.) (2018). *In Comentário ao Regulamento (...)*, op. cit, p. 56.

³⁸⁶ No entanto, é possível ao trabalhador recusar? Com fundamento em quê? Na proteção da sua privacidade?

³⁸⁷ De acordo com WP 249, *Opinion 2/2017 on data processing at work* - wp249, consultado em: 06.10.2019, disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169.

³⁸⁸ A desenvolver no capítulo IV.

³⁸⁹ Quando se verifique um caso de violação das normas vertidas no RGPD, no que concerne ao *profiling*, a Lei n.º 58/2019, de 8 de agosto, dispõe que se está perante uma contraordenação muito grave, cfr. als, h) e i) do n.º 1 do art. 37.º, punida com coima nos termos do n.º 2.

³⁹⁰ Avaliação de impacto sobre a proteção de dados.

³⁹¹ WP251rev01 (redação de 2018). *Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679*, consultado em: 07.02.2020, disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

Entretanto, e antes de mais importa definir AIPD. Segundo ANA FAZENDEIRO³⁹², “uma avaliação de impacto consiste” numa apreciação realizada pelo responsável com vista à identificação e minimização de riscos pelo “incumprimento das regras de proteção de dados”³⁹³. Para ALEXANDRE PINHEIRO, é aplicada uma AIPD quando o tratamento envolva a utilização de novas tecnologias e possa produzir riscos nos direitos e liberdades das pessoas singulares³⁹⁴.

O RGPD determina, no art. 35.^o³⁹⁵, a obrigatoriedade de elaborar uma AIPD quando esteja presente, designadamente, o tratamento automatizado de dados, onde se inclui: a) o *profiling*, que conduza à tomada de decisões com interferência nos titulares de dados³⁹⁶; b) operações de tratamento em larga escala “que visem o tratamento de uma grande quantidade de dados pessoais a nível regional ou nacional (...)”, v.g., uma empresa que labore em todo o território nacional e mantenha relações internacionais; c) o tratamento de dados biométricos e também o “controlo de zonas acessíveis ao público em grande escala³⁹⁷, nomeadamente se forem utilizados mecanismos optoelectrónicos”^{398,399}.

As avaliações de impacto devem, pelo menos, incluir: i) uma descrição das operações de tratamento, sistematizada, e das finalidades do tratamento; ii) uma avaliação da necessidade e proporcionalidade das operações relativamente aos objetivos; iii) uma avaliação dos riscos para os direitos e liberdades dos titulares; iv) medidas que dirimam os riscos, onde se devem incluir garantias, medidas de segurança, *inter alia*, com vista a assegurar a proteção de dados pessoais e o cumprimento do RGPD⁴⁰⁰.

Uma AIPD, de acordo com ALEXANDRE PINHEIRO, realiza-se em três fases. Numa primeira é realizada uma descrição sistemática das operações, das finalidades e dos

³⁹² Cfr. Fazendeiro, A. (2018). *In Regulamento Geral sobre a Proteção (...)*, op. cit., p. 26.

³⁹³ *Idem*, p. 26.

³⁹⁴ Vide Pinheiro, A. S. (Coord.) (2018). *In Comentário ao Regulamento (...)*, op. cit, p. 459.

³⁹⁵ Epígrafe de Avaliação de Impacto sobre a Proteção de Dados.

³⁹⁶ V. g. na relação laboral, ao analisar-se o perfil social de um trabalhador, pode o empregador decidir não contratar ou cessar o contrato de trabalho, caso considere que este tem, por exemplo, comportamentos inadequados.

³⁹⁷ Ex: Estações ferroviárias.

³⁹⁸ Câmaras de vigilância ou sensores de movimento.

³⁹⁹ De acordo com Pinheiro, A. S. (Coord.) (2018). *In Comentário ao Regulamento (...)*, op. cit, p. 460.

⁴⁰⁰ Veja-se Fazendeiro, A. (2018). *In Regulamento Geral sobre a Proteção (...)*, op. cit., pp. 26 e 27; Pinheiro, A. S. (Coord.) (2018). *In Comentário ao Regulamento (...)*, op. cit, p. 461.

interesses do responsável, fase descritiva; num segundo momento, na fase avaliativa, é efetuada uma avaliação que vai relacionar as operações, os objetivos e os riscos; por fim a decisão [fase decisória], nesta, e considerando a existência de riscos, são adotadas garantias e medidas de segurança para proteger os dados pessoais.

As AIPD, enquanto instrumento de responsabilidade, conferem ao responsável a capacidade de aferir os riscos que possam existir para os titulares dos dados. Através destas avaliações, os responsáveis conseguem evidenciar a instituição de medidas adequadas para cessar os riscos e o cumprimento do RGPD, podendo: incluir-se nestas medidas a informação ao titular da existência de *profiling*, servir para explicar a importância e consequências do tratamento de dados concedendo o poder ao titular, *v.g.*, de opor-se à decisão.

Em relação às AIPD, uma última nota, para referir que a avaliação de impacto se trata de uma avaliação “*ex ante*”⁴⁰¹. Sempre que se verifique, na avaliação, que o tratamento apresenta um elevado risco que não possa ser atenuado, a autoridade nacional de controlo deve ser consultada antes da realização do tratamento de dados pessoais.

Atente-se que o considerando (96) alerta para o facto de quando perante trabalhos de elaboração de medidas legislativas que envolvam o tratamento de dados pessoais, deve ser consultada a autoridade de controlo⁴⁰². Constatámos que a Lei n.º 58/2019, de 8 de agosto, executadora do RGPD em Portugal, não diz muito sobre a AIPD, apenas dispõe no sentido da necessidade de ser efetuada uma consulta à lista difundida pela CNPD, com os tipos de tratamentos cuja avaliação prévia de impacto não é obrigatória, não ficando, no entanto, os responsáveis impedidos de realizar uma avaliação prévia por iniciativa própria⁴⁰³.

Ponderado o exposto, entendemos que deveria ter sido dado mais enfoque a esta temática, porque no âmbito das relações laborais, o *profiling* e a AIPD, merecem uma especial atenção pelo responsável pelo tratamento. Não obstante a falta de uma

⁴⁰¹ Vide Pinheiro, A. S. (Coord.) (2018). *In Comentário ao Regulamento (...)*, op. cit, p. 459.

⁴⁰² Em Portugal, tal ocorreu aquando dos trabalhos para elaboração da Lei n.º 58/2019, publicada em 08 de agosto. Assembleia da República (Proposta de Lei n.º 120/XIII), consultado em 04.11.2019, disponível em: <https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalleIniciativa.aspx?BID=42368>.

⁴⁰³ Cfr. art. 7.º da Lei n.º 58/2019, de 8 de agosto e art. 35.º do RGPD.

expressividade legislativa mais vinculada, existem empresas que se encontram a modificar as suas normas internas.

À laia de conclusão queremos notar que as novas tecnologias podem sim colocar em perigo a privacidade e a proteção dos titulares de dados, quando o empregador exerce, sem necessidade, adequação e proporcionalidade controlo dos meios que colocam à disposição do trabalhador, pelo que é importante um uso adequado, consciente pelo trabalhador e proibido um controlo “arbitrário e injustificado”⁴⁰⁴ pelo empregador. Destarte, o respeito de ambas as partes entre si, é fundamental para que as tecnologias não servissem de fundamento à violação da privacidade.

O RGPD não veio mudar drasticamente o estabelecido na Diretiva 95/46/CE, veio sim introduzir algumas alterações, necessárias para adequar a proteção de dados à nova realidade tecnológica. Outrossim, e porque é de aplicação direta, sem necessidade de transposição, produzir a “harmonização das regras aplicáveis”⁴⁰⁵ entre os vários EM da UE.

Por fim, referir que o tratamento de dados deixou de estar sujeito a notificação a autoridade de controlo (CNPD) com a publicação da Lei n.º 58/2019, de 08 de agosto, excetuando-se os casos expressamente previstos no RGPD e na própria Lei – n.º 2 do art. 62.º.

⁴⁰⁴ Moreira, T. A. C. (2010). *In A privacidade dos trabalhadores e o controlo (...)*, op. cit., p. 62.

⁴⁰⁵ Mota, J. (2018). *In O consentimento no Regulamento Geral sobre a Proteção de Dados*, InforBanca, n.º 112, Fevereiro, consultado em: 25.01.2020, disponível em: <https://ifb.pt/wp-content/uploads/2018/04/IFB-InforBanca-112-Fev18.pdf>.

CAPÍTULO IV – As novas tecnologias informáticas e o trabalhador

1. O uso das novas tecnologias de informação: internet e correio eletrónico

A vida das empresas mudou nestas últimas décadas, consequência da explosão tecnológica. Os trabalhadores têm ao seu dispor, meios eletrónicos, disponibilizados pelos empregadores para a prestação da sua atividade profissional.

Conforme vem sendo defendido, a privacidade fica em risco, pois o trabalhador, por uma questão de praticidade, usa as ferramentas profissionais para fins pessoais. Importa notar que a “troca de emails”⁴⁰⁶, é vigiada pelo empregador. Mas, não é só a troca de emails que coloca em risco a privacidade do trabalhador, este deve também ter cuidado com os sites que consulta, pois eles deixam *a digital print*, permitindo ao empregador a criação de perfis.

De igual modo, a disponibilização, pelo empregador, de “plataformas de comunicação e interação”⁴⁰⁷ entre os trabalhadores, coloca em perigo a proteção da informação pessoal, lá colocada, relativamente ao tratamento efetuado, mormente se existe adequação quanto às finalidades.

1.1 Para fins privados do trabalhador

Todos estes facilitismos, concedidos pelas empresas, podem comportar um *periculu*. Neste sentido, é importante para os trabalhadores tenham consciência que existe controlo, pelo empregador, sobre a utilização dos meios eletrónicos. Concomitantemente, não devem os trabalhadores descuidar o dever de zelo quando utilizam as ferramentas informáticas para fins pessoais⁴⁰⁸.

Contudo, e de acordo com GARCIA MARQUES os trabalhadores utilizam o correio eletrónico porque “têm uma legítima expectativa de privacidade no local de

⁴⁰⁶ Vide Marques, G. e Martins, L. (2006). *In Direito da Informática (...)*, op. cit., p. 172.

⁴⁰⁷ Cfr. Pinheiro, A. S. (2015). *In Privacy e proteção de dados pessoais (...)*, op. cit., p. 812.

⁴⁰⁸ V.g.: cede o email profissional à escola que o filho frequente, para um contacto mais rápido.

trabalho”⁴⁰⁹, quando comunicam através dos dispositivos eletrônicos profissionais, aplicando-se o “princípio geral da confidencialidade da correspondência”⁴¹⁰.

a) Correio eletrônico: é uma ferramenta de eleição ao nível laboral, tendo-se tornado, “se não no principal, pelo menos num dos principais meios de comunicação nas empresas”⁴¹¹, pois ela tem mais vantagens, relativamente aos meios tradicionais porque permite a transmissão da informação em tempo real ao(s) destinatário(s)⁴¹². Deste modo, faz todo o sentido que seja uma aposta forte, das empresas modernas⁴¹³, para difusão de mensagens⁴¹⁴.

Por conseguinte, não nos parece aceitável que, no seio da relação laboral, seja proibido o uso do correio eletrónico para fins pessoais, isto é, “para fins que não sejam estritamente profissionais”⁴¹⁵. Quanto às empresas, é importante, enquanto entidades empregadoras, terem em consideração fatores como: a salvaguarda da liberdade de expressão, a livre iniciativa do trabalhador, os custos, a privacidade e a utilização deste meio comunicacional, aquando da definição de regras empresariais⁴¹⁶. Deste modo pode conseguir-se a promoção de algum equilíbrio entre os trabalhadores, o empregador e o uso do correio eletrónico, ou seja, entre os denominados “interesses e direitos conflituantes”⁴¹⁷.

Consideramos, bem como alguma doutrina⁴¹⁸, que a melhor forma de promoção de equilíbrio, ocorra através da definição de regras concretas e concisas sobre o uso da internet e do correio eletrónico para fins privados. Estas regras deverão ficar definidas em regulamentos internos ou outro documento que consubstancie, expressamente, como

⁴⁰⁹ Assim preconiza Marques, G. e Martins, L. (2006). *In Direito da Informática (...)*, op. cit., p. 377.

⁴¹⁰ *Idem*, p. 377.

⁴¹¹ Cfr. Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., p. 43, que considera esta ferramenta revolucionária, rápida, de baixo custo e por isso a escolha favorita das empresas para o desempenho da atividade profissional. Ademais, segura pois está protegida pelo direito fundamental vertido no art. 34.º da CRP, relativo ao sigilo da correspondência.

⁴¹² *Idem*, p. 365.

⁴¹³ *Ibidem*, p. 365.

⁴¹⁴ V.g.: muita da comunicação efetuada com Agentes de Execução processa-se através desta ferramenta.

⁴¹⁵ Assim, propugna Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., p. 366.

⁴¹⁶ *Idem*, p. 366.

⁴¹⁷ Gomes, J. M. V. (2007). *In Direito do Trabalho, (...)*, op. cit., p. 368.

⁴¹⁸ Veja-se Gomes, J. M. V. (2007). *In Direito do Trabalho, (...)*, op. cit., p. 377 e Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., pp. 366 e 367.

pode ser efetuada a utilização dos meios comunicacionais empresariais, cumprindo assim o disposto na lei laboral⁴¹⁹.

Os problemas podem surgir quando é feita a monitorização pelo empregador, e são consultadas as mensagens. Atente-se que o controlo não pode ser realizado sem considerar alguns dos princípios da proteção de dados que vêm consolidar a garantia da privacidade do trabalhador e da confidencialidade das mensagens transmitidas através do correio eletrónico. Por conseguinte, devem ser atendidos os princípios da necessidade, da proporcionalidade e da transparência⁴²⁰.

Uma medida importante, por exemplo, é colocar a informação, no assunto do email, v.g.: privado ou pessoal, assim, e aquando de uma monitorização, o empregador deve evitar aceder ao conteúdo de uma mensagem deste tipo.

1.1.1 O poder de controlo do empregador: problemas e limites

Considerando o facto de a relação laboral se basear numa relação de poder, na qual o trabalhador surge na posição de “sujeito juridicamente subordinado”⁴²¹ ao dever de obediência e instruções do empregador, é importante notar que o empregador pode também exercer o poder disciplinar quando o trabalhador incumpe com as regras definidas pelo empregador.

Pese embora, a relação de sujeição inerente à relação laboral, ainda assim o empregador não pode exercer o seu poder para controlar, a todo o tempo e por qualquer meio o trabalhador, pois o “contrato de trabalho pressupõe o reconhecimento da dignidade do trabalhador”⁴²². Compreende-se que a empresa, tenha a faculdade de vigiar e controlar, na fase de execução do contrato de trabalho, a prestação realizada pelo trabalhador⁴²³, pois esta competência está dentro do âmbito do poder diretivo atribuído ao empregador^{424, 425}. Todavia, não deve a empresa olvidar o respeito pelo direito à

⁴¹⁹ Cfr. n.º 2 do art. 22.º do CT.

⁴²⁰ Vide Marques, G. e Martins, L. (2006). *In Direito da Informática (...)*, op. cit., p. 378.

⁴²¹ Cfr. Amado, J. L. (2019). *In Contrato de trabalho (...)*, op. cit., p. 203.

⁴²² Veja-se Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., p. 329.

⁴²³ *Idem*, p. 368.

⁴²⁴ Nos termos do art. 97.º e 98.º do CT.

⁴²⁵ Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., p. 369.

privacidade do trabalhador, devendo a intromissão ser o menos invasiva possível observando o princípio da proibição de excesso⁴²⁶.

Quando a entidade empregadora atribui ao trabalhador um *email*, pode estar a criar um problema, tanto para ela como para o trabalhador caso não defina regras ou institua procedimentos concretos. Pelos regulamentos internos, vai definir claramente as fronteiras que delimitam o seu uso, estabelecendo como e quando pode o trabalhador usá-la e quando e o que pode ser monitorizado⁴²⁷ ou acedido, servindo esta medida como preventiva de maus usos ou abusos de ambas as partes, podendo minimizar os conflitos.

Importa também notar, que não é pelo facto de a empresa disponibilizar instrumentos eletrónicos aos seus trabalhadores que lhe assiste o direito de controlar o uso dessas ferramentas, é importante que a empresa tenha regras claras que definam a política de utilização, que os trabalhadores as conheçam para que possam prevenir-se.

Uma outra situação a salientar – existência de regra que proíba o uso para fins pessoais⁴²⁸. O facto de existir tal regra proibitiva, que antes de tudo, consideramos contraproducente, esta não dá o poder ao empregador para aceder, indiscriminadamente ao conteúdo das mensagens trocadas, o direito à privacidade mantém-se. A empresa pode monitorizar o **para quem e o quando**, mas respeitando sempre o princípio da proporcionalidade *lato sensu*⁴²⁹ e em estrita observância dos princípios da proteção de dados pessoais (arts. 5.º, 12.º, 13.º, *inter alia*, do RGPD e arts. 20.º e 21.º do CT)⁴³⁰.

⁴²⁶ *Idem*, p. 377.

⁴²⁷ Pelo que Guerra, A. (2004). *In A privacidade no local de trabalho: as novas tecnologias (...)*, op. cit., p. 370, considera que a atribuição de um *email* ao trabalhador tem as suas implicações, nomeadamente pelo facto do “empregador, por consulta ao servidor central, pode ver ou ter acesso ao conteúdo das informações trocadas entre os trabalhadores e os seus representantes”.

⁴²⁸ Considera Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., p. 624, uma regra “pouco prática, irrealista e contraproducente”.

⁴²⁹ Vide Guerra, A. (2004). *In A privacidade no local de trabalho: as novas tecnologias (...)*, op. cit., pp. 374 a 378.

⁴³⁰ Também a CNPD emitiu orientações acerca dos princípios que devem ser observados em matéria de proteção no âmbito laboral. Vide CNPD. (2002). Princípios sobre a privacidade no local de trabalho, consultado em 15.03.2020, disponível em <https://www.cnpd.pt/home/orientacoes/PRINCIPIOS-controloE-mails-telefones-Internet.pdf> e CNPD. (2013). Deliberação n.º 1638/2013. Orientações sobre tratamento dados pessoais decorrentes do controlo da utilização para fins privados das tecnologias de informação e comunicação em contexto laboral. consultado em 15.03.2020, disponível em: https://www.cnpd.pt/home/orientacoes/Delib_controlo_comunic.pdf.

Os problemas com a criação e atribuição de endereços eletrónicos ou de aplicativos em redes sociais, surgem com o controlo que a empresa tem de fazer, mas não só, pois também o facto de poder fazer uso destes, mas fora do local de trabalho, comporta problemas, mormente: direito à privacidade e o direito à desconexão⁴³¹. Esta tecnologias tornaram o controlo mais “presente e incisivo”⁴³² com a consequente afetação da privacidade do trabalhador, que se crê ser um dos limites^{433,434} a este controlo. Outro limite centra-se no respeito pela confidencialidade das mensagens recebidas, transmitidas pelo trabalhador.

Os motivos que justificam a monitorização e acesso, são outro dos problemas. Na maioria das vezes são invocadas razões de segurança, relacionadas com vírus ou mensagens *spam*⁴³⁵. Porém, o empregador em vez de aceder pode primeiro questionar o trabalhador para denunciar tais mensagens, retendo-as numa caixa de correio e reportando essa situação ao departamento informático da empresa. Postulamos que esta é uma política a implementar nas empresas.

Todos estes cenários colocam os direitos dos trabalhadores numa posição periclitante, porque o empregador tem o grande poder de controlar os seus subordinados, aumentando através da informática a capacidade de acesso e recolha de informação dos trabalhadores⁴³⁶.

⁴³¹ Para maior desenvolvimento veja-se Moreira, T. A. C. (2016). *In O direito à desconexão dos trabalhadores*. Questões Laborais, n.º 49, pp. 7-28.

⁴³² Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., p. 613.

⁴³³ Posição sustentada por Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., p. 329: “o direito à privacidade penetra (...) na relação de trabalho, erigindo-se como um importante limite aos poderes do empregador”.

⁴³⁴ De acordo com Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., p. 410, os limites ao poder de controlo centram-se, também, no contrato de trabalho. Deste modo, fora do contexto laboral, não pode haver um controlo que incida sobre a conduta do trabalhador.

⁴³⁵ Tipo de mensagem de correio eletrónico, geralmente com intuito publicitário ou fraudulento, enviada para grande número de destinatários que não forneceram o seu endereço para esse fim. “spam”, in Dicionário Priberam da Língua Portuguesa [em linha], 2008-2020, <https://dicionario.priberam.org/spam> [consultado em 07-04-2020].

⁴³⁶ Cfr. Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., p. 616.

Em suma, e citando TERESA MOREIRA, “os direitos à privacidade e à dignidade dos trabalhadores nunca podem ceder perante argumentos de maior produtividade ou eficácia” que visem legitimar um controlo desacerbado pelo empregador⁴³⁷.

1.1.2 Caso paradigmático: Acórdão TEDH Barbulescu v Romania

Ao longo do presente estudo, temos defendido que o direito à privacidade e o direito à confidencialidade das mensagens, são direitos que assistem o trabalhador, e que os referidos direitos são tutelados por garantias previstas na legislação internacional, constitucional e infraconstitucional. Pese embora, estas garantias, constata-se que ainda assim estes direitos sofrem constantes violações por parte dos empregadores⁴³⁸, sendo inclusive objeto de debate no Tribunal Europeu dos Direitos do Homem (TEDH).

De facto, não é pacífica a conciliação dos poderes dos empregadores com os direitos dos trabalhadores, *in casu*, dos direitos constitucionalmente previstos (reserva da vida privada e da confidencialidade da correspondência dos trabalhadores), pois os primeiros consideram deter na sua esfera, o direito a controlar os trabalhadores na prestação da atividade profissional. Este conflito de direitos, conseqüentemente fomenta o recurso aos tribunais para verificação e correção das possíveis violações.

Em 2016, Mr. Barbulescu, pelo facto de não concordar com as decisões, concernentes ao seu caso, proferidas pelos Tribunais Romenos, levou o seu processo ao TEDH na expectativa que este Tribunal Superior considerasse o despedimento ilícito.

Na primeira análise do caso, o TEDH⁴³⁹ decidiu a favor da entidade empregadora, considerando lícito o despedimento do trabalhador que, em contexto laboral, utilizou para

⁴³⁷ Veja-se Moreira, T. A. C. (2010). *In As novas tecnologias de informação e comunicação e o poder de controlo eletrónico do empregador. Scientia Iuridica*. Braga. Universidade do Minho, tomo 59, n.º 323, pp. 553-579.

⁴³⁸ A título ilustrativo invocam-se a seguinte jurisprudência - TRP: Processo n.º 101/13.5TTMTS.P1, de 08 de setembro de 2014, Processo n.º 208/14.1TTVFR-D.P1, de 15 de dezembro de 2016, Processo n.º 159/18.0T8PNF-A.P1, de 07 de dezembro de 2018; do TRL: Processo n.º 24163/09.0T2SNT.L1-4 de 07 de março de 2012 ou ainda do TRG: Processo n.º 15/11.3TTVRL.G1, de 11 de junho de 2015, disponíveis em <http://www.dgsi.pt/>.

⁴³⁹ *Application* n.º 61496/008 Barbulescu v Romania, de 12 de janeiro de 2016, consultado em: 15.10.2018, disponível em: <https://hudoc.echr.coe.int/eng#%7B%22fulltext%22:%5B%22barbulescu%22%5D,%22sort%22:%5B%22kupdate%20Des%22%5D%7D>

fins pessoais e no horário de trabalho um aplicativo informático criado pela entidade empregadora.

In casu, pelo período de um ano, aproximadamente o trabalhador desempenhou as funções de engenheiro numa empresa privada⁴⁴⁰, que lhe solicitou a criação de uma conta na *internet*, nomeadamente no *Yahoo Messenger*, para maior celeridade no contacto com os clientes. A 13 de julho de 2007, Mr. Barbulescu foi informado sobre a monitorização das suas comunicações. Porém, a monitorização ocorreu entre 05 e 13 desse mesmo mês, sem ter sido informado, previamente o trabalhador. Desta vigilância resultou o conhecimento, para o empregador, que a conta da *internet* tinha sido usada para fins pessoais⁴⁴¹.

A empresa, invocando a violação de regras internas que determinavam a proibição do “uso dos recursos ou meios da empresa para fins pessoais”⁴⁴², cessou o vínculo laboral com o trabalhador. Na nossa opinião, bem como na de ISA ANTÓNIO, a decisão proferida, em 2016, pelo TEDH, traduz-se num “retrocesso”⁴⁴³ da proteção dos direitos, não só do cidadão em geral, mas em especial do trabalhador. Por conseguinte, fez renascer a discussão associada ao Direito do Trabalho atual. Tal discussão assenta na necessidade de conciliação dos direitos fundamentais dos trabalhadores com a liberdade de iniciativa privada da organização da empresa, cuja necessária concordância prática tem implicado a aplicação de coordenadas constitucionais⁴⁴⁴ no que concerne aos fundamentos e limites.

[ending%22\].%22documentcollectionid%22:\[%22JUDGMENTS%22\].%22itemid%22:\[%22001-159906%22\]}.](#)

⁴⁴⁰ Sublinhado nosso.

⁴⁴¹ Note-se que a informação, ao trabalhador, sobre a monitorização, foi realizada *a posteriori*, violando-se, desde logo, o direito do trabalhador a ser informado.

⁴⁴² Veja-se António, I. (2016). *In O Direito Fundamental do Trabalhador à confidencialidade das Comunicações Eletrónicas no Contexto Laboral e o Despedimento Com Justa Causa (?)*. *In Transformações recentes do Direito do Trabalho Ibérico, Livro Razão*, CIJE – Centro de Investigação Jurídico Económica, Faculdade de Direito do Porto. Consultado em: 23.11.2019, disponível em: https://sigarra.up.pt/fdup/pt/web_gessi_docs.download_file?p_name=F1854330697/Livro_Razao.pdf, p. 11.

⁴⁴³ Cfr. António, I. (2016). *In O Direito Fundamental do Trabalhador à confidencialidade (...)*, op. cit., p. 11.

⁴⁴⁴ Vide Martins, J. Z. (2016). *In Comentário ao acórdão do Tribunal Europeu dos Direitos do Homem, Barbulescu contra a Roménia, de janeiro de 2016, proc. 61496/08*. *Revista do Ministério Público* 145: Janeiro - Março 2016 [pp. 177-205], consultado em: 10.03.2019, disponível em: http://rmp.smmmp.pt/wp-content/uploads/2016/04/7.RMP_145_Joao_Zenha_Martins.pdf, p. 179.

Consideramos que esta decisão, do TEDH, suscita um conjunto de várias questões relacionadas com as “relações de trabalho”⁴⁴⁵, nomeadamente: **a)** os regulamentos internos que definam regras de utilização dos instrumentos eletrónicos da empresa, são uma mais valia? **b)** devem os trabalhadores tomar conhecimento dos mesmos, por que via⁴⁴⁶? **c)** existindo consentimento e presença *in loco* do trabalhador ao acesso, será igualmente lícito, se envolver terceiros?

A posição adotada pelo TEDH, na decisão de janeiro de 2016, é de tal forma estranha que despoletou um interesse na comunidade jurídica com várias análises sobre a mesma.

É importante reter a ideia sobre a existência de direitos para ambas as partes [empregador/trabalhador]. Ao primeiro assiste o direito de exigir o cumprimento de obrigações pelo segundo, que tem o direito à privacidade e à reserva das comunicações e correspondência que emita ou receba. Desta situação decorre que o desrespeito pela confidencialidade das comunicações, configura a prática de um crime de violação de correspondência⁴⁴⁷.

Segundo ISA ANTÓNIO, o acórdão do TEDH “viola, claramente os direitos do trabalhador à privacidade da correspondência e das telecomunicações”⁴⁴⁸, pois o empregador acedeu ao conteúdo das mensagens sem informar o trabalhador e sem a devida autorização pelas entidades competentes. Importa clarificar que o empregador pode exigir que o trabalhador exerça as suas funções, mas não o pode controlar, indiscriminadamente, pelo que não podem ser admissíveis meios ilícitos, abusivos,

⁴⁴⁵Nas palavras de Martins, J. Z. (2016). *In Comentário ao acórdão do TEDH (...)*, op. cit., p. 180.

⁴⁴⁶ Será o envio de um email suficiente para a tomada de conhecimento, no qual inclui uma declaração de informação, com, v.g. o seguinte texto: Desta forma, enviamos a presente Declaração de Informação, que descreve o modo como são recolhidos, tratados e protegidos os dados pessoais de todos os colaboradores e colaboradoras das empresas do Grupo XPTO, no estrito respeito e cumprimento do RGPD e da Lei n.º 58/2019.? Depreende-se que basta a leitura do referido email, para que se opere a tomada de conhecimento pelo trabalhador.

⁴⁴⁷ Cfr. art. 194.º do CP.

⁴⁴⁸ Cfr. António, I. (2016). *In O Direito Fundamental do Trabalhador à confidencialidade (...)*, op. cit., p. 14.

inconstitucionais como mecanismos de controlo do desempenho das atividades laborais⁴⁴⁹.

A decisão do TEDH não foi unânime, teve um voto contra. De acordo com PINTO de ALBUQUERQUE, outros fatores deveriam ter sido analisados, nomeadamente: **a)** a não existência de um regulamento interno que definisse a utilização dos aparelhos eletrónicos; **b)** o acesso às mensagens enviadas/recebidas pelo trabalhador, sem a sua autorização e sem a sua presença; **c)** a forma como as comunicações foram utilizadas e divulgadas durante o processo que culminou no despedimento.

Considerando-se a *internet* como uma ferramenta importante para a democracia e para a liberdade de expressão enquanto direito fundamental, PINTO de ALBUQUERQUE defende que os estados têm a obrigação de manter um justo equilíbrio entre o direito a “expressar-se com a liberdade e o respeito pela privacidade devendo evitar-se a colisão entre direitos internacionalmente consagrados”⁴⁵⁰ ou a colisão entre estes direitos e os direitos e liberdades dos outros⁴⁵¹.

Na opinião de PINTO de ALBUQUERQUE uma proibição total do acesso à *internet* pelos empregados, para fins pessoais, é inadmissível, porque nos dias de hoje é difícil separar as duas realidades [profissional e pessoal]. Em vez de proibir, é importante que os trabalhadores tenham conhecimento sobre as regras que definem o uso das tecnologias de informação.

No nosso entendimento, estas regras devem definir políticas de uso, não só no local de trabalho, mas também fora dele, pois é muito fácil levar o trabalho connosco para casa. A existência de um regulamento, disponibilizado aos trabalhadores fá-los tomar consciência do que podem e não podem fazer, e assim deverão fazer um uso mais criterioso das ferramentas informáticas que o empregador lhe disponibiliza. Defendemos ainda que é imperiosa a comunicação, expressa a todos os trabalhadores, sobre a

⁴⁴⁹ Para António, I. (2016). *In O Direito Fundamental do Trabalhador à confidencialidade (...)*, op. cit., p. 19.

⁴⁵⁰ Cfr. art. 10.º da CEDH e art. 8.º da CEDH.

⁴⁵¹ Para o juiz do TEDH, existe, a nível internacional um défice de normas que regulem o uso da internet e que garantam a proteção em contexto laboral.

existência dos regulamentos, bem como a tomada de conhecimento, igualmente expresso sobre os mesmos.

Quanto à monitorização, também a sua existência deve ser comunicada aos trabalhadores, antes da sua implementação e realização. O empregador tem de informar sobre os fins da monitorização, âmbito de aplicação, meios técnicos e duração da mesma. Para o juiz do TEDH e doutrinador, bem como para nós, ela deve ser o menos invasiva possível. Por conseguinte, o empregador deve ter em atenção o tipo de acesso que realiza e os dados recolhidos [através da monitorização, ou seja, pelo acesso às mensagens] devendo ser adequados aos fins, inicialmente definidos. Por conseguinte, qualquer alteração deve ser protegida de acesso não autorizados, bem como de um uso indevido⁴⁵².

A primeira decisão do TEDH, pela sua peculiaridade, teve efeitos na doutrina, veja-se agora a posição sustentada por ZENHA MARTINS. Para o autor, o TEDH quando aplica a CEDH visa a proteção dos Direitos do Homem e apenas quando sejam violados direitos que estejam enquadrados no âmbito da responsabilidade do EM que adota a CEDH. No entendimento de ZENHA MARTINS, a análise do TEDH deveria incidir sobre a verificação ou não da violação dos direitos previstos na CEDH e não analisar se a decisão da entidade empregadora de cessar o vínculo contratual com o trabalhador tinha fundamento.

Todavia, não podem ser ignorados os conflitos que surgem entre o direito à reserva da intimidade da vida privada e os direitos da entidade empregadora, ao que após ponderação do TEDH concluiu este pela não existência de violação do art. 8.º da CEDH. De acordo com a análise crítica de ZENHA MARTINS, a decisão no sentido da não existência de violação do art. 8.º da CEDH, pelo empregador, talvez tenha ocorrido, para estranheza do autor e também nossa, porque o tribunal não considerou relevante aferir se

⁴⁵² De acordo com Pinto de Albuquerque. *In Application* n.º. 61496/008 Barbulescu v Romania, de 12 de janeiro de 2016 [tradução nossa]: os tribunais Romenos não consideraram todos os meios de garantia da proteção da confidencialidade das mensagens do trabalhador, e nem este Tribunal (TEDH) providenciou a necessária sanção da violação, tendo sido esse o facto que levou a dissentir na decisão. O juiz Pinto de Albuquerque sugere ainda a criação de um regulamento específico sobre a utilização de aplicativos informáticos, em contexto laboral. Tal regulamento deve esclarecer, *inter alia*, a forma como é realizada a monitorização ou quais as garantias de segurança para os trabalhadores (como são usados, consultados e destruídos os dados acedidos).

a monitorização tinha sido, comunicada, *ex ante*, ao trabalhador quando esta preocupação tinha já sido considerada noutras decisões, privilegiando o direito à reserva da intimidade da vida privada⁴⁵³, bem como da correspondência. No ordenamento jurídico nacional, os trabalhadores preservam o direito à reserva da intimidade da vida privada por força do art. 16.º do CT e o direito à confidencialidade das mensagens e de acesso à informação, *ex vi* do disposto no art. 22.º do CT.

A previsão de monitorização, em regulamentos internos, deve ficar definida como aleatória e nunca focalizada num só trabalhador, na medida em que quando assim suceda, existe um incumprimento do princípio da igualdade⁴⁵⁴. Outrossim, se verifica o desrespeito pelo princípio da proibição de excesso⁴⁵⁵. Ora, se a conduta do trabalhador não indiciava a existência de ilícitos, a monitorização realizada não foi necessária, adequada e exigível. Concomitantemente, não observou, o TEDH, o disposto no RGPD, que em síntese defende um controlo: **a)** transparente; **b)** necessário; **c)** equilibrado e **d)** proporcional.

Relava notar que a “via analítica seguida pelo TEDH”⁴⁵⁶, acaba por não valorizar todas as garantias que tem sido realizadas na interpretação dos preceitos da CEDH, podendo abrir caminhos, a interpretações, que vão imunizar os comportamentos das empresas e vão diminuir os laços de confiança entre as partes envolvidas na relação laboral, parecendo legitimar, por outro lado “a adoção de políticas empresariais de controlo da atividade profissional por parte dos empregadores no sentido que melhor lhes aprouver, desresponsabilizando-os quanto à assunção de regras transparentes e proporcionais”⁴⁵⁷.

O caso *Barbulescu v Romania*, foi objeto de uma segunda análise pelo TEDH, tendo a decisão proferida em 09 de setembro de 2017, e ao inverso do ocorrido na de janeiro de 2016, seguido no sentido de decidir pela existência de violação do art. 8.º da CEDH.

⁴⁵³ Vide Martins, J. Z. (2016). *In Comentário ao acórdão do TEDH (...)*, op. cit., pp. 185 e 186.

⁴⁵⁴ Assim preconiza Martins, J. Z. (2016). *In Comentário ao acórdão do TEDH (...)*, op. cit., p. 192.

⁴⁵⁵ *Idem*, p. 193.

⁴⁵⁶ *Ibidem*, p. 201.

⁴⁵⁷ Nas palavras de Martins, J. Z. (2016). *In Comentário ao acórdão do TEDH (...)*, op. cit., pp. 201 e 202.

perceberá que aquela mensagem terá um conteúdo pessoal. Todavia, e caso dúvidas subsistam, então para aceder ao conteúdo deve convocar o trabalhador ou entidade que o represente, garantindo deste modo a privacidade do trabalhador e não violando a correspondência, pois obteve o consentimento do emissor, destinatário da mensagem, respeitando o princípio da proibição de excesso.

Conforme preconiza TERESA MOREIRA, o empregador tem outras formas de verificar se o comportamento do trabalhador não é adequado, sem violar direitos fundamentais, *v.g.*, o “sigilo das comunicações”⁴⁶³, podendo controlar, *inter alia*, o tempo gasto pelos trabalhadores no uso e acesso à rede informática⁴⁶⁴.

A segunda decisão do TEDH, veio tentar mostrar que o problema poderá não estar no controlo realizado pelo empregador, visto que este é legítimo, mas que se coloca nos limites. Ou seja, até onde pode ir o controlo?⁴⁶⁵.

O caso *Barbulescu v Romania*, tornou-se numa situação paradigmática, primeiro por ter produzido duas decisões em sentido diverso, segundo por analisar pela primeira vez uma situação que envolve uma entidade privada, e terceiro porque veio consubstanciar a necessidade de na análise do art. 8.º da CEDH se incluir também a violação de mensagens, enviadas ou recebidas com fins privados, em contexto laboral.

1.2 Os meios de vigilância à distância

As relações laborais, pela introdução da informática sofreram grandes modificações na organização e tempo de trabalho, tendo o aumento das novas tecnologias, bem como questões relacionadas com dados conduzindo ao aumento de problemas relacionados com a privacidade⁴⁶⁶.

⁴⁶³ Moreira, T. A. C. (2017). *In Breve comentário à decisão do TEDH, (...)*, op. cit., p. 155.

⁴⁶⁴ *Idem*, p. 155.

⁴⁶⁵ *Ibidem*, p. 157.

⁴⁶⁶ Vide Moreira, T. A. C. (2004). *In Da Esfera Privada do Trabalhador e o Controlo do Empregador*, Coimbra Editora, p. 293.

Moreira, T. A. C. (2012). *In Novas Tecnologias: Um Admirável Mundo Novo do Trabalho? Revista de Direitos e Garantias Fundamentais*, Vitória, n. 11, p. 15-52, jan./jun. 2012, consultado em: 15.03.2019, disponível em: <http://sisbib.emnuvens.com.br/direitosegarantias/article/view/209;http://dx.doi.org/10.18759/rdgf.v0i11.209>, p. 15

A explosão informática no mundo laboral originou a introdução de instrumentos eletrónicos [como o correio eletrónico e os sistemas de videovigilância] “capazes de ameaçar a privacidade (...) dos trabalhadores”⁴⁶⁷. A utilização destas ferramentas, e de acordo com TERESA MOREIRA, tornam “o controlo do empregador cada vez mais presente e intrusivo”⁴⁶⁸ conduzindo à redução do grau de privacidade e ao aumento de novas questões legais. Desta forma, o empregador tem a porta aberta para reunir informação sobre os trabalhadores pela observação, na descoberta de interesses e preferências, facilitando o *profiling* dos trabalhadores⁴⁶⁹.

1.2.1 Correio eletrónico [ferramenta profissional e pessoal]

O recurso ao uso do correio eletrónico, pelas empresas, veio facilitar o modo de trabalho e potenciar uma mais rápida transmissão da informação. No entanto, para o trabalhador, não se traduziu somente na facilidade de desempenho da sua atividade laboral, pois esta ferramenta possibilita uma forma de vigilância à distância. Ou seja, o empregador consegue controlar o trabalhador, verificar como usa a ferramenta, para que fins, visto que a informação fica armazenada digitalmente⁴⁷⁰. Segundo o GT249⁴⁷¹ “é possível que um empregador” aplique uma monitorização polivalente em vez de incidir somente sobre o endereço de correio eletrónico. Significa isto, que o empregador pode aceder inclusive ao conteúdo do email enviado, recebido. É por este motivo que antes da entidade empregadora implementar uma qualquer tecnologia de monitorização deve realizar uma AIPD⁴⁷².

Conforme nos transmite GARCIA MARQUES⁴⁷³, tudo pode ser monitorizado eletronicamente, sendo o correio eletrónico uma ferramenta informática, também a sua

⁴⁶⁷ Cfr. Moreira, T. A. C. (2012). *In Novas Tecnologias: Um Admirável Mundo (...)*, op. cit., p.16.

⁴⁶⁸ Vide Moreira, T. A. C. (2012). *In Novas Tecnologias: Um Admirável Mundo (...)*, op. cit., p.17.

⁴⁶⁹ *Idem*, p. 17.

⁴⁷⁰ Em servidores.

⁴⁷¹ Grupo de Trabalho do Artigo 29.º (2017). *Opinion 2/2017 on data processing at work. WP249*, consultado em: 06.10.2019, disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169, p. 15.

⁴⁷² Grupo de Trabalho do Artigo 29.º (2017). *Opinion 2/2017 on data (...)*, op. cit., p. 18.

⁴⁷³ Vide Marques, G. e Martins, L. (2006). *In Direito da Informática (...)*, op. cit., p. 172.

utilização potencia uma forma de vigilância constante à distância, ainda que assim não devesse ser.

A problemática do uso apropriado do correio eletrónico não é exclusiva do ordenamento jurídico português. A prática da monitorização, em Portugal⁴⁷⁴, pelo recurso aos meios de vigilância à distância é proibida ao empregador quando tenha como finalidade controlar o desempenho do trabalhador, conforme n.º 1 do art. 20.º do CT, sendo apenas lícita quando vise a proteção e segurança de pessoas e bens, exigindo-se que o empregador informe o trabalhador sobre a existência e finalidade dos meios de vigilância utilizados. Por conseguinte, deve a entidade empregadora, por regulamento, *v.g.*, definir regras sobre a utilização do correio eletrónico e sobre a sua monitorização, bem como se o mesmo consiste num meio de vigilância à distância⁴⁷⁵.

Consideramos que havendo monitorização, esta traduz-se num meio capaz de transmitir informação ao empregador sobre o desempenho do trabalhador, bem como de informação não profissionais que este tenha enviado ou recebido. Deste modo, e de acordo com a Deliberação n.º 1638/2013 da CNPD⁴⁷⁶, o controlo do correio eletrónico deve ser exercido em observância dos princípios da proporcionalidade e da informação, estando vedado ao empregador o controlo à distância da prestação do trabalhador, *e.g.*, através do acesso remoto ou partilha do ambiente de trabalho. O recurso a estas ferramentas só é legal quando a sua finalidade seja a assistência técnica pedida e consentida pelo trabalhador⁴⁷⁷.

⁴⁷⁴ Noutros ordenamentos jurídicos como EUA ou Espanha, “a prática do *monitoring* é considerada lícita” existindo a sensação de que a tendência de proteção se inclina mais para o empregador do que para o trabalhador. Já no ordenamento jurídico Francês, a jurisprudência tende a proteger mais o trabalhador. Todavia, verifica-se a existência de uma dualidade de interpretações por faltar a regulamentação concreta destas matérias. Para maior desenvolvimento, veja-se, Moreira, T. A. C. (2004). *In Da Esfera Privada do Trabalhador e o Controlo do Empregador*, Coimbra Editora, pp. 296 e ss.

⁴⁷⁵ Vide Moreira, T. A. C. (2004). *In Da Esfera Privada do Trabalhador (...)*, op. cit., p. 318.

⁴⁷⁶ CNPD. (2013). Deliberação n.º 1638/2013. *Orientações sobre tratamento dados (...)*, op. cit., p. 18.

⁴⁷⁷ *Idem*, p. 24.

1.2.1.1 O acesso às comunicações e sua divulgação

Ao qualificar-se o correio eletrónico como um meio de vigilância à distância, chama-se a atenção para o facto de, a existir monitorização, esta não deve ser permanente e sistemática, mas sim pontual e aleatória⁴⁷⁸ sem aceder ao conteúdo das mensagens.

As mensagens enviadas pelo trabalhador ou a ele dirigidas têm garantia de confidencialidade conferida aos mais altos níveis legislativos. O n.º 1 do art. 34.º da CRP consagra como inviolável a correspondência, esta tem garantia de sigilo, pelo que se pratica um crime quando ocorra a sua violação, cfr. art. 194.º do CP⁴⁷⁹. Naturalmente, e de acordo com o n.º 4 do art. 34.º da CRP, também é proibida a ingerência de entidades públicas, e de igual modo privadas⁴⁸⁰, *ex vi* art. 18.º da CRP.

Ao nível das normas laborais, estatui o art. 22.º do CT que o trabalhador goza do direito de reserva e confidencialidade, relativamente ao conteúdo das mensagens de carácter pessoal e acesso a informação de carácter não profissional que envie, receba ou consulte, designadamente através do correio eletrónico. Donde se conclui que as comunicações do trabalhador têm, à primeira vista, carácter pessoal, sendo deste modo proibido o acesso ou divulgação do conteúdo das mensagens mesmo que revestindo formas mais modernas de comunicação (email)⁴⁸¹.

Por fim referir, e conforme preconiza MENEZES LEITÃO, que a proibição vertida no n.º 1 do art. 20.º do CT abrange qualquer meio de vigilância à distância que permita controlar o desempenho do trabalhador, nele se incluindo câmaras de vídeo ou escutas telefónicas⁴⁸². Porém, em nossa opinião, o correio eletrónico também se consubstancia numa ferramenta que permite uma vigilância à distância.

⁴⁷⁸ *Ibidem*, pp.18 e 19.

⁴⁷⁹ Ramalho, M. R. P, Carvalho, P. M. (2013). *Conferência Estado De Direito E Direitos Fundamentais: A Concretização Dos Direitos Fundamentais Pelos Tribunais*. In *Colóquios e Conferências Parlamentares*, consultado 10.03.2019, disponível em: http://www.cej.mj.pt/cej/estudos-e-publica/fichpdf/conferencias/Conferencia_CACDLG-CEJ.pdf, p. 52.

⁴⁸⁰ Vide Leitão, L. M. T. M. (2019). In *Direito do trabalho (...)*, op. cit., p. 175.

⁴⁸¹ De acordo com Ramalho, M. R. P, Carvalho, P. M. (2013). *Conferência Estado (...)*, op. cit., p. 52 e Leitão, L. M. T. M. (2019). In *Direito do trabalho (...)*, op. cit., p. 175.

⁴⁸² Veja-se Leitão, L. M. T. M. (2019). In *Direito do trabalho (...)*, op. cit., p. 172.

Na jurisprudência, podemos verificar pela decisão do TRL⁴⁸³ que o envio de mensagens de pessoa a pessoa (*email*) preenche os requisitos de correspondência privada, logo a inviolabilidade vincula toda e qualquer pessoa. Também neste sentido uma decisão do TRP⁴⁸⁴, que vem reforçar a garantia da confidencialidade das mensagens e da privacidade dos utilizadores do correio eletrónico [trabalhadores], seja enquanto emissor, seja enquanto destinatário, notando que devem ser respeitados os princípios da finalidade, transparência e da notificação à CNPD, bem como o princípio da proporcionalidade.

1.2.1.2 (I)licitude do despedimento pelo uso do correio eletrónico(?)

Já anteriormente se abordou, no caso Barbulescu, esta problemática, tendo-se concluído que as mensagens enviadas ou recebidas por um trabalhador gozam do direito à confidencialidade.

Este assunto tem sido muito debatido, jurisprudencialmente. Neste sentido, destacamos alguns acórdãos, entre os quais o do STJ de 05 de julho de 2007. *In casu*, um trabalhador enviou a outra colega, no horário de expediente um email. O empregador tomou conhecimento do conteúdo do email, pelo acesso ao mesmo, tendo o STJ⁴⁸⁵ sido chamado a decidir sobre a licitude do despedimento do trabalhador, para aferir se o empregador podia ou não ter acedido ao conteúdo do email. Na decisão, o tribunal considerou que o acesso e a divulgação do conteúdo do email, constituíram uma violação de direitos fundamentais, designadamente o direito à confidencialidade das mensagens e o direito à privacidade, considerando pelo exposto, o despedimento ilícito.

⁴⁸³ TRL, Processo n.º 2970/07.4, de 05 de junho de 2008. Relator: MJD Leopoldo Soares, consultado em: 04.11.2019, disponível em: <http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/6c195267c4ce32e480257474003464f7?OpenDocument>.

⁴⁸⁴ TRP, Processo n.º 208/14.1TTVFR-D.P1, de 15 de dezembro de 2016. Relatora: MJD Paula Leal de Carvalho, consultado em: 05.11.2019, disponível em: <http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/df89d957d1942212802580a70058cc70?OpenDocument>.

⁴⁸⁵ STJ, Processo n.º 07S043, de 05 de julho de 2017. Relator: MJD Mário Pereira, consultado em: 17.01.2020, disponível em: <http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/54d3c9f0041a33d58025735900331cc3>.

Outras decisões mais recentes produzidas pelo Tribunal da Relação de Lisboa⁴⁸⁶ e de Guimarães⁴⁸⁷ vêm chamar a atenção para outros factos. Nos exemplos indicados, em ambas as decisões se confirma a confidencialidade das mensagens, e mais, neles se adverte para a necessidade de existência de regulamentação nas empresas, quer para o uso do correio eletrónico, quer para o facto de o mesmo ser monitorizado, bem como a necessidade de análise casuística dos factos. No entanto, as decisões finais são distintas.

O TRG considerou que existiu quebra de confiança no desempenho das atividades, pois o trabalhador tinha um cargo de responsabilidade no qual imperava o sigilo, não devendo ter descurado o mesmo. Por conseguinte, e avaliados os critérios de proporcionalidade, o douto Tribunal valida a sentença recorrida, improcedendo o recurso, considerando deste modo o despedimento lícito. Já na decisão do TRL, a troca de mensagens não produziu prejuízos, aparentes, para a empresa, tendo neste caso considerado o despedimento ilícito.

Concluimos que devem ser ponderados os factos que conduziram à aplicação da sanção pelo empregador, e esta dever ser casuística. Pese embora esta análise, é evidente que existe a confidencialidade das mensagens enviada, recebidas pelo trabalhador. O dilema coloca-se na gestão que o empregador faz da informação que tem ao seu dispor, devendo, outrossim, ele ser mais cuidadoso com a mesma, bem como nas sanções que aplica. Temos notado que o despedimento é, normalmente a sanção mais aplicada. Porém, há pelo menos, um caso em que a decisão foi de instauração de processo disciplinar⁴⁸⁸ antes de se avançar para o despedimento.

⁴⁸⁶ TRL, Processo n.º 24163/09.0T2SNT.L1-4 de 07 de março de 2012. Relator: MJD José Eduardo Sapateiro, consultado em: 22.10.2018, disponível em: <http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/109499c90995e66d802579bf0050cfa4?OpenDocument>.

⁴⁸⁷ TRG, Processo n.º 15/11.3TTVRL.G1, de 11 de junho de 2015. Relator: MJD Antero Veiga, consultado em: 15.03.2019, disponível em: <http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/602f7d06304fc8bc80257eb20036e5fe?OpenDocument>.

⁴⁸⁸ Veja-se o TRP, Processo n.º 101/13.5TTMTS.P1, de 08 de setembro de 2014. Relatora: MJD Maria José Costa Pinto, consultado em: 15.03.2019, disponível em: <http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/917c9c56c1c2c9ae80257d5500543c59?OpenDocument>.

Porém, depreende-se que seja mais simples optar pelo despedimento, pois existindo a quebra da confiança entre as partes, a relação laboral tornar-se-á ainda mais complexa. No entanto, não concordamos com a posição adotada pelos empregadores em geral, quando optam pela sanção máxima, ou seja, o despedimento.

1.2.2 Videovigilância: o que é?

1.2.2.1 Fonte de segurança ou fonte potencial de abusos?

Todos nós sabemos que a videovigilância é uma forma de controlar à distância, seja pela recolha de imagens⁴⁸⁹, seja pela recolha de sons.

A videovigilância traduz-se num sistema que visa a proteção pelo efeito dissuasor, devendo por isso estar instalado em locais bem visíveis. Atualmente, predominam dois tipos de sistemas: os circuitos fechados de televisão e os sistemas de vídeo sobre *internet protocol*⁴⁹⁰ permitindo a captação de imagens em tempo real.

O recurso à videovigilância tem assumido finalidades essenciais, *e.g.*, monitorizar a via pública, fluxos de trânsito, a segurança de pessoas e bens em locais de risco, *v.g.*, plataformas das estações ferroviárias ou em passagens de nível⁴⁹¹, proteção do património ou segurança no meio laboral⁴⁹².

Conforme preconiza TERESA MOREIRA, os sistemas de videovigilância têm cada vez maior complexidade, e por esse motivo, podem potenciar mais “atentados à privacidade”⁴⁹³ das pessoas em geral, mas, especialmente dos trabalhadores.

Os equipamentos informáticos das empresas, sofrem atualizações com grande periodicidade. Estas atualizações permitem, aos utilizadores, terem sempre ao seu dispor tecnologias mais avançadas, inclusive de monitorização e vigilância. Os mais modernos equipamentos, vem equipados com *webcams* e microfones, estes dispositivos consubstanciam um perigo acrescido, pois podem ser acedidos permitindo a divulgação

⁴⁸⁹ Na opinião de Marques, G. e Martins, L. (2006). *In Direito da Informática (...)*, op. cit., p. 170.

⁴⁹⁰ Veja-se Castro, C. S. (2005). *In Direito da Informática, Privacidade (...)*, op. cit., p. 125.

⁴⁹¹ A título exemplificativo.

⁴⁹² Para maior desenvolvimento veja-se: Marques, G. e Martins, L. (2006). *In Direito da Informática (...)*, op. cit., p. 171 e Castro, C. S. (2005). *In Direito da Informática, Privacidade (...)*, op. cit., p. 123.

⁴⁹³ Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., p. 450.

de conversas ou imagens na *internet*. Pelo que, conseqüentemente a proteção dos trabalhadores, da sua privacidade, fica em risco na medida em que a informação, eventualmente recolhida pode ficar armazenada em bases de dados, em ficheiros podendo “vir a ser objeto de tratamento de dados”⁴⁹⁴.

Conforme preconiza a doutrina nacional⁴⁹⁵ as “imagens e os sons”⁴⁹⁶ captados no seio laboral são considerados dados pessoais se neles existir a possibilidade de serem identificadas as pessoas que estejam visíveis ou audíveis. Por conseguinte, o tratamento que for realizado deve reger-se pelos princípios inerentes à proteção de dados, vertidos no RGPD, bem como na legislação laboral.

1.2.2.2 Implementação e utilização de imagens

Como se sabe, muitos locais de trabalho têm instalados sistemas de videovigilância. De acordo com o n.º 2 do art. 20.º do CT é lícita a utilização destes sistemas sempre que tenha por finalidade a proteção de pessoas e bens ou quando particulares exigências à natureza da atividade o justifiquem. Pelo que a utilização de um equipamento que tenha por finalidade, única e exclusiva, controlar a prestação do trabalhador, não é permitida por se tratar de um meio de vigilância à distância. Como se viu, as finalidades não podem relacionar-se diretamente com a atividade do trabalhador. A licitude da utilização destes meios assenta nos requisitos do mencionado n.º 2 do art. 20.º do CT. Deste modo, as provas que sejam obtidas pela utilização do mesmo e que se reportem ao controlo do desempenho profissional do trabalhador são ilícitas⁴⁹⁷.

Segundo AMADEU GUERRA, deve ser aplicado um conjunto de disposições legais⁴⁹⁸ aquando da implementação de um sistema de videovigilância, que vão delimitar

⁴⁹⁴ *Idem*, pp. 452 e 453.

⁴⁹⁵ Na opinião de: Castro, C. S. (2005). *In Direito da Informática, Privacidade (...)*, op. cit., pp. 126, 127 e Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., pp. 466, 467.

⁴⁹⁶ Vide Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., p. 466.

⁴⁹⁷ Vide TRG, Processo n.º 20/14.7T8VRL.G1, de 03 de março de 2014. Relatora: MJD Manuela Fialho, consultado em: 15.03.2019, disponível em: <http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/302fdd824b16519780257f85004f8071?OpenDocument&Highlight=0,correspond%C3%Aancia,trabalhador>.

⁴⁹⁸ DL n.º 35/2004, de 21 de fevereiro, art. 20.º do CT. Note-se que Guerra, A. (2004). *In A privacidade no local de trabalho: as novas tecnologias (...)*, op. cit., p. 350, refere a Lei n.º 67/98, de 26 de outubro,

as condições de tratamento de imagem e som capturadas através do sistema supramencionado⁴⁹⁹. A videovigilância, no local de trabalho, pode ser vista por dois prismas diferentes. Ou seja, podem ser aproveitados sistemas instalados para segurança de pessoas e bens para monitorizar os trabalhadores ou pode a entidade empregadora querer colocar os sistemas para verificar o comportamento dos trabalhadores^{500,501}.

Importa ter presente o facto, de pela recolha e tratamento de imagens, se poder identificar ou se tornarem identificáveis trabalhadores, neste pressuposto e conforme preconiza TERESA MOREIRA, “no seio da relação laboral incluem-se entre os dados pessoais (...), os dados obtidos através da videovigilância”⁵⁰² abarcando as imagens e sons recolhidos, seja por CCTV seja pela *internet*. De acordo com o GT89, parecer 4/2004, os dados recolhidos através de sistemas de videovigilância integram-se no conceito de dados pessoais, pois existindo uma gravação, existe tratamento de dados. Para o GT89, não é exigível a visualização de rostos, basta que sejam captadas imagens que permitam, pela junção de várias características particulares, identificar ou tornar identificável um sujeito⁵⁰³. Deste modo, terão plena aplicabilidade o RGPD, a Lei n.º 58/19, de 8 de agosto, bem como os preceitos previstos no CT, que vão delimitar a ingerência, do recurso aos sistemas de vigilância à distância⁵⁰⁴.

Quando o empregador decide adotar, como forma de controlo⁵⁰⁵, dispositivos audiovisuais é importante ter em mente o facto de os trabalhadores serem merecedores de

todavia, em virtude da aplicação do RGPD em 25 de maio de 2018 e da Lei n.º 58/19, de 08 de agosto, devem agora ser tidos, estes diplomas, em consideração.

⁴⁹⁹ Vide Guerra, A. (2004). *In A privacidade no local de trabalho: as novas tecnologias (...)*, op. cit., p. 350.

⁵⁰⁰ *Idem*, p. 358.

⁵⁰¹ Relativamente à segunda opção, esta tem de ser muito bem analisada e justificada pelos sindicatos e/ou comissão de trabalhadores, bem como pela CNPD, para que não sejam violados direitos fundamentais dos trabalhadores, exigindo-se “um balanceamento – em termos de proporcionalidade – dos valores conflituantes”, nas palavras de Guerra, A. (2004). *In A privacidade no local de trabalho: as novas tecnologias (...)*, op. cit., p. 359.

⁵⁰² Cfr. Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., p. 472.

⁵⁰³ Grupo de Trabalho do Artigo 29.º (2004). *Parecer 4/2004 sobre o Tratamento de Dados Pessoais por meio de Videovigilância*. WP89, consultado em: 06.03.2020, disponível em: <https://www.gdpd.gov.mo/uploadfile/2014/0505/20140505071008284.pdf>, pp. 14 e 15.

⁵⁰⁴ Veja-se Leitão, L. M. T. M. (2019). *In Direito do trabalho (...)*, op. cit., pp. 171 a 174.

⁵⁰⁵ Cfr. STJ, Processo n.º 73/12.3TTVNF.P1.S1, de 13 de novembro de 2013. Relator: MJD Mário Belo Morgado, consultado em: 15.03.2019, disponível em: <http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/e32eab3444364cb980257c2300331c47?>

proteção quanto aos dados pessoais, quer no momento da decisão de instalação e quer no momento da efetiva aplicação. Destarte, e primeiramente o empregador deve informar o trabalhador em que medida poderão os direitos fundamentais ser afetados pelas novas medidas de controlo, para que, em momento ulterior, após a instalação, tenha o empregador os cuidados necessários no controlo realizado e no fluxo da informação obtida⁵⁰⁶.

Na jurisprudência nacional, e de acordo com a análise do TRP⁵⁰⁷ o trabalhador pode resolver o contrato se o sistema de implementação de videovigilância não respeitar o requisito da informação prévias dos trabalhadores.

Ademais, e aquando da fase de escolha do sistema de vigilância, a ser usado para controlo do trabalhador, devem ser considerados os princípios da finalidade, da proporcionalidade, da licitude⁵⁰⁸ e da informação, para garantia da proteção dos dados pessoais do trabalhador que irão ser objeto de tratamento⁵⁰⁹.

A licitude da escolha de um sistema de controlo à distância é o cerne do problema, assim secunda TERESA MOREIRA. A autora entende que é importante saber “quais os interesses do empregador que assumem o requisito de relevantes no local de trabalho”⁵¹⁰ para justificar a recolha de imagens ou sons. Constata-se que a licitude assenta sobre os requisitos: segurança de pessoas e dos bens da empresa⁵¹¹. Porém, questionamos se o facto de no CT, art. 20.º, n.º 2, ser referido somente finalidade a proteção e segurança de pessoas e bens ou quando particulares exigências inerentes à natureza da atividade o

[OpenDocument](#), “o poder de direção do empregador, enquanto realidade naturalmente inerente à prestação de trabalho e à liberdade de empresa, inclui os poderes de vigilância e controle, os quais, têm, no entanto, de se conciliar com os princípios de cariz garantístico que visam salvaguardar a individualidade dos trabalhadores e conformar o sentido da ordenação jurídica das relações de trabalho em função dos valores jurídico-constitucionais está dentro do âmbito”.

⁵⁰⁶ Secundado por Moreira, T. A. C. (2010). In *A Privacidade dos Trabalhadores (...)*, op. cit., p. 486.

⁵⁰⁷ TRP, Processo n.º 787/10.2TTVCT.P1, de 04 de março de 2013. Relator: MJD Ferreira da Costa
Consultado em: 15.03.2019, disponível em:
<http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/b655a445dc93958780257b340054d89c?OpenDocument&Highlight=0.teresa.coelho.moreira>.

⁵⁰⁸ Vide Moreira, T. A. C. (2010). In *A Privacidade dos Trabalhadores (...)*, op. cit., pp. 487 e ss.

⁵⁰⁹ Grupo de Trabalho do Artigo 29.º (2004). *Parecer 4/2004 sobre o Tratamento (...)*, op. cit., p. 25.

⁵¹⁰ Cfr. Moreira, T. A. C. (2010). In *A Privacidade dos Trabalhadores (...)*, op. cit., p. 493.

⁵¹¹ Tendo presente o Grupo de Trabalho do Artigo 29.º (2004). *Parecer 4/2004 sobre o Tratamento (...)*, op. cit., p. 25, a legislação nacional laboral – art. 20.º do CT.

justifiquem, não terá o legislador criado abertura a interpretação extensivas, concedendo ao empregador uma grande margem de inclusão de possibilidades.

Por conseguinte, defende-se que a instalação de sistemas de videovigilância, seja regida pela proteção dos direitos fundamentais dos trabalhadores e que seja fundamentada como medida de prevenção.

Todavia, e reforçando o anteriormente dito, o controlo não pode ser exercido a todo o tempo, ou seja, “de tipo orwelliano, constante, insidioso e vexatório”⁵¹², devendo ser considerada ilícita se visar, exclusivamente a monitorização da execução da atividade laboral dos trabalhadores, defendendo-se um uso correto, necessário e adequado, coerente com a justificação que fundamentou a instalação. Também a jurisprudência assim o preconiza, veja-se o acórdão produzido pelo TRC, quando diz: “CT **proíbe**⁵¹³ a utilização de meios de vigilância à distância para controlar de forma dedicada e permanente o desempenho profissional do trabalhador”⁵¹⁴.

No entanto, gostaríamos de notar a existência de atividades que justificam a existência de videovigilância. Este sistema, com uma poupança custos, permite verificar se são perpetrados ilícitos, veja-se o caso das passagens de nível ferroviárias, nas quais muitos condutores incumprem com a regras e trânsito [sinalização sonora, luminosa e física] e colocam a sua, bem como a vida dos passageiros ferroviários em perigo. Pese embora, a vantagem de vigiar os incumpridores, não deve depois desvirtuar a finalidade primária e servir para monitorizar quem na passagem de nível, ou imediações, trabalhe. Em caso de necessidade, deve sim, ser utilizada para proteger os trabalhadores quando perante um acidente ou incidente rodoferroviário.

⁵¹² Assim preconiza Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., p. 495.

⁵¹³ Sublinhado nosso.

⁵¹⁴ TRC, Processo n.º 359/13.0TTFIG-A.C1, de 06 de fevereiro de 2015. Relator: MJD Azevedo Mendes, consultado em: 15.03.2019, disponível em: <http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/fe545bb508b68e6980257dee004bf0bd?OpenDocument>.

1.2.2.3 RGD e a nova lei de execução na videovigilância

Com as alterações legislativas produzidas pelo RGD e pela nova Lei de execução nacional, a CNPD aglutinou um conjunto de informações concernentes com a preocupação dos cidadãos quanto às modificações que a nova lei trouxe para o ordenamento jurídico nacional, e que achamos importantes referir neste trabalho.

Relativamente à matéria da videovigilância, o Regulamento europeu de *data protection*, determina não ser necessário o pedido prévio de autorização à CNPD para instalação destes sistemas. Porém, mantém-se a obrigatoriedade de atender a vários requisitos legais para a instalação do sistema de videovigilância⁵¹⁵.

Quanto à questão das autorizações emitidas antes de 25 de maio, as mesmas mantêm-se válidas, desde que não violem as disposições previstas no RGD ou na lei executória, art. 19.º. Pese embora, tenha deixado de ser necessária a autorização prévia, o direito de informação mantém-se inalterado. Deste modo, os titulares de dados pessoais continuam a ter direito a ser informados sobre a utilização de dispositivos de captura de imagem e/ou som, pelo que o aviso informativo deve atender ao previsto nos n.ºs 5 e 6 do art. 31.º da Lei n.º 34/13, de 16 de maio.

No que ao prazo de conservação concerne, e se não existir, numa organização, regulamentação específica que imponha prazos diferentes, a conservação das imagens deve manter-se pelo período de 30 dias, findo este tempo, devem ser eliminadas no espaço temporal de 48 horas, exceto se no âmbito de procedimento criminal, no qual pode subsistir a necessidade de dilatar o prazo de 30 dias.

A implementação de um sistema de videovigilância, por via de regra, visa a proteção de pessoas e bens, seja para dissuadir práticas ilícitas, seja para permitir a identificação de um perpetrador, num processo criminal. Destarte, importa referir que a instalação de câmaras deve garantir um perímetro de segurança necessário aos fins a que se destina. Deste modo, os aparelhos audiovisuais não podem incidir sobre vias públicas ou locais que não sejam de domínio exclusivo do responsável, na medida em que podem

⁵¹⁵ Estes requisitos podem chamar à colação vários diplomas legais, além do RGD, como seja a Lei n.º 58/19, de 08 de agosto; a Lei n.º 34/16, de 16 de maio ou o contrato, de acordo com o que for mais favorável à real aplicação, pelo deve ser efetuada sempre uma análise casuística.

afetar o direito à privacidade de terceiros. Existem ainda outros locais nos quais não podem ser capturadas imagens⁵¹⁶.

No âmbito laboral, vigoram as condições impostas pelo CT para a vigilância à distância. Neste contexto, e contrariando o disposto no RGPD, prevalece a necessidade de autorização prévia à CNPD para a instalação de sistemas de videovigilância, que não podem ser usados para um controlo permanente do desempenho do trabalhador, devendo ainda ser observados os princípios da proporcionalidade, da intromissão mínima e da transparência⁵¹⁷. A nosso ver, a prevalência de autorização prévia da CNPD, traduz-se numa vantagem para o trabalhador, para defesa dos seus interesses, contra instalações abusivas pelo empregador. No entanto, para não contrariar o vertido do RGPD⁵¹⁸, e visto ter sido redigida uma norma legal nacional para executar o regulamento, o legislador nacional poderia ter previsto também na nova lei esta garantia, evitando-se interpretações diversas.

Tal como antedito, o direito do trabalhador a ser informado sobre a vigilância mantém-se. A informação deve ser transmitida, previamente, não só ao trabalhador como também aos seus representantes, devendo a informação incluir a identidade do responsável pelo tratamento e a finalidade da vigilância, garantindo a realização de um procedimento transparente, de acordo com o vertido no n.º 3 do art. 20.º do CT e no art. 21.º do mesmo diploma.

1.3 Videovigilância na relação laboral

1.3.1 A visualização de imagens e sua divulgação

Na relação laboral, os problemas podem surgir quando o empregador recorre às imagens e/ou sons captados por sistemas de videovigilância, pois o simples facto de se poder aceder, pode colocar em risco o direito à privacidade dos trabalhadores⁵¹⁹. Neste sentido, requer-se a observação do princípio da adequação da visualização de imagens,

⁵¹⁶ Instalações sanitárias, interior dos elevadores, vestiários, *inter alia*, nos termos da al. d), do n.º 1 do art. 19.º da Lei n.º 58/19, de 08 de agosto.

⁵¹⁷ Cfr defende Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores (...)*, op. cit., pp. 520 e ss.

⁵¹⁸ Vide art. 36.º do RGPD, que determina o fim da função de supervisão das autoridades controlo *a priori* para uma função de fiscalização *a posteriori*.

⁵¹⁹ Veja-se Castro, C. S. (2005). *In Direito da Informática, Privacidade (...)*, op. cit., p. 144.

exclusivamente ao fim pretendido, nos termos da al. c) do n.º 1 do art. 5.º do RGPD, visto que as imagens, os sons têm de ser recolhidos para finalidades determinadas, impondo-se ainda uma obrigação de minimização dos dados⁵²⁰.

Se o princípio da pertinência e adequação se relaciona com a necessidade de conservação das imagens, questionamo-nos sobre qual o período pelo qual devem as imagens ser conservadas. Consideramos que é importante uma definição concreta deste prazo, em matérias laborais, sendo certo que não se afigura tarefa fácil, a definição de prazos para todas as finalidades. Todavia, em vez de criar um prazo, diretamente relacionado com as finalidades, e porque as mesmas podem ser muito distintas, por que não criar um prazo para os dados tratados no âmbito laboral? Ou, se pensarmos nas câmaras de CCTV, cuja finalidade seja a segurança de pessoas e bens, porque não usar o prazo de 30 dias previsto no n.º 2 do art. 31.º da Lei n.º 34/13, de 16 de maio, alterado pela Lei n.º 46/19, de 08 de julho. Neste caso, o n.º 3 do art. 21.º do CT poderia ter de ser mais concreto, e definir, expressamente, este prazo, quando a finalidade fosse a segurança dos trabalhadores?

Quanto ao acesso, existe o entendimento de na maior parte das situações, este deva ser restringido ao respeito pelo tratamento e aos que efetuam as operações de tratamento⁵²¹. No entanto, se o fim se relacionar com a segurança de pessoas e bens, é aceitável que sejam comunicadas às entidades competentes, quando solicitadas no âmbito do respetivo processo criminal⁵²², veja-se, a título ilustrativo o Ac. do TRC, de 06 de fevereiro de 2015, bem como no decurso da investigação.

No que concerne ao acesso, pelo empregador, às imagens recolhidas quando se verifique que o trabalhador incorre numa infração, as mesmas só podem ser utilizadas no âmbito de processo penal e, apenas para efeitos de apuramento de responsabilidade disciplinar, nos termos dos n.ºs 4 e 5 do art. 28.º da Lei n.º 58/19, de 8 de agosto.

⁵²⁰ Princípio da minimização dos dados.

⁵²¹ Cfr. Castro, C. S. (2005). *In Direito da Informática, Privacidade (...)*, op. cit., p. 146.

⁵²² Vide TRC, Processo n.º 359/13.0TTFIG-A.C1, de 06 de fevereiro de 2015. Relator: MJD Azevedo Mendes, consultado em: 15.03.2019, disponível em:

<http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/fe545bb508b68e6980257dee004bf0bd?OpenDocument>, ponto III do sumário.

À luz da lei portuguesa, as imagens não podem visar o controlo da qualidade do trabalho. Os trabalhadores só podem ser filmados no exercício das suas funções se isso servir para proteger e garantir a segurança de pessoas e de bens. Mesmo nesse caso, a entidade empregadora terá de informar os trabalhadores sobre a existência e a finalidade das câmaras.

A obrigação de informar deverá ser cumprida através da afixação das seguintes mensagens: “Este local encontra-se sob vigilância de um circuito fechado de televisão” ou “Este local encontra-se sob vigilância de um circuito fechado de televisão, procedendo-se à gravação de imagem e som”, acompanhadas do símbolo da câmara de filmar. Além disso, as entidades têm também de comunicar o tratamento de dados à Comissão Nacional de Proteção de Dados.

No caso de serem cumpridos todos os requisitos legais, as imagens servem como prova em tribunal. De acordo com o Ac. do TRP, de 07.12.2018⁵²³, quando o sistema de vigilância está legalmente autorizado no local de trabalho, e o trabalhador não agiu com cuidado, criando constrangimentos ao empregador, o Tribunal decidiu que neste contexto é admissível a visualização, em sede de audiência de discussão e julgamento, das imagens de videovigilância recolhidas no local de trabalho, como meio probatório para fim disciplinar. Neste sentido postula também o Ac. também do TRP, de 26.06.2017.

Porém, e de acordo com o TEDH⁵²⁴ existe violação da privacidade nos termos do art. 8.º da CEDH quando o sistema instalado não observe os princípios da informação e da transparência para com os trabalhadores. No presente caso, as requerentes operavam como caixeiras e assistentes de vendas num supermercado. O empregador, para verificar porque tinha prejuízos decidiu colocar câmaras, **visíveis e ocultas**⁵²⁵, tendo sido as requerentes informadas, somente sobre as visíveis. No entendimento do Tribunal, o

⁵²³ TRP, Processo n.º 159/18.OT8PNF-A.P1, de 07 de dezembro de 2018. Relator MJD: Domingos Morais, consultado em: 15.03.2019, disponível em: <http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/cc2a4b78e8ec279d8025839800517f79?OpenDocument>.

⁵²⁴ *Applications nos. 1874/13 and 8567/13 López Ribalda and Others v. Spain*, de 17 de outubro de 2019, consultado em: 02.04.2020, disponível em: <https://hudoc.echr.coe.int/eng#%7B%22itemid%22%3A%22001-197098%22%7D>.

⁵²⁵ Sublinhado nosso.

sistema de videovigilância instalado pelo empregador, que teria funcionado por período continuado, não teria também cumprido os requisitos previstos na legislação. Contudo, e considerando as circunstâncias específicas do caso (furto), o grau de ingerência na vida privada e as legítimas razões que justificaram a instalação do sistema de vídeo vigilância, os tribunais de trabalho espanhóis, formaram a convicção que a interferência na vida privada das requerentes não terá violado o princípio da proporcionalidade. Ademais, a conclusão foi no sentido de que, pelo facto de as irregularidades cometidas, aliadas à dimensão dos prejuízos, teria sido afetado o bom funcionamento da empresa. *A final*, o TEDH decidiu que não houve violação do art.º 8.º da CEDH, nem do n.º 1 do art. 6.º da CEDH, concretamente sobre o uso das imagens obtidas através de sistemas de videovigilância.

CAPÍTULO V – A Autoridade de Controlo Nacional: CNPD

1. A CNPD após publicação da Lei n.º 58/19, de 8 de agosto

Como se sabe a autoridade independente de controlo, em Portugal, em matéria de proteção de dados é a Comissão Nacional de Proteção de Dados, funciona junto da Assembleia da República, exercendo os seus poderes em todo o território nacional⁵²⁶. Enquanto entidade administrativa, caracteriza-se pela sua independência, relativamente ao Governo e às outras entidades por ele reguladas. Segundo CATARINA CASTRO, a propensão destas entidades centra-se na proteção de matérias sensíveis que devem ser tratadas com cuidado e mantidas fora de interesses partidários⁵²⁷.

Juridicamente, a CNPD encontra-se estatuída na Lei Fundamental, art. 35.º, n.º 2, onde se dispõe no sentido de: “A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua **proteção, designadamente através de entidade administrativa independente**”⁵²⁸.

Na Administração Pública, a CNPD é “um órgão colegial”⁵²⁹. A sua visão assenta na prossecução dos fins do Estado definidos na Constituição e demais diplomas legais. As competências desta entidade administrativa independente centram-se na defesa dos dados pessoais dos cidadãos, na realização do interesse público, que se consubstanciam em funções essenciais enquanto órgão administrativo.

Além das funções administrativas, a CNPD cumula ainda funções consultivas, de decisão administrativa, de investigação, bem como funções sancionatórias quando estejam em causa o tratamento de dados pessoais dos cidadãos.

Com a entrada em vigor do RGPD, em 25 de maio de 2018, produziu-se uma alteração no paradigma das funções das autoridades de controlo, tendo sido modificado o esquema de autorização prévia ao tratamento para um esquema de monitorização, fiscalização ulterior. Ou seja, o RGPD veio determinar que para realizar o tratamento de

⁵²⁶ Vide Castro, C. S. (2005). *In Direito da Informática, Privacidade (...)*, op. cit., p. 323.

⁵²⁷ *Idem*, p. 323.

⁵²⁸ Sublinhado nosso.

⁵²⁹ Cfr. Castro, C. S. (2005). *In Direito da Informática, Privacidade (...)*, op. cit., p. 325.

dados, na maioria das situações deixa de ser necessário efetuar um pedido de autorização às autoridades de controlo, a CNPD no caso português, sendo necessária a comunicação do tratamento e das finalidades, para que num momento posterior, seja possível a esta entidade auditar, fiscalizar o cumprimento do disposto no Regulamento. Todavia, e de acordo com o n.º 5, do art. 36.º do RGPD, é concedido aos EM a previsão de mecanismos de controlo prévio, em casos especiais⁵³⁰.

De acordo com a Lei n.º 58/19, de 8 de agosto, que executa o RGPD em Portugal e revoga⁵³¹ a Lei de Proteção de Dados⁵³², a CNPD permanece como autoridade de controlo nacional para efeitos do RGPD e da lei de execução do Regulamento. Determina o art. 4.º que a CNPD conserva a natureza de entidade administrativa independente, dotada de personalidade jurídica de direito público com poderes de autoridade, que funciona junto da AR e é administrativa e financeiramente autónoma.

A CNPD, em matéria de proteção de dados pessoais, tem a função de controlar e fiscalizar o cumprimento do previsto no RGPD e na Lei n.º 58/19, de 8 de agosto, para garantir a defesa dos direitos, liberdades e garantias das pessoas singulares no que concerne ao tratamento dos seus dados pessoais.

Em suma, a grande alteração consiste no facto de não existir a obrigatoriedade de autorização prévia, mas de passar agora a deter um papel de fiscalizadora *a posteriori*. No entanto, gostaríamos de notar, que nos casos dos sistemas de videovigilância, quando para instalação no local de trabalho, mantém-se a necessidade de pedido de autorização prévio. Esta situação tem despoletado opiniões⁵³³ que condenam o facto de o legislador nacional não ter revogado a medida, de acordo com o RGPD. Todavia, em nossa opinião, e de acordo com o art. 36.º, n.º 5 do RGPD, os EM podem manter os pedidos de autorização prévios, em casos especiais, pelo que ao tomar esta posição, o legislador

⁵³⁰ Pinheiro, A. e Duarte, T. (2019). In *A videovigilância no Código do Trabalho à luz do RGPD e da Lei Nacional de Execução*. Jornal Público, consultado em 06.03.2020, disponível em: <https://www.publico.pt/2019/10/30/sociedade/opiniao/videovigilancia-codigo-trabalho-luz-rgpd-lei-nacional-execucao-1891769>.

⁵³¹ Cfr. art. 66.º da Lei n.º 58/19, de 08 de agosto.

⁵³² Lei n.º 67/98, de 26 de outubro.

⁵³³ Vide Brito, P. (2019). In *A videovigilância, a Lei Nacional de Execução do RGPD e o Código do Trabalho*, consultado em 06.03.2020, disponível em: <https://www.bas.pt/comunicacao/noticias/a-videovigilancia-a-lei-nacional-de-execucao-do-rgpd-e-o-codigo-do-trabalho/>.

nacional considerou que os trabalhadores necessitam de garantir a proteção contra instalações de sistemas de videovigilância abusivas, pelo empregador, posição que também nós postulamos.

CONCLUSÃO

Estarão as empresas a respeitar a confidencialidade das comunicações e a privacidade dos trabalhadores? Porque continuam então os trabalhadores numa posição tão fragilizada? Quais os limites de ingerência do empregador nas comunicações dos trabalhadores? Podem estas ser monitorizadas a todo o tempo? Quais as repercussões para a relação laboral? O que pode ser mudado na relação laboral? O RGPD e a Lei de execução clarificam a proteção de dados dos trabalhadores? Poderemos vir a assistir a uma mudança de paradigma quando for possível considerar o consentimento como requisito na relação de trabalho? Poderá a CNPD ter uma função mais vigorosa na aplicação de sanções às empresas que violem o estatuído no RGPD? Estas são algumas das questões que tentámos responder e que podem *qui sabit*, ser alvo de uma outra análise futura.

A sociedade tem vivido grandes mudanças e tem assistido a iguais transformações no que concerne às tecnologias de informação no local de trabalho potenciando modificações a nível laboral. Todas estas mudanças, ainda que beneficiando trabalhadores e empregadores, “tem originado novos desafios para os sujeitos laborais e novas questões”⁵³⁴, traduzindo-se num dilema empresarial que urge considerar.

Sendo impensável trabalharmos sem recorrer às tecnologias de informação, através do computador ou de outros dispositivos, é fundamental atentar à proteção da privacidade dos seus utilizadores e dos seus dados, conferida não só pelo direito à autodeterminação informativa, mas também por outros direitos fundamentais, laborais e de *data protection*.

Assim, o nosso estudo primou pela caracterização do direito à privacidade dos trabalhadores. Estes, enquanto pessoas, são assim detentores de direitos de personalidade, por este facto concluímos que se encontram abrangidos por garantias protecionais internacionais, constitucionais e infraconstitucionais. Ao nível legal, consideramos que o nosso ordenamento jurídico é vanguardista na proteção destes direitos, pois os mesmos veem a ser tratados há largos anos.

⁵³⁴ MOREIRA, Teresa Alexandra Coelho, in “*A Privacidade dos Trabalhadores e as Novas Tecnologias de Informação e Comunicação (...)*”, (2010), P. 586.

Seguidamente, e porque com o uso das novas tecnologias de informação existe maior possibilidade de acesso a dados pessoais, enquadrámos o nosso estudo no âmbito do RGPD, tendo-se aferido que este diploma vem somar-se a todos os diplomas legais existentes. O RGPD tem, assim, aplicabilidade nos trabalhadores, pois estes são também titulares de dados pessoais, efetivando [ou devendo efetivar], ainda mais a garantia da privacidade e do sigilo da correspondência.

No entanto, entendemos que em matéria de *data protection* ainda existe um longo caminho a percorrer, *v.g.*, se se pretender ver o consentimento como requisito preponderante, na medida em que, atualmente, o mesmo é superado por razões contratuais, na relação laboral. Ou seja, nunca é opção pedir o consentimento do trabalhador para o tratamento dos seus dados pessoais, pois este tratamento é efetuado ao abrigo da relação contratual. Nesta matéria, consideramos que a Lei n.º 58/19, de 8 de agosto, poderia ter ido mais além, produzindo maiores clarificações à execução do RGPD em Portugal, dedicando mais atenção à definição de prazos de conservação dos dados, matéria que entendemos ser pertinente para: reduzir as dúvidas do trabalhador.

A garantia da privacidade, e do tratamento de dados, pelas empresas relativamente aos trabalhadores, pode ser bem efetivada, sendo para isso muito importante que estejam recetivas a implementar as várias garantias de segurança que a lei determina, tais como: não ingerência na correspondência dos trabalhadores, sem seu conhecimento e consentimento; adoção de medidas técnicas e organizativas que a *data protection* possibilita, aplicando a proteção de dados desde a conceção e por defeito para prevenção do direito à privacidade.

Importa reforçar que sendo impossível trabalhar sem recorrer ao uso de ferramentas informáticas a nível laboral, então e para minimizar violações⁵³⁵, espera-se a criação de um equilíbrio, através da definição de regras concretas e concisas que estabeleçam a forma de utilização das tecnologias de informação pelos trabalhadores. Tais regras devem ser elencadas num regulamento interno, comunicado aos trabalhadores quando iniciam a relação laboral, ou se já no decurso da mesma existam alterações, então deve ocorrer nova comunicação, para que a relação seja transparente.

⁵³⁵ O expectável seria que as mesmas não ocorressem.

De salientar, que caso ocorra monitorização a mesma não seja invasiva, em observância pelo princípio da proibição de excesso, devendo restringir-se ao assunto e nunca ao conteúdo. Defendemos que antes de se aceder se questione o trabalhador sobre as mensagens que suscitem dúvidas, de forma a que estas possam ser clarificadas.

É importante que as empresas, com vista a evitar dilemas relacionados com violações da privacidade ou da correspondência, informem os trabalhadores sobre: como, quando e para que fins pode ser utilizado o correio eletrónico ou outros dispositivos informáticos colocados ao seu dispor pela entidade empregadora, sendo contraproducente um controlo a todo o tempo, pois pode colocar em risco o direito à liberdade de expressão.

Relativamente à captação de imagens e sons, seja por aparelhos de CCTV, seja através de webcam instaladas nos computadores, a monitorização deve ser exercida com moderação, nunca com a finalidade única e exclusiva de controlar a prestação do trabalhador, devendo assentar na questão da segurança de pessoas e bem. A sua implementação deve ser comunicada e publicitada porque além da violação da privacidade podem ser violados dados pessoais. Quanto à divulgação, as empresas devem ponderar quaisquer divulgações de imagens, sem o consentimento do titular dos dados [trabalhador], no qual seja identificado ou possa ser identificável, devendo a videovigilância reger-se pela proteção dos direitos fundamentais dos trabalhadores e dos dados pessoais.

Por outro lado, consideramos que, quando monitorizado, e se verificarem atos ilícitos do trabalhador, devam sim existir sanções. Contudo estas devem ser proporcionais à gravidade do ato cometido. Entendemos que num procedimento disciplinar não deve logo ser aplicada uma “sanção máxima” [entenda-se: o despedimento], mas que a mesma comece num patamar mais baixo e vá “crescendo” caso haja reincidência do trabalhador.

Considerando tudo o explanado neste trabalho, ainda nos questionamos sobre o porquê de existirem tantos litígios laborais por violação a privacidade e do sigilo da correspondência, quando existem diversos diplomas legais que determinam a sua proteção.

REFERÊNCIAS BIBLIOGRÁFICAS

Abrantes, J. J. (2008). *In Algumas notas sobre o direito do trabalhador à reserva da vida privada*. Estudos comemorativos dos 10 anos da Faculdade de Direito da Universidade Nova de Lisboa. Coimbra: Almedina. Vol. 2, p. [241-248] ISBN 978-972-40-3460-7

Albuquerque, P. P. (2008). *In Comentário do Código Penal à Luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem*. Lisboa: Universidade Católica Editora. ISBN: 978-972-54-0220-7

Amado, J. L. (2019). *In Contrato de trabalho: noções básicas*. Coimbra: Edições Almedina. ISBN 978-972-40-8014-7

Araújo, A. M. R. (2017). *In As transferências transatlânticas de dados pessoais*. Revista de Direitos Humanos e Democracia, ano 5, n.º 9, jan/jun

Canotilho, J. J. G. & Moreira, V. (2014). *In Constituição da República Anotada – Vol. I, 4ª edição*. Coimbra: Editora, ISBN 978-972-32-2286-9

Castro, C. S. e (2005). *In Direito da Informática, Privacidade e Dados Pessoais*. Coimbra: Almedina. ISBN 972-40-2424-5

Dias, J. de F. (1999). *In Comentário Conimbricense do Código Penal, Parte Especial, Tomo I, arts. 131.º a 201.º*. Coimbra Editora. ISBN: 972-32-0854-7

Fazendeiro, A. (2018). *In Regulamento Geral sobre a Proteção de Dados Algumas notas sobre o RGPD, 3.ª Edição*. s.l. Edições Almedina. ISBN: 978-972-407-6294

Fuster, Gloria Gonzalez (2017). *In Law, Governance and Technology Series, Issues in Privacy and Data Protection, volume 16*. Springer International Publishing. ISBN 978-3-319-05022-5

Gomes, J. M. V. (2007). *In Direito do Trabalho, Relações Individuais de Trabalho, Vol. I*, Coimbra Editora. ISBN 978-972-32-1482-6

Guerra, A. (2004). *In A privacidade no local de trabalho: as novas tecnologias e o controlo dos trabalhadores através de sistemas automatizados: as alterações do código do trabalho*. Coimbra: Almedina. ISBN 972-402-224-2

Leitão, L. M. T. M. (2019). *In Direito do trabalho, 6ª edição*. Coimbra: Edições Almedina. ISBN: 978-972-40-8090-1

Marques, G. e Martins, L. (2006). *In Direito da Informática, 2.ª edição refundida e atualizada*. Coimbra. Edições Almedina. ISBN: 978-972-40-2859-0

Miranda, J. & Medeiros, R. (2010). *In Constituição Portuguesa Anotada, Tomo I, 2ª edição revista, atualizada e ampliada, art.º 1.º a 79.º*. Coimbra: Editor Wolters Kluwer Portugal sob a marca Coimbra Editora, s.n., ISBN: 978-972-32-1822-0

Moreira, T. A. C. (2004). *In Da Esfera Privada do Trabalhador e o Controlo do Empregador*, Coimbra Editora. ISBN: 972-32-1228-5

Moreira, T. A. C. (2010). *In A privacidade dos trabalhadores e o controlo eletrónico da utilização da Internet, Questões Laborais*. Coimbra, n.º 35/36. ISSN 0872-8267. A.17

Moreira, T. A. C. (2010). *In A Privacidade dos Trabalhadores e as Novas Tecnologias de Informação e Comunicação: contributo para um estudo dos limites do poder de controlo electrónico do empregador*. Teses de doutoramento. s.l. Edições Almedina. ISBN 978-972-40-4208-4

Moreira, T. A. C. (2010). *In As novas tecnologias de informação e comunicação e o poder de controlo electrónico do empregador*. Scientia Iuridica. Braga. Universidade do Minho, tomo 59, n.º 323, pp. 553-579. ISSN: 0870-8185

Moreira, T. A. C. (2016). *In O direito à desconexão dos trabalhadores*. Questões Laborais, n.º 49, pp. 7-28. Coimbra. ISSN: 0872-8267. A.23

Moreira, T. A. C. (2017). *In Breve comentário à decisão do TEDH, de 5 de setembro de 2017 – Barbulescu v. Romania*. Prontuário de Direito do Trabalho, n.º 2, pp. 143-158. ISSN 0873-4895

Neves, R. C. (2011). *In As ingerências nas comunicações electrónicas em processo penal*. 1.ª Edição, Coimbra: Coimbra Editora grupo Wolters Kluwer. ISBN 978-972-321-942-5

Pinheiro, A. S. (2015). *In Privacy e proteção de dados pessoais: a construção dogmática do direito à identidade informacional*. Tese de doutoramento. Lisboa: AAFDL- Associação Académica da Faculdade de Direito de Lisboa, ISBN 5606939008169

Pinheiro, A. S. (Coord.) (2018). *In Comentário ao Regulamento Geral de Proteção de Dados*, s.l.: Edições Almedina; ISBN 978-972-40-7786-4

Porto, M. L. e Anastácio. G. (2012). *In Tratado de Lisboa, Anotado e Comentado*. Coimbra. Edições Almedina. ISBN: 978-972-40-4613-6

Quintas, P. & Quintas, H. (2016). *In Código do Trabalho Anotado e Comentado*” 4ª edição, s.l.: Editora: Almedina, ISBN: 978-972-40-6757-5

Rodrigues, B. S. (2009). *In Das Escutas Telefónicas À obtenção da prova (em ambiente) digital - Tomo II, 2ª Edição Revista, Atualizada e Aumentada* Coimbra: Editora, ISBN: 978-989-95779-2-3

Rueda Martín, M. Á. (2004). *In Protección penal de la intimidad personal e informática: los delitos de descubrimiento y revelación de secretos de los artículos 197 y 198 del código penal*. Barcelona: Atelier. ISBN 849-315-106-8

Vasconcelos, P. P. (2017). *In Direito de Personalidade*. Coimbra. Edições Almedina. ISBN: 972-40-2994-8

JURISPRUDÊNCIA

Tribunal Europeu dos Direitos do Homem

Application n.º. 61496/008 *Barbulescu v Romania*, de 12 de janeiro de 2016, consultado em: 15.10.2018, disponível em: [https://hudoc.echr.coe.int/eng#{%22fulltext%22:\[%22barbulescu%22\],%22sort%22:\[%22kdate%20Descending%22\],%22documentcollectionid%22:\[%22JUDGMENTS%22\],%22itemid%22:\[%22001-159906%22\]}](https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22barbulescu%22],%22sort%22:[%22kdate%20Descending%22],%22documentcollectionid%22:[%22JUDGMENTS%22],%22itemid%22:[%22001-159906%22]})

Application n.º. 61496/008 *Barbulescu v Romania*, de 05 de setembro de 2017, consultado em: 15.10.2018, disponível em: [https://hudoc.echr.coe.int/eng#{%22fulltext%22:\[%22barbulescu%22\],%22sort%22:\[%22kdate%20Descending%22\],%22documentcollectionid%22:\[%22JUDGMENTS%22\],%22itemid%22:\[%22001-177082%22\]}](https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22barbulescu%22],%22sort%22:[%22kdate%20Descending%22],%22documentcollectionid%22:[%22JUDGMENTS%22],%22itemid%22:[%22001-177082%22]})

Applications nos. 1874/13 *and* 8567/13 *López Ribalda and Others v. Spain*, de 17 de outubro de 2019, consultado em: 02.04.2020, disponível em: [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-197098%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-197098%22]})

Supremo Tribunal de Justiça

Processo n.º 07S043, de 05 de julho de 2017. Relator: MJD Mário Pereira, consultado em: 17.01.2020, disponível em: <http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/54d3c9f0041a33d58025735900331cc3>

Processo n.º 73/12.3TTVNF.P1.S1, de 13 de novembro de 2013. Relator: MJD Mário Belo Morgado, consultado em: 15.03.2019, disponível em: <http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/e32eab3444364cb980257c2300331c47?OpenDocument>

Processo n.º 296/17.9T8FAR.E1.S1, de 06 de março de 2019. Relator: MJD Leones Dantas, consultado em: 04.01.2020, disponível em: https://www.stj.pt/wp-content/uploads/2019/06/sum_acor_social_marco_2019.pdf

Tribunal da Relação de Coimbra

Processo n.º 359/13.0TTFIG-A.C1, de 06 de fevereiro de 2015. Relator: MJD Azevedo Mendes, consultado em: 15.03.2019, disponível em: <http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/fe545bb508b68e6980257dee004bf0bd?OpenDocument>

Tribunal da Relação de Évora

Processo n.º 244/17.6T8PTM.E1, de 06 de dezembro de 2017. Relator: MJD Moisés Silva, consultado em: 05.01.2020, disponível em: <http://www.dgsi.pt/jtre.nsf/-/DC3C8C21D1195564802581FD003421B6>

Processo n.º 747/18.5T8PTM.E1, de 28 de março de 2019. Relator: MJD Paula d Paço, consultado em: 15.01.2020, disponível em: <http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/55801c7296f02f54802583d90052c54c?OpenDocument&Highlight=0,whatsapp>

Tribunal da Relação de Guimarães

Processo n.º 15/11.3TTVRL.G1, de 11 de junho de 2015. Relator: MJD Antero Veiga, consultado em: 15.03.2019, disponível em: <http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/602f7d06304fc8bc80257eb20036e5fe?OpenDocument>

Processo n.º 20/14.7T8VRL.G1, de 03 de março de 2014. Relatora: MJD Manuela Fialho, consultado em: 15.03.2019, disponível em: <http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/302fdd824b16519780257f85004f8071?OpenDocument&Highlight=0,correspond%C3%Aancia,trabalhador>

Tribunal da Relação de Lisboa

Processo n.º 2970/07.4, de 05 de junho de 2008. Relator: MJD Leopoldo Soares, consultado em: 04.11.2019, disponível em:

<http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/6c195267c4ce32e480257474003464f7?OpenDocument>

Processo n.º 24163/09.0T2SNT.L1-4 de 07 de março de 2012. Relator: MJD José Eduardo Sapateiro, consultado em: 22.10.2018, disponível em:

<http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/109499c90995e66d802579bf0050cfa4?OpenDocument>

Processo n.º 2330/16.0T8LSB-4, de 25 de janeiro de 2017. Relator: MJD Leopoldo Soares, consultado em: 04.11.2019, disponível em:

<http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/a2a6b4fcf4d104af802580cd00373bc7?OpenDocument>

Processo n.º 23019/16.5T8LSB.L1-8, de 23 de fevereiro de 2017. Relator: MJD Isoleta Almeida Costa, consultado em: 04.11.2019, disponível em: <http://www.dgsi.pt/jtrl.nsf/-/26988FB6EF65C551802580DF0034F791>

Processo n.º 15070/18.T8LSB.L1-4, de 11 de julho de 2019. Relator: MJD Filomena Manso, consultado em: 05.11.2019, disponível em:

<http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/974eaa48f5719bc3802584390032b39f?OpenDocument>

Tribunal da Relação do Porto

Processo n.º 787/10.2TTVCT.P1, de 04 de março de 2013. Relator: MJD Ferreira da Costa Consultado em: 15.03.2019, disponível em:

<http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/b655a445dc93958780257b340054d89c?OpenDocument&Highlight=0,teresa,coelho,moreira>

Processo n.º 101/13.5TTMTS.P1, de 08 de setembro de 2014. Relatora: MJD Maria José Costa Pinto, consultado em: 15.03.2019, disponível em: <http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/917c9c56c1c2c9ae80257d5500543c59?OpenDocument>

Processo n.º 68/14.2TTMTS.P1, de 01 de fevereiro de 2016. Relatora: MJD Fernanda Soares, consultado em: 05.11.2019, disponível em: <https://dre.pt/pesquisa-avancada/-/asearch/104279975/details/maximized?emissor=Tribunal+da+Rela%C3%A7%C3%A3o+do+Porto&perPage=100&types=JURISPRUDENCIA&search=Pesquisar>

Processo n.º 276/13.3TTSTS.P1, de 15 de fevereiro de 2016. Relator: MJD Jorge Loureiro, consultado em: 05.11.2019, disponível em: <https://dre.pt/web/guest/pesquisa/-/search/104284775/details/maximized?perPage=100&sort=whenSearchable&sortOrder=DESC&q=valor%2Fen%2Fen>

Processo n.º 208/14.1TTVFR-D.P1, de 15 de dezembro de 2016. Relatora: MJD Paula Leal de Carvalho, consultado em: 05.11.2019, disponível em: <http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/df89d957d1942212802580a70058cc70?OpenDocument>

Processo n.º 6909/16.2T8PRT.P1, de 26 de junho de 2017. Relator: MJD Jerónimo Freitas, consultado em: 05.01.2020, disponível em: <http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/213e51a9c28137de80258169003b373d?OpenDocument>

Processo n.º 159/18.0T8PNF-A.P1, de 07 de dezembro de 2018. Relator: MJD Domingos Morais, consultado em: 15.03.2019, disponível em: <http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/cc2a4b78e8ec279d8025839800517f79?OpenDocument>

ARTIGOS ELETRÓNICOS

António, I. (2016). *In O Direito Fundamental do Trabalhador à confidencialidade das Comunicações Eletrónicas no Contexto Laboral e o Despedimento Com Justa Causa (?)*. *In Transformações recentes do Direito do Trabalho Ibérico, Livro Razão*, CIJE – Centro de Investigação Jurídico Económica, Faculdade de Direito do Porto. Consultado em: 23.11.2019, disponível em: https://sigarra.up.pt/fdup/pt/web_gessi_docs.download_file?p_name=F1854330697/Livro_Razao.pdf

Brito, P. (2019). *In A videovigilância, a Lei Nacional de Execução do RGPD e o Código do Trabalho*, consultado em 06.03.2020, disponível em: <https://www.bas.pt/comunicacao/noticias/a-videovigilancia-a-lei-nacional-de-execucao-do-rgpd-e-o-codigo-do-trabalho/>

Cavoukian, A (2011). *In Privacy by Design The 7 Foundational Principles*, consultado em 07.02.2020, disponível em: <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>

Carvalho, P. M. (2013). *In Conferência Estado de direito e direitos fundamentais: A concretização dos direitos fundamentais pelos tribunais*. Julho, Assembleia da República, consultado em: 04.11.2019, disponível em: http://www.cej.mj.pt/cej/estudos-e-publica/fich-pdf/conferencias/Conferencia_CACDLG-CEJ.pdf

CNPD. (2002). *Princípios sobre a privacidade no local de trabalho*, consultado em 15.03.2020, disponível em <https://www.cnpd.pt/home/orientacoes/PRINCIPIOS-controloE-mails-telefones-Internet.pdf>

CNPD. (2004). Deliberação n.º 61/ 2004. *Orientação: os princípios sobre o tratamento de dados por videovigilância*. consultado em 25.03.2020, disponível em: <https://www.cnpd.pt/home/orientacoes/DEL61-2004-VIDEOVIGILANCIA.pdf>

CNPD. (2013). Deliberação n.º 1638/2013. *Orientações sobre tratamento dados pessoais decorrentes do controlo da utilização para fins privados das tecnologias de informação e comunicação em contexto laboral*. consultado em 15.03.2020, disponível em: https://www.cnpd.pt/home/orientacoes/Delib_controlo_comunic.pdf

CNPD. (2019). Deliberação n.º 2019/494 sobre a Lei n.º 58/19, de 08 de agosto, consultado em 06.03.2020, disponível em https://www.cnpd.pt/home/decisoies/Delib/DEL_2019_494.pdf

Dray, G. (2019). *In Direitos Fundamentais e de Personalidade do Trabalhador*, 3.ª Edição, Centro de Estudos Judiciários (CEJ), Jurisdição do Trabalho e da Empresa, consultado em 23.11.2019, disponível em: http://www.cej.mj.pt/cej/recursos/ebooks/trabalho/eb_DireitoPersonalidade2019.pdf?id=9&username=guest

Festas, D. O. (2004). *In O direito à reserva da intimidade da vida privada do trabalhador no Código do Trabalho*. Revista da Ordem dos Advogados, ano 64, Vol. I/II, consultado em: 17.03.2019, disponível em: <https://portal.oa.pt/comunicacao/publicacoes/revista/ano-2004/ano-64-vol-i-ii-nov-2004/artigos-doutrinais/david-de-oliveira-festas-o-direito-a-reserva-da-intimidade-da-vida-privada-do-trabalhador-no-codigo-do-trabalho-star/>

Grupo de Trabalho do Artigo 29.º (2004). *Parecer 4/2004 sobre o Tratamento de Dados Pessoais por meio de Videovigilância*. WP89, consultado em: 06.03.2020, disponível em: <https://www.gpdp.gov.mo/uploadfile/2014/0505/20140505071008284.pdf>

Grupo de Trabalho do Artigo 29.º (2007). *Orientações sobre o conceito de dados pessoais*. WP136, consultado em: 06.10.2019, disponível em: https://ec.europa.eu/justice/article-29/documentation/opinionrecommendation/files/2007/wp136_pt.pdf

Grupo de Trabalho do Artigo 29.º (2011). *Orientações sobre o consentimento*. WP187, consultado em: 25.01.2020, disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf

Grupo de Trabalho do Artigo 29.º (2017). *Opinion 2/2017 on data processing at work*. WP249, consultado em: 06.10.2019, disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169

Grupo de Trabalho do Artigo 29.º (2018). *Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679*. WP251 ver.01., consultado em: 07.02.2020, disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

Grupo de Trabalho do Artigo 29.º (2018). *Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679*. WP259 rev.01., consultado em 01.02.2020, disponível em: https://www.cnpd.pt/bin/rgpd/docs/wp259rev0.1_PT.pdf

Kranenborg, H. (2014). *In The EU Charter of Fundamental Rights, A commentary*. Edit Steve Peers et. Al., Hart Publishing, consultado em 26.12.2019, disponível em: https://books.google.pt/books?id=htOdBQAAQBAJ&pg=PA235&lpg=PA235&dq=herke+kranenborg+,+art.+8&source=bl&ots=FFUC7mCIJ9&sig=ACfU3U0yjmuE7PE0kdFzOobev_1CkFHkOQ&hl=ptPT&sa=X&ved=2ahUKEwjChrmE9djmAhWhx4UKHXtDDH4Q6AEwAXoECAgQAQ#v=onepage&q=herke%20kranenborg%20%2C%20art.%208&f=false

Lopes, S. (2014). *In Direitos Fundamentais e de Personalidade do Trabalhador*, 2ª edição, Centro De Estudos Judiciários (CEJ), consultado em 06.07.2019, disponível em: http://www.cej.mj.pt/cej/recursos/ebooks/trabalho/eb_DireitoPersonalidade2019.pdf?id=9&username=guest

Lopes, S. (2019). *In Direitos Fundamentais e de Personalidade do Trabalhador*, 3ª edição, Centro De Estudos Judiciários (CEJ), consultado em 23.11.2019, disponível em: http://www.cej.mj.pt/cej/recursos/ebooks/trabalho/Direitos_fundamentais_e_de_personalidade_do_trabalhador_2ed_mar2014.pdf

Martins, J. Z. (2016). *In Comentário ao acórdão do Tribunal Europeu dos Direitos do Homem, Barbulescu contra a Roménia, de janeiro de 2016, proc. 61496/08*. Revista do Ministério Público 145: Janeiro - Março 2016 [pp. 177-205], consultado em: 10.03.2019, disponível em: http://rmp.smmp.pt/wp-content/uploads/2016/04/7.RMP_145_Joao_Zenha_Martins.pdf

Mota, J. (2018). *In O consentimento no Regulamento Geral sobre a Proteção de Dados*, InforBanca, n.º 112, Fevereiro, consultado em: 25.01.2020, disponível em: <https://ifb.pt/wp-content/uploads/2018/04/IFB-InforBanca-112-Fev18.pdf>

Moreira, T. A. C. (2012). *In Novas Tecnologias: Um Admirável Mundo Novo do Trabalho?* Revista de Direitos e Garantias Fundamentais, Vitória, n. 11, p. 15-52, jan./jun. 2012, consultado em: 15.03.2019, disponível em: <http://sisbib.emnuvens.com.br/direitosegarantias/article/view/209>
<http://dx.doi.org/10.18759/rdgf.v0i11.209>

Pinheiro, A. e Duarte, T. (2019). *In A videovigilância no Código do Trabalho à luz do RGPD e da Lei Nacional de Execução*. Jornal Público, consultado em 06.03.2020, disponível em: <https://www.publico.pt/2019/10/30/sociedade/opiniao/videovigilancia-codigo-trabalho-luz-rgpd-lei-nacional-execucao-1891769>

Rallo, A. (2018). *In Privacy and Freedom, European Data Protection Law Review*, n.º 4, 2, consultado em 04.11.2019, disponível em: https://edpl.lexxion.eu/data/article/12795/pdf/edpl_2018_02-006.pdf;
DOI: <https://doi.org/10.21552/edpl/2018/2/5>

Ramalho, M. R. P, Carvalho, P. M. (2013). *Conferência Estado De Direito E Direitos Fundamentais: A Concretização Dos Direitos Fundamentais Pelos Tribunais. In Colóquios e Conferências Parlamentares*, consultado 10.03.2019, disponível em: http://www.cej.mj.pt/cej/estudos-epublica/fichpdf/conferencias/Conferencia_CACDLG-CEJ.pdf

Warren, S. D. & Brandeis, L. D. (1890) *In The Right to Privacy*, Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220 disponível em: <https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>

PÁGINAS ELETRÓNICAS

Assembleia da República (Proposta de Lei n.º 120/XIII), consultado em 04.11.2019, disponível em:

<https://www.parlamento.pt/AtividadeParlamentar/Paginas/DetalleIniciativa.aspx?BID=42368>

Assembleia da República. Debates parlamentares, consultado em: 23.11.2019, disponível em:

<http://debates.parlamento.pt/catalogo/r3/dar/s2a/13/03/107/2018-05-02/100?pgs=89-103&org=PLC&plcdf=true>

Comissão Nacional de Proteção de Dados, consultado em 11.10.2019, disponível em:

<https://www.cnpd.pt/bin/cnpd/historia.htm>

Grupo de Trabalho do Artigo 29.º:

http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358

Parlamento. Iniciativa. A proposta de lei

<http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c324679595842774f6a63334e7a637664326c756157357059326c6864476c3259584d7657456c4a535339305a58683062334d76634842734d5449774c56684a53556b755a47396a&fich=ppl120-XIII.doc&Inline=true>