



# **A proteção de dados em contexto laboral: a necessidade do consentimento do trabalhador**

Mestrado em Solicitadoria de Empresa

Ana Rafaela Marto Saragoça

Leiria, abril de 2020

*Esta página foi intencionalmente deixada em branco*



# **A proteção de dados em contexto laboral: a necessidade do consentimento do trabalhador**

Mestrado em Solicitadoria de Empresa

Ana Rafaela Marto Saragoça

Dissertação realizada sob a orientação da Professora Doutora Ana Lambelho.

Leiria, abril de 2020



*Esta página foi intencionalmente deixada em branco*

# **Originalidade e Direitos de Autor**

A presente dissertação é original, elaborada unicamente para este fim, tendo sido devidamente citados todos os autores cujos estudos e publicações contribuíram para a elaborar.

Reproduções parciais deste documento serão autorizadas na condição de que seja mencionada a Autora e feita referência ao ciclo de estudos no âmbito do qual a mesma foi realizada, a saber, Curso de Mestrado em Solicitadoria de Empresa, no ano letivo 2018/2019, da Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria, Portugal, e, bem assim, à data das provas públicas que visaram a avaliação destes trabalhos.

*Esta página foi intencionalmente deixada em branco*

# Agradecimentos

*Aos meus pais,*

Por todo o apoio e motivação.

*Ao Fábio,*

Por acreditar em mim.

*À Doutora Ana Lambelho,*

Por toda a ajuda.

*Esta página foi intencionalmente deixada em branco*

# Resumo

A presente dissertação tem como objetivo estudar o consentimento enquanto fundamento do tratamento dos dados pessoais do trabalhador na relação de trabalho.

A questão, embora não seja nova, ganhou acuidade com a entrada em vigor do RGPD e, posteriormente, com a Lei n.º 58/2019, de 08 de agosto.

Para atingir o objetivo a que nos propusemos, dividimos a presente dissertação em dois capítulos.

No primeiro capítulo fizemos uma breve exegese pelos diplomas legais, nacionais e internacionais, que regulam os direitos de personalidade do trabalhador, por forma a enquadrarmos a temática do consentimento que explorámos, no capítulo seguinte.

No segundo capítulo, analisámos diversos cenários do quotidiano da relação laboral, desde a celebração do contrato de trabalho, até à sua cessação, visando identificar o fundamento mais adequado a utilizar, em cada situação, para o tratamento dos dados e, em particular, se o consentimento o poderia ser. A questão do consentimento, enquanto fundamento legitimador do tratamento de dados na relação laboral, é particularmente sensível em virtude da especial relação de subordinação em que o trabalhador se encontra, o que impede, na maioria das vezes, um consentimento livre e esclarecido.

Por assim ser, depois de analisarmos várias situações em que se impõe ao empregador o tratamento de dados do trabalhador, e de averiguarmos qual é, no caso, o fundamento para o seu tratamento, concluímos que, em princípio, o consentimento não é fundamento bastante para o tratamento de dados pessoais do trabalhador.

**Palavras-chave:** “dados pessoais”, “consentimento” e “trabalhadores”.

*Esta página foi intencionalmente deixada em branco*

# Abstract

The purpose of this dissertation is to study consent as a basis for the treatment of the personal data of the worker in the employment relationship.

The issue, although not new, gained acuity with the strong entry of the GDPR and, subsequently, with law n° 58/2019 of August 8.

In order to achieve the objective, we set ourselves, we decided to divide this dissertation into two chapters.

In the first one, we did a brief exegesis on the legal, national and international diplomas which regulate the worker's personality rights in order to frame the theme of consent explored in the next chapter.

In the second chapter, we analyzed different scenarios of the daily life of the employment relationship, from the conclusion of the employment contract, until its termination, aiming to identify the most adequate basis to use, in each situation, for the treatment of data and, in particular if consent could be one of the criterion.

The issue of consent as a legitimate basis for data processing in the employment relationship is particularly sensitive due to the special subordination relationship in which the worker finds himself, which prevents, in most cases, free and informed consent.

So, after analyzing several situations in which data processing of the worker is imposed on the employer, and finding out what, in this case, is the basis for its treatment, we conclude that, in principle, consent is not a sufficient basis for the processing of the employee's personal data.

**Keywords:** “personal data”, “consent” and “workers”

*Esta página foi intencionalmente deixada em branco*

# Índice

|   |             |
|---|-------------|
| <b>Originalidade e Direitos de Autor .....</b>  | <b>iii</b>  |
| <b>Agradecimentos .....</b>   | <b>v</b>    |
| <b>Resumo .....</b>   | <b>viii</b> |
| <b>Abstract .....</b>   | <b>ix</b>   |
| <b>Lista de siglas e acrónimos .....</b>  | <b>xiv</b>  |
| <b>1. Introdução.....</b>   | <b>1</b>    |
| <b>Capítulo 1. Os direitos de personalidade e os dados pessoais dos trabalhadores.....</b>  | <b>3</b>    |
| <b>1. Delimitação e concretização dos conceitos .....</b>   | <b>3</b>    |
| <b>2. Enquadramento Legal .....</b>   | <b>9</b>    |
| 2.1. A proteção constitucional.....   | 9           |
| 2.2. O Código Civil .....   | 17          |
| 2.3. O Regulamento Geral da Proteção de Dados .....   | 22          |
| 2.3.1. Das Diretivas ao Regulamento.....  | 22          |
| 2.3.2. Princípios orientadores do tratamento de dados.....  | 29          |
| 2.4. O Código do Trabalho.....  | 34          |
| 2.5. Outros instrumentos de Direito Internacional .....   | 46          |
| <b>Capítulo 2. O consentimento do trabalhador na utilização dos dados pessoais .....</b>  | <b>49</b>   |
| <b>1. Os problemas gerais do consentimento do trabalhador como requisito de licitude do tratamento.....</b>                       | <b>53</b>   |
| <b>2. Os casos de desnecessidade do consentimento do trabalhador para o tratamento de dados pessoais .....</b>                    | <b>59</b>   |
| <b>3. Os casos em que o consentimento do trabalhador constitui base legítima para o tratamento de dados pelo empregador .....</b> | <b>75</b>   |
| <b>Conclusão .....</b>  | <b>84</b>   |
| <b>Bibliografia .....</b>   | <b>87</b>   |
| <b>Jurisprudência.....</b>  | <b>91</b>   |

*Esta página foi intencionalmente deixada em branco*

## Lista de siglas e acrónimos

|             |   |
|-------------|---|
| Ac.         | Acórdão   |
| Al.         | Alínea  |
| Art.        | Artigo  |
| Arts.       | Artigos   |
| CC          | Código Civil  |
| CNPD        | Comissão Nacional de Proteção de Dados                    |
| CEDH        | Convenção Europeia dos Direitos do Homem                  |
| Cfr.        | Confrontar  |
| CRP         | Constituição da República Portuguesa                      |
| CT          | Código do Trabalho  |
| DUDH        | Declaração Universal dos Direitos do Homem                |
| EDBP        | Comité Europeu para a Proteção de Dados                   |
| <i>e.g.</i> | <i>exempli gratia</i>                                     |
| FRA         | <i>European Union Agency for Fundamental Rights</i>       |
| GT29°       | Grupo do Artigo 29°                                       |
| IAPP        | <i>International Association of Privacy Professionals</i> |
| LPDP        | Lei da Proteção de Dados Pessoais                         |
| n.º         | Número  |
| n.ºs        | Números   |
| NIF         | Número de Identificação Fiscal                            |
| NTIC        | Novas Tecnologias de Informação e Comunicação             |
| PE          | Parlamento Europeu  |
| RGPD        | Regulamento Geral de Proteção de Dados                    |
| RH          | Recursos Humanos  |
| STJ         | Supremo Tribunal de Justiça                               |
| TC          | Tribunal Constitucional                                   |
| T.R.        | Tribunal da Relação                                       |
| <i>v.g.</i> | <i>verbi gratia</i>                                       |

*Esta página foi intencionalmente deixada em branco*



# 1. Introdução

O século XXI surgiu acompanhado de desenvolvimentos e grandes mudanças na sociedade, especialmente no que toca ao tema das novas tecnologias. Esta tecnologia avançada traduziu-se numa especial ajuda ao nível da ciência e da saúde. Contudo, conduziu também ao aparecimento de consequências negativas para os indivíduos.

Pese embora sejam visíveis as vantagens de termos uma sociedade conectada apenas através de um clique, não podemos esquecer que surgiu com esta conexão a facilidade de acesso às informações pessoais de cada indivíduo, seja através de redes sociais, seja através dos dispositivos eletrónicos (que constituem também instrumentos de trabalho) que, para funcionarem, necessitam de aceder àquelas informações.

De facto, com as NTIC surgem vários instrumentos informáticos capazes de ameaçar a privacidade das pessoas em geral, e dos trabalhadores em especial.

A reflexão de Teresa Moreira funciona brilhantemente como uma introdução ao tema, quando assevera que “esta situação levanta um verdadeiro e quase insolúvel desafio à privacidade já que através destas inovações tecnológicas é possível efetuar, quase de forma ilimitada, a recolha e o tratamento de informações pessoais (...) a que acresce a circulação informacional em moldes quase inimagináveis” (Moreira, 2011a), p. 12).

Com a realidade a apresentar “hoje novos riscos, novas ameaças para a privacidade, a identidade e a liberdade pessoais, renovando questões jurídicas tradicionais em contextos, mas também colocando questões, novos desafios ao Direito” (Calvão, 2018, pp. 21-22), cabe agora aos juristas ajustarem-se à realidade das inovações, não sendo exceção o caso do Direito Laboral.

Com o suprarreferido, pareceu-nos de grande relevância abordar o tema da proteção de dados em contexto laboral, especialmente a necessidade do consentimento do trabalhador para a análise e recolha dos seus dados, tema que tem vindo a originar questões, particularmente após a aprovação do novo RGPD, devido à possibilidade de provocar uma violação dos direitos de personalidade dos trabalhadores.

Propomos, com o nosso trabalho, responder à questão da necessidade, ou não, do consentimento do trabalhador para o tratamento dos seus dados pessoais, em diversos casos do quotidiano deste, enquanto tal. Ou seja, pretendemos identificar as situações em que o consentimento é o fundamento para que o empregador possa tratar os dados pessoais do trabalhador e, bem assim, aquelas outras em que o não é.

Dessarte, o plano de trabalho desta dissertação iniciou-se com a apresentação do tema e, posteriormente, com o período de investigação e análise, que se revelou de grande dificuldade por ser um tema muito recente, não havendo estudos na área, sendo, portanto, a doutrina e a jurisprudência escassas.

Fazemos uma ressalva de que nem sempre nos foi possível recorrer às edições mais recentes da bibliografia utilizada, porquanto, em virtude das restrições à circulação e funcionamento dos serviços, impostas na sequência da pandemia Covid-19, o acesso às bibliotecas e outras instituições afins, onde poderíamos obter bibliografia mais recente, foi impossível.

# Capítulo 1. Os direitos de personalidade e os dados pessoais dos trabalhadores

## 1. Delimitação e concretização dos conceitos

“O conceito de proteção de dados foi criado, na Europa, para delimitar a informação relativa a uma pessoa singular identificada ou identificável e, assim, delimitar o objeto de boa parte da ação dos instrumentos tecnológicos”. (Calvão, 2018, p. 19)

A LPDP transpôs para a ordem jurídica portuguesa a Diretiva n.º 95/46/CE, do PE e do Conselho, 24/10/95 e define, no art. 3º, al. a), dados pessoais como “qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável ('titular dos dados'); é considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social”.

Esta Diretiva foi revogada pelo Regulamento (UE) 2016/679 do PE e do Conselho, de 27 de abril de 2016, designado comumente por RGPD.

O RGPD, no seu n.º 1 do art. 4º, veio modificar ligeiramente a anterior definição prevista da Diretiva, considerando os dados pessoais como a “informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular”.

O Grupo do Artigo 29º, doravante designado por GT29<sup>1</sup>, no Parecer 4/2007<sup>2</sup>, classifica o conceito de dados pessoais que consta na Diretiva 95/46/CE, de 24 de outubro, baseado em quatro elementos: a) “qualquer informação”; b) “relativa a”; c) “identificada ou identificável” e d) “pessoa singular”.

Quanto ao primeiro conceito, “qualquer informação”, este suscita uma interpretação ampla, abrangendo tanto a informação objetiva, como subjetiva (veja-se o exemplo de opiniões ou avaliações de terceiros sobre a pessoa), disponível em qualquer formato, incluindo eletronicamente (tratamento automatizado). Da perspetiva do conteúdo da informação, o conceito de dados pessoais inclui não só os “dados sensíveis”, previstos no art. 9.º do RGPD e que incidem sobre esfera da vida privada e familiar da pessoa *stricto sensu*, mas também informações mais gerais, ou seja, qualquer tipo de atividade realizada pela pessoa.

O considerando 14 do RGPD acrescenta que “tendo em conta a importância do desenvolvimento que, no âmbito da sociedade de informação, sofrem atualmente as técnicas de captação, transmissão, manipulação, gravação, conservação ou comunicação de dados de som e de imagem relativos às pessoas singulares, há que aplicar a presente diretiva ao tratamento desses dados”.

No mesmo sentido, Catarina Castro admite que “constituirão dados pessoais, toda a informação, seja ela numérica, alfabética, gráfica, fotográfica, acústica ou de qualquer outro tipo, relativa a uma pessoa física identificada ou identificável” (Castro, 2005, p. 71).

Os dados biométricos do trabalhador assumem agora, claramente, a natureza de dados pessoais, definidos pelo RGPD como os “dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos” – art. 4º, definição XIX.

---

<sup>1</sup> Este Grupo de Trabalho era um órgão consultivo composto por um representante da autoridade de proteção de dados de cada Estado-Membro da UE, da Autoridade Europeia para a Proteção de Dados e da Comissão Europeia, criado pelo Artigo 29.º da Diretiva 95/46/EC do Parlamento Europeu e do Conselho, que lidou com as questões relacionadas com a proteção de dados pessoais e da privacidade até 25 de maio de 2018; após a data mencionada precedentemente, o Grupo do Artigo 29 deixou de existir e foi substituído pelo Comité Europeu para a Proteção de Dados (EDPB).

<sup>2</sup> Documento disponível em [https://www.gdpd.gov.mo/uploadfile/others/wp136\\_pt.pdf](https://www.gdpd.gov.mo/uploadfile/others/wp136_pt.pdf)

De acordo com o GT29º, consideram-se dados biométricos as “propriedades biológicas, características fisiológicas, traços físicos ou ações reproduzíveis, na medida em que essas características e/ou ações sejam simultaneamente únicas a essa pessoa e mensuráveis, mesmo que os padrões utilizados na prática para medi-las tecnicamente envolvam um certo grau de probabilidade” (GT29º, 2007, p. 9).

Significa isto que os dados biométricos assumem um carácter duplo, pois fornecem informação sobre o corpo humano e permitem uma identificação clara e única da pessoa. São, em termos gerais, considerados “identificadores” por gozarem de um elo único com uma determinada pessoa, que possibilita a sua identificação, sendo exemplos as impressões digitais ou outros dados de ADN que proporcionam informação sobre o corpo humano.

Fernández Orrico afirma que “*una clasificación doctrinal de la naturaleza de los datos biométricos sería la que los distingue entre aquellos que se caracterizan por ser más estáticos, que tienen que ver con los rasgos fisiológicos y que más han avanzado desde el punto de vista tecnológico*” (Orrico, 2020, p. 304), motivo porque o seu estudo se foi tornando tão relevante ao longo dos tempos.

Quanto ao segundo pressuposto, “relativa a”, a informação considera-se como “relativa” a uma pessoa quando é sobre essa pessoa. É relativamente fácil estabelecer essa conexão no caso do trabalhador: basta pensar nos dados “relativos” à situação do trabalhador que o departamento de RH da empresa dispõe, como é o exemplo dos registos médicos.

Este elemento desempenha um papel crucial na determinação do âmbito material do conceito. Neste ponto, há uma dificuldade de determinar se os dados são pessoais quando a informação veiculada pelos dados está relacionada com objetos e não com pessoas. De acordo com o GT29º (2007, pp. 10-11) que referimos anteriormente, nestes casos recorre-se a um de três elementos para determinar se uma informação é relativa a uma pessoa - conteúdo, finalidade ou resultado.

O conteúdo está preenchido quando se dá informação sobre determinada pessoa, independentemente do fim que o responsável pelo tratamento lhe quer empregar ou do impacto que essa informação possa causar na pessoa em causa. Quanto à finalidade, os dados são “relativos” a determinada pessoa quando são usados com a finalidade de avaliar, tratar ou influenciar o estatuto ou o comportamento desta. Os dados podem ser

considerados também como “relativos” a uma pessoa, quando o seu uso cause um resultado de impacto nos direitos e interesses dessa determinada pessoa, levando a tratamento de forma diferente por parte de terceiros.

Quanto ao terceiro elemento, pessoa “identificada ou identificável”, considera-se “identificada” quando, de entre um grupo de pessoas, se distingue de todos os outros; é “identificável” quando, apesar da pessoa ainda não ter sido identificada, é possível fazê-lo. A identificação pode ser feita de forma direta (sendo o exemplo mais comum, o nome) ou indireta (quando se obtém a identidade através de informações combinadas). Regra geral, as informações detêm um caráter especial e único relativo à pessoa em causa.

Este elemento preocupa-se com as condições ao abrigo das quais uma pessoa possa ser considerada identificável, sobretudo nos meios suscetíveis de serem razoavelmente utilizados pelo responsável pelo tratamento, ou por terceiro, na identificação da pessoa. Neste sentido, podemos ter em conta o considerando 26 do RGPD: “para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica”.

Segundo o mesmo considerando suprarreferido, os dados pessoais que tenham sido pseudonimizados, que possam ser atribuídos a uma pessoa singular mediante a utilização de informações suplementares, deverão ser considerados informações sobre uma pessoa singular identificável. A pseudonimização ajuda a reduzir os riscos para os titulares de dados em questão e ajuda os responsáveis pelo tratamento e os seus subcontratantes a cumprir as suas obrigações de proteção de dados (considerando 28 do RGPD).

Por fim, quanto à expressão “pessoa singular”, é imediatamente utilizada nos considerandos 1 e 2 do RGPD quando relatam que “a proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental”, dados pessoais que “deverão respeitar, independentemente da nacionalidade ou do local de residência dessas pessoas, os seus direitos e liberdades fundamentais, nomeadamente o direito à proteção dos dados pessoais”.

Uma última questão prende-se com a possibilidade de o pseudónimo constituir um dado identificável. O pseudónimo é um nome fictício, usado por um indivíduo como

alternativa ao seu nome legal, e que visa camuflar a sua identidade, permitindo, contudo, recolher dados relativos à pessoa em causa.

O GT29º responde que:

“os dados sob pseudónimo reidentificáveis podem ser considerados como informação sobre pessoas que são indiretamente identificáveis. De facto, utilizar um pseudónimo significa que é possível remontar até à pessoa, de modo que a identidade da pessoa pode ser descoberta, mas isto apenas em circunstâncias pré-definidas. Nesse caso, apesar de se aplicarem as regras de proteção de dados, os riscos existentes para as pessoas no que toca ao tratamento dessa informação indiretamente identificável serão na maioria dos casos reduzidos, de forma que a aplicação destas regras será justificadamente mais flexível do que informação tratada sobre pessoas diretamente identificáveis.” (GT29º, 2007, p. 19)

Note-se que o tratamento de dados pessoais deve processar-se de forma transparente (*cf.* art. 5º, n.º 1, al. a) do RGPD) e no estrito respeito pela reserva da vida privada, pelo que deve considerar-se o estatuído no art. 8º da CEDH (“qualquer pessoa tem direito ao respeito pela sua vida privada e familiar, do seu domicílio e da sua correspondência”).

Existe, desta forma, uma relação intrínseca entre os dados pessoais e os direitos de personalidade previstos na legislação portuguesa, nomeadamente, nos arts. 14º e ss. do CT.

Dado que a Lei não define direitos de personalidade, a doutrina<sup>3</sup> tem tentado defini-los. De acordo com o Acórdão do STJ, de 01 de março de 2016, Rabindranath Capelo de Sousa (1978, pp. 73 e ss.) escreveu:

“conclui-se que a lei não contém uma definição geral ou uma definição do direito de personalidade, este abrange, na sua proteção, no âmbito do direito civil, todos aqueles «direitos subjetivos, privados, absolutos, gerais, extra-patrimoniais, inatos, perpétuos, intransmissíveis, relativamente indisponíveis, tendo por objecto os bens e as manifestações interiores da pessoa humana, visando tutelar a integridade e o desenvolvimento físico e moral dos indivíduos e obrigando todos os sujeitos de direito a absterem-se de praticar ou deixar de praticar actos que ilicitamente ofendam ou ameacem ofender a personalidade alheia sem o que incorrerão em responsabilidade civil e/ou na sujeição às providências cíveis adequadas a evitar a ameaça ou a atenuar os efeitos da ofensa cometida»”.

---

<sup>3</sup>Outros autores definiram direitos de personalidade, nomeadamente João Leal Amado (Amado, 2018, p. 190), António Monteiro e Mota Pinto (Monteiro & Pinto, 2012, p. 208), e Pedro Vasconcelos (Vasconcelos, 2010, pp. 39-40).

“Os direitos de personalidade visam permitir à pessoa titular desse direito subjetivo defender a sua identidade, honra, liberdade, ou seja, aquilo que lhe é próprio. Pretende-se com o seu exercício excluir um comportamento negativo de outrem.” (Cabral, 2016, p. 1).

Os direitos de personalidade são caracterizados como absolutos (oponíveis *erg omnes*), não patrimoniais (são insuscetíveis de avaliação pecuniária), intransmissíveis (não podem ser transmitidos para terceiros), indisponíveis (o seu titular não pode transmitir ou extinguir o direito da sua esfera jurídica), irrenunciáveis (não são suscetíveis de serem extintos ou alienados por um ato de vontade do titular), impenhoráveis (não podem ser utilizados para o pagamento de obrigações) e imprescritíveis (nunca prescrevem).

Os direitos de personalidade incidem sobre “a vida da pessoa, a sua saúde física, a sua integridade física, a sua honra, a sua liberdade física e psicológica, o seu nome, a sua imagem, a reserva sobre a intimidade da sua vida privada. É este um *círculo de direitos necessários* (...)” (Monteiro & Pinto, 2012, p. 209).

Dessarte, é possível concluir que estes direitos compreendem tanto o organismo físico como a componente espiritual e psíquica dos indivíduos.

Os direitos de personalidade e os dados pessoais estão previstos em diversas Leis, as quais tencionamos analisar no ponto 2. deste capítulo. Assim sendo, pese embora o nosso trabalho se centre no trabalhador, não podemos deixar de fazer referência a outras normas que o protegem.

Pese embora haja um capítulo específico para a matéria do trabalhador, refira-se desde já que os direitos de personalidade “invadem” a relação de trabalho, “erigindo-se como um importante limite aos poderes do empregador e, ao mesmo tempo, como uma garantia do exercício de vários direitos fundamentais” (Moreira, 2011b), p. 65), distinguindo, desta forma, o estatuto geral do cidadão e o estatuto do trabalhador que, por força do contrato de trabalho e da subordinação jurídica consequente, vê a sua liberdade e os seus direitos condicionados.

## 2. Enquadramento Legal

### 2.1. A proteção constitucional

Os direitos de personalidade são também direitos fundamentais, pelo que encontram proteção na nossa lei fundamental<sup>4</sup>.

Estes direitos de personalidade fundamentais merecem consagração em diversas disposições distribuídas pela CRP, nomeadamente nos arts. 13º, 24º a 27º, 34º a 38º, 41º a 48º, 51º e 61º e 62º. Não tencionamos, contudo, analisar cada um deles, mas sim os que julgamos fundamentais para a presente dissertação, elencando estes artigos com o fim de mera exposição. Não podíamos começar de outra forma se não com a análise do art. 35º da CRP.

De acordo com Catarina Castro (2005, p. 32), a Constituição da República Portuguesa foi a primeira Constituição Europeia a integrar uma norma especial em matéria de proteção de dados pessoais, nomeadamente o art. 35º da CRP enquanto direito especial de personalidade; este pretende, até aos dias de hoje, a proteção do cidadão, quanto aos perigos que pode causar o uso da informática.

O art. 35º consagra a proteção dos cidadãos perante o tratamento dos seus dados pessoais (tanto informatizados, como constantes de ficheiros manuais), cabendo à própria Lei delimitar este conceito de dados, *in casu* previsto no RGPD, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização; a sua tutela está garantida por uma entidade administrativa independente: a CNPD.

O seu n.º 1 reconhece um direito básico (*hebeas data*) do titular dos dados, que se divide em três vertentes: o direito de acesso aos dados informatizados que lhes digam respeito, os direitos à sua retificação e/ou atualização e o direito de conhecer a finalidade a que se destinam.

---

<sup>4</sup> Podemos “distinguir direitos de personalidade de direitos fundamentais, desde logo a partir de um critério formal, que consistiria no facto de os primeiros receberem uma proteção imediata resultante do CC e os segundos da Constituição, mas esta afirmação apenas é correta em termos estritamente formais pois, como é sabido, existem direitos fundamentais que não estão consagrados na Constituição, assim como existem direitos de personalidade constantes de normas do texto fundamental”. (Cabral, 2016, p. 7).

A primeira vertente consiste no direito do titular conhecer os dados guardados informaticamente que lhe pertençam; a segunda vertente compreende a possibilidade de corrigir os dados que se encontram desconformes com a realidade, ou desatualizados, e, por último, a terceira vertente expõe “um *direito à autodeterminação sobre informações referentes a dados pessoais* que exige uma proteção clara quanto ao «desvio dos fins» a que se destinam essas informações” (Canotilho & Moreira, 2007, p. 553).

O n.º 3 estatui que “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”.

O elenco que o artigo prevê, referente à regra geral de interdição absoluta de tratamento de dados automatizados, representa as categorias de dados pessoais cujo tratamento poderá revelar-se mais arriscado para o respetivo titular, no sentido de promover uma possível discriminação (por exemplo, na contratação de um trabalhador).

O acesso a todos os dados pessoais supramencionados é interdito a terceiros, tendo em conta que aumenta a hipótese de violação da esfera privada do titular dos dados, arriscando a sua utilização de forma, ou para meios ilícitos, ou para um fim que o titular desconhece ou não assentiu. Além da proibição do acesso a dados alheios, se a análise do artigo for feita de forma ampla, considera-se também a divulgação destes mesmos dados a particulares ou entidades. Estamos, deste modo, perante o *right to be alone* de cada pessoa.

Contudo, o artigo prevê uma exceção a este acesso, a saber, se o acesso aos dados por parte de terceiros for exigido pela necessidade de defesa de direitos constitucionalmente protegidos, como a defesa da existência do Estado, o combate à criminalidade, a proteção de direitos fundamentais de outrem, entre outros (Canotilho & Moreira, 2007, p. 555).

A garantia de livre acesso às redes informáticas de uso público, prevista constitucionalmente, regula a proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.

O artigo, por um lado, impõe este “acesso” como um requisito para se poder usufruir da liberdade de expressão na *Internet*, sendo necessário que o Estado crie

condições e tome medidas necessárias que assegurem esta liberdade. A *Internet* é, atualmente, um meio para o desenvolvimento desta liberdade, “oferecendo” conhecimento em diversas áreas.

Cabe ao legislador determinar os meios mais adequados para uma proteção segura dos dados pessoais, defendendo Gomes Canotilho e Vital Moreira (2010, p. 557), que estes dados podem dividir-se em três categorias: dados sensíveis, que usufruem de uma reserva de proibição com possibilidade de tratamento caso haja consentimento do titular, dados sujeitos a controlo prévio, que carecem de autorização da CNPD para o seu tratamento, e dados isentos de notificação.

Em conjugação com o art. 35º, o art. 26º da CRP consagra outros direitos pessoais, que aspiram a proteção do círculo nuclear da pessoa, correspondendo de um modo geral, aos direitos de personalidade.

Quanto ao primeiro direito previsto no artigo, o Tribunal Constitucional designa a identidade pessoal como:

“V – (...) aquilo que caracteriza cada pessoa enquanto entidade individualizada que se diferencia de todas as outras pessoas por uma determinada vivência pessoal. Num sentido muito amplo, o direito à identidade pessoal abrange o direito de cada pessoa a viver em concordância consigo própria, sendo, em última análise, expressão da liberdade de consciência projetada exteriormente em determinadas opções de vida. O direito à identidade pessoal postula um princípio de verdade pessoal. Ninguém deve ser obrigado a viver em discordância com aquilo que pessoal e identitariamente é. O direito à identidade pessoal liga-se, ainda, à proibição da discriminação do artigo 13.º, n.º 2, da Constituição, pois as características aí identificadas são, na sua generalidade, constitutivas da identidade pessoal.”

(Ac. TC datado de 24 de abril de 2018)

O direito à identidade pessoal tem como objeto não só os meios de identificação da pessoa (v.g. nome ou pseudónimo, analisados com mais afincos no 72º do CC), mas também a verdade pessoal; abarca igualmente situações da vida real que não integram a vida pessoal, tal como a adulteração ou a utilização de elementos da vida pessoal do indivíduo.

O direito ao desenvolvimento da personalidade constitui, no ordenamento jurídico português, um direito subjetivo fundamental, não obstante ser um direito de personalidade, visando proteger primordialmente o aspeto dinâmico e evolutivo da personalidade humana.

De acordo com Canotilho & Moreira (2007, p. 463), o direito ao desenvolvimento da personalidade comporta duas esferas: uma de proteção da integridade da pessoa, e outra de proteção da liberdade de exteriorização ou seja, a liberdade de escolha máxima em todos as particularidades do “modo de vida”.

O direito à capacidade civil e o direito à cidadania residem, respetivamente, no direito a participar nas relações jurídicas, e no direito à Pátria. A privação a ambos os direitos só pode efetuar-se nos casos e termos previstos na lei, não podendo ter como fundamento motivos políticos (*cf.* n.º 4 do art. 26º da CRP).

O direito ao bom nome e reputação “traduz a representação que os outros têm sobre o valor de uma pessoa, o apreço social pelas qualidades e valores sociais que adornam cada indivíduo” que “não deixa de ser apenas uma especificação ou particularização do direito à dignidade e à integridade moral” (Ac. STJ, datado de 13 de julho de 2017).

Nas palavras de Gomes Canotilho e Vital Moreira, “consiste essencialmente no direito a não ser ofendido ou lesado na sua honra, dignidade ou consideração social mediante imputação feita por outrem, bem como no direito a defender-se dessa ofensa e a obter a consequente reparação” (Canotilho & Moreira, 2007, p. 466). Na lição de Antunes Varela, poder-se-á dizer que o prejuízo do bom nome traduz-se no abalo do prestígio de que a pessoa goze ou o bom conceito em que ela seja tida no meio social em que vive ou exerce a sua atividade (Varela, 2008, p. 549).

Este direito dispõe da particularidade de constituir um limite a demais direitos, nomeadamente os direitos à informação, expressão ou liberdade de imprensa (arts. 37º e 38º da CRP), subsistindo deste modo uma colisão de direitos constitucionais.

O direito à imagem está previsto igualmente no art. 79º do CC, onde pretendemos desenvolver o conceito, pelo que não é nosso intuito fazer uma análise extensa neste ponto. “Como direito autónomo, é um direito ao controlo da captação e divulgação de elementos de identificação *visual* da pessoa – corresponde, neste sentido, a uma proteção da inviolabilidade pessoal em relação à *projeção física*” (Pinto P. M., 2018, p. 620). O STJ afirma que:

“O art. 16º da CRP consagra autonomia conceptual ao direito à imagem distinguindo-a de outros direitos fundamentais como sejam o direito à intimidade ou o direito à honra. Podendo concorrer uma ofensa ao direito à imagem com

outros, mais comumente com o direito à intimidade ou à honra, como seria o caso de se a imagem representa momento da vida privada de alguém ou representa partes íntimas do corpo, o facto é que, parece ser doutrina firme, que o direito à imagem possui autonomia conceptual e constitucional, o que o torna susceptível.”

(Ac. STJ datado de 07 de junho de 2011)

Abonando a opinião de Gomes Canotilho e Vital Moreira (2007, p. 467), este direito abrange o direito de definir a sua própria autoexposição, ou seja, o direito de cada um de não ser fotografado, ou de ver o seu retrato exposto em público sem o seu consentimento, incluindo desta forma o consentimento tácito (veja-se o exemplo de um jornalista em reportagem televisiva), bem como o direito de não ver a sua imagem apresentada em montagem ofensiva ou distorcida, que constituirá uma “falsificação da personalidade”.

O direito à palavra configura um direito paralelo ao direito à imagem e implica a interdição da escuta ou gravação de elementos sonoros de expressão (palavras) sem o consentimento da pessoa, como por exemplo a gravação ilícita de conversas pessoais.

Gomes Canotilho e Vital Moreira abraçam a tese de que o direito à palavra se circunscreve em três outros direitos:

“(a) direito à voz, como atributo de personalidade, sendo ilícito, sem consentimento da pessoa, registar e divulgar a sua voz (com ressalva, é claro, do lugar em que ela foi utilizada); (b) direito às «palavras escritas», que pretende garantir a autenticidade e o rigor da reprodução dos termos, expressões, metáforas escritas e ditas por uma pessoa; (c) direito ao auditório, ou seja, a decidir o círculo de pessoas a quem é transmitida a palavra”. (Canotilho & Moreira, 2007, p. 467).

O direito à reserva da intimidade da vida privada e familiar visa a “proteção da privacidade do indivíduo, no seu sentido mais amplo, incluindo-se todas as atividades da vida privada e íntima do cidadão. Trata-se de um conjunto de informações acerca do indivíduo que ele pode decidir manter sob seu exclusivo controlo, ou comunicar, decidindo a quem, quando, onde e em que condições” (Galante, 2010, p. 66).

Desde já, é importante entender a teoria defendida por Menezes Leitão, em que o critério de determinação do conteúdo do direito à privacidade assenta sobre a distinção de três esferas concêntricas:

“a) uma *esfera íntima*, abrangendo a vida familiar, saúde, comportamentos sexuais e convicções políticas e religiosas, cuja proteção é, em princípio, absoluta; b) uma *esfera privada*, cuja proteção é relativa, podendo ceder em caso de conflito com

direitos e interesses superiores; c) uma *esfera pública*, relativas às situações que são objeto de conhecimento público e que, por isso, podem ser livremente divulgadas.” (Leitão, 2004, p. 38)

Canotilho & Moreira (2007, p. 467) explicam que o direito em análise se reparte em dois direitos menores: “(a) o direito a impedir o acesso de estranhos a informações sobre a vida privada e familiar e (b) o direito a que ninguém divulgue as informações que tenha sobre a vida privada e familiar de outrem (*cfr.* art. 80º do CC)”.

Visto que este direito está regulado em especial no art. 16º do CT, artigo que pretendemos analisar, não podemos deixar de fazer uma remissão para o capítulo 2.3.

A proteção legal contra quaisquer formas de discriminação foi um direito introduzido na quinta revisão feita à Constituição, e visa proteger o cidadão de qualquer desigualdade de tratamento. A título de exemplo, o art. 13º, n.º 2 da CRP apresenta-nos um grande elenco; contudo, não é taxativo, existindo inúmeros casos no quotidiano que não se encontram especificados na Lei.

Trata-se de um direito que protege a igualdade e não discriminação, incluindo no acesso ao trabalho, que aponta também para a efetivação e promoção da exigência da igualdade de tratamento.

O n.º 2 do art. 26º prevê que “a lei estabelecerá garantias efetivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias”; o que nos parece que se trata claramente de um corolário do direito à reserva da intimidade da vida privada e familiar de cada indivíduo (direito previsto no n.º 1).

Constitui-se uma imposição legiferante ao legislador, que está impelido de estabelecer garantias; caberá, neste caso, ao sujeito Estado cumprir esta obrigação. Canotilho & Moreira (2007, p. 471) repartem estas garantias, desde logo, nas sanções penais e de carácter civil.

Quanto às sanções penais, o legislador tipifica e penaliza os comportamentos que violem a intimidade da pessoa nos arts. 190º e ss. do Código Penal. Podem incluir-se nestes, as situações de gravação ou manipulação de imagens, conversas, ou informações pessoais, presentes em ficheiros informáticos, ou a publicação destas ou de outros aspetos da vida íntima.

Por outro lado, as sanções de carácter civil traduzem-se fundamentalmente no instituto da responsabilidade civil. “São, sobretudo, de natureza ressarcitória, destinando-se a possibilitar a compensação dos danos morais e materiais resultantes de comportamentos lesivos da intimidade (...). Podem também consistir em medidas judicialmente decretadas” (Canotilho & Moreira, 2007, p. 471).

Note-se que o artigo refere não só a utilização de informações abusivas, mas também aquelas que são contrárias à dignidade humana pelo que o artigo abrange também quaisquer informações que possam despersonalizar ou degradar os seres humanos.

Este artigo 26º preceitua ainda que “a lei garantirá a dignidade pessoal e a identidade genética do ser humano, nomeadamente na criação, desenvolvimento e utilização das tecnologias e na experimentação científica”, que traduz a elevação a nível constitucional formal da chamada «bioconstituição» que, segundo António Baracho, citado por Raquel Sparemberger e Adriane Thiesen, constitui:

“conjunto de normas (princípios e regras) formal ou materialmente constitucionais, que tem como objeto as ações ou omissões do Estado ou de entidades privadas, com base na tutela da vida, na identidade e integridade das pessoas, na saúde do ser humano atual ou futuro” (Sparemberger & Thiesen, 2010, p. 36).

A dignidade humana é um valor intrínseco reconhecido a cada indivíduo, fundado na sua autonomia ética, apoiando-se numa obrigação geral de respeito pelo ser humano, e traduzida num elenco de deveres e direitos correlatos.

A consagração do direito à dignidade pessoal reporta à pessoa concreta e insubstituível (homem ou mulher), na sua vida real e quotidiana, vinculando igualmente as entidades privadas (art. 18º, n.º 1 da CRP). “Ao distinguir entre dignidade pessoal e identidade genética, a Constituição pretende desde logo garantir a pessoa contra a criação, desenvolvimento e utilização de tecnologias e experimentação científica que deixando imperturbada a identidade genética violam a dignidade pessoal” (Canotilho & Moreira, 2007, p. 472).

Em harmonia com o art. 26º, n.º 1 da CRP, surge o art. 34º, que estabelece a inviolabilidade do domicílio e do sigilo da correspondência, bem como de outros meios de comunicação privada. Ao caracterizar estes direitos como invioláveis, limita-se, na maior medida possível, a possibilidade de restrições.

O artigo divide-se em dois grandes direitos: o direito à inviolabilidade de domicílio e o direito ao sigilo da correspondência e à inviolabilidade dos meios de comunicação privada.

Importa para a presente dissertação o direito ao sigilo da correspondência e à inviolabilidade dos meios de comunicação privada, que abrange todo o tipo de correspondência dirigida a determinada pessoa, incluindo não só cartas ou encomendas, mas todo o tipo de telecomunicações que, aliás, são os meios mais empregues contemporaneamente, sendo impedida a propagação e divulgação do seu conteúdo por quem a elas tiver acesso, conforme o disposto no n.º 4 da presente norma.

O Tribunal Constitucional, quanto a este direito previsto no art. 34º, afirma que:

“BB) decorre do normativo supra, que o legislador ordinário ao pretender acautelar o bem jurídico constitucionalmente garantido - o direito à privacidade e a garantia da comunicação - veio proibir, antes de mais, a própria "abertura" de um escrito que "se encontre fechado", e isto, independentemente, de o seu conteúdo versar ou não sobre matéria privada, ou mesmo de se tomar ou não conhecimento desse mesmo conteúdo. Ou seja, é a própria "abertura" que é punida de 'per se'.

(Ac. TC, datado de 10 de dezembro de 2008)

Com o desenvolvimento da tecnologia, deve estender-se esta proteção a qualquer meio de comunicação privada, como o correio eletrónico, ou todo o tipo de correspondência utilizava via Internet, incluindo conversas pessoais nas redes sociais.

Este direito pode considerar-se, pela sua natureza, um direito "*erga omnes*", porquanto a sua aplicação abarca tanto o domínio das relações públicas, como privadas, não existindo exceções no âmbito de relações especiais de poder (Canotilho & Moreira, 2007, p. 544), apenas sendo possível restringir este direito em processo criminal (n.º 4).

Dessarte, conclui-se que a Constituição consagra direitos, liberdades e garantias coincidentes com os direitos de personalidade do trabalhador, direitos estes que são diretamente invocáveis e protegidos, tornando-se muito difícil restringi-los.

## 2.2. O Código Civil

O CC não nos apresenta um artigo específico para o conceito de dados pessoais. Porém, apresenta-nos, na sua secção II do capítulo relativo às pessoas singulares da Parte Geral (dentro do subcapítulo relativo às pessoas e do título da relação jurídica, notadamente nos arts. 70º e ss.), a proteção dos direitos de personalidade, que podem ser considerados “o corresponsivo privatístico dos direitos fundamentais que incidem sobre bens da personalidade (os “direitos pessoais” previstos no artigo 26º da Constituição)” (Pinto P. M., 2018, p. 325).

Pese embora estas normas não sejam dirigidas diretamente ao trabalhador, este não deixa de gozar destes direitos, nem deixa de existir uma ligação com os direitos de personalidade previstos em outros Códigos (v.g. CT), tendo alguns deles correspondência análoga noutras Leis. Nas palavras de Maria Guimarães:

“A raiz antropocêntrica do direito civil justifica o lugar nuclear reservado à tutela da personalidade humana neste ramo do direito. A personalidade humana exige do direito o reconhecimento da essencialidade da personalidade jurídica, a inseparabilidade da personalidade jurídica da personalidade humana, com a consequente inadiabilidade do reconhecimento da personalidade jurídica e a ilimitabilidade da sua tutela, não se compadecendo com um *numerus clausus* ou mesmo com uma enumeração mais ou menos pormenorizada de direitos de personalidade, necessariamente refém das concepções dominantes de uma determinada época e, portanto, datada.” (Guimarães, 2018, p. 25)

O art. 70º funda a cláusula de proteção geral da personalidade, constituindo desta forma uma norma de exalta pertinência. O n.º 1 deste artigo decreta que a lei protege os indivíduos contra qualquer ofensa ilícita ou ameaça de ofensa à sua personalidade física ou moral. Dessarte, o artigo indica o âmbito de aplicação da cláusula geral da personalidade e descreve a personalidade física e moral (que beneficiam de apelo nos arts. 25º e 26º da CRP) como sendo o critério material.

Retiramos do n.º 1 desta norma que os direitos de personalidade não abrangem apenas a tutela dos aspetos (físicos ou morais) do ser humano, mas também o seu desenvolvimento, abrangendo a proteção contra “novas ofensas” que vão surgindo com o desenvolvimento tecnológico.

O reconhecimento da inclusão do desenvolvimento da personalidade neste artigo conduz, contudo, a uma necessidade de proteção acrescida por o conteúdo do artigo ser tão

vasto. O ofendido pode, desta forma, requerer as providências adequadas conforme a situação, com a finalidade de evitar a consumação da ameaça ou atenuar os efeitos da ofensa já cometida (v.g. n.º 2). Este preceito clarifica os meios de tutela (civil) dos direitos de personalidade, não prejudicando a possibilidade de recurso à tutela penal, ou às providências cautelares comuns, previstas nos arts. 393º a 395º do CPC.

A responsabilidade referida no n.º 2 é a prevista nos arts. 483º e ss. do CC – responsabilidade civil por factos ilícitos, ilicitude que consiste na violação de um direito de outrem, e que origina a possibilidade de pedido indemnizatório com uma função reparadora (art. 496º do CC), consistindo no ressarcimento, em termos patrimoniais, dos danos patrimoniais e dos danos não patrimoniais sofridos pelas vítimas (*cf.* Galante, 2010, p. 109).

A Lei prevê nos arts. 72º e ss do CC os direitos especiais de personalidade.

O primeiro direito de personalidade protegido civilmente é o direito à identidade pessoal, que comporta o direito ao nome (art. 72º), mas também ao pseudónimo. Permite não só que todas as pessoas usem o seu nome, enquanto função de identificação e distinção<sup>5</sup>, como que se oponham a que outrem o use ilicitamente para sua identificação ou outros fins, como por exemplo o uso abusivo por outrem, nos termos do art. 334º.

Este artigo faculta ao titular o uso exclusivo do nome como identidade pessoal perante terceiros, bem como o poder de se defender judicialmente no caso de usurpação ou utilização indevida por parte de outrem, identidade pessoal que se encontra protegida constitucionalmente no art. 26º da CRP, nomeadamente na parte inicial do n.º 1.

José González (2011, p. 100) considera que o nome individual se pode repartir em nome pessoal e nome profissional pelo que, caso o trabalhador opte por possuir um nome profissional, este terá proteção similar.

Contudo, de acordo com o Tribunal Constitucional, “não pode ser constituído em termos tais que crie dúvidas sobre a pessoa a quem pertence ou dê azo a que se confunda essa pessoa com outra ou outras. De contrário, o nome deixa de desempenhar a função que lhe é própria de contradistinguir o respetivo titular” (Ac. TC, datado de 11 de outubro de 2000).

---

<sup>5</sup>*Cfr.* José González (2011, p. 100), Ana Prata (2017, p. 111) e Pinto (2018, p. 345).

Em harmonia com o n.º 2 do art. 72º, o titular do nome não pode, especialmente no exercício de uma atividade profissional, usá-lo de modo a prejudicar os interesses de quem tiver nome total ou parcialmente idêntico, isto é, censura-se a utilização prejudicial, negligente ou emocional deste nome semelhante.

Consequentemente, nestes casos, e recorrendo ao art. 70º, n.º 2 do CC estudado *supra*, o tribunal decretará as providências mais adequadas ao caso concreto que, segundo juízos de equidade, melhor conciliem os interesses em conflito. Deve articular-se a norma com o art. 484º do CC que decreta que “quem afirmar ou difundir um facto capaz de prejudicar o crédito ou o bom nome de qualquer pessoa, singular ou coletiva, responde pelos danos causados”.

O pseudónimo, regulado no art. 74º, é um nome fictício, usado pelo titular como um meio de identificação alternativo ao nome pessoal, sendo uma outra forma de individualização. O pseudónimo goza da mesma proteção que o direito ao nome; contudo, o artigo obriga a que preencha o requisito de ser notório perante a comunidade.

Quanto ao direito sobre escritos pessoais (arts. 75º a 78º do CC), podemos distinguir entre as cartas-missivas e outros escritos confidenciais (que fazem parte da vida íntima) e cartas não confidenciais (que se encontram na esfera privada). Os primeiros desfrutam do mesmo regime devido à remissão feita no art. 77º, e prevê-se um dever de reserva e a necessidade de consentimento para a publicação destas; para as segundas, prevê-se “um dever do destinatário de “usar dela em termos que não contrariem a expectativa do autor”” (Pinto P. M., 2018, p. 348).

Devido às inovações tecnológicas, defendemos que se torna necessário abranger o regime das “cartas” (documentos escritos em papel dirigidos a determinado destinatário) a outros meios de comunicação, particularmente à comunicação feita por meios eletrónicos (v.g. telemóvel, *e-mail*).

A natureza confidencial desta correspondência depende, por um lado, da declaração de vontade do remetente por meio de notificação para tal e, por outro, do próprio teor da carta ou escrito (*e.g.* conteúdo abrangido por sigilo profissional, matérias relativas a aspetos familiares ou de saúde, entre outros).

De mencionar que, de acordo com Antunes (2012, p. 169), pode subsistir um conflito de direitos entre o remetente e o destinatário; a saber, se o remetente beneficiar de

direito de autor e à reserva sobre a palavra escrita, e, por outro lado, o destinatário gozar de um direito de propriedade sobre a carta, o que permite a sua livre utilização. Nestes casos, atender-se-á ao disposto no art. 335º do CC.

Tanto as cartas-missivas como os escritos confidenciais, só podem ser publicados com o consentimento do seu autor ou com o suprimento judicial desse consentimento (art. 76º do CC), sob pena de se admitir o recurso aos meios de tutela previstos no art. 70º, n.º 2.

O CC prevê também a tutela do direito à imagem, previsto no art. 79º, que constitui um corolário do direito fundamental previsto no art. 26º, n.º 1 da CRP, e visa proteger a representação da imagem das pessoas singulares.

De acordo com Ana Prata, “o conceito operatório relevante para a nossa ordem jurídica é antes o de ‘retrato’ que toma apenas *hoc casu* por base a consideração da aparência exterior da pessoa para a representar visualmente de forma tal (...) que permita a sua identificação ou reconhecimento” (Prata, 2017, p. 116), incluindo a imagem captada e reproduzida pelos novos meios digitais.

O n.º 1 do artigo em análise obriga o titular da imagem a dar consentimento para a exposição, representação ou “lançamento” desta no comércio. Numa interpretação extensiva, que revela para o nosso tema, defendemos que este deve aplicar-se também aquando da captação da imagem, no contexto laboral.

Ora, a inexistência de consentimento para o uso da imagem, ou a utilização em termos distintos daqueles que presidiram à prestação do consentimento (que deve ser, regra geral, expresso e limitado), faculta ao titular um direito de reação à utilização ilícita da sua imagem, pelo facto de não querer ser associada ou de a divulgação ser lesiva (*cf.* Antunes, 2012, p. 186).

A dispensa do consentimento apenas é permitida no caso ordinário da notoriedade ou do cargo desempenhado (v.g. público ou político), situação em que cremos que deve considerar-se existir consentimento tácito quando o visado procura, por si, publicidade ou notoriedade pública, através da publicação da sua imagem. Em contexto laboral, veja-se o exemplo de um(a) jornalista, ou de um trabalhador que aparece numa conferência de imprensa.

Em suma, o direito à imagem, tal como os restantes direitos de personalidade, é irrenunciável e inalienável (art. 81º do CC). Contudo, “admite a limitação voluntária, não estando proibidas limitações lícitas ao exercício do direito à imagem que, não afetando esse direito, apenas incidem sobre expressões do mesmo.” (Galante, 2010, p. 61).

O art. 80º dedica-se ao direito à reserva sobre a intimidade da vida privada, que deve conjugar-se com o art. 16º do CT, e constitui um direito de considerável importância para o tema do nosso trabalho, porquanto apresenta diversas vertentes como são o caso do direito à inviolabilidade da correspondência ou das comunicações, temáticas fulcrais do nosso estudo, que estão intrinsecamente conectadas com a proteção dos dados pessoais.

“O direito à reserva sobre a intimidade da vida privada é um direito residual, cujo conteúdo é preenchido pelo espaço deixado em branco pelos demais direitos especiais, como o direito à imagem e sobre cartas-missivas” (Antunes, 2012, p. 203). Este “não deve ser considerado como um princípio da propriedade privada, mas uma inviolabilidade da personalidade. A expressão “*right to be let alone*” (direito de poder ficar sozinho), evoca a ideia de que a vítima diz respeito à própria pessoa, e esta tem o direito de a proteger da interferência de outros indivíduos” (Galante, 2010, p. 67).

Constata-se no n.º 1 que todos devem guardar reserva quanto à intimidade da vida privada de outrem, garantindo-se desta forma a proteção de três prismas: os direitos a não acesso abusivo da vida privada de outrem, ao não aproveitamento deste acesso e a não divulgar factos ou informações dessa vida de terceiro. Desta forma, visa-se a limitação, ou mesmo o impedimento, à inserção de estranhos na esfera íntima ou privada da pessoa.

A finalidade deste direito é a proteção da tranquilidade e da liberdade da vida do seu titular, afirmando o STJ que compreende:

“V – (...) todos aqueles aspetos que fazem parte do domínio mais particular e íntimo que se quer manter afastado de todo o conhecimento alheio, com exclusão da vida normal de relação, ou seja, dos factos que o próprio interessado, apesar de pretender subtraí-los ao domínio do olhar público, isto é, da publicidade não resguarda do conhecimento e do acesso dos outros.”

(Ac. STJ, datado de 17 de dezembro de 2009)

Segundo Ana Prata (2017, p. 119), neste artigo utiliza-se uma dupla cláusula geral, nos n.ºs 1 e 2, que fornece ao critério do julgador bases objetivas de ponderação, nomeadamente a natureza do caso e a condição das pessoas.

Mencionar “a natureza do caso” subjaz a consideração pelos interesses subjacentes aos factos ou circunstâncias relativas à vida privada, e a “condição das pessoas” remete para o estatuto que esta detém, ou seja, a posição ou cargo ocupado.

Em relação ao critério subjetivo, Mota Pinto expõe que o titular do direito “pode desde logo modelar o *próprio objeto de proteção* do direito à reserva” (Pinto, 2018, p. 350), uma vez que a realidade é que cada indivíduo, *per si*, tem o direito de expor ou, pelo contrário, resguardar a sua vida privada e conseqüentemente a quantidade de informação sobre esta.

Pese embora a extensão da reserva de privacidade esteja condicionada, segundo o n.º 2 do art. 80º do CC, pela “condição das pessoas”, não se justifica qualquer que seja a intromissão e/ou violação. “Apenas se pode garantir, diversamente, que há pessoas cuja esfera de privacidade é superior e outras, ao contrário, a quem pertence uma extensão de reserva mais reduzida” (González, 2011, p. 114).

A violação deste direito conduz à possibilidade de o interessado acionar os meios de tutela do art. 70º, n.º 2 do CC. Contudo, o titular não pode reagir no caso de publicitar aspetos da sua vida privada, por iniciativa própria.

Feita a análise, conclui-se que a tutela dos direitos de personalidade (também) no Código Civil demonstra, mais uma vez, a importância que estes têm na vida do cidadão comum, englobando o cidadão enquanto trabalhador.

## **2.3. O Regulamento Geral da Proteção de Dados**

### **2.3.1. Das Diretivas ao Regulamento**

Ao longo dos anos, a proteção da privacidade de cada ser humano não gerou apenas preocupação na legislação portuguesa, mas sim por todo o mundo: “*the right to personal data protection has been codified in multilevel legal frameworks (...), first as a right to respect private life and then as a freedom and an individual human right*” (Ogriseg, 2017, p. 22).

A legislação europeia relativa à proteção dos dados pessoais estreou-se com a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, atualmente revogada pelo RGPD, que estatuiu que os Estados-membros deviam assegurar a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais, a fim de manter, em especial, a segurança dos dados e impedir qualquer tratamento não autorizado.

A Diretiva 97/66/CE do PE e do Conselho de 15 de dezembro de 1997, revogada com a entrada em vigor da Diretiva 2002/58/CE, foi criada quando se deu um “boom” na introdução nas redes públicas de telecomunicações da Comunidade Europeia de novas tecnologias digitais avançadas. O art. 5º proibia a colocação de dispositivos de escuta, o armazenamento ou outros meios de interceção ou vigilância de comunicações por terceiros, sem o consentimento dos titulares dos dispositivos (exceto se autorizados por lei).

A Diretiva 2000/31/CE do PE e do Conselho, de 8 de junho de 2000, transposta para a legislação nacional através do DL n.º 7/2004, de 07 de janeiro, regula o “comércio eletrónico no mercado interno e tratamento de dados pessoais”, versa sobre determinados aspetos legais dos serviços da sociedade de informação, ou seja, qualquer serviço, em princípio pago à distância, por meio de equipamento eletrónico de processamento.

A Diretiva 2002/58/CE do PE e do Conselho de 12 de julho de 2002 aborda o tratamento de dados pessoais e a proteção da privacidade no setor das comunicações eletrónicas (*cf.* art. 3º, al. x) da Lei n.º 5/2004 de 10 de fevereiro) e revogou a Diretiva 97/66/CE. A presente visa assegurar o respeito dos direitos fundamentais, em especial os previstos nos arts. 7º e 8º da Carta dos Direitos Fundamentais da União Europeia, regulando nos arts. 4º e 5º a segurança e a confidencialidade dos dados, respetivamente.

A Diretiva 2006/24/CE do PE e do Conselho, de 15 de março de 2006, regula a conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis, ou de redes públicas de comunicações.

A Diretiva (UE) 2016/680 tem como objetivo a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução

de sanções penais, incluindo a salvaguarda e prevenção de ameaças à segurança pública, sendo a Diretiva com conteúdo mais semelhante ao atual RGPD.

A Diretiva (UE) 2016/681 protege também os dados pessoais de todos os cidadãos europeus, *in casu*, os dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave.

Atualmente, *“new types of systematic and potentially pervasive data processing at work, less visible than traditional one such as overt CCTV cameras and more invasive of private life as employees work remotely, create significant challenges to privacy and data protection”* (Ogriseq, 2017, p. 3). Posto isto, sentiu-se a necessidade, na UE, de reforçar os direitos fundamentais dos cidadãos naquela que é chamada a era digital, em que vigora uma rápida evolução tecnológica, onde a recolha e a partilha de dados pessoais é cada vez mais frequente, contribuindo desta forma para a facilidade da livre circulação de dados pessoais.

Foi assim criada aquela que é hoje a principal norma reguladora em matéria de proteção de dados: o RGPD - Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, aplicável a partir de 25 de maio de 2018, ao tratamento de dados pessoais efetuado no contexto de todas as atividades de um estabelecimento de um responsável pelo tratamento, ou de um subcontratante situado no território da União.

Sobre a entrada em vigor do RGPD, Mayer-Schönberger e Yann Padova defendem que este “abriu portas” à entrada da figura do “*Big Data*” nos Estados-membros aderentes, visando um tratamento melhorado e mais célere de dados de grande dimensão, que os métodos tradicionais já não alcançam:

*“the new European Union General Data Protection Regulation (GDPR) (...) opens up some concrete doors for Big Data to flourish although it falls short of abandoning traditional data protection principles altogether. The new data protection setup is far from being simple or transparent, leaves much clarity to be desired, and gives significant leeway to Member States, but it is a remarkable step towards enabling Big Data in Europe”* (Mayer-Schönberger & Padova, 2016, p. 318).

Sendo um Regulamento, e não uma Diretiva, tem aplicabilidade direta no sistema jurídico dos Estados-membros, não sendo necessário ser transposto para a legislação interna. Tem, por isso, a virtualidade de debelar o problema, criado pela transposição da

Diretiva n.º 95/46/CE, da diversidade dos sistemas jurídicos dentro da UE e, deste modo, contribuir para a harmonização da legislação e, por esta via, para a segurança jurídica e para a coerência do sistema de tratamento de dados pessoais na União (Saldanha, 2018, p. 15)<sup>6</sup>.

De qualquer forma, com o objetivo de assegurar a implementação e execução do RGPD na ordem jurídica nacional, entrou em vigor na legislação nacional, no dia oito de agosto de 2019, a Lei n.º 58/2019, que se traduz na Lei que assegura a execução do RGPD, e que se traduz igualmente na nova Lei de Proteção de Dados portuguesa.

O RGPD 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” (art. 2º, al. a)) quando “efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União (art. 3º), desde que as atividades não estejam compreendidas no âmbito das alíneas a) e b) do n.º 2 do art. 3º.

O tratamento dos dados, de acordo com o ponto 2) do art. 4º, é uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

Quanto à segurança dos dados, regulada no art. 32º, o responsável pelo tratamento e o subcontratante têm a obrigação de colocar em prática medidas técnicas e organizativas para evitar interferências não autorizadas nas operações de tratamento, que devem ser selecionadas consoante os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos para os direitos e liberdades das pessoas singulares. O responsável ou o subcontratante pelo tratamento pode responder pela

---

<sup>6</sup> Como veremos mais á frente, este propósito uniformizador pode não conseguir ser cabalmente alcançado, nomeadamente em matéria laboral, face ao caráter amplo e remissivo do artigo 88.º do RGPD.

violação dos dados do trabalhador, através de ação judicial, de acordo com o art. 79º do RGPD.

Uma das grandes novidades do RGPD são as severas coimas, aplicáveis pelas autoridades de controlo, tanto a pessoas colectivas, como singulares, previstas no art. 83º, e que visam reforçar a execução das regras do presente regulamento, bem como reforçar e harmonizar as sanções administrativas para violações do presente regulamento, além das medidas adequadas impostas pela autoridade de controlo (Considerandos (148) e (150)). Em Portugal, cabe à CNPD garantir o cumprimento do RGPD, incluindo estas normas, nos termos do art. 4º, n.º 2 da Lei de Execução.

Pese embora não seja intenção desenvolver este tema, refira-se apenas que a Lei de Execução propõe ainda uma divisão em contraordenações muito graves ou graves, previstas nos arts. 37º e 38º respetivamente, pelo que nos parece que as restantes não enquadradas nos artigos serão consideradas leves.

O n.º 1 do art. 88º do RGPD determina que:

“1. Os Estados-Membros podem estabelecer, no seu ordenamento jurídico ou em convenções coletivas, normas mais específicas para garantir a defesa dos direitos e liberdades no que respeita ao tratamento de dados pessoais dos trabalhadores no contexto laboral, nomeadamente para efeitos de recrutamento, execução do contrato de trabalho, incluindo o cumprimento das obrigações previstas no 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.”

Ainda que a referência seja breve e concisa, estabelece a importância do tratamento dos dados pessoais em contexto laboral pois, com as inovações tecnológicas, o tipo de dados é cada vez mais diverso, sendo os casos presentes no artigo algumas das novas origens.

Na legislação nacional, o tema está consagrado no art. 28º da Lei de Execução, com a epígrafe “Relações laborais”. O n.º 1 estatui que “o empregador pode tratar os dados pessoais dos seus trabalhadores para as finalidades e com os limites definidos no Código do Trabalho e respetiva legislação complementar ou noutros regimes setoriais, com as

especificidades estabelecidas no presente artigo”, legislação que estudámos em capítulos anteriores.

Neste sentido,

*“processing personal data is generally prohibited, unless it is expressly allowed by law, or the data subject has consented to the processing. While being one of the more well-known legal bases for processing personal data, consent is only one of six bases mentioned in the GDPR. The others are: contract, legal obligations, vital interests of the data subject, public interest and legitimate interest as stated in Article 6 GDPR”.*<sup>7</sup>

A citação supra revela todos os fundamentos para o tratamento de dados. Contudo, não podemos deixar de manifestar a nossa opinião de que existem alguns mais usuais no quotidiano laboral (v.g. consentimento, a execução do contrato, as obrigações legais e o interesse legítimo do empregador), pelo que serão os fundamentos mais abordados na nossa reflexão.

O consentimento é o fundamento do tratamento que é objeto do nosso estudo, consistindo numa “manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento” (art. 4º, definição XI, do RGPD). Isto significa que o tratamento dos dados teve como fundamento a concordância do titular dos dados para esse ato.

Abordando sucintamente cada um dos fundamentos suprarreferidos nos parágrafos anteriores, e começando pela execução do contrato, este trata das relações de trabalho desde o nascimento da relação (contratação) ao seu fim (cessação do contrato de trabalho).

Nas palavras de Carlos Domènech,

*“el contrato de trabajo es el vínculo entre el empresario y el trabajador definido en el art. 1.1 del RDL 2/15 (ET/2015), como aquel en cuya virtud los trabajadores voluntariamente prestan sus servicios retribuidos por cuenta ajena y dentro del ámbito de organización y dirección de otra persona, física o jurídica, denominada empleador o empresario”* (Domènech, 2017, p. 146).

Numa primeira fase, o tratamento de dados destaca-se na seleção de pessoal, nomeadamente na gestão de currículos, definição de perfis (art. 4º, ponto 4) do RGPD), por

---

<sup>7</sup> Disponível para consulta em <https://gdpr-info.eu/issues/consent/>

exemplo através da análise das redes sociais do candidato, ou na obtenção de dados nas tão usuais “entrevistas” de emprego, em que facilmente se consegue chegar a dados da esfera íntima do trabalhador (v.g. estado civil, crenças ou testes psicológicos). Na fase do nascimento da relação laboral, deve ter-se em conta, segundo o autor suprarreferido, o próprio contrato de trabalho, em especial o conteúdo das cláusulas.

Na fase da execução do contrato, existem certos atos em que o tratamento está claramente autorizado, desnecessitando do consentimento do trabalhador para o tratamento, como são os casos concretos dos atos administrativos de pagamento à Segurança Social ou outros descontos realizados a favor do Estado. Além destes casos, temos as situações mais usuais e críticas, que pretendemos estudar no capítulo 2 desta tese, e que se prendem com a utilização das NTIC, em que é dúbia a necessidade de consentimento para o tratamento dos dados.

O tratamento de dados é também permitido quando baseado no cumprimento da lei/obrigações legais, como poderemos contemplar na exceção ao princípio da proibição de tratamento de dados sensíveis prevista no art. 9º, n.º 2, al. b) do RGPD, conjuntamente com a permissão de tratamento conjeturada na al. c) do art. 6º.

Nos casos do parágrafo anterior ou no tratamento de dados pessoais para o exercício de funções de interesse público ou o exercício da autoridade pública (arts. 6º, al. e) e art. 9º, als. g) e i) do RGPD), é lícito o prolongamento da conservação dos dados pessoais, mesmo que tenham deixado de ser necessários para a finalidade para que foram recolhidos, quando tal se revele necessário para o exercício do direito de liberdade de expressão e informação (Considerando (65) do RGPD), bem como é lícito o não apagamento dos dados nas situações previstas no n.º 1 do art. 17º - n.º 3, al. b) do mesmo artigo do RGPD).

Por fim, mas não menos relevante (até pelo contrário), um dos fundamentos mais importantes é a prossecução de interesses legítimos da entidade empregadora, aferíveis em função do caso concreto.

Segundo o Parecer 2/2017<sup>8</sup> elaborado pelo GT29º,

“se um empregador pretender invocar o fundamento jurídico do artigo 7.º, alínea f), a finalidade do tratamento deve ser legítima, assim como o método escolhido ou a

---

<sup>8</sup> Disponível para consulta em [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=610169](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169)

tecnologia específica com que o tratamento é realizado deve ser necessário para o interesse legítimo do empregador. Assim, o tratamento deve ser proporcional às necessidades da empresa, ou seja, a finalidade, a que se pretende dar resposta. O tratamento de dados no local de trabalho deve ser realizado da forma menos intrusiva possível e ser dirigido para as áreas específicas de risco.” (GT29º, 2017, p. 9)

Note-se que, nestes casos, ao trabalhador reserva-se o direito de se opor ao tratamento pelos fundamentos legítimos e imperiosos previstos e regulados no art. 14º do RGPD.

Ademais, é essencial que existam medidas específicas de atenuação para garantir um equilíbrio adequado entre o interesse legítimo do empregador e os direitos e liberdades fundamentais dos empregados, direitos que estudamos em pontos anteriores deste capítulo, ao estudar os direitos de personalidade presentes nas diversas Leis portuguesas.

Isto significa que para poder utilizar este fundamento, o empregador está não só obrigado a assegurar-se que o tratamento é estritamente necessário para a finalidade em causa, mas também que é proporcional ou seja, tem de se certificar que todos os dados objeto de tratamento de dados são necessários e que os direitos de privacidade dos trabalhadores não se sobrepõem ao interesse legítimo.

É essencial mencionar que todas as citações do GT29º que fizemos, e faremos futuramente, referem sempre o art. 7º, e não 6º, pois o Parecer não incidia sobre os fundamentos referidos no RGPD, mas sim na Diretiva 95/46/CE. Contudo, sendo os mesmos nos dois instrumentos jurídicos, cremos que faz todo o sentido usar este Parecer na nossa análise, inclusivamente no capítulo 2, mesmo que a nossa dissertação já tenha como estudo o RGPD.

### **2.3.2. Princípios orientadores do tratamento de dados**

Com a atualização constante e célere das novas tecnologias, para que o RGPD e a UE consigam acompanhar a modernização dos meios de processamento, é necessária uma aplicação intensa de regras e princípios em cada ato de tratamento, de forma a proteger os interesses e privacidade dos titulares dos dados. Nesse seguimento, os princípios, direitos e liberdades são omnipresentes no RGPD.

Os princípios orientadores do tratamento de dados pessoais estão previstos no art. 5º do RGPD. Defendemos que, estando os princípios do tratamento de dados imediatamente a seguir ao âmbito do RGPD e, portanto, no princípio, apenas pode significar que o legislador pretendeu colocar o artigo numa posição de uma colossal importância.

Em matéria de princípios, Carlos Domènech afirma:

“El Reglamento, en cambio, se aparta de tal sistemática y regula, por un lado, los principios relativos al tratamiento, en los que sitúa los antiguos principios de calidad y otros nuevos como la minimización y la limitación del plazo de conservación o el principio de responsabilidad proactiva, que añade a la obligación del responsable de garantizar los principios relativos al tratamiento la de que sea capaz de demostrarlo.” (Domènech, 2017, p. 97)

Para o nosso subcapítulo, interessam então os princípios relativos ao tratamento dos dados e que são eles: licitude, lealdade e transparência, limitação da finalidade, minimização de dados, exatidão, limitação do prazo de conservação, integridade e confidencialidade e responsabilidade proativa.

Os princípios da licitude, lealdade e transparência encontram-se previstos na al. a) do art. 5º do RGPD.

O princípio da licitude (al. a) do art. 5º) implica a “existência, desde logo, de uma recolha lícita, portanto, baseada no consentimento do titular dos dados, e para uma finalidade específica, ou, em certas ocasiões, de um fundamento legítimo previsto na lei – nacional ou comunitária – ou no regulamento que permita esse tratamento” (Saldanha, 2018, p. 44).

Isto significa que o princípio da legalidade fala por si só: o tratamento de dados pessoais requer uma base/fundamento legal para que se considere legítimo. Estes fundamentos são os referidos no subcapítulo anterior, isto é, os previstos no art. 6º do RGPD.

Neste sentido, Maria Cario e Miguel Cayo afirmam:

“los Estado miembros puedan mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del presente Reglamento, con relación a la licitud del tratamiento, tanto en aquellos casos en que el mismo es necesario para el cumplimiento de una obligación legal aplicable al responsable del mismo, como en aquellos supuestos en que también es necesario para el cumplimiento de

una misión realizada en interés público, por el ejercicio de poderes públicos conferidos al responsable de dicho tratamiento.” (Caro & Gayo (coord), 2016, p. 143)

O princípio da justiça estatui que o processamento de dados deve ser feito de boa-fé, acreditando-se realmente que está a ser feito de forma honesta e legal, devendo existir um equilíbrio justo entre os dados pessoais que as empresas recolhem e processam, com as razões pelas quais o fazem.

O considerando (60) refere-se tanto ao princípio da justiça como ao da transparência quando determina que “os princípios do tratamento equitativo e transparente exigem que o titular dos dados seja informado da operação de tratamento de dados e das suas finalidades. O responsável pelo tratamento deverá fornecer ao titular as informações adicionais necessárias para assegurar um tratamento equitativo e transparente tendo em conta as circunstâncias e o contexto específicos em que os dados pessoais forem tratados”.

O princípio da transparência, referido no parágrafo anterior, implica que “todas as informações ou comunicações acerca dos direitos do titular dos dados, relacionadas com o tratamento de dados pessoais, devem ser de fácil acesso e compreensão. Devem ser formuladas numa linguagem simples e clara” (Saldanha, 2018, p. 46).

O considerando (39) admite que a licitude e a equitabilidade no tratamento de dados devem ser aplicadas às pessoas singulares quanto aos dados recolhidos, utilizados, consultados ou sujeitos a qualquer outro tipo de tratamento a que lhe dizem respeito, bem como a informação de como são ou poderão vir a ser tratados, parecendo-nos que estes dados podem não ser obrigatoriamente colhidos de forma direta, perante o seu titular, sendo possível a sua origem numa recolha exterior. Ademais, o titular dos dados deve conhecer a identidade do responsável pelo tratamento dos mesmos, os fins a que o tratamento se destina, bem como as informações que se destinam a assegurar que seja efetuado com equidade e transparência. As pessoas singulares a quem os dados dizem respeito deverão ser alertadas para os riscos, regras, garantias e direitos associados ao tratamento dos dados pessoais e para os meios de que dispõem para exercer os seus direitos relativamente a esse tratamento.

Também o GT29<sup>o</sup> para a proteção de dados se preocupou em publicar algumas diretrizes sobre o princípio da transparência sob o RGPD<sup>9</sup>, analisando os requisitos da transparência e elencando as informações que devem ser facultadas aos titulares dos dados, bem como as suas limitações.

O princípio da limitação da finalidade, especificado na al. b) do art. 5<sup>o</sup>, estatui que os dados têm de ser recolhidos para finalidades determinadas, explícitas e legítimas, não logrando ser tratados posteriormente de uma forma incompatível com essas finalidades, exceto para um tratamento com o objetivo de investigação científica ou histórica, ou para fins estatísticos (art. 89<sup>o</sup>, n.º 1 do RGPD). Estas finalidades devem ser comunicadas ao titular dos dados, na fase da recolha do consentimento.

Deste modo, o processamento para outra finalidade distinta requer outra permissão legal ou consentimento, exceto se o fim for compatível com o primeiro.

O princípio da minimização de dados determina que a recolha dos dados deve ser adequada, pertinente e limitada ao que é necessário, relativamente às finalidades para as quais são tratados – al. c) do art. 5<sup>o</sup>.

“Este princípio deve ser recebido pelos responsáveis pelo tratamento de dados como uma norma de segurança. Quanto menor for a informação retida, principalmente se desnecessária para as finalidades da organização, menor é o risco de, em caso de perda da informação, de forma ilegal ou por negligência, causar danos aos direitos e liberdades dos titulares dos dados. Dessa forma, restringem-se as potenciais sanções que essa violação pode originar para o responsável pelo tratamento.” (Saldanha, 2018, p. 47)

Contudo, apesar da recolha de dados ter de ser limitada em termos da quantidade, da extensão do processamento e do período de armazenamento, os dados devem ser suficientes para o tratamento.

O princípio está intrinsecamente relacionado com o princípio da limitação de finalidades, diferindo na medida em que requer a restrição de quais dados são armazenados, bem como os dados obtidos.

O princípio da exatidão estabelece que os dados devem ser exatos e atualizados, devendo os responsáveis pelo tratamento excluir ou alterar todos os dados imprecisos ou

---

<sup>9</sup> Disponível em [https://www.cnpd.pt/bin/rgpd/docs/wp260rev01\\_pt.pdf](https://www.cnpd.pt/bin/rgpd/docs/wp260rev01_pt.pdf)

desatualizados. Assim sendo, imediatamente após o responsável se aperceber que os dados estão desatualizados, deve apagá-los.

Desta forma, a precisão é uma característica que se impõe a ter em conta em todas as “atividades” realizadas pelo responsável pelo tratamento dos dados, afetando inclusivamente todos os direitos fundamentais de que os titulares de dados dispõem durante o processo, como é o exemplo do direito ao apagamento ou do direito de retificação. Quanto ao direito de retificação, os titulares dos dados têm o direito de ter as informações incorretas corrigidas e as informações incompletas concluídas.

O princípio da limitação do prazo de conservação impõe que os dados sejam conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados.

Como já estudado no subcapítulo anterior, os dados podem ser conservados durante períodos mais longos nas situações do art. 89º, n.º 1 do RGPD ou seja, quando os dados pessoais são tratados para fins de arquivo no interesse público, para fins de investigação científica ou histórica, ou para fins estatísticos, casos em que a empresa necessita de tomar as medidas técnicas e organizacionais corretas.

Os princípios da integridade e confidencialidade obrigam a que os dados pessoais sejam tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas.

Os dados pessoais devem ser protegidos pelos responsáveis pelo tratamento contra o acesso não autorizado, usando medidas técnicas e organizacionais apropriadas. Para tal, é necessário avaliar o risco de violação dos dados, com o objetivo de implementar a segurança apropriada para os dados. Por isso mesmo o RGPD, no seu art. 35º, prevê que, quando a utilização de novas tecnologias no tratamento de dados (tendo em conta a sua natureza, âmbito, contexto e finalidades) implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o

tratamento, a uma avaliação de impacto<sup>10</sup> das operações de tratamento previstas sobre a proteção de dados pessoais.

Também o n.º 2 do art. 5º prevê um princípio do tratamento: a responsabilidade proativa, que se traduz na obrigação do responsável pelo tratamento comprovar o cumprimento do estatuído no n.º 1 ou seja, que todos os princípios suprarreferidos são cumpridos. Deste modo, o responsável pelo tratamento terá não só de estabelecer medidas que visam implementar em todas as empresas as normas do RGPD no tratamento dos dados, mas garantir a efetividade destas medidas de promoção, sob pena de aplicação de sanções e/ou coimas.

Este princípio aplica-se a todas as empresas, independentemente de onde esteja sediada, ou seja, incluindo as empresas que não têm presença física na UE devem cumprir o GDPR.

## **2.4. O Código do Trabalho**

De maior importância para o nosso estudo, encontramos os direitos de personalidade no início do CT, no Título II “Contrato de trabalho”, Capítulo I “Disposições gerais”, secção II “Sujeitos” e subsecção II “Direitos de personalidade”, especificamente nos arts. 14º a 22º.

Sendo o trabalhador a “personagem principal” do nosso trabalho, a análise dos direitos de personalidade no Código do Trabalho parece-nos ter uma especial relevância, bem como o artigo que foi dedicado pelo legislador aos dados pessoais, situação que não aconteceu noutras Leis. Contudo, não analisaremos, neste capítulo, todos os artigos suprarreferidos, mas sim aqueles que julgamos terem uma conexão, mesmo que indireta, entre os direitos de personalidade do trabalhador e os seus dados pessoais. Por isso mesmo, optámos por não analisar os arts. 14º e 15º, sem, com isso, subestimar a importância destas normas.

Teresa Moreira advoga que o Código do Trabalho deseja “proteger a situação pessoal do trabalhador perante as novas realidades relacionadas com os desenvolvimentos

---

<sup>10</sup> Cfr. Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «susceptível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679, disponibilizadas em [https://www.cnpd.pt/bin/rgpd/docs/wp248rev.01\\_pt.pdf](https://www.cnpd.pt/bin/rgpd/docs/wp248rev.01_pt.pdf)

tecnológicos, tais como o desenvolvimento da informática, a utilização e o manuseamento de tecnologias de informação e comunicação, o incremento e utilização de técnicas de captação e armazenamento de imagens e de dados pessoais, bem como a utilização da ciência médica para efeitos de realização de testes ou exames (...)” (Moreira, 2011b), p. 99).

Desta proteção resultaram limites a determinados poderes presentes na relação entre trabalhador-empregador pois, embora haja subordinação do primeiro em relação ao segundo, os direitos de personalidade pertencentes ao sujeito mais frágil da relação tornaram-se preservados.

Neste mesmo sentido, Sónia Kietzmann Lopes escreveu:

“o trabalhador é, na grande maioria dos casos, o contraente mais fraco, desde logo por o rendimento do trabalho constituir, também em regra, a sua única fonte de subsistência. Assim, face ao espectro de não alcançar ou de perder esse meio de sobrevivência, o candidato ao emprego ou o trabalhador estão (...) psicologicamente condicionados na reivindicação dos seus direitos, liberdades e garantias. O reconhecimento da existência desta compressão de direitos, aliado à ideia de que o trabalhador não perder o direito à individualidade, ou seja, de que não deixa de ser pessoa, só por estar integrado na empresa, aumentou o enfoque sobre os direitos fundamentais do trabalhador no âmbito da relação de trabalho (...). Foi nesta esteira que o Código do Trabalho, aprovado pela Lei n.º 99/2003, de 27 de agosto, dedicou, pela primeira vez na legislação laboral portuguesa, um conjunto de normas aos direitos de personalidade do trabalhador (...).” (Lopes, 2014, pp. 17-18)

O direito à *reserva da intimidade privada* está regulado no art. 16º, que determina que “o empregador e o trabalhador devem respeitar os direitos de personalidade da contraparte, cabendo-lhes, designadamente, guardar reserva quanto à intimidade da vida privada”. Isto significa que é vedada a possibilidade de divulgação e difusão de aspetos íntimos e privados por ambas as partes.

O âmbito de aplicação deste artigo está previsto no art. 80º do CC que refere que todos os indivíduos devem guardar reserva quanto à intimidade da vida privada de outrem, sendo a extensão da reserva definida conforme a natureza do caso e a condição das pessoas. Embora estes artigos sejam de natureza diferente, um laboral e outro civilista, complementam-se.

Uma questão pertinente é a de saber se é admissível a limitação voluntária da reserva da vida privada por meio de consentimento. Mota Pinto advoga que:

“parece ser indispensável, não só exigir a integridade do consentimento para assegurar a existência de uma verdadeira vontade restritiva, como que a restrição não ultrapasse certos limites impostos pela ordem pública. Assim, não se deve admitir uma renúncia global, completa e irrevogável, à esfera da vida privada futura, ou por períodos de tempo alargados” (Pinto P. M., 2018, p. 634).

Guilherme Dray, de quem perfilhamos a ideia, defende que “mesmo nos casos em que haja consentimento por parte do trabalhador quanto à tomada de conhecimento pelo empregador de determinados aspetos da vida privada daquele, continua a incidir sobre o empregador o dever de os não relevar a terceiros, ou vice-versa” (Dray et al., 2013, p. 153).

O artigo elenca alguns aspetos atinentes à esfera íntima e pessoal. Por um lado, comporta determinadas práticas pessoais e familiares do quotidiano do trabalhador, bem como certos aspetos privados da sua vida de que pretende manter segredo de terceiros, pelo que o primeiro pode dispor livremente da sua vida extraprofissional, sendo interdito ao empregador indagar factos dessa sua esfera privada, a não ser que se considere existir uma ligação direta com as suas funções. Por outro lado, engloba também a divulgação de factos e informações, mesmo que obtidas de forma lícita, respeitantes à privacidade de ambas as partes da relação contratual.

Apadrinhamos a opinião de Paula Quintas quando defende que a vontade do trabalhador deve ser respeitada. Nesse sentido diz que “o *eu de cada um* determinará o que pode ou deve ser partilhável. O que nos obriga ao respetivo enquadramento da figura do consentimento informado, ponderando que se encontra cumprido com a máxima lisura, clareza e assertividade o dever de informação que cabe ao empregador acatar” (Quintas, 2013, p. 220).

Também na CRP está consagrado o direito em estudo; a saber, o n.º 2 do art. 18º, que ampara a tese de que a reserva da intimidade da vida privada deve ser regra, e não a exceção, estando consignado que “a lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na Constituição, devendo as restrições limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos”.

Esposando a teoria de Mota Pinto, a violação do direito em estudo constitui um ato ilícito, pelo que o trabalhador não pode apenas defender-se nos termos do art. 337º, n.º 1 do CC, como pode originar responsabilidade civil, regulada no art. 483º, n.º 1 do CC. (Pinto, 2018, p. 585).

A reserva da vida da intimidade privada estabelecida no art. 16º do CT é concretizada nos arts. 17º a 22º do CT, em que o legislador regula o direito à proteção de dados pessoais, o tratamento de dados biométricos, e de testes e exames médicos, o uso dos meios de vigilância à distância, e a confidencialidade de mensagens e de acesso a informação.

O conceito da “*proteção de dados pessoais*” tem especial atenção com a defesa da inviolabilidade da vida pessoal do trabalhador, a que se refere igualmente o art. 16º do CT, sendo, portanto, uma projeção da reserva da intimidade privada.

Com a evolução da tecnologia, ergue-se a capacidade de recolha, armazenamento e tratamento de dados pelo que o conceito de proteção de dados, enquanto expressão da relação do tratamento de dados com o direito à privacidade, assume uma maior relevância.

Através da interpretação do proémio do n.º 1 do art. 17º, constatamos que a grande diferença entre o presente artigo e o anterior é que este engloba não só os trabalhadores, mas também os candidatos a emprego que entram em contacto com o empregador, seja por conta do próprio ou através de terceira pessoa, estes últimos numa fase de provas de seleção no âmbito de concursos públicos e contratos de promessa de trabalho. Abarca-se na proteção de dados o pedido para recolha de determinadas informações, previstas nas als. a) e b) do n.º 1, relativas à vida privada e saúde, respetivamente.

Contudo, as alíneas supramencionadas gozam de exceções e condicionantes, estas previstas na segunda parte da al. a), nomeadamente quando estas sejam estritamente necessárias e relevantes para avaliar a respetiva aptidão no que respeita à execução do contrato de trabalho e seja fornecida, por escrito, a respetiva fundamentação, o que implica que entre o pedido de informações pessoais e as funções exigidas pelo posto de trabalho tem de existir um nexo de necessidade (*cf.* Redinha, 2014, p. 828).

Conquanto seja comprovada a existência de um nexo de necessidade, e abraçando a doutrina de Redinha, é de ter em conta os princípios de necessidade, proporcionalidade e adequação. Posto isto, “não são admitidas incursões na vida privada para além do *quantum* necessário à formulação do juízo, sendo que as informações recolhidas têm que, além disso, ter imediata relevância para as finalidades que o legislador considera objetivamente justificáveis para derrogação do princípio da reserva da intimidade privada” (Redinha, 2014, p. 829).

O empregador não poderá, desta forma, questionar ou indagar o trabalhador sobre aspetos ou pormenores da vida pessoal, deste que excedam o necessário para a formulação de um juízo, com o simples objetivo de preencher determinado posto de trabalho na empresa.

No caso da al. b) do n.º 1 do art. 17º do CT, “o empregador não pode exigir a candidato a emprego ou a trabalhador que preste informações relativas à sua saúde ou estado de gravidez, salvo quando particulares exigências inerentes à natureza da atividade profissional a justifiquem e seja fornecida por escrito a respetiva fundamentação”.

Esta norma é consagrada com o objetivo de “inviabilizar que o empregador pudesse subordinar a celebração do contrato de trabalho, ou a sua subsistência às condições de saúde do trabalhador” (Marecos, 2012, p. 113).

No CT2003, permitia-se que, com o consentimento do candidato a emprego, a entidade patronal acesse aos resultados dos exames do primeiro; esta norma era incompreensível, considerando o desequilíbrio de poder existente no vínculo laboral, sendo difícil afirmar que o consentimento era livre. Ademais, o empregador carecia de fundamentos que justificassem a aspiração de conhecer os motivos pelos quais o trabalhador estava apto, ou não, para o exercício das funções solicitadas (*cf.* Marecos (2012, p. 107)).

Assim sendo, aquando da nova redação do Código do Trabalho, o legislador retirou a possibilidade deste consentimento do trabalhador, sendo apenas possível, desde 2009, o médico que realiza os devidos exames, indicar se o trabalhador é apto ou inapto para o posto de trabalho a que se candidata.

Por outro lado, outra derrogação que o artigo inclui, e muito bem, é o estado de gravidez, que pode constituir um fator discriminatório. Ilustrando, teremos o caso de uma candidata a emprego que se encontra grávida, não tencionando o empregador sujeitar-se à contratação desta devido à necessidade de licença parental, num futuro próximo. Relembramos que a parte final da alínea b) apresenta exceções, como já foi referido. Situações exemplificativas destas exceções serão as de profissionais de saúde ou pilotos de aeronaves.

Se porventura a situação em apreço for considerada exceção, exige-se a intermediação de um médico do trabalho ou profissional de saúde, sujeito a sigilo

profissional, pelo que apenas este terá acesso e controlo dos dados de saúde. Assim sendo, este só pode comunicar ao empregador se o trabalhador está, ou não, apto a desempenhar a atividade (n.º 2 do art. 17º).

Assim sendo, defendemos que, após a alteração que se verificou no CT2003, tanto o artigo em estudo como o art. 19º, n.º 3 não admitem, de todo, a revelação de resultados de exames, mesmo com o consentimento do trabalhador<sup>11</sup>.

O art. 17º garante ainda ao trabalhador o direito de controlar os seus dados pessoais que estão na posse do empregador, a conhecer o seu teor, e os fins a que os mesmos se destinam. Ora, parece-nos que as informações a que se refere o artigo serão todas as de natureza pessoal e íntima, passíveis de ser recolhidas nos termos do n.º 1 do art. 17º, de forma lícita.

Quanto ao tratamento de ficheiros e acessos informáticos utilizados pelo empregador para tratamento de dados pessoais do candidato a emprego ou trabalhador, o artigo remete para a legislação em vigor relativa à proteção de dados pessoais, sendo que, em Portugal, se refere atualmente à Lei n.º 58/2019, de 8 de agosto.

O Código do trabalho regula também os “*dados biométricos*”, que se inserem na categoria de dados especiais, previstos no art. 9º do RGPD. Nestas situações “constituem os dados recolhidos através de sistemas que se baseiam na análise e mensuração de dados biológicos em comparação com uma amostra digital (*template*)” (Redinha, 2014, p. 833); a saber, entre outros, a impressão digital, o ADN, a geometria da mão ou da face, o padrão da íris, o reconhecimento da retina, ou até o formato da orelha.

Resumidamente, e quanto à forma de funcionamento destes sistemas, Maria Redinha apadrinha a tese de que “os sistemas de autenticação ou de reconhecimento biométrico baseiam-se nas características físicas e comportamentais únicas e distintivas de cada ser humano que podem ser apreendidas através de sensores e representadas sob um formato numérico que permite um resultado ou uma decisão automáticos” (Redinha, 2014, p. 833).

De acordo com o art. 9º do RGPD, no que concerne ao tratamento de dados biométricos, a regra geral é a sua interdição, admitindo algumas exceções no seu n.º 2. O tratamento destes dados está sujeito, obrigatoriamente, a “avaliação de impacto sobre a

---

<sup>11</sup> Neste sentido, cf. Guilherme Dray (2013, p. 161), Moreira (2011b), pp. 107-108) e Marecos (2012, p. 117).

proteção de dados” (*cf.* art. 35º, n.º 3, al. b) do RGPD), tendo em conta que o tratamento implica um elevado risco para os direitos e liberdades do trabalhador; esta avaliação corre nos termos dos artigos 35º e 36º do RGPD.

Assim sendo, “a sua utilização será permitida desde que prossiga finalidades lícitas, nomeadamente desde que se confina nos limites do poder de direção do empregador, não contenda com a dignidade ou privacidade do trabalhador e não imponha um incómodo ou uma exposição excessivos para o resultado a atingir” (Redinha, 2014, p. 834). No caso de o empregador não respeitar estes requisitos, propicia uma contraordenação muito grave.

Torna-se relevante atender ao corolário dos princípios da necessidade e proporcionalidade, quando se estabelece um limite temporal aos dados abrangidos pelo n.º 2 do art. 18º, sendo que os dados só podem ser conservados durante o período necessário para a prossecução das finalidades do tratamento, devendo ser eliminados no momento em que o trabalhador é transferido para outro local de trabalho, ou no caso do contrato de trabalho cessar.

A proteção prevista para a realização de “*testes e exames médicos*” do trabalhador, e do candidato a emprego, constitui uma manifestação do princípio de reserva previsto no art. 17º. Este artigo pretende inviabilizar que a entidade empregadora possa subordinar a celebração do contrato de trabalho, ou a sua manutenção, às condições de saúde.

Em termos gerais, o empregador não pode exigir a realização ou apresentação de testes ou exames médicos que comprovem o estado de saúde, com o objetivo de decidir se admite o potencial candidato a preencher determinado posto de trabalho ou conserva o trabalhador na empresa, exceto nas situações previstas em legislação relativa a segurança e saúde no trabalho ou quando particulares exigências inerentes à atividade o justifiquem, devendo ser apresentada a respetiva fundamentação por escrito (n.º 1, *in fine*).

A legislação que regula a SST é a Lei n.º 102/2009, de 10 de setembro e a Lei n.º 12/2005, de 26 de janeiro, que permitem ao empregador a realização de exames de saúde, desde que adequados a comprovar e avaliar a aptidão física e psíquica do trabalhador para o exercício da atividade, tanto aquando a admissão do trabalhador, como durante a execução do contrato, se justificado (*cf.* Lopes S. K., 2014, p. 32).

No que concerne à Lei n.º 12/2005, o art. 13º, com a epígrafe “*testes genéticos no emprego*” estatui que, por um lado, “a contratação de novos trabalhadores não pode

depende de seleção assente no pedido, realização ou resultados prévios de testes genéticos” (n.º 1) – candidatos a emprego - e, por outro lado, que “às empresas e outras entidades patronais não é permitido exigir aos seus trabalhadores, mesmo que com o seu consentimento, a realização de testes genéticos ou a divulgação de resultados previamente obtidos” (n.º 2), excetuando-se as situações elencadas nos n.ºs 3 e 4 deste mesmo artigo.

De referir que a presente lei define, no art. 6º, n.º 1, “a informação genética como a informação de saúde que verse as características hereditárias de uma ou de várias pessoas, aparentadas entre si ou com características comuns daquele tipo (...)”.

Seja no caso dos exames obrigatórios pela SST, ou no âmbito das restantes exceções, concluímos pelo n.º 3 do art. 17º que o empregador não pode ter acesso ao resultado dos exames, recebendo somente comunicação, por parte do médico responsável, quanto à (in)aptidão para a execução da atividade; em caso negativo, o médico do trabalho deve indicar, sendo caso disso, outras funções que aquele possa desempenhar (art. 110º, n.º 2 da Lei 102/2009).

Significa isto que os testes ou exames a que são sujeitos o trabalhador ou o candidato não podem deter uma aplicação abusiva, discriminatória ou arbitrária. Consideramos, nesses casos, que violamos o direito à vida privada, caso não se respeite esta norma, pelo que se deve atender ao princípio da proporcionalidade aquando da decisão de exigir ao candidato a emprego ou ao trabalhador “a realização ou apresentação de testes ou exames médicos, de qualquer natureza, para comprovação das condições físicas ou psíquicas”.

O n.º 2 do art. 19º decreta que “o empregador não pode, em circunstância alguma, exigir a candidata a emprego ou a trabalhadora a realização ou apresentação de testes ou exames de gravidez” pelo que não abre qualquer exceção relativa a esta norma, tendo em conta o carácter intrusivo na intimidade da trabalhadora, bem como um potencial fator discriminatório que o estado de gravidez pode desencadear no acesso, progressão ou manutenção do vínculo jurídico-laboral (*cf.* Redinha, 2014, p. 839). Neste ponto, remete-se para a análise já feita sobre a al. b) do n.º 1 do art. 17º do CT.

A regulamentação dos “*meios de vigilância à distância*” deriva da utilização das novas tecnologias de informação e comunicação (não havendo correspondência no CT2003), sendo de extrema relevância devido ao rápido desenvolvimento da tecnologia,

alargando a cada dia que passa o leque de equipamentos e sistemas de vigilância e a consequente facilidade de violação da esfera de reserva privada e pessoal do trabalhador.

O princípio geral consiste no empregador não poder utilizar meios de vigilância a distância no local de trabalho, mediante o emprego de equipamento tecnológico, com a finalidade de controlar o desempenho profissional do trabalhador, sob pena da ilicitude do ato.

Este princípio não é sinónimo de que estes meios de vigilância são obrigatoriamente negativos, pois as utilizações destes sistemas são úteis no que concerne à proteção e segurança das pessoas e bens, contanto que a sua utilização não viole a proteção dos dados pessoais e a intimidade do trabalhador, sob pena de se criar um ambiente que pode ser hostil no local de trabalho.

Neste sentido, também Redinha afirma que “se o empregador é o proprietário dos equipamentos e sistemas tecnológicos instalados na empresa e portanto adstritos à execução da prestação de trabalho, o trabalhador, no tempo e local de trabalho, não deixa de ser titular do direito a uma zona de reserva pessoal, pelo que a articulação de ambos os direitos pode ser, na prática, de difícil alcance” (Redinha, 2014, p. 841).

Os equipamentos suprarreferidos pressupõem a monitorização não presencial do trabalhador (ou do seu desempenho) por quaisquer meios técnicos, eletrónicos ou não. Exemplos são as câmaras de vídeo, equipamento audiovisual, microfones dissimulados, mecanismos de escuta, registo telefónico ou GPS, e atualmente outros *softwares* avançados de controlo da atividade do trabalhador.

Contudo, a utilização de equipamentos referidos no n.º 1 do art. 20º é lícita sempre que tenha por finalidade a proteção e segurança de pessoas e bens ou quando particulares exigências inerentes à natureza da atividade o justifiquem. Exemplo comum será nos estabelecimentos com venda ao público, em que existe possibilidade de furto dos bens, ou, no segundo caso, o exemplo das comunicações entre os pilotos de aviação e os controladores aéreos no decurso de uma viagem, por motivos de segurança.

Mais uma vez, e adotando a filosofia de Dray:

“importa atender aos princípios da proporcionalidade, necessidade e adequação: qualquer decisão sobre a realização de controlo a distância da atividade laboral deve ser criteriosa, evitando-se que os benefícios que o empregador pretende obter

sejam desproporcionados em relação ao grau de lesão que vai ser causado à privacidade dos trabalhadores.” (Dray et al., 2013, p. 162).

Note-se que a licitude da utilização dos meios de vigilância carece de informação ao trabalhador sobre a existência e finalidade dos meios de vigilância utilizados. Parece-nos que esta comunicação ao trabalhador deve ser feita de forma escrita e expressa, fundamentando o emprego dos meios de vigilância, e explicitando qual o meio, constituindo assim prova irrefutável de que o trabalhador foi notificado.

O uso da videovigilância obriga a entidade empregadora a afixar nos locais sujeitos a vigilância os seguintes dizeres, consoante os casos: «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”, sob pena de contraordenação, podendo a decisão condenatória ser objeto de publicação nos termos do art. 562º, n.º 2 do CT. Podemos acrescentar a possibilidade de existir responsabilidade civil por parte do empregador, caso o uso dos meios de vigilância seja ilícito.

O art. 21º versa também sobre os meios de vigilância à distância, especificamente sobre a sua “*Utilização*” pelo que os arts. 20º e 21º estão intrinsecamente ligados.

É importante mencionar que, com a entrada em vigor do RGPD, passámos de um sistema de heterorregulação para um sistema de autorregulação de proteção de dados, pelo que agora se instalou a desnecessidade de solicitar autorização à CNPD para a utilização de meios tecnológicos de vigilância à distância (vulgo CCTV); ora, resulta daqui que os n.ºs 1 e 2 deste artigo 21.º do CT se tornaram obsoletos (cf. Nascimento & Gama (2019, p. 4)).

Os dados pessoais recolhidos através dos meios de vigilância à distância são conservados durante o período necessário para a prossecução das finalidades da utilização a que se destinam, devendo ser destruídos no momento da transferência do trabalhador para outro local de trabalho ou da cessação do contrato de trabalho (n.º 3), sob pena de se considerar a existência de contraordenação grave.

Contudo, é primordial conjugarmos a norma em apreço com o RGPD, na medida em que nos apercebemos que a destruição dos dados pode ocorrer em momentos distintos dos constantes no n.º 3 do art. 21º do CT, contanto que o princípio da “limitação da

conservação”, previsto no art. 5º, n.º 1, al. e) do RGPD, expõe que os dados devem ser “conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados”, com as devidas exceções.

Por fim, o CT regula ainda a “*confidencialidade de mensagens e de acesso a informação*”, tendo uma correspondente consagração constitucional no art. 34º da CRP, decretando o seu n.º 1 que “o domicílio e o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis”. Estes artigos são uma projeção do art. 16º do CT e do art. 26º, n.º 1 da CRP, ou seja, da reserva da intimidade da vida privada e familiar.

Estabelece-se que o trabalhador goza do direito de reserva e confidencialidade relativamente ao conteúdo das mensagens de natureza pessoal e acesso a informação de carácter não profissional, nomeadamente através do correio eletrónico, não obstante o empregador gozar do direito de estabelecer regras de utilização dos meios de comunicação na empresa. Nas palavras de Regina Redinha,

“o n.º 1 proclama o direito de reserva e confidencialidade sobre mensagens pessoais e informação de natureza não profissional consultada pelo trabalhador no tempo e local de trabalho da prestação, através da utilização de meios ou instrumentos de trabalho, colocados à sua disposição pelo trabalhador. O bem jurídico aqui protegido é ainda, como nos artigos precedentes, à exceção da liberdade de expressão e da integridade física e moral, o círculo de reserva, pessoal, privada e íntima do indivíduo. É, no entanto, percussora a preocupação por algumas novas formas de agressão da personalidade e a sua inclusão em torno de um núcleo tradicional que já fazia parte da tutela civil.” (Redinha, 2014, p. 846).

Ora, na primeira vertente, conteúdo das mensagens de natureza pessoal, parece-nos que se incluem todas as mensagens em suporte escrito ou oral, recebidas ou emitidas no local de trabalho, desde o correio eletrónico às missivas postais (cartas, telegramas, encomendas ou bilhetes) bem como às chamadas telefónicas. Compreendem-se igualmente mensagens deixadas em atendedor automático, PDA (*personal digital assistant*), telemóveis, chamadas em *chat rooms*, comentários nas redes sociais, entre outros.

Estas mensagens têm de conter uma natureza pessoal, tal como referido no próprio artigo, o que se torna penoso de distinguir quando a mensagem não possui um invólucro físico e está mantida num instrumento laboral pertencente ao empregador. Cremos que

para uma correta distinção, será produtivo tentar perceber se algum do conteúdo da mensagem se conexas (mesmo que indiretamente), ou não, com a atividade laboral<sup>12</sup>.

Quanto às mensagens dirigidas para um equipamento propriedade do empregador, considerado um equipamento coletivo, cremos que as mensagens não se presumem pessoais visto que, se o fossem, o trabalhador teria mais zelo pela sua confidencialidade. Aliás, a probabilidade do empregador apenas constatar a natureza pessoal da mensagem após analisar o seu teor, é colossal.

Por outro lado, quando falamos de acesso a informação de carácter não profissional, incluem-se os dados recolhidos, conservados ou reencaminhados pelo trabalhador, de carácter pessoal, no seu computador, seja através do correio eletrónico ou suporte digital. Se estes meios forem postos à disposição por parte do empregador, visando servir como instrumentos de trabalho, depreendemos que o empregador pode circunscrever o acesso para contactos extraprofissionais.

Com efeito, verifica-se uma divergência entre a tutela da personalidade do trabalhador e o poder de direção da entidade empregadora, porquanto o direito que o trabalhador dispõe de conservar o tráfego de mensagens de natureza extraprofissional não anula o direito de o empregador estabelecer certos cânones que restrinjam o proveito dos meios que o próprio disponibilizou para fins pessoais.

Se o uso dos meios para fins pessoais for autorizado, a entidade empregadora não poderá inteirar-se ou divulgar o conteúdo das mensagens de natureza pessoal, ou os acessos levados a cabo pelo trabalhador com carácter extraprofissional (*cf.* Lopes S. K., 2014, p. 41). Neste seguimento, se o empregador aceder ao conteúdo das mensagens, não o poderá fazer valer contra o trabalhador em sede de procedimento disciplinar, sendo a prova considerada nula, nos termos do art. 32º, n.º 8 da CRP.

Na falta de autorização, se o trabalhador não acatar as diretrizes indicadas, propõem-se duas hipóteses: se o empregador conhecer a natureza pessoal, é-lhe interdito o acesso ao seu conteúdo, aplicando-se o art. 335º do CC; se o empregador desconhecer a natureza pessoal, não se aplica a responsabilização por violação do direito de

---

<sup>12</sup> Também neste sentido advoga Teresa Moreira (2011, p. 51). O controlo das comunicações eletrónicas dos trabalhadores *in* Estudos de Direito do Trabalho.

personalidade com os consequentes corolários inerentes, sendo a ação justificada por correr no exercício do poder de direção, sem que lhe possa ser exigível outro comportamento (Redinha, 2014, pp. 851-852). Na segunda hipótese, o trabalhador pode incorrer na prática de ilícito disciplinar nos termos do art. 128º, n.º 1, al. e) do CT.

Dessarte, observa-se, mais uma vez, a relevância que o legislador deu à tutela dos direitos de personalidade dos trabalhadores, desde a celebração do contrato de trabalho, até à sua cessação e, consequentemente, ao princípio geral de prevalência destes direitos (do trabalhador) sobre os poderes da entidade empregadora.

## **2.5. Outros instrumentos de Direito Internacional**

“In the European Union, the right to a private life and associated freedoms are considered fundamental human rights.” (IAPP , 2018, p. 1).

“A clear starting point for framing standards for the protection of individuals was the Universal Declaration of Human Rights (‘Human Rights Declaration’), adopted on 10 December 1948 by the General Assembly of the United Nations.” (IAPP , 2018, p. 1).

Neste instrumento jurídico internacional (DUDH), consagrou-se no artigo 12.º o direito à proteção contra intromissões de terceiros, especialmente do Estado, na vida privada e familiar.

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

A previsão deste artigo 12º tem correspondência no n.º 1 do artigo 8º da CEDH (originalmente designado por “Council of Europe invited individual states to sign the European Convention on Human Rights”), que surgiu em Roma, no ano de 1950, tendo entrado apenas em vigor no dia 3 de setembro de 1953, e que se pode considerar, até aos dias de hoje, o mais importante instrumento de Direitos Humanos a nível europeu.

Neste instrumento, o art. 8º garante o direito ao respeito pela vida privada e familiar, pelo domicílio e pela correspondência. Este artigo “alude ao direito à coibição de estranhos quanto ao acesso a informações e disposições da vida conexas como privada pelo próprio, da mesma forma que se percebe o direito como uma interdição à divulgação das informações que se tenham sobre a vida privada de outrem” (Canotilho & Moreira, 2007, p. 467).

“This article therefore protects the rights of individuals for their personal information to remain private, but again, this is not an absolute right and necessity, and proportionality may justify breaching an individual’s privacy rights in the public interest” (IAPP, 2018, p. 2).

“Em 1959, foi criado em Estrasburgo, França, o Tribunal Europeu dos Direitos do Homem (TEDH) para garantir que as Partes Contratantes cumprem as obrigações assumidas ao abrigo da CEDH. O TEDH assegura o cumprimento das obrigações assumidas pelos Estados ao abrigo da Convenção.” (FRA, 2014, p. 14). Segundo a Agência dos Direitos Fundamentais da União Europeia, “o TEDH esclareceu que o artigo 8.º da CEDH não só obriga os Estados a absterem-se de praticar atos suscetíveis de violar este direito consagrado na Convenção, como impõe também, em certos casos, uma obrigação positiva de assegurar ativamente o respeito efetivo pela vida privada e familiar” (FRA, 2014, p. 15).

Note-se, porém, que este direito “não é um direito absoluto, devendo, pelo contrário, ser conciliado com outros interesses legítimos, sejam de outras pessoas (interesses privados) ou da sociedade no seu todo (interesses públicos)” (FRA, 2014, p. 67), exceções que não tencionamos abordar na presente dissertação por ser um tema vasto.

“Mais tarde, em 1981, e em consequência do surgimento, nos anos 60 do século XX, das tecnologias de informação e da necessidade, na década seguinte, da existência de um conjunto de resoluções sobre proteção de dados, com base precisamente no art. 8º, foi estabelecida a Convenção 108” (Saldanha, 2018, p. 3).

Em suma, esta Convenção<sup>13</sup> visa a proteção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal. “In Convention 108, the Council of Europe took the view that those holding and using personal information in computerised form have a

---

<sup>13</sup> Disponível para consulta em <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>

social responsibility to safeguard such personal information, particularly as at that time, decisions that affect individuals were increasingly based on information stored in computerised data files” (IAPP , 2018, p. 6).

Segundo a FRA, a Convenção 108:

“protege as pessoas contra os abusos que podem acompanhar a recolha e o tratamento de dados pessoais e procura simultaneamente regular o fluxo transfronteiriço de dados pessoais. Quanto à recolha e tratamento de dados pessoais, os princípios estabelecidos na Convenção respeitam, em especial, à recolha e tratamento automatizado de dados de forma leal e lícita, armazenados para finalidades determinadas e legítimas, não podendo ser utilizados para fins incompatíveis com essas finalidades nem conservados por tempo superior ao necessário. Dizem também respeito à qualidade dos dados, estabelecendo, em especial, que têm de ser adequados, pertinentes e não excessivos (proporcionalidade), bem como exatos” (FRA, 2014, p. 16).

Não podemos deixar de reiterar que certamente existem outros instrumentos de carácter internacional relativos à proteção de dados. Contudo, tendo em conta o carácter sumário deste ponto, apenas abordámos os instrumentos que cremos ter a maior relevância e impacto em tantos países pelo mundo.

## Capítulo 2. O consentimento do trabalhador na utilização dos dados pessoais

O consentimento surge no RGPD como um fundamento geral de licitude de tratamento de dados pessoais (artigo 6.º, n.º 1, al. a) e artigo 7.º). O artigo 6.º do RGPD faz referência ao consentimento como um dos seis fundamentos diferentes para legitimar o tratamento de dados pessoais, estando este previsto na alínea a), ao afirmar que “o tratamento só é lícito se e na medida em que (...) a) o titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas”.

Os restantes fundamentos para o tratamento de dados pessoais repousam, genericamente, na execução de um contrato (art. 6.º, n.º 1, al. b), numa obrigação jurídica do empregador (art. 6.º, n.º 1, al. c), em interesses vitais (art. 6.º, n.º 1, al. d), no interesse público ou ao exercício da autoridade pública (art. 6.º, n.º 1, al. e), ou, e provavelmente o mais comum, em interesses legítimos do empregador (art. 6.º, n.º 1, al. f)).

No que respeita à noção de consentimento, quando foi transposta para a lei nacional a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, surgiu pela primeira vez um conceito de consentimento em matéria de proteção de dados, aposto no art. 2.º, al. h) da LPDP, agora revogada pela Lei n.º 58/2019, que se traduzia em: “qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objeto de tratamento.”

Vulgarmente, e recorrendo a um dicionário, o conceito de consentimento consiste essencialmente, no “ato ou efeito de consentir, na manifestação que autoriza algo, na manifestação a favor de algo ou alguém, numa tolerância, num acordo ou conformidade de opiniões, ou ordem.”<sup>14</sup>

Contudo, o consentimento, no âmbito da proteção de dados, traduz-se no primeiro dos seis fundamentos para o tratamento dos dados, previstos no art. 6.º do RGPD, tornando-

---

<sup>14</sup> Definição de "consentimento", in Dicionário Priberam da Língua Portuguesa, 2008-2020, disponível em <https://dicionario.priberam.org/consentimento> [consultado em 02-04-2020].

se, desta forma, num critério de legitimação das atividades de tratamento de dados pessoais, tese defendida no art. 8º, n.º 2 da Carta dos Direitos Fundamentais, ao prever que o consentimento do trabalhador proporciona que os dados pessoais sejam objeto de tratamento. Constitui, esta noção, uma tutela do direito à privacidade e à proteção dos dados pessoais, direitos fundamentais do trabalhador no âmbito do seu vínculo laboral, na qualidade de pessoa singular, especialmente perante uma situação de subordinação jurídica.

Fazemos uma brevíssima referência ao direito comparado, mencionando que, ao contrário de Portugal, nem todos os países optaram por transpor este conceito para as suas leis nacionais. Na legislação estrangeira, nomeadamente em França e no Reino Unido, a definição de consentimento não coincidia com a proposta pelo Conselho Europeu. Aliás, como explica o GT29º:

“o conceito de consentimento nem sempre foi transposto de forma literal ao nível nacional. A título exemplificativo, refira-se que o consentimento, como conceito geral, não foi definido na legislação francesa relativa à proteção de dados. Não obstante, o seu significado tem sido explicado de forma precisa e consistente na jurisprudência da autoridade de proteção de dados (CNIL), por referência à definição contida na Diretiva da Proteção de Dados Pessoais. No Reino Unido, o conceito de consentimento tem sido desenvolvido pela jurisprudência por referência ao texto da diretiva. Para além disso, o consentimento tem sido por vezes explicitamente definido em setores específicos, como por exemplo no contexto da privacidade eletrónica e da administração ou saúde em linha. O conceito desenvolvido na legislação específica irá, desta forma, interagir com o conceito desenvolvido na legislação geral de proteção de dados. (GT29º, 2011b), p. 7)

Atualmente, o art. 4º, n.º XI do RGPD, define o consentimento como a “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.” (nosso sublinhado)

O consentimento carece de alguns requisitos, a saber: tem de ser informado, específico, inequívoco e livre.

É informado quando o titular dos dados é esclarecido quanto à identidade do controlador, qual o tipo de dados que será processado, bem como o objetivo e modo do tratamento.

De acordo com o GT29°, o consentimento só se considera informado, se ao trabalhador forem comunicados determinados dizeres, nomeadamente a identidade do responsável pelo tratamento, a finalidade de cada uma das operações de tratamento em relação às quais se procura obter o consentimento, que dados serão recolhidos e utilizados, a existência do direito de retirar o consentimento, como se processa a utilização dos dados para decisões automatizadas, se adequado ao caso, e os possíveis riscos de transferências de dados, nos termos do art. 46° do RGPD (*cf.* GT29° (2017a), pp. 14-15)).

O titular dos dados também deve ser informado sobre o seu direito de retirar o consentimento a qualquer momento e, quando seja o caso, sobre os possíveis riscos de transferência de dados, quando haja ausência de medidas de proteção dos dados ou outras salvaguardas apropriadas.

É específico se ao trabalhador for solicitado o seu consentimento em relação a uma ou mais finalidades específicas, e que o mesmo tenha uma livre escolha em relação a cada uma delas. Isto significa que a declaração deve ser redigida de forma clara e precisa, alertando para as possíveis consequências do tratamento dos dados, e definindo o conjunto de atividades limitadas para que é prestado o consentimento.

Para a validade deste requisito, deve ser pedido o consentimento, quantas vezes necessário, para cada operação de processamento de dados diferente.

Atenda-se neste pressuposto ao princípio da limitação de finalidades (art. 5°, n.º 1, al. b) do RGPD), abordado no capítulo anterior, que delimita as finalidades para as quais os dados são processados, após o trabalhador consentir na sua recolha inicial, afirmando, assim, que os dados pessoais do trabalhador não possam ser tratados posteriormente de uma forma incompatível com as inaugurais finalidades.

Considerando que o requisito da especificidade está preenchido, o consentimento deve também ser inequívoco, ou seja, é necessária uma declaração expressa ou um claro ato afirmativo do consentimento por parte do titular dos dados.

Defendemos a tese do GT29°, quando afirma que, num contexto digital, “o titular de dados possa emitir a declaração necessária preenchendo um formulário eletrónico, enviando uma mensagem de correio eletrónico, carregando um documento digitalizado com a assinatura do titular dos dados ou utilizando uma assinatura eletrónica” (GT29°, 2017a), p. 21).

Nuno Saldanha (2018, p. 45) defende que a declaração de consentimento deve ser previamente disponibilizada pelo responsável pelo tratamento, de forma inteligível e informada, pelo que deve ser escrita numa linguagem clara e simples, sem cláusulas abusivas. Se essa declaração escrita referir múltiplas matérias, têm de existir garantias suficientes de que o titular dos dados está plenamente consciente do consentimento dado.

Um último requisito, mas não menos relevante que os restantes, é a necessidade de o consentimento ser livre. Considera-se livre quando é dado voluntariamente, de forma genuína, livre de pressão ou influência inadequada que possa afetar o resultado da sua escolha.

A necessidade de verificação destes requisitos é cumulativa, o que torna particularmente difícil a utilização do consentimento como fundamento do tratamento no âmbito da relação de trabalho, tendo em conta que o poder diretivo do empregador se sobrepõe à autonomia privada do trabalhador, associada, na maioria das vezes, à dependência económica do trabalhador (Coutinho & Moniz, 2019, p. 19).

Esta consequência do contrato de trabalho, e consequentemente do desequilíbrio de poder entre as partes, coloca o trabalhador numa posição frágil, que implica a incapacidade de manifestar a sua vontade de forma livre<sup>15</sup>.

Refira-se que, além dos quatro requisitos do art. 4º do RGPD, também o art. 7º do mesmo Regulamento refere uma condição para um consentimento válido; a saber, quanto ao pedido de consentimento através de declaração dada por escrito, que diga também respeito a outros assuntos, obrigando o legislador a que o pedido seja apresentado de uma forma que o distinga claramente desses outros assuntos de modo inteligível e de fácil acesso, e numa linguagem clara e simples.

---

<sup>15</sup> No mesmo sentido, *vide*, na doutrina espanhola, por exemplo, Maria Caro e Miguel Gaio, “la tratamiento de los datos personales recabados de la relación laboral ha de estar legitimada atendiendo a los usos y finalidades para las que se obtuvieron, no queriendo por ello decidir que exista un amparo legal para la recogida de cualquier dato personal en el ámbito de las relaciones laborales por parte del empresario ni que esta pueda estar disfrazada bajo una apariencia de necesidad laboral” (Caro & Gayo (coord), 2016, pp. 624-625).

## 1. Os problemas gerais do consentimento do trabalhador como requisito de licitude do tratamento

O primeiro fundamento previsto no RGPD que permite o tratamento lícito do trabalhador é o consentimento – ver al. a) do n.º 1 do art. 6º.

Desde logo, o Grupo Trabalho do art. 29º indica “o *desequilíbrio de poder* como um dos problemas gerais do consentimento, atendendo à dependência que resulta da relação empregador/trabalhador, quando é provável que o trabalhador dê o seu consentimento para o tratamento de dados para que a execução de um contrato prossiga (*condicionalidade*)”.

Aliás, este é, sem dúvida, o maior problema do fundamento do consentimento.

Se analisarmos o RGPD, o considerando (43) relata que o consentimento não constitui fundamento jurídico válido para o tratamento de dados pessoais “em casos específicos em que exista um *desequilíbrio* manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública pelo que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa.”

O considerando citado no parágrafo anterior indica-nos que o próprio legislador já previa o *desequilíbrio de poder* como um obstáculo ao livre consentimento. Neste seguimento, cremos que, na relação laboral, o *desequilíbrio de poder* é, sem dúvida, uma situação de grande impacto, demonstrada na impossibilidade de o trabalhador dar o seu consentimento livremente, que se traduz usualmente na figura da **subordinação jurídica**.

De acordo com Maria Fernandes (2009, pp. 15-16), do contrato de trabalho configura um vínculo jurídico complexo, emergindo dele uma vertente obrigacional, à qual corresponde o binómio prestação de trabalho/prestação retributiva ou seja, pelo trabalho prestado pelo trabalhador, é devida uma remuneração, e a vertente laboral integrada pelo binómio subordinação jurídica/poderes laborais, tendo em conta o *desequilíbrio de poderes* decorrentes da relação laboral, isto é, da relação entre empregador-trabalhador.

Do supracitado, infere-se que a subordinação jurídica resulta, desde logo, do poder disciplinar atribuído pela própria lei ao empregador, o qual se pode encontrar atribuído no art. 329º, n.º 4 do CT, e, por outro lado, pela relação de dependência necessária da conduta

pessoal do trabalhador face às ordens e regras impostas pelo empregador, derivadas do vínculo laboral. Neste sentido, diz o Tribunal da Relação de Coimbra:

“a subordinação jurídica típica de uma relação de trabalho subordinado implica uma posição de supremacia do credor da prestação de trabalho e a correlativa posição de sujeição do trabalhador, cuja conduta pessoal, na execução do contrato, está necessariamente dependente das ordens, regras ou orientações ditadas pelo empregador, dentro dos limites do contrato e das normas que o regem.”

(Ac. T.R. Coimbra, datado de 03 de abril de 2014)

Esta conduta relaciona-se, então, com a pessoa do trabalhador “uma vez que identifica o seu posicionamento subjetivo no contrato de trabalho (apenas uma pessoa pode ser subordinada); por este motivo, *a um estado de dependência pessoal* (a *persönliche Abhängigkeit* a que se refere a doutrina germânica) do trabalhador perante o credor” (Ramalho, 2012, p. 31).

No instituto da subordinação jurídica destacam-se assim “os poderes patronais de direção e correlativas situações passivas do trabalhador dependente, devedor de obediência, submetido à autoridade, controlado e disciplinado” (Xavier, 2014, p. 309). Significa isto que se “protege de forma veemente os titulares de um vínculo contratual laboral enquanto deixa sem tutela os prestadores de trabalho desprovidos de tal vínculo” (Carvalho, Machado, & Costa, 2018, p. 15).

Também o conceito de dependência económica pode tratar-se de um grande fator chave, associado à subordinação jurídica (e não um sinónimo<sup>16</sup>), para a existência de um desequilíbrio de poderes, quando o trabalhador se encontra numa situação em que a retribuição é o único meio de subsistência. Nestas situações, é justificada a atitude que o trabalhador toma, ao aceitar as imposições do empregador.

Tal como advoga o Grupo do Artigo 29º, é a dependência que constitui um obstáculo à possibilidade de se caracterizar o consentimento como livre. A realidade é que o fenómeno laboral acarreta uma coação sobre o trabalhador, tendo este medo de que, se recusar o pedido do empregador, sofra efeitos negativos e prejudiciais no local de trabalho e na sua profissão.

---

<sup>16</sup> Quanto à distinção, cf. Fernandes A. M. (2012, p. 116)

Nesse seguimento, atendendo mais uma vez à doutrina deste Grupo de Trabalho, a dependência que resulta da relação empregador/trabalhador, é improvável que o trabalhador possa recusar ao seu empregador o consentimento para o tratamento dos seus dados pessoais sem que haja medo ou risco real de consequências negativas, decorrentes da recusa.

Desta forma, a desigualdade de poderes será sempre o problema primordial do consentimento do trabalhador, não sendo possível distinguir quando é dado de livre vontade, ou não. Por isso mesmo, em muitas situações que poderemos estudar infra, tem de se atender a outros fundamentos previstos no RGPD para se poder tomar a decisão de tratar os dados, ou não.

No mesmo sentido, Francisco Coutinho e Graça Moniz afirmam que os requisitos do consentimento elencados no RGPD (manifestação de vontade livre, específica e informada) são, no mínimo:

“pressupostos de difícil concretização no contexto de uma relação de trabalho, onde a autonomia privada do trabalhador se encontra sujeita, de forma legítima, ao poder diretivo do empregador e, igualmente relevante, muitas vezes cortada pela dependência económica do trabalhador relativamente ao seu vínculo laboral (e à remuneração resultante deste). Situação que o pode colocar especialmente fragilizado e, até, incapaz de manifestar a sua vontade de forma livre. Esta construção abstrata de putativa sujeição do trabalhador perante a sua entidade empregadora é especialmente relevante perante o entendimento jurisprudencial sustentado pela generalidade dos tribunais portugueses no sentido de que o vínculo laboral é caracterizado pela subordinação jurídica do trabalhador perante a entidade empregadora”. (Coutinho & Moniz, 2019, p. 19)

Assim sendo, qualquer trabalhador que esteja perante uma situação em que a sua posição é inferior à do empregador, não tem liberdade suficiente para dar uma resposta ou tomar uma decisão (usualmente opor-se) de forma genuína e livre, salvo raras exceções, tantas as que pretendemos demonstrar no ponto 3 deste capítulo.

Perante esta exposição, é possível concluir que em situações de alegado ou pressuposto de equilíbrio próprio (subordinação jurídica) entre os intervenientes do vínculo laboral, o consentimento não pode integrar fundamento de licitude para o tratamento dos dados pessoais.

Neste mesmo sentido, afirma o GT29º que, “embora o consentimento possa constituir, em casos excepcionais, um fundamento válido para o tratamento de dados

personais, deve ser feita uma verificação cuidadosa, caso a caso, por forma a aferir se o consentimento é, na verdade, suficientemente livre” (GT29º, 2011b), p. 18).

Ainda no âmbito do requisito do livre consentimento, a Lei de Execução do RGPD em Portugal, consagrou expressamente na sua al. a) do n.º 3 do art. 28º uma situação em que o consentimento não pode ser requisito para o tratamento e análise de proteção de dados pessoais do trabalhador, situação esta que, ao contrário de muitas outras normas, não foi transcrita do RGPD.

Citando o legislador, “salvo norma legal em contrário, o consentimento do trabalhador não constitui requisito de legitimidade do tratamento dos seus dados pessoais: a) Se do tratamento resultar uma vantagem jurídica ou económica para o trabalhador”.

Contudo, a CNPD emitiu, ao dia três de setembro do ano transato, a Deliberação n.º 494/2019 que determina a não aplicação de alguns artigos consagrados na Lei de Execução do RGPD, nomeadamente, da al. a) do n.º 3 do artigo 28.º. Como fundamento para tal, expõe o seguinte:

“ora, o disposto na alínea a) do n.º 3 do artigo 28.º, ao determinar precisamente a solução oposta, restringe excessivamente a relevância do consentimento do trabalhador, com isso eliminando qualquer margem de livre arbítrio dos trabalhadores mesmo quando há condições para a sua manifestação sem risco para os seus direitos e interesses. Nessa medida, esta disposição traduz uma restrição injustificada e desproporcionada do disposto na alínea a) do n.º 1 do artigo 6.º e da alínea a) do n.º 2 do artigo 9.º do RGPD.” (CNPD, 2019, p. 10)

A validade do consentimento apenas deve ser posta em causa se existir receio, por parte do trabalhador, de sofrer consequências negativas pela recusa, ou se o mesmo se sentir coagido de alguma forma (cfr. GT29º, 2017a), p. 6). Nenhuma das situações parece enquadrar-se no caso.

Ademais, se analisarmos o entendimento do GT29º, nas Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679, este afirma que “o responsável pelo tratamento tem de demonstrar que a retirada do consentimento não implica quaisquer custos para o titular dos dados e, logo, que não existe desvantagem evidente para quem retira o consentimento” (GT29º, 2017a), p. 11).

Ora, analisando a asserção “*a contrario*”, entende-se que apenas quando do tratamento resulte uma vantagem jurídica para o trabalhador é que o seu consentimento pode considerar-se válido.

Desta forma, a al. a) do n.º 3 do art. 28º da Lei n.º 58/2019 torna-se incompreensível, pois limita excessivamente a pertinência do consentimento do trabalhador (previsto no RGPD), e, conseqüentemente, reprime o livre arbítrio dos trabalhadores, ou seja, o poder de tomar uma decisão, mesmo num contexto em que tem o direito a manifestá-lo.

Neste sentido, Ana Lambelho e Marisa Dinis afirmam que “*la correcta interpretación del percepto es la que, salvo norma en contrario, el consentimiento no suele ser fundamento del tratamiento si de ello resulta una desventaja jurídica o económica para el trabajador (lo que sucederá en la mayoría de los casos)*” (Lambelho & Dinis, 2020, p. 416).

Por último, e por admitirmos que não é, provavelmente, um problema tão claro como os restantes que abordaremos supra, este requisito pressupõe um outro problema por falta de formação nas empresas.

Esta asserção provém das usuais situações em que o procedimento para obter o consentimento do trabalhador não permite aos titulares dos dados dar consentimento, separadamente, para diferentes operações de tratamento de dados pessoais, como o legislador previu no considerando (32): “nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins”.

Podemos dar o exemplo do DPO, contratado usualmente pelo empregador, solicitar a um trabalhador, no mesmo pedido e em simultâneo, o seu consentimento para publicar uma fotografia do mesmo no site da empresa e para disponibilizar o seu contacto pessoal. Este consentimento não é granular, uma vez que o responsável pelo tratamento não pode, à luz do RGPD, interligar várias finalidades de tratamento sem tentar procurar separar o consentimento para cada finalidade; por conseguinte, não é válido.

Assim sendo, e na perspetiva do GT29º, a qual adotamos, o consentimento só é válido quando “a solução para satisfazer as condições inerentes a um consentimento válido passa pela granularidade, ou seja, a separação dessas finalidades e a obtenção de consentimento para cada uma das delas.” (GT29º, 2017a), p. 11).

Em suma, o consentimento do trabalhador raramente é fundamento legítimo para o tratamento dos dados dos trabalhadores, pois, no contexto do contrato de trabalho, aquele nunca é verdadeiramente livre para não recusar esse consentimento. Desta forma, resta-nos adotar a tese do GT29º, ao referir que:

“os empregados raramente estão em posição de dar, recusar ou revogar livremente o consentimento, dada a dependência que resulta da relação entre o empregador e o empregado. Exceto em situações excepcionais, o empregador tem de invocar outro fundamento jurídico que não o consentimento, como a necessidade de tratar os dados para o seu interesse legítimo. No entanto, um interesse legítimo em si mesmo não é suficiente para prevalecer sobre os direitos e liberdades dos empregados.”

Nos capítulos seguintes, pretendemos analisar determinadas situações da relação laboral de forma a concluirmos se, e tendo em conta os problemas que o consentimento levanta, este será o fundamento mais adequado para o tratamento de dados pessoais.

## **2. Os casos de desnecessidade do consentimento do trabalhador para o tratamento de dados pessoais**

A desnecessidade do consentimento por parte do trabalhador para o tratamento dos seus dados não é sinónimo de o empregador tratar os seus dados de forma totalmente livre, sem fundamento ou limites. Significa sim que o RGPD prevê outro(s) fundamento(s) para tal tratamento.

O considerando (40) do RGPD<sup>17</sup> estatui que:

“para que o tratamento seja lícito, os dados pessoais deverão ser tratados com base no consentimento do titular dos dados em causa ou noutro fundamento legítimo, previsto por lei, quer no presente regulamento quer noutro ato de direito da União ou de um Estado-Membro referido no presente regulamento, incluindo a necessidade de serem cumpridas as obrigações legais a que o responsável pelo tratamento se encontre sujeito ou a necessidade de serem executados contratos em que o titular dos dados seja parte ou a fim de serem efetuadas as diligências pré-contratuais que o titular dos dados solicitar.”

Isto significa que todas as situações que envolvam o tratamento de dados pessoais, ou a possibilidade de violar a esfera privada do trabalhador, devem ser analisadas casuisticamente, de forma a conseguir entender-se qual o fundamento que melhor se enquadra a cada circunstância.

Segundo o GT29º, no Parecer 2/2017, dotado em 8 de junho de 2017, que versa sobre o tratamento de dados no local de trabalho, os principais, e mais usuais, fundamentos para o tratamento dos dados pessoais do trabalhador são: o consentimento (art. 6º, al. a)), a execução do contrato (art. 6º, al. b)), as obrigações legais (art. 6º, al. c)) e o interesse legítimo do empregador (art. 6º, al. f)), todos os artigos do RGPD.

O fundamento da execução do contrato está previsto no art. 6º, n.º 1, al. b) do RGPD: quando o “tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados”; ou seja, é permitido ao encarregado de proteção de dados tratar os dados pessoais do trabalhador quando os mesmos forem necessários para a concretização do contrato de trabalho.

---

<sup>17</sup> Disponível para consulta em <https://protecao-dados.pt/wp-content/uploads/2017/07/Regulamento-Geral-Prote%C3%A7%C3%A3o-Dados.pdf>

Esta “concretização” do contrato implica, entre outros, o cumprimento das obrigações previstas em lei ou em instrumentos de regulamentação coletiva de trabalho, ou de gestão, planeamento e organização do trabalho.

Neste sentido, acreditamos que o fundamento da execução do contrato de trabalho consiste, usualmente, no fundamento de legitimidade a que os empregadores podem apelar para habilitar a generalidade das operações de tratamento que impliquem dados pessoais dos trabalhadores; a saber, na elaboração do contrato de trabalho do trabalhador, aquando da inscrição deste na Segurança Social, bem como no processamento e pagamento da remuneração e complementos remuneratórios.

O fundamento do cumprimento de obrigações legais permite que os dados do trabalhador possam ser tratados e analisados na medida em que tal tratamento seja necessário ao cumprimento de obrigações jurídicas a que o empregador, ou o seu responsável pelo tratamento, esteja sujeito em virtude das exigências da legislação da União Europeia ou de um Estado-Membro (neste caso, a legislação portuguesa em vigor).

Veja-se o exemplo do tratamento de dados pessoais do trabalhador quando o seu fim for a cobrança e entrega de quotas sindicais, dever a cargo do empregador quando o instrumento de regulamentação coletiva de trabalho (IRCT) assim o preveja.

Já se o fundamento utilizado para tratar os dados se fundar num interesse legítimo, podem tratar-se os dados do trabalhador, quando esse tratamento não prevaleça sobre interesses, direitos ou liberdades fundamentais do próprio.

Segundo Francisco Coutinho e Graça Moniz,

“a invocação de um interesse legítimo para o tratamento pela entidade empregadora, nos termos da alínea f) do número 1 do art. 6.º do RGPD, implica que a própria finalidade do tratamento de dados pessoais deve ser também legítima, o tratamento deve ser realizado mediante métodos ou tecnologias específicas que, por referência à finalidade de tratamento, sejam de considerar estritamente necessários, adequados, proporcionais e aplicados da forma menos intrusiva possível para a privacidade e respeito de outros direitos fundamentais da pessoa singular. Este crivo, demarcadamente apertado, coloca sobre as entidades empregadoras o ónus de assegurar que se encontram aptas a demonstrar que tomaram as medidas adequadas a garantir o necessário equilíbrio entre a prossecução de uma finalidade (legítima) de tratamento de dados e o respeito pelas liberdades e direitos fundamentais dos trabalhadores e as expectativas razoáveis destes na relação com as suas entidades empregadoras.” (Coutinho & Moniz, 2019, p. 31)

Significa, tal afirmação, que o interesse legítimo do empregador poderá ser invocado como fundamento jurídico, mas apenas se o tratamento dos dados for estritamente necessário para uma finalidade legítima e estiver conforme com os princípios da proporcionalidade (v.g. a análise a redes profissionais e a instalação da videovigilância ou do GPS, com as devidas limitações).

De acordo com o GT29º (2017b), p. 2), este fundamento implica que o tratamento de dados no local de trabalho deva ser realizado da forma menos intrusiva possível e ser dirigido para as áreas específicas de risco, sendo reservado ao trabalhador invocar o direito de oposição ao tratamento, por fundamentos legítimos e imperiosos, nos termos do artigo 14º do RGPD.

Ora, temos assim uma panóplia de fundamentos que poderão ser usados para o tratamento e análise dos dados pessoais dos trabalhadores, não se esgotando as hipóteses no consentimento por parte do trabalhador. Aliás, sem nos querermos adiantar, usualmente o consentimento não é de todo o requisito para o tratamento dos dados. Mas vejamos infra alguns dos casos mais comuns.

Como nos parece óbvio, o processo de recrutamento de pessoal é a primeira situação alvo de tratamento de dados do (futuro) trabalhador e, aos dias de hoje, a “operação” mais usual para tratamento de dados durante o processo de recrutamento, pelo menos para as grandes empresas, é a análise das redes sociais.

Nas palavras de Olga García Coca:

*“las redes sociales, concebidas como modelo colaborativo y abierto a la participación de todos los usuarios posibles, han supuesto un gran avance en la selección de demandantes de empleo por la agilización y simplificación que pueden suponer para el proceso de selección de personal. La navegación por las citadas redes sociales propicia que el intermediador laboral pueda acceder a, y tratar, una gran cantidad de información sobre las personas que están buscando un empleo, por lo que habrá que analizar si estos sistemas ofrecen la protección suficiente al titular del dato.”* (Coca, 2016, p. 71)

Independentemente das características do candidato, o uso das redes sociais pelos futuros trabalhadores é generalizado e comum e, pese embora algumas destas redes concedam a opção aos usuários de manterem o seu perfil privado, muitos dos utilizadores

deixam inúmeras informações pessoais acessíveis ao público em geral, pelo que o empregador pode acreditar que o processo de tratamento de dados é válido e justificado<sup>18</sup>.

Contudo, e em primeiro lugar, este processo tem de atender à barreira entre redes sociais e redes profissionais, sob pena de pode traduzir-se numa violação da privacidade. De acordo com o GT29º o tratamento pelo empregador deve ter alguns cuidados:

“o empregador deve, antes da inspeção do perfil no meio social, ter em conta se o perfil no meio social do candidato diz respeito a fins profissionais ou privados, uma vez que isto pode ser uma indicação importante para a admissibilidade jurídica da inspeção dos dados. Além disso, os empregadores apenas estão autorizados à recolha e ao tratamento de dados pessoais respeitantes aos candidatos a emprego, na medida em que a recolha desses dados é necessária e pertinente para o desempenho da função à qual estão a candidatar-se.” (GT29º, 2017b), p. 13)

Quanto a redes profissionais como o *LinkedIn*, merecem uma análise lícita com fundamento no interesse legítimo do empregador, porquanto as informações nelas expostas são, maioritariamente, profissionais (como por exemplo, a formação e a experiência do trabalhador). Dúvidas poderão subsistir quanto a outro tipo de aplicações como o *Facebook* ou o *Instagram*, tendo em conta que, não obstante serem tendencialmente consideradas redes sociais não profissionais, podem ser usadas para fins profissionais.

Pressupondo que a análise é feita apenas sobre redes sociais com fins profissionais, temos diversas hipóteses na análise do perfil: i) o perfil é público; ii) o perfil é privado; iii) o perfil é privado, mas o empregador acede por interposta pessoa.

Precedentemente, é significativa a compreensão de que o simples facto do próprio candidato a emprego, enquanto utilizador das redes sociais, disponibilizar uma grande quantidade de informação sobre si mesmo, dificulta a terceiros a definição da fronteira entre a informação pública ou privada. Estas informações (que se podem traduzir em fotografias, estados ou comentários), recentes ou de longa data, tornam-se num risco para o candidato, nomeadamente no que toca à possibilidade de o empregador encontrar fatores discriminatórios.

---

<sup>18</sup> Neste sentido, *cfr.* GT29º (2017b), p. 13), no *Parecer 2/2017 sobre o tratamento de dados no local de trabalho*.

Quando o empregador se depara com um perfil público, implica que a “fonte” de recolha de informações é de livre acesso por vontade do candidato a emprego, pelo que o tratamento de dados facilmente é considerado lícito com base no interesse legítimo do empregador; assim sendo, permite-se a análise às redes sociais do trabalhador enquanto instrumento de perceção e análise à possibilidade de recrutar um futuro trabalhador, não sendo permitido ao trabalhador, posteriormente, alegar a violação da sua privacidade, caso não seja o admitido.

Pelo contrário, associa-se um perfil privado, à vontade do candidato a emprego desejar que as suas informações tenham um carácter restrito ou seja, uma circunstância em que a privacidade ganha destaque, pelo que a consulta das mesmas fica condicionada pela autorização do titular da conta. Até que seja dada esta autorização (v.g. através da aceitação de pedido de amizade), não será possível ao empregador tratar quaisquer dados.

Contudo, esta privacidade não é tão linear quanto deveria ser, pois o empregador poderá ter acesso a esta conta pessoal através de terceiros ou até por contas falsas/perfis fictícios, o que consiste não só numa intrusão na vida privada do candidato ilícita, como numa verdadeira violação do princípio da boa-fé. Ora, é inteligível que o empregador, nestes casos, não tem qualquer fundamento para o tratamento dos dados pessoais a que tiver acesso. Aliás, poderá incorrer em responsabilidade pré-contratual (art. 102º do CT).

Já na fase de execução de contrato, o art. 19º, n.º 1, *in fine* do CT possibilita que seja solicitado ao candidato a emprego, ou ao trabalhador, a realização ou apresentação de testes ou exames médicos, para comprovação das condições físicas ou psíquicas, em determinados casos; a saber, quando estes tenham por finalidade a proteção e segurança do trabalhador ou de terceiros, ou quando particulares exigências inerentes à atividade o justifiquem.

Já foi indicado, aquando a análise que referimos supra, que estamos perante dados delicados, que têm alguns limites como, por exemplo, a necessidade de ser fornecida por escrito, ao candidato a emprego ou trabalhador, a respetiva fundamentação.

Resta saber qual o fundamento para o tratamento dos dados resultantes dos resultados dos exames, quando, além de passíveis de serem solicitados, devem ser promovidos pelo empregador. Ora, estando a realização destes prevista e regulada no art.

19º do CT, e na Lei n.º 108/2009, de 10 de setembro, no que diz respeito aos exames relacionados com a segurança e saúde no trabalho, o fundamento será a obrigação jurídica.

Ainda neste contexto, ou seja, quanto ao tratamento de dados de saúde, faça-se uma importante referência ao art. 9º, n.º 1, al. h) do RGPD, tendo em conta que o próprio Regulamento permite esta exceção ao tratamento destes dados sensíveis.

A recusa da realização dos testes por parte do trabalhador conduzirá à prática de uma infração disciplinar<sup>19</sup>, que poderá determinar a aplicação de uma sanção pelo empregador, por constituir uma violação à norma imperativa prevista no art. 128º, n.º 1, al. j) do CT, que abrange os exames necessários ao abrigo do art. 108º da Lei n.º 102/2009. No caso de ser o candidato a emprego que recusa a realização de exames médicos legalmente exigíveis, a consequência será a licitude da sua exclusão do processo de contratação.

Decidindo-se pela contratação de determinado candidato, a empresa necessitará de dados pessoais do trabalhador, tanto para a elaboração do contrato de trabalho, como para a sua inscrição na Segurança Social (SS). Vejamos desde já exemplos inteligíveis dos dados de identificação do trabalhador enquanto cidadão: nome completo, idade, data de nascimento, morada, número de identificação fiscal e de beneficiário da segurança social, número do cartão de cidadão.

Isto significa que será legítimo ao empregador instar o trabalhador a fornecer estes dados, entre outros, pois constituem informações pessoais imprescindíveis para ambas as situações supramencionadas. Esta legitimidade, ao abrigo do RGPD, fundamenta-se assim pela execução do contrato, previsto no art. 6º, n.º 1, al. b) por constituírem “diligências pré-contratuais”.

Desta forma, nada há a ponderar sobre a necessidade do consentimento, ou não, para o tratamento de qualquer dado que seja estritamente necessário para a admissão do trabalhador ao serviço. De qualquer das formas, se fosse necessário, afigura-se que, mais uma vez, o consentimento não se poderia considerar livre, tendo em conta a figura já estudada da subordinação jurídica.

---

<sup>19</sup> O conceito de infração disciplinar é inexistente na lei. Face a esta lacuna, Abranches Pinto define a infração disciplinar como “o comportamento contrário a uma certa norma jus-laboral que vincula o trabalhador, ou seja, o comportamento do trabalhador que se apresente como desvio à conduta juridicamente esperada.” (Pinto, 2010, p. 51).

Ainda quanto aos dados pessoais do trabalhador, pode questionar-se quanto ao facto de o trabalhador estar filiado em sindicato, ou seja, em que circunstâncias o empregador pode tratar os dados que recolhe para, nomeadamente, entregar à associação sindical, as quotizações sindicais.

O direito de livre filiação sindical está previsto constitucionalmente no art. 55º da CRP, e constitui um corolário do direito à igualdade no acesso a emprego e no trabalho, conforme o exposto no art. 24º, n.º 1 do CT. Ainda neste âmbito, os arts. 457º e 458º do CT regulam a cobrança e entrega de quotas sindicais.

Ao analisar os artigos, constatamos no n.º 3 do art. 457º a possibilidade de proceder ao tratamento informático de dados pessoais dos trabalhadores, desde que exclusivamente utilizados para cobrança e entrega de quotas sindicais, acrescentando o n.º 1 do art. 458º que o empregador deve proceder à cobrança e entrega de quotas sindicais quando o instrumento de regulamentação coletiva de trabalho (IRCT) aplicável o preveja e o trabalhador o autorize.

Esta norma podia suscitar uma contradição com o n.º 3 do art. 35º da CRP, que determina que a informática não pode ser utilizada para tratamento de dados referentes a filiação sindical; contudo, na sua parte final, preveem-se três exceções, uma delas a autorização prevista por lei.

Isto posto, depreende-se que o fundamento para o tratamento do dado pessoal “filiação sindical” será o cumprimento de uma obrigação legal, previsto na al. c) do n.º 1 do art. 6º do RGPD; contudo, apenas será válido se o tratamento incidir sobre a cobrança e entrega das quotas sindicais.

Paralelamente aos dados de identificação do trabalhador, também o processamento e pagamento da retribuição e complementos remuneratórios ao trabalhador são exemplos de operações indissociáveis à gestão corrente de recursos humanos no seio empresarial (*in casu*, mensal) que necessitam de um fundamento legítimo para o tratamento dos dados.

A especificidade destas últimas situações é a possibilidade de tratamento de dados, tanto ao abrigo da execução do contrato, como das obrigações legais.

O processamento e pagamento da retribuição e complementos remuneratórios ao trabalhador são atos que resultam diretamente da execução do contrato, pelo que será este o fundamento para o tratamento dos dados indispensáveis àquelas operações.

Por outro lado, pode usar-se também o fundamento das obrigações legais, tendo em conta que a alínea b) do número 1 do art. 127º do CT impõe ao empregador o dever de pagar pontualmente a devida retribuição (justa e adequada) ao trabalhador, ou seja, a entidade empregadora tem a obrigação legal de assalariar o funcionário. Desta forma, o empregador necessita, obrigatoriamente, de utilizar os dados pessoais do trabalhador aquando do processamento dos salários.

Mais uma vez, o empregador não necessitará do consentimento do trabalhador para o tratamento dos seus dados pessoais, pois a lei outorga essa autorização.

Aquando o processamento dos salários, se o empregador realizar uma alteração nos sistemas estruturais para migrar os dados dos trabalhadores de um sistema antigo de folha de pagamento para um novo, é provável que seja solicitado, novamente, um fundamento legítimo para o tratamento dos dados. Também neste caso promovemos a ideia que não será necessário pedir o consentimento do trabalhador, sendo processado com base no interesse legítimo do empregador.

Não nos parece que este fundamento possa constituir um problema para o trabalhador, tendo em conta que esta transferência interna de dados não terá grandes probabilidades de violar os direitos e liberdades do trabalhador, tendo em conta que esses dados já estariam na posse do empregador.

Após o processamento e pagamento dos salários, é necessário também comunicar, em certos casos, e quando pedido, alguns dados às autoridades fiscais. Neste caso, estamos novamente perante uma obrigação legal de tratamento dos dados do trabalhador, em que não é essencial o consentimento do trabalhador, pois constitui uma obrigação para o empregador.

Também os tratamentos dos dados através de operações de tratamento decorrentes da utilização de monitorização das TIC no local de trabalho, não podiam deixar de ser objeto de estudo na nossa dissertação.

Quanto a este tema, o GT29º afirma que:

“um teste de proporcionalidade deve ser efetuado antes da implantação de qualquer ferramenta de monitorização, a fim de verificar se todos os dados são necessários, se esse tratamento excede os direitos de privacidade gerais que os empregados têm também no local de trabalho e quais as medidas que devem ser tomadas para garantir que as violações do direito à vida privada e do direito à confidencialidade das comunicações são limitadas ao mínimo estritamente necessário.” (GT29º, 2017b), p. 28)

Começemos por um instrumento que é objeto de muito estudo pela doutrina e jurisprudência: a videovigilância.

A videovigilância traduz-se na recolha de imagens que se realiza através de câmaras, conduzindo-se à sua recolha num “circuito fechado”, o que contende não só com o direito à imagem como, também, com o direito à autodeterminação informativa. O GT29º, sobre este meio de vigilância, expôs:

“tendo em conta que o tratamento deve ser lícito (de acordo com o n.º 1, alínea a), do artigo 6.º da Diretiva), o responsável pelo tratamento deve verificar previamente se a vigilância está em conformidade com as disposições gerais e específicas aplicáveis a esse setor - leis, regulamentos, códigos de conduta com significado jurídico. Essas disposições também poderão ser fixadas para fins de segurança pública, assim como para fins que não estejam relacionados com o tratamento de dados pessoais - por exemplo, a necessidade de obter autorizações pontuais de órgãos administrativos e de cumprir as suas instruções.” (GT29º, 2004, p. 16)

É no art. 20º do CT que encontramos regulado o uso da videovigilância, sendo a regra geral a sua proibição, se a finalidade for a de controlo do desempenho profissional do trabalhador.

Neste mesmo sentido, o art. 19º da Lei de Execução prevê a licitude dos sistemas de videovigilância, se a sua finalidade for (e apenas) a proteção de pessoas e bens, assegurando os requisitos previstos no artigo 31.º da Lei n.º 34/2013, de 16 de maio, ou seja, o regime do exercício da atividade de segurança privada.

Além destas normas, deve ter-se ainda em conta todas as disposições do direito nacional, especificamente os princípios constitucionais e as demais disposições do direito civil no que se refere, em especial, às aplicáveis ao direito à imagem, bem como a todas as normas relativas aos direitos de personalidade, que estudamos no primeiro capítulo.

As disposições referidas supra tendem a concluir que apenas deve ser permitida a monitorização em lugares específicos, sendo sempre interdita a monitorização de áreas

sensíveis, nomeadamente aquelas que impliquem a vigilância da qualidade e quantidade da atividade de trabalho, implicando, assim, a violação da privacidade do trabalhador.

Aliás, o n.º 2 do art. 19º da Lei de Execução elenca os locais do local de trabalho em que a videovigilância é expressamente proibida; a saber, “o interior de áreas reservadas aos trabalhadores, designadamente zonas de refeição, vestiários, ginásios, instalações sanitárias e zonas exclusivamente afetas ao seu descanso”, aos quais acrescentamos os locais religiosos, quando os haja.

Ainda no que concerne ao art. 19º da Lei de Execução, é importante analisar o n.º 4, que apenas permite a captação de som no período em que as instalações vigiadas estejam encerradas ou mediante autorização prévia da CNPD. Não é, contudo, uma novidade legislativa; aliás, a norma veio apenas “reanimar” o disposto no n.º 9 do artigo 31º do Regime do Exercício da Atividade de Segurança Privada.

Esta norma torna-se mais restritiva que o Código do Trabalho, que permite, nos termos dos arts. 20º e 21º do CT, a captação de som e imagem em qualquer momento da atividade, desde que necessário, adequado e proporcional (art. 21º, n.º 2 do CT)<sup>20</sup>.

Depreende-se, então, que desde que a videovigilância seja instalada pelo empregador de acordo e nos termos da lei, com os limites que a própria indica e que já abordamos nos parágrafos anteriores, o tratamento dos dados do trabalhador é lícito pelo disposto no art. 6º, n.º 1, al. f) do RGPD ou seja, pelo interesse legítimo do trabalhador em proteger quaisquer locais onde exista a possibilidade de se pôr em causa a segurança de pessoas e bens.

Nos restantes locais, ou seja, em todos aqueles que haja risco sério de controlo excessivo do trabalhador, defendemos que não existe qualquer fundamento para o tratamento lícito destes dados.

Ainda nos sistemas de vigilância à distância, também a geolocalização, meio que outrora não se afirmava na sociedade como nos tempos contemporâneos, é um meio que carece de um fundamento legítimo para que o empregador possa tratar os dados que possam ser recolhidos através deste instrumento pois, facilmente poderá ser instalado de forma a verificar constantemente os movimentos e o comportamento do trabalhador.

---

<sup>20</sup> Neste sentido, *vide* Lambelho & Dinis (2020, p. 417).

Quando falamos em geolocalização, esta abrange vários serviços; contudo, em termos laborais, o exemplo mais conhecido deverá ser o GPS (*Global Positioning System*), maioritariamente das vezes instalado nos veículos da empresa, visando determinar a sua localização; contudo, este sistema pode recolher também dados sobre o comportamento de condução de cada trabalhador.

Sobre os serviços de geolocalização, o GT29º afirma que:

“os dispositivos de localização de veículos não são dispositivos de localização do pessoal. A sua função é determinar ou monitorizar a localização dos veículos em que são instalados. Os empregadores não devem considerá-los como dispositivos de localização ou monitorização do comportamento ou do paradeiro dos condutores ou outros empregados, nomeadamente enviando alertas relacionados com a velocidade do veículo.” (GT29º, 2011, p. 15)

Estes sistemas, tal como é fácil compreender pelo descrito supra, constituem um grande risco para a violação da privacidade do trabalhador, no caso do desvirtuamento da função, ou seja, se a sua instalação por parte do empregador tenha como fim obter um panorama íntimo dos hábitos e padrões do trabalhador que utiliza o veículo, executando facilmente um perfil. Se a monitorização não puder ser desativada após o horário laboral, é fácil ter acesso à vida privada do trabalhador (v.g. horários de saída e entrada na sua residência, visitas a hospitais ou locais de culto religioso, entre outros).

Nestes casos, e de acordo com o Parecer do GT29º, conceito que adotamos, é uma situação em que, mais uma vez, o consentimento é um fundamento de tratamento crítico devido à subordinação jurídica. Em vez de pedirem o consentimento, terão de recorrer a outro fundamento legítimo de tratamento. Assim sendo, para o tratamento de dados, poderemos usar um, de dois fundamentos legais, conforme a circunstância:

“um empregador poderá ser obrigado a instalar tecnologia de localização nos veículos para demonstrar o cumprimento de outras **obrigações jurídicas** como, por exemplo, garantir a segurança dos empregados que conduzem esses veículos. O empregador pode também ter um **interesse legítimo** em poder localizar os veículos a qualquer momento. Ainda que os empregadores tivessem um interesse legítimo para atingir estes fins, em primeiro lugar, deve ser apreciada a questão de saber se o tratamento é necessário para esses fins, e se a aplicação atual está em conformidade com os princípios da proporcionalidade e da subsidiariedade.” (GT29º, 2017b), p. 24) (nosso negrito)

Quando o empregador recorre ao fundamento do interesse legítimo, tem de existir uma necessidade que seja devidamente justificada. Nestes casos, “os empregadores devem verificar se é comprovadamente necessário monitorizar a localização exata dos empregados para um fim legítimo e, principalmente, ponderar essa necessidade face aos direitos e liberdades fundamentais dos trabalhadores” (GT29º, 2011, p. 15), ou se podem recorrer a meios menos intrusivos (v.g. o exemplo dado pelo GT29º, ao escolher-se um sistema que emita um alerta quando um empregado atravessa uma linha de demarcação virtual preestabelecida).

Ainda nos sistemas de vigilância, encontramos a figura do registo de tempos de trabalho e de assiduidade e pontualidade por parte do empregador. Esta figura traduz-se em sistemas que permitem a monitorização pelos empregadores de quem entra nas suas instalações e/ou em determinadas áreas das suas instalações.

Esta figura de controlo já é conhecida há muitos anos, desde os tempos em que se começou a usar a expressão “picar o ponto”; a diferença dos meios de hoje em dia foca-se no desenvolvimento da tecnologia.

O GT29º, no documento “Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679”, dá-nos um exemplo no que toca a este ponto, e que se traduz na possibilidade de o empregador possuir uma sala com servidores onde os dados empresariais sensíveis, relativos aos trabalhadores e aos clientes são armazenados; nesse sentido, o empregador instala um sistema de controlo de acesso que regista a entrada e a saída dos trabalhadores que têm a devida autorização para entrar na sala.

Nestes casos, o tratamento dos dados só será lícito com fundamento no interesse legítimo do empregador, na aceção do art. 6.º, al. f) do RGPD, com a condicionante dos trabalhadores serem informados sobre a operação do tratamento.

No entanto, se a finalidade deste tratamento for a monitorização contínua da frequência da entrada e da saída exatas dos trabalhadores, já não existe fundamento legítimo para o tratamento, dado que o tratamento não pode prevalecer sobre o direito ao respeito da vida privada dos empregados (*in casu*, existe sempre o risco de proporcionar um nível de controlo invasivo do trabalhador no local de trabalho).

As novas tecnologias instaladas nestes sistemas podem originar outra circunstância de tratamento de dados, nomeadamente quando são instaladas tecnologias que envolvem o tratamento de dados biométricos.

O art. 28º, n.º 6 da Lei de Execução do RGPD legitima o tratamento dos dados biométricos dos trabalhadores para fins de controlo de acesso às instalações da entidade empregadora, ou para fins de controlo de assiduidade dos trabalhadores (*cf.* Nascimento & Gama, 2019, pp. 5-6).

Nestes casos, há que ter em conta que os dados biométricos são utilizados como uma configuração de identificação universal, que engloba características pessoais do trabalhador, que só devem ser obtidas pelo empregador quando absolutamente necessárias para um tratamento específico, situações que devem ser avaliadas casuisticamente, e devidamente justificadas.

Defendemos então que o empregador deve tentar recorrer a um meio menos invasivo, tendo em conta que os dados biométricos são instrumentos de avaliação das características fisiológicas das pessoas (*v.g.* impressões digitais, reconhecimento da íris, reconhecimento da voz, a análise do ADN, entre outros). Se não lhe for possível, há que fazer uma avaliação casuística, de forma a entender se o interesse legítimo será fundamento para o tratamento. Neste sentido, também o GT29º defende que:

“os empregadores poderiam avaliar se é comprovadamente necessário utilizar dados biométricos dos empregados com uma finalidade legítima e ponderar essa necessidade face aos direitos e liberdades fundamentais dos trabalhadores. Nos casos em que a necessidade possa ser devidamente justificada, a base jurídica do tratamento poderia assentar no **interesse legítimo** do responsável pelo tratamento dos dados, na aceção da alínea f) do artigo 7.º (...)”. (GT29º, 2012, p. 12) (nosso negrito)

Ainda quanto ao tratamento de dados biométricos, o art. 9º, n.º 2, al. b) do RGPD legitima o tratamento de dados biométricos, se necessário, para efeitos do cumprimento de obrigações e do exercício de direitos específicos do empregador ou do trabalhador em matéria de legislação laboral, de segurança social e de proteção social, desde que permitido pelo direito da União ou dos Estados-Membros, ou por uma convenção coletiva nos termos do direito dos Estados-Membros que preveja garantias adequadas dos direitos fundamentais e dos interesses do titular dos dados.

Isto posto, nas situações suprarreferidas, o tratamento poderá ser legítimo com base no cumprimento de obrigações legais, desde que devidamente justificado, e permitido pelo direito da UE ou por convenção coletiva de trabalho, também regulada pelos termos nos Estados-Membros.

Desta análise ao tratamento de dados biométricos, depreende-se que estamos perante mais um contexto em que o consentimento do trabalhador não é fundamento para o tratamento dos dados, mas sim o interesse legítimo do empregador, ou o cumprimento de uma obrigação legal, conforme a situação.

Além das análises já feitas, não poderíamos esquecer as mensagens enviadas através de correio eletrónico. Primordialmente à análise de qual será o fundamento legítimo para o tratamento destes dados, há que distinguir, desde logo, mensagens de natureza pessoal e de natureza profissional.

Esta distinção é relevante pois as mensagens pessoais pertencem exclusivamente ao trabalhador, ao contrário das mensagens de natureza profissional que são endereçadas à empresa ou escritório onde se desenrola a atividade laboral. Ora, as primeiras devem sempre ser interditas à análise do empregador, constituindo a violação da privacidade do trabalhador.

Naturalmente, é possível que haja uma dificuldade na distinção de emails ou mensagens privadas e profissionais, se for usado o mesmo correio eletrónico ou dispositivo móvel.

Porventura, sempre que possível, é desejável que o empregador faculte um email profissional ao trabalhador. Aliás, é a atitude sugerida pelo legislador no art. 22º, n.º 2 do CT, que indica no artigo que o empregador deve estabelecer regras de utilização dos meios de comunicação na empresa, nomeadamente do correio eletrónico, regras que devem ser instruídas ao trabalhador, logo que celebra o contrato de trabalho.

Se o procedimento suprarreferido for o adotado pela sociedade de que o empregador é titular, poderá não subsistir violação dos direitos de privacidade do trabalhador, pois tanto os restantes trabalhadores, como a entidade empregadora, estão informados de que todas as mensagens que o trabalhador envia e/ou recebe são dirigidas à empresa.

Se estivermos perante uma situação destas, cremos que o empregador poderá encontrar fundamento para o tratamento desses dados na alínea f) do art. 6º do RGPD ou seja, o interesse legítimo do empregador, no sentido em que, mesmo que a mensagem de caráter profissional seja enviada para o correio eletrónico de um trabalhador em específico, o seu conteúdo respeita a um problema da empresa em geral, pelo que não se põem em causa os direitos, liberdades ou garantias do trabalhador.

Durante o período de execução da relação laboral, que inclui a maioria das situações referidas no presente e no anterior ponto do capítulo, admite-se ao empregador a avaliação do seu trabalhador, à luz do seu poder de direção, previsto no art. 97º do CT, que consiste no poder de estabelecer os termos em que o trabalho deve ser prestado, dentro dos limites decorrentes do contrato e das normas que o regem.

Assim sendo, não será necessário o consentimento do trabalhador, pois, nestes casos, pode recorrer-se ao fundamento da execução do contrato de trabalho. Aliás, ser necessário o consentimento do trabalhador era sinónimo de impedir o poder de direção. Note-se, contudo, que neste poder de direção do empregador, compreende-se uma avaliação, por exemplo, presencial (pouco invasiva).

Todavia, a questão do consentimento pode colocar-se nesta sede, na medida em que existem muitas formas de controlo da atividade do trabalhador, e a proteção dos direitos de personalidade e as normas de proteção de dados impõem que se utilize o meio menos invasivo possível.

Contudo, o empregador pode utilizar meios mais evasivos para a avaliação do trabalhador, nomeadamente os meios tecnológicos, tais como o controlo através de computador (meios de comunicação), em que o empregador tem todos os registos de *sites* ou programas onde o trabalhador entre, ou possa filmar todas as videoconferências que este faz. O mesmo sucede com as avaliações de clientes da empresa/escritório, como é o exemplo atual e usual dos clientes das plataformas digitais de prestação de serviços presenciais.

Este tipo de avaliação apenas deveria ser lícito com base no consentimento do trabalhador; porém, difícil será considerar este consentimento verdadeiramente livre, pelo que nos atrevemos a usar a expressão “consentimento não consentido”, considerando a

posição de inferioridade e carência do trabalhador em relação ao potencial empregador, ou seja, e mais uma vez, a figura da subordinação jurídica.

Por conseguinte, deve atender-se, sempre que se pretender utilizar estes meios, aos princípios previstos no art. 5º do RGPD (v.g. licitude, lealdade, transparência, justiça, limitação da finalidade, minimização de dados, exatidão, limitação do prazo, integridade, confidencialidade e responsabilidade proativa), e que foram estudados devidamente no ponto 2.3.2 do primeiro capítulo.

Assim sendo, e apenas quando os respeitarem a todos, se poderá utilizar estes meios como forma de avaliação, recorrendo ao fundamento da execução do contrato; caso contrário, a avaliação não será lícita.

Em jeito de término, citamos Francisco Coutinho e Graça Moniz, que, no seu artigo, apresentam uma conclusão análoga à que chegamos:

“Dado o desequilíbrio próprio dos intervenientes típicos de uma relação laboral, e tendo em conta a referida necessidade de compatibilização dos interesses em conflito, o consentimento por parte do trabalhador não deverá, nem poderá constituir fundamento de legitimidade para o tratamento dos dados pessoais deste. No entanto, esse afastamento do consentimento enquanto fundamento de legitimidade para o tratamento de dados pessoais de trabalhadores, não impede as entidades empregadoras de procederem ao tratamento de dados pessoais em contexto laboral quando outros fundamentos de legitimidade se manifestem. A necessidade do tratamento dos dados para a execução do contrato de trabalho no qual o trabalhador é parte constitui um dos fundamentos de licitude mais expeditos, do qual as entidades empregadoras se poderão socorrer para proceder ao tratamento de dados pessoais intrinsecamente ligados com a execução e gestão da relação contratual, que poderá e deverá ser complementada pela realização de operações de tratamento de dados pessoais necessárias ao cumprimento das suas obrigações legais.” (Coutinho & Moniz, 2019, p. 35)

Ora, torna-se evidente que raras são as situações em que o consentimento é o fundamento mais adequado para o tratamento de dados. Contudo, existem exceções, que pretendemos indicar no ponto seguinte.

### **3. Os casos em que o consentimento do trabalhador constitui base legítima para o tratamento de dados pelo empregador**

Ora, tendo em conta as conclusões que retiramos do ponto anterior, e acolhendo a tese do GT29º, podemos afirmar com certeza que os trabalhadores raramente estão em posição de dar, recusar ou revogar livremente o consentimento, dada a subordinação jurídica a que estão sujeitos, especialmente no que toca à dependência financeira que resulta da relação entre trabalhador e empregador.

Contudo, cabe agora saber, neste ponto, se nunca o poderá ser.

Assim sendo, e tendo em conta o desequilíbrio de poderes que vigora na relação laboral, “os empregados só podem dar o seu livre consentimento em circunstâncias excepcionais, quando as consequências não tiverem qualquer tipo de relação com a aceitação ou a rejeição de uma oferta” (GT29º, 2017b), p. 28).

O GT29º descreve como livre consentimento “uma decisão voluntária, tomada por uma pessoa na posse de todas as suas faculdades, sem qualquer tipo de coerção, de carácter social, financeiro, psicológico ou outro. (...) O recurso ao consentimento deve limitar-se a casos em que a pessoa em causa tenha uma liberdade de escolha genuína e possa subsequentemente retirar o consentimento sem correr riscos.” (GT29º, 2011b), p. 15)

Significa, então, que o consentimento apenas será válido se o trabalhador puder exercer uma verdadeira escolha, o que implica que o trabalhador não se sinta, de qualquer forma, coagido pelo empregador, ou que da sua escolha resultem consequências negativas para o próprio, corolários que podem surgir no seio da noção de desequilíbrio de poder na relação laboral.

Há ainda a ter em conta que, nas circunstâncias em que o consentimento estiver agregado a uma parte não negociável das condições gerais do contrato, presume-se que este não é dado de uma forma livre, porquanto não é igualmente válido (*cfr.* GT29º (2017a), p. 6)).

O GT29°, após inúmeras análises, e da emissão de pareceres bastantes, chegou a uma conclusão similar ao que se pode retirar da nossa dissertação ou seja, são muito poucas as situações em que o consentimento é livre. Contudo, elas existem.

Iniciando, como já fizemos no ponto 2., pela fase de recrutamento do trabalhador, há que ponderar qual será o fundamento para tratar os dados pessoais do *Curriculum Vitae* (doravante CV), documento que usualmente é enviado ou entregue pelo candidato ao possível futuro empregador.

Ora, quando o candidato a emprego envia o seu currículo a um empregador pode fazê-lo no âmbito de uma candidatura espontânea ou em resposta a um anúncio. Em ambos os casos, a disponibilização de dados pessoais é feita pelo candidato de forma livre. No caso das ofertas de emprego, deve o futuro empregador explicitar em que termos fará o tratamento dos dados dos candidatos. Pensamos que, nestes casos, o consentimento do candidato poderá constituir fundamento bastante para o tratamento dos seus dados, desde que respeitado o princípio da necessidade, proporcionalidade e adequação.

Há que fazer uma ressalva de que nem todos os dados poderão ser solicitados ao candidato a emprego no formulário disponibilizado ao candidato, como é o exemplo de questionar o estado de saúde, ou gravidez. Para tais dados, não irá existir nenhum tratamento, com as devidas exceções já estudadas no ponto anterior.

No mesmo sentido, defendemos que também os candidatos que não forem recrutados deverão dar o seu consentimento explícito para o tratamento dos seus dados pessoais em processos de recrutamento futuros, sob pena do empregador ter de atender aos princípios da finalidade e da limitação do prazo de conservação.

Parece-nos que, para tal, deve ser enviada uma comunicação escrita ao candidato (até porque, independentemente de o candidato enviar o CV, ou preencher o formulário, em princípio, a sua morada consta em ambos), onde especifica que a única finalidade é a conservação dos dados para a possibilidade de um recrutamento futuro (consentimento informado e específico), indicando igualmente o prazo da conservação dos dados, ao abrigo do art. 5º, n.º 1, al. e) do RGPD.

Este consentimento pode ser considerado, na nossa opinião, válido, tendo em conta que o candidato tem livre escolha de dar, ou não, o seu consentimento (livre) e, ao enviar uma carta ou comunicação ao empregador, está a expressar a sua vontade (expresso).

Outra situação de um caso em que o consentimento se manifesta fundamento de tratamento é indicado pelo GT29<sup>o</sup> nas “Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679”. Veja-se uma equipa de filmagem que pretende filmar determinada parte de um escritório onde se encontram trabalhadores, no seu posto de trabalho. Ora, o GT29<sup>o</sup> afirma que o empregador pode oferecer aos trabalhadores uma solução, no caso de não quererem ser filmados.

Ora, se o trabalhador dispõe da possibilidade de recusar a sua filmagem sem ser penalizado, caso dê o seu consentimento, este considera-se prontamente livre, dado de forma voluntária e livre de pressão, não existindo aqui, ao contrário dos exemplos dados no ponto anterior, uma situação em que o titular dos dados possa sentir medo ou risco de consequências negativas decorrentes da recusa perante o seu empregador porque, caso assim o preferisse, podia ser colocado noutra local de trabalho equivalente, numa outra zona do edifício, enquanto durasse a filmagem.

Concluindo, nesta situação, para os trabalhadores serem filmados, tem de ser solicitado o consentimento dos trabalhadores que se sentam nessa zona do escritório para serem filmados, uma vez que podem aparecer em segundo plano, nas filmagens do vídeo.

Joana Mota acrescenta que o consentimento não pode ser considerado válido pelo simples facto de o trabalhador, após ter sido informado de forma transparente sobre as filmagens, decida dirigir-se à referida área que se encontra a ser fotografada; nestes casos, o consentimento pode considerar-se inequívoco, mas não expresso, na medida em que o mesmo apenas se infere do comportamento do trabalhador<sup>21</sup>.

Fazemos jus à opinião do GT29<sup>o</sup>, ao concordar que, havendo opção, o empregador deve, sempre que possível, oferecer ao trabalhador a possibilidade de escolher livremente se concorda que os seus dados sejam tratados, após expor todas as escolhas possíveis.

Além deste “cenário”, o GT29<sup>o</sup> apresenta ainda outro exemplo, no Parecer 15/2011, em que o consentimento deve ser o fundamento utilizado para o tratamento lícito dos dados em contexto laboral: “uma empresa decide criar uma intranet que conterà os nomes e principais funções dos trabalhadores. É perguntado a cada trabalhador se gostaria de ter a fotografia colocada junto do respetivo nome. As pessoas que pretendem ter a fotografia na

---

<sup>21</sup> Cfr. Mota, 2018, p. 9.

intranet são convidadas a enviar uma fotografia para um determinado endereço.” (GT29º, 2011b), p. 15).

Ora, nesta situação, o trabalhador tem uma verdadeira escolha entre enviar, ou não, a sua fotografia ao empregador para ser introduzida na dita intranet. No caso de o trabalhador ter recebido informação adequada (consentimento informado), se este optar por enviar a fotografia, podemos considerar que há não só um consentimento explícito, como lícito, preenchendo todos os requisitos previstos no RGPD.

Ainda neste contexto, o GT29º admite que, no caso de o empregador possuir fotografias digitais do trabalhador e pedir o consentimento do segundo para que as mesmas sejam colocadas na intranet para os fins já referidos, se o trabalhador clicar num botão para prestar o seu consentimento, estamos identicamente perante um consentimento válido e lícito.

Isto sucede, pois, como explicamos anteriormente, em ambos os casos, é inteiramente respeitada a escolha dos trabalhadores sobre se a sua fotografia aparece na intranet ou não, o que implica uma escolha livre do trabalhador, que não implicará consequências negativas para o próprio.

Outra situação a integrar neste ponto, é a disponibilização, pelo empregador, do contacto pessoal do trabalhador a terceiros.

Por norma, quando o candidato a emprego entrega o seu currículo, inclui o seu contacto telefónico pessoal e, muitas das vezes, é esse número que o empregador utiliza para contactar o trabalhador, após a sua contratação. A grande problemática surge quando um terceiro pede o contacto do trabalhador, por algum motivo.

Vejamos o exemplo de um escritório de advocacia em que cada trabalhador tem o seu telefone pessoal, que serve exclusivamente para comunicar com o empregador, bem como os restantes trabalhadores. Pode acontecer que um cliente peça o número pessoal do trabalhador/funcionário, o que possibilita a violação da privacidade, bem como a intromissão na vida íntima do trabalhador.

Nestes casos, em que o cliente pode comunicar com o trabalhador através do número da empresa, ou que pode adquirir (ou ser oferecido pelo empregador) um outro cartão SIM, julgamos que deve ser sempre necessário o consentimento do trabalhador, de

que não temos dúvidas preencher todos os requisitos necessários à luz do RGPD, incluindo a liberdade.

Também é possível chegar a esta conclusão, se tentarmos analisar a utilização dos restantes fundamentos para um tratamento lícito. Contemplemos: desde logo, é perceptível que a disponibilização do contacto não provem de nenhuma obrigação jurídica a que o empregador esteja sujeito; ademais, se por um lado, não é possível encontrar um fundamento legítimo do empregador, por ter outras possibilidades, muito menos será exequível com alicerce na necessidade da execução do contrato.

Depreende-se à vista disso que o trabalhador não só tem uma livre escolha, como esta situação não frui de qualquer outro fundamento que tenha cabimento para amparar licitamente o tratamento.

Ainda com a conclusão que retiramos dos parágrafos supra em mente, cremos que o mesmo sucede com a disponibilização do email pessoal do trabalhador, por parte do empregador, a terceiros, considerando que o trabalhador poderá ter um email profissional, usado em exclusividade na sua atividade, e que deve ser esse a ser disponibilizado a terceiros ou, no caso de inexistência, o email geral da empresa.

Por outro lado, poderá surgir a questão do trabalhador disponibilizar o seu email pessoal a terceiros (v.g. a clientes da empresa), tendo sido devidamente informado pelo empregador que essa ação não era permitida pela empresa, devendo sempre providenciar o email da empresa.

Ora, o trabalhador incumpe diretamente uma ordem do seu empregador, violando, conseqüentemente, o dever de obediência, nos termos do art. 128º, n.ºs 1, al. e) e 2 do CT, pelo que incorre num ilícito disciplinar.

Ainda aquando da execução do contrato, poderemos ter a situação do empregador oferecer uma vantagem ou benefício, por livre vontade, ao seu trabalhador, como é o exemplo da oferta de um seguro de saúde, que abrangerá também o agregado familiar. *In casu*, há a ponderar qual, e se há lugar, a fundamento para o tratamento dos dados pessoais do trabalhador, e aos pertencentes ao agregado (v.g. nome completo, idade, NIF, NISS, entre outros dados de identificação).

Antes de mais, rejeitamos o tratamento com base numa obrigação jurídica ou no interesse legítimo do empregador, pois estamos perante uma simples oferta que o empregador está a conceder ao trabalhador, bem como à sua família.

O mesmo sucede com o fundamento da execução do contrato, pois, e pese embora o trabalhador, em princípio, não tivesse oportunidade de obter o seguro, se não tivesse celebrado o contrato de trabalho, o seguro de saúde não está intrinsecamente interligado com o contrato em si.

Cabe então analisar se o consentimento do trabalhador é válido, e necessário, nesta circunstância.

Pressupondo que o trabalhador aceita o seguro, desde logo o trabalhador terá de assinar os devidos e necessários documentos, pelo que os requisitos de um consentimento informado, inequívoco e expresso estarão respeitados, tendo em conta que o trabalhador pode ler as condições, sabe que o consentimento é apenas com aquele fim e, sobretudo, realiza uma ação positiva, que facilmente demonstra a sua vontade (assinar o contrato de seguro).

Quanto ao requisito da liberdade, o trabalhador tem a livre escolha de aceitar ou rejeitar a oferta, não nos sendo possível abonar a ideia de que o trabalhador poderá ter medo de consequências negativas pela rejeição, ou decidirá sob coação do empregador. Aliás, o trabalhador é o único sujeito da relação laboral, neste contexto, que tem algo a ganhar.

Assim sendo, tanto os dados do trabalhador, como do agregado, poderão ser validamente tratados com fundamento no seu consentimento.

Há, contudo, e a nosso ver, uma especificidade que deve ser mencionada quanto aos dados do agregado familiar (convém relembrar, os dados de identificação): não obstante os dados pessoais serem tratados com base no seu consentimento, entenda-se que, independentemente de falarmos do cônjuge, descendentes ou até ascendentes do trabalhador, estes não fazem parte da relação laboral.

Logo, os dados do agregado serão, naturalmente, tratados ao abrigo do art. 6º, n.º 1, al. a) do RGPD, mas, neste tratamento, não se põe em causa, por exemplo, a figura da

subordinação jurídica. O agregado familiar terá de consentir diretamente perante a entidade patronal do trabalhador em causa.

Numa situação similar, o empregador organiza um fim de semana de convívio entre os trabalhadores e as suas famílias, e precisa dos dados dos familiares.

*In casu*, os dados dos familiares nunca poderiam ser tratados à luz dos fundamentos da execução do contrato, do interesse legítimo do empregador ou de uma obrigação jurídica, tendo em conta que estes sujeitos não são parte na relação laboral.

Resta analisar, mais uma vez, o fundamento do consentimento. Desde logo, é de fácil entendimento que a família do trabalhador, quando confrontada com o pedido dos seus dados para a organização de um fim de semana de convívio, estará ciente de que forma e qual é a finalidade deste tratamento, pelo que se apresenta um consentimento informado e inequívoco.

Para mais, ao aceitar o convite, e fornecer os seus dados, está expressamente a consentir o tratamento (ação positiva), pelo que temos mais um requisito cumprido; quanto ao requisito da liberdade, tanto o trabalhador, como a família, podem optar por aceitar ir, ou não, ao supradito convívio; aliás, neste caso, nem surge a questão de medo de consequência na rejeição.

É, pois, mais uma situação em que o consentimento é devidamente válido, desde que seja dado por cada um dos familiares ou seja, titular dos dados pessoais a ser tratados.

Também, aquando da cessação da relação laboral, poderão surgir dúvidas quanto ao facto de se saber se o consentimento do trabalhador pode fundamentar a transferência de dados entre o antigo e o atual empregador. Para responder a esta questão, atenda-se ao art. 20º do RGPD, que respeita ao direito à portabilidade dos dados.

Este artigo concede dois direitos ao trabalhador: por um lado, a receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática e, por outro, *a possibilidade de transmitir os seus dados pessoais ao novo empregador, sem que o primeiro, a quem os dados pessoais foram fornecidos, o possa impedir.*

Em princípio, o novo empregador pode tratar os dados pessoais do seu trabalhador. Contudo, o número 1 do artigo contempla limites a este tratamento, explicitando as

situações em que tal pode suceder. São elas quando o tratamento se basear no consentimento dado nos termos do artigo 6º, n.º 1, al. a), ou no artigo 9º, n.º 2, al. a), ou num contrato referido no artigo 6º, n.º 1, al. b).

Depreende-se da norma, que os dados do trabalhador só podem ser tratados pelo novo empregador se o titular dos dados já tiver dado consentimento para o tratamento dos dados, e este for válido (casos que serão escassos, nomeadamente os estudados no presente capítulo), ou no caso de se tratar de dados que são imprescindíveis à execução do contrato. Em ambas as situações, é também imperativo que o tratamento seja somente realizado por meios automatizados.

Lambelho & Dinis (2020, p. 415) mencionam ainda que os dados constantes do art. 9º, n.º 1 do RGPD ou seja, os dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa, não são passíveis de serem objeto de transmissão.

Analisadas as barreiras ao tratamento deste dado, concluímos pelo número 2 da norma, ao permitir que o trabalhador exerça o seu direito de portabilidade dos dados, possibilitando que os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento, sempre que tal seja tecnicamente possível, que se viabiliza o consentimento como fundamento de licitude do tratamento dos dados, com as devidas limitações.

Designadas e apreciadas as ocasiões onde poderá recorrer-se ao consentimento como fundamento de tratamento, importa relembrar que o consentimento, mesmo que dado livremente, poderá sempre ser retirado.

Conforme o previsto no n.º 3 do art. 7º do RGPD, “o titular dos dados tem o direito de retirar o seu consentimento a qualquer momento. A retirada do consentimento não compromete a licitude do tratamento efetuado com base no consentimento previamente dado. Antes de dar o seu consentimento, o titular dos dados é informado desse facto. O consentimento deve ser tão fácil de retirar quanto de dar.”

Assim sendo, o consentimento não pode ser considerado válido se não for permitida uma forma eficaz de revogação do mesmo.

E, no caso de tal suceder, acreditamos que o tratamento de dados pessoais deste não poderá prosseguir com outro dos cinco fundamentos legais, pois se o tratamento dos dados podia ter sido efetuado primordialmente com recurso a outro fundamento legal, garantir ao trabalhador que na situação em concreto, os dados só poderiam ser tratados se consentido, pode considerar-se não só uma atitude desleal por parte do empregador, como também uma falta de segurança jurídica.

## Conclusão

Chegados à fase final da dissertação, podemos asseverar desde já que alcançámos os objetivos a que nos propusemos.

O RGPD representou um colossal impacto no conceito de dados pessoais, que passa a ter a seguinte redação: “informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»)”. É de salientar que este conceito tem um vínculo inevitável com os direitos de personalidade, que se traduzem nos direitos que incidem sobre os aspetos físicos e/ou morais da personalidade de cada pessoa, aos direitos da pessoa enquanto pessoa, e até aos direitos da pessoa sobre si mesma.

Refira-se ainda que o RGPD não se limitou a modificar o conceito de dados pessoais, mas clarificou também os princípios orientadores do seu tratamento, de forma a proteger os interesses e a privacidade dos titulares dos dados, após a eclosão de novas tecnologias, e o desenvolvimento das já existentes; a saber, os elencados no art. 5º do RGPD.

Com o alargamento do uso das novas tecnologias, como suprarreferido, o trabalhador viu ameaçada a sua privacidade no local de trabalho.

Nesta sequência, o RGPD veio a criar um artigo, o artigo 6º, que elenca as situações em que o empregador pode, lícitamente, tratar os dados pessoais do trabalhador. O consentimento do trabalhador é, desde logo, um desses fundamentos para o lícito tratamento, previsto na alínea a).

O estudo do consentimento merece, não só uma especial atenção, mas também alguma cautela na análise. Este estudo implica a verificação dos requisitos que o integram, e que têm de estar preenchidos cumulativamente, constituindo assim uma condição de validade.

Constituem tais requisitos o consentimento informado, específico, expresso e livre, pelo que se subentende que o consentimento deve ser dado através de uma manifestação expressa para uma finalidade única e especificada, que lhe foi devidamente explicada, e sobre a qual incide uma livre escolha, sem qualquer contrapartida.

A desigualdade de poder na relação laboral é o problema que mais afeta a validade do consentimento, considerando que o trabalhador depende, em termos económicos e financeiros, do empregador; o trabalhador torna-se, assim, a parte mais débil da relação laboral ao reçar consequências negativas, se o consentimento for recusado. Consequentemente, o requisito da liberdade, salvo raras exceções, não está preenchido, pelo que o consentimento deve ser visto como um fundamento a que se deve recorrer excecionalmente.

Neste seguimento, o empregador vê-se obrigado a recorrer aos restantes fundamentos do art. 6º do RGPD para tratar dados legitimamente; a saber, a execução do contrato (al. b)), o cumprimento de obrigação jurídica (al. c)) ou o interesse legítimo do empregador (al. f)).

Exemplos, entre outros, a enquadrar nestas alíneas, são o de tratamento dos dados pessoais na elaboração do contrato de trabalho (na al. b)), a videovigilância com atenção aos limites determinados pela lei (na al. f)), o processamento de salários e o pagamento das quotizações sindicais (na al. c)) ou o tratamento de dados biomédicos, em que os dados podem tratar-se tanto como fundamento no interesse legítimo, como na execução do contrato.

Contudo, o consentimento pode ser fundamento para o tratamento em algumas situações; a saber, os exemplos do GT29º, o tratamento de dados constantes no formulário elaborado pelo empregador, e preenchido voluntariamente pelo trabalhador na fase de recrutamento, a disponibilização do contacto pessoal do trabalhador a clientes, o tratamento de dados do trabalhador, e da sua família, quer na oferta de seguro de saúde com proteção do agregado familiar, quer para a organização de fim de semana de convívio, e na transferência dos dados pessoais entre o antigo e o atual empregador.

Dessarte, cremos que conseguimos analisar e responder à questão a que nos propusemos analisar no início deste trabalho ou seja, em que medida o consentimento poderia ser fundamento para o tratamento de dados pessoais do trabalhador, bem como em que casos se poderia aplicar, esclarecendo também que outros fundamentos poderiam ser utilizados ao invés, nomeadamente no ponto 2. e 3. do segundo capítulo, respostas que acreditamos serem claras e objetivas, e que poderão enriquecer a bibliografia existente sobre um tema que consideramos atual.

*Esta página foi intencionalmente deixada em branco*

## Bibliografia

- Amado, J. L. (2018). Os poderes patronais e os direitos do trabalhador enquanto pessoa e cidadão. Em *Contrato de Trabalho (2ª Edição)*. Coimbra: Almedina.
- Antunes, A. F. (2012). *Comentário aos artigos 70º a 81º do Código Civil (Direitos de personalidade)*. Lisboa: Universidade Católica Editora.
- Cabral, A. P. (2016). Direitos de personalidade versus Direitos fundamentais. Em *Atas - Congresso 50 anos do Código Civil Português* (pp. 1-9). ISCTE.
- Calvão, F. U. (2018). *Direito da proteção de dados pessoais - Relatório sobre o programa, os conteúdos e os métodos de ensino da disciplina*. Porto: Universidade Católica Editora.
- Canotilho, J. G., & Moreira, V. M. (2007). *Constituição da República Portuguesa Anotada - Volume I (4ª Edição)*. Coimbra: Coimbra Editora.
- Caro, M. Á., & Gayo (coord), M. R. (2016). *Reglamento General de Protección de Datos*. Madrid: Reus, SA.
- Carvalho, C., Machado, C., & Costa, R. (2018). *Coleção Estudos n.º 7 - Instituto do Conhecimento AB: Desafios Laborais*. Coimbra: Almedina.
- Castro, C. S. (2005). *Direito da informática, privacidade e dados pessoais*. Coimbra: Almedina.
- CNPD. (2019). *Deliberação/2019/494*. Lisboa.
- Coca, O. G. (2016). *La protección de datos de carácter personal en los procesos de búsqueda de empleo*. Murcia: Ediciones Laborum.
- Coutinho, F. P., & Moniz, G. C. (2019). *Anuário de Proteção de Dados 2019*. Lisboa: CEDIS, Centro de I & D sobre Direito e Sociedade.
- Domènech, C. P. (2017). *El Derecho a la Protección de Datos en el Contrato de Trabajo*. Pamplona: Editorial Aranzadi.
- Dray, G., Martinez, P. R., Monteiro, L. M., Vasconcelos, J., Brito, P. M., & Silva, L. G. (2013). *Código do Trabalho (9ª Edição)*. Coimbra: Almedina.
- Fernandes, A. M. (2012). *Direito do Trabalho (16ª Edição)*. Coimbra: Almedina.
- Fernandes, M. (2009). *Os limites à subordinação jurídica do trabalhador - Em especial ao dever de obediência*. Lisboa: Quid Juris.
- FRA. (2014). *Manual da Legislação Europeia sobre Proteção de Dados*.

- Galante, F. (2010). *Da tutela da personalidade, do nome e da correspondência confidencial*. Lisboa: Quid Juris - Sociedade Editora.
- González, J. A. (2011). *Código Civil Anotado - Volume I (artigos 1º a 396º)*. Lisboa: Quid Juris - Sociedade Editora.
- GT29º. (2004). *Parecer 4/2004 sobre o Tratamento de Dados Pessoais por meio de Videovigilância*.
- GT29º. (2007). *Parecer 4/2007 sobre o conceito de dados pessoais*.
- GT29º. (2011a)). *Parecer 13/2011 sobre serviços de geolocalização em dispositivos móveis inteligentes*.
- GT29º. (2011b)). *Parecer 15/2011 sobre a definição de consentimento*.
- GT29º. (2012). *Parecer 3/2012 sobre a evolução das tecnologias biométricas*.
- GT29º. (2012). *Parecer 3/2012 sobre a evolução das tecnologias biométricas*.
- GT29º. (2017a)). *Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679*.
- GT29º. (2017b)). *Parecer 2/2017 sobre o tratamento de dados no local de trabalho*.
- Guimarães, M. R. (2018). A tutela da pessoa e da sua personalidade: algumas questões relativas aos direitos à imagem, à reserva da vida privada e à reserva da pessoa íntima ou direito ao carácter. Em *A tutela geral e especial da personalidade humana - 2017* (pp. 25-47). CEJ.
- IAPP . (2018). *European Data Protection - Law and Practice*.
- Lambelho, A., & Dinis, M. (2020). La protección de datos de los trabajadores en Portugal: el diálogo entre el Código de Trabajo, el RGPD y la nueva Ley de Protección de Datos. Em M. R.-P. Royo, & A. T. Signes, *Vigilancia y control en el Derecho del Trabajo Digital* (pp. 401-421). Navarra: Editorial Aranzadi, S. A. U. .
- Lambelho, A., & Gonçalves, L. A. (2012). *Poder disciplinar - Justa causa de despedimento*. Lisboa: Quid Juris.
- Leitão, L. M. (2004). *Código do Trabalho anotado (2ª Edição)*. Coimbra: Almedina.
- Lopes, S. K. (2014). Direitos fundamentais e direitos de personalidade do trabalhador à luz do Código do Trabalho . Em *Direitos Fundamentais e de Personalidade do Trabalhador (2ª Edição)* (pp. 17-43). CEJ.
- Marecos, D. V. (2012). *Código do Trabalho Anotado (2ª Edição)*. Coimbra: Coimbra Editora.

- Mayer-Schönberger, V., & Padova, Y. (2016). Regime Change? Enabling Big Data Through Europe's New Data. *The Columbia Science & Technology Law Review* (Vol. XVII), 317-335.
- Monteiro, A. P., & Pinto, P. M. (2012). *Teoria Geral do Direito Civil (4ª Edição)*. Coimbra: Coimbra Editora.
- Moreira, T. C. (2011a). As novas tecnologias de informação e comunicação e o poder de controlo eletrónico do empregador. Em *Estudos do Direito do Trabalho* (pp. 11-34). Coimbra: Almedina.
- Moreira, T. C. (2011b). Direitos de Personalidade. Em *Código do Trabalho - A revisão de 2009* (pp. 93-114). Coimbra: Coimbra Editora.
- Mota, J. (2018). O consentimento no Regulamento Geral sobre a Proteção dos Dados. Em *Inforbanca* (p. 8). Lisboa: Instituto de Formação Bancária.
- Nascimento, R., & Gama, A. (2019). RGPD em Contexto Laboral. *Boletim da Ordem dos Advogados*.
- Ogriseq, C. (2017). GDPR and Personal Data Protection in the Employment Context. *Labour & Law Issues - Vol. 3*, ISSN 2421-2695.
- Orrico, J. F. (2020). Límites a la biometría como medio de identificación y control de los trabajadores: necesidad de su regulación. Em M. R.-P. Royo, & A. T. Signes, *Vigilancia y control en el Derecho del Trabajo Digital* (pp. 301-326). Navarra: Editorial Aranzadi, S.A.U.
- Pinto, N. A. (2010). *Instituto Disciplinar Laboral*. Coimbra: Coimbra Editora.
- Pinto, P. M. (2018). *Direitos de personalidade e direitos fundamentais - Estudos*. Coimbra: GESTLEGAL.
- Prata, A. (2017). *Código Civil Anotado - Volume I (Artigos 1º a 1250º)*. Coimbra: Almedina.
- Quintas, P. C. (2013). *Os direitos de personalidade consagrados no Código do Trabalho na perspectiva exclusiva do trabalhador subordinado - Direitos (Des)figurados*. Coimbra: Almedina.
- Ramalho, M. R. (2012). *Tratado de Direito do Trabalho: Parte II - Situações Laborais Individuais (4ª Edição)*. Coimbra: Almedina.
- Redinha, M. R. (2014). Da proteção da personalidade no Código do Trabalho. Em *Para Jorge Leite - Escritos jurídico-laborais - Volume I* (pp. 819-853). Coimbra: Coimbra Editora.
- Saldanha, N. (2018). *Novo Regulamento Geral de Proteção de Dados - O que é? A quem se aplica? Como implementar?* Lisboa: FCA - Editora de Informática.

Sousa, M. R., & Alexandrino, J. M. (2000). *Constituição da República Portuguesa Comentada*. Lisboa: LEX.

Sparemberger, R. F., & Thiesen, A. B. (jan./jun. de 2010). O direito de saber a nossa história: identidade genética e dignidade humana na conceção da bioconstituição. *Direitos Fundamentais & Democracia*, pp. 33-65.

Varela, J. A. (2008). *Das obrigações em geral - Volume I (10ª edição)*. Coimbra: Almedina.

Vasconcelos, P. P. (2010). *Teoria Geral do Direito Civil*. Coimbra: Almedina.

Xavier, B. (2014). *Manual de Direito do Trabalho (2ª Edição)*. Lisboa: Verbo.

*Esta página foi intencionalmente deixada em branco*

## Jurisprudência

Acórdão do Tribunal Constitucional, Plenário, datado de 24 de abril de 2018, Processo n.º 95/17 (C. Pedro Machete)

Acórdão do Supremo Tribunal de Justiça, 7ª Secção, datado de 13 de julho de 2017, Processo n.º 3017/11.6TBSTR.E1.S1 (Lopes do Rego)

Acórdão do Supremo Tribunal de Justiça, 1ª Secção, datado de 01 de março de 2016, Processo n.º 1219/11.4TVLSB.L1.S1 (Garcia Calejo)

Acórdão do Tribunal da Relação de Coimbra, datado de 03 de abril de 2014, Processo n.º 5/13.1T4AGD.C1 (Jorge Loureiro)

Acórdão do Supremo Tribunal de Justiça, 1ª Secção, datado de 17 de dezembro de 2009, Processo n.º 159/07.6TVPRT-D.P1.S1 (Hélder Roque)

Acórdão do Supremo Tribunal de Justiça, 1ª Secção, datado de 07 de junho de 2011, Processo n.º 1581/07.3TVLSB.L1.S1 (Gabriel Catarino)

Acórdão do Tribunal Constitucional, 2ª Secção, datado de 10 de dezembro de 2008, Processo n.º 397/08 (C. Joaquim de Sousa Ribeiro)

Acórdão do Tribunal Constitucional, 3ª Secção, datado de 11 de outubro de 2000, Processo n.º 761/99 (C. Messias Bento)

Acórdão do Tribunal Constitucional, 2ª Secção, datado de 30 de outubro de 1985, Processo n.º 198/85 (C. Cardoso da Costa)