escola superior de tecnologia e gestão
instituto politécnico de leiria

O tratamento de dados biométricos no contexto laboral

Mestrado em Solicitadoria de Empresa

Olga Hrytsiuk

Leiria, março de 2022

escola superior de tecnologia e gestão
instituto politécnico de leiria

O tratamento de dados biométricos no contexto laboral

Mestrado em Solicitadoria de Empresa

Olga Hrytsiuk

Dissertação realizada sob a orientação da Professora Doutora Ana Lambelho

Leiria, março de 2022

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 2020/2021, 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.

PÁGINA DEIXADA PROPOSITADAMENTE EM BRANCO

Resumo

A evolução das tecnologias informáticas traz novos desafios para todos, e as empresas não são exceção. O presente trabalho tem como objetivo o estudo e o enquadramento, de forma completa mas não exaustiva, dos dados pessoais no âmbito laboral, em particular dos dados biométricos, tendo em conta a crescente utilização de sistemas biométricos nos locais de trabalho para controlo de assiduidade, registo de tempos de trabalho e para controlo de acessos. Pretende-se, de forma geral, perceber as especificidades legais do controlo através dos sistemas biométricos na relação laboral, com base na legislação vigente.

Começaremos por definir alguns conceitos fundamentais para o desenvolvimento dos trabalhos, fazendo também um enquadramento geral do contrato de trabalho e, bem assim, explicando sinteticamente o surgimento dos dados pessoais e da sua consagração no mundo e no ordenamento jurídico português.

Posteriormente, abordaremos algumas questões fundamentais sobre os dados pessoais dos trabalhadores, tais como os fundamentos de licitude para o tratamento dos mesmos no âmbito laboral, os princípios que devem sempre ser respeitados e tidos em conta e os direitos dos titulares dos dados. A nossa abordagem terá sempre em conta, por ser inevitável, os dados pessoais em geral. Terminamos com as conclusões sobre quais os fundamentos de legitimidade para o tratamento de dados biométricos no contexto laboral.

Palavras-chave: contrato de trabalho, dados pessoais, dados biométricos, trabalhador, entidade empregadora, RGPD.

PÁGINA DEIXADA PROPOSITADAMENTE EM BRANCO

Abstract

The evolution of computer technologies brings new challenges for everyone, and companies are no exception. This paper aims to study and frame, in a complete but not exhaustive way, personal data in the labor field, particularly biometric data, taking into account the increasing use of biometric systems in the workplace for attendance control, work time period recording and access control. It is intended, in general, to understand the legal specificities of control through biometric systems in the labour relationship, based on current legislation.

We will begin by defining some fundamental concepts for the development of the work, while also making a general framework for the employment contract, as well as briefly explaining the emergence of personal data and its consecration in the world and in the Portuguese legal system.

Subsequently, we will address some fundamental issues regarding workers' personal data, such as the legal grounds for processing them in the employment context, the principles that must always be respected and taken into account, and the rights of the subjects' data. Our approach will always take into account personal data in general, because it is unavoidable. We will end with the conclusions on what the legitimacy grounds are for processing biometric data in the employment context.

Keywords: labor contract, personal data, biometric data, employee, employer, GDPR.

PÁGINA DEIXADA PROPOSITADAMENTE EM BRANCO

Índice

PÁGINA DEIXADA PROPOSITADAMENTE EM BRANCO

Lista de siglas e de abreviaturas

AEPD - Autoridade Espanhola de Proteção de Dados

al./als. – alínea/alíneas

art./arts. – artigo/artigos

CC – Código Civil

CDFUE - Carta dos Direitos Fundamentais da União Europeia

CEPD – Comité Europeu para a Proteção de Dados

cfr. – confrontar/conforme

CNPD – Comissão Nacional de Proteção de Dados

Coord. - coordenadores

CRP – Constituição da República Portuguesa

CT – Código do Trabalho

dir. - diretores

Diretiva – Diretiva 95/46/CE do Parlamento Europeu e do Conselho

DUDH – Declaração Universal dos Direitos Humanos

et al. - *et alia*

GT29 - Grupo de Trabalho de Proteção de Dados do artigo 29.º

Lei de Execução - Lei n.º 58/2019, de 08 de Agosto

p./pp. – página/páginas

RGPD ou Regulamento – Regulamento Geral sobre a Proteção de Dados

TFUE – Tratado de Funcionamento da União Europeia

UE – União Europeia

PÁGINA DEIXADA PROPOSITADAMENTE EM BRANCO

Introdução

É certo que a crescente evolução das tecnologias informáticas trouxe diversas melhorias ao mundo e às relações pessoais em geral. No entanto, e por outro lado, entre muitas outras coisas, verificou-se também um aumento de informação a circular em rede e, bem assim, um aumento dos diversos usos que lhe foram sendo atribuídos. Tal facto, aliado à circulação, muitas vezes descontrolada, de dados pessoais, gerou uma necessidade de reformulação da regulamentação aplicável em matéria de proteção de dados pessoais, que teve na sua génese a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro (Mota & Pedral, 2019, p. 142).

A matéria dos dados pessoais e, em especial, dos dados biométricos, assume especial relevância. Esta encontra-se prevista no capítulo dos direitos, liberdades e garantias pessoais, em concreto no art. 35.º da nossa Lei Fundamental.

A dependência do ser humano às novas tecnologias é inegável e estas não poderiam passar à margem do Direito do Trabalho. As relações laborais foram, inevitavelmente, sofrendo mudanças, tendo esta nova realidade transformado em profundidade a estrutura empresarial, no que toca tanto à organização da atividade do trabalhador como à sua monotorização (Cunha & Santos, 2021, p. 2 e Moreira, 2012, p. 16). Aliás, num futuro breve, com os avanços e progressos de forma exponencial das novas tecnologias, acreditamos que certamente, as relações laborais sofrerão mudanças, surgindo também novos desafios, uma vez que as tecnologias avançam muito rapidamente, sendo difícil o Direito acompanhá-las ao mesmo ritmo.

Também no âmbito laboral vão surgindo novas tecnologias informáticas, suscetíveis de ameaçar a privacidade das pessoas em geral e, em especial, dos trabalhadores. As entidades empregadoras procedem à recolha de diversos dados pessoais dos trabalhadores, muitas vezes sem a consciência plena de que o tratamento de dados pessoais tem regras jurídicas próprias e rigorosas. O tratamento posterior desses dados é, muitas vezes realizado, sem que a entidade empregadora se dê conta de que poderá afetar a privacidade e intimidade dos trabalhadores, por vezes de forma desproporcionada e/ou injustificada. É por isso que a proteção da privacidade dos trabalhadores é, atualmente, uma obrigação do Direito do Trabalho moderno, perante a incapacidade de o trabalhador, por si só, salvaguardar os seus direitos numa situação de subordinação jurídica e eventual dependência económica (Henriques & Luís, 2019, p. 14).

Nesse sentido, as entidades empregadoras viram-se confrontadas com novos desafios relacionados com os direitos dos trabalhadores em relação a todas as formas de tratamento de dados e ao controlo dos trabalhadores através dos mesmos (Guerra, 2004, p. 17).

Se até há relativamente pouco tempo, a título de exemplo, os registos dos tempos de trabalho eram efetuados de forma simples, com recurso a uma folha e com a assinatura na mesma, atualmente, grande parte das empresas modernas têm vindo a adotar novos sistemas, como os sistemas de controlo biométrico, que apesar de não serem uma novidade recente, têm vindo a conhecer maior utilização. Esta tecnologia é fiável, eficiente e económica para as entidades empregadoras, pelo que mostra ser uma mais-valia. No entanto, por outro lado, é também, indiscutivelmente, mais invasiva para a esfera privada do trabalhador, podendo trazer possíveis violações dos seus direitos. Os dados biométricos, com a entrada em vigor do RGPD, fazem parte das categorias especiais de dados pessoais, merecendo, pois, proteção especial.

Assim, e sabendo que, em regra, o tratamento de dados pessoais sensíveis é proibido nos termos do art. 9.º, n.º 1 do RGPD, importa que seja feita uma reflexão, aquando da implementação destes sistemas, para perceber quando e com que fundamento é que esses sistemas de controlo são admissíveis e, bem assim, as implicações que o tratamento de dados biométricos tem na privacidade dos trabalhadores. Procuraremos estudar quando e em que termos pode ser feito o tratamento de dados biométricos dos trabalhadores no âmbito laboral, na medida em que apresenta algumas especificidades relativamente ao regime geral do tratamento de dados pessoais.

Quanto à metodologia utilizada no presente trabalho, esta recai sobre a análise da legislação aplicável, bibliografia relacionada com esta temática e alguma jurisprudência. Sempre que pertinente, recorremos a dados estatísticos e a documentos de entidades que atuam no domínio da proteção de dados, como a Comissão Nacional de Proteção de Dados e o Comité Europeu para a Proteção de Dados.

CAPÍTULO I – Generalidades

1. Delimitação dos conceitos e enquadramento da temática

1.1. A biometria e os sistemas biométricos

A biometria[1] é a ciência que permite identificar um indivíduo através de métodos automatizados, baseados em traços de natureza morfológica, física ou fisiológica (como, a título de exemplo, a impressão digital, a íris ou a retina) ou na análise comportamental (como a assinatura escrita, a forma de andar) (Lopes, 2018).

Assim, não só importa perceber de que características se trata mas também, se todas elas podem ser consideradas. A verdade é que, o que releva para estes efeitos, é que os traços biométricos utilizados preencham uma série de condições essenciais e cumulativas, a saber: devem ser universais (estar presentes, em princípio, em todas as pessoas[2]); distintas entre pessoas (exclusivas de cada indivíduo, permitindo fazer a diferenciação entre estes); permanentes (manter-se inalteráveis no tempo e independentemente das condições ambientais[3]); e, por último, devem ser viáveis de recolha/acessíveis (prontamente disponibilizadas para análise através de instrumento técnico simples e facilmente quantificáveis)[4] (Jain et al., 2003, p. 4 e Baz Rodríguez, 2019, p. 245).

Existem, assim, operações distintas com base na utilização de dados biométricos, através da utilização de diferentes sistemas biométricos, que são sistemas automáticos que permitem o reconhecimento de seres vivos através dos seus traços inerentes (Fernández Orrico, 2020, p. 303). E podemos falar de dois modos de sistemas biométricos – o modo de verificação (também denominado por autenticação), em que o sistema valida a identidade de uma pessoa comparando os dados biométricos capturados com o(s) seu(s) modelo(s) biométrico(s) armazenado(s) na base de dados do sistema (ou seja, valida se a

[1] A palavra biometria é formada por bio (vida) e metria (medida) - "biometria", in *Dicionário Priberam da Língua Portuguesa* [em linha], https://dicionario.priberam.org/biometria, último acesso em 05-12-2021.

[2] O facto de uma característica biométrica ser considerada universal, não invalida que algumas pessoas possam não a ter, uma vez que podem tê-la perdido, por exemplo, devido a acidente, doença ou outra circunstância particular (Guerra, 2004, p. 190).

[3] No entanto, casos raros existem em que os dados biométricos podem sofrer alterações com a passagem do tempo ou por razões de doença (Cordeiro, 2020, p. 140).

[4] Nas palavras de Varges Gomes "é esta sua característica de quantificação e susceptibilidade de medição, sempre variável relativamente a todas e cada uma delas, que vai permitir, quer o processo inicial de inscrição ou registo na respetiva base de dados, na sequência do processo de algoritmização e numeralização, quer, posteriormente, quando da sua comparação, levando então à maior ou menor, probabilidade da identificação ou da autenticação" (*apud* Guerra, 2004, p. 191).

informação é daquela pessoa ou não[5]); e o modo de identificação, em que o sistema tenta fazer uma correspondência entre um dado biométrico e os dados de todos os utilizadores da base de dados, com a finalidade de estabelecer a identidade de um indivíduo (o sistema não apresenta resultados se o indivíduo não estiver inscrito na base de dados do sistema[6]) (Jain et al., 2003, pp. 4-5). No presente trabalho, utilizaremos o verbo genérico "reconhecer" sempre que não seja necessário fazer distinção entre o modo de verificação e o de identificação.

Para a realização das operações acima referidas, é necessário que os dados biométricos sejam recolhidos e armazenados e, para isso, os dados das pessoas são capturados por sensores específicos correspondentes a cada tipo de dado, sendo associados a um identificador. De forma genérica, o armazenamento é efetuado através da digitalização da "imagem" obtida ou através da transformação num *template* (a medição do dado biométrico do indivíduo converte-se num código através de um modelo matemático), que é igualmente associado à pessoa em causa e passará a constar do registo, na respetiva base de dados (Castro, 2005, pp. 83-84). Assim, para o seu funcionamento, o sistema biométrico requer a parte física (*hardware*) que são, habitualmente, os sensores que realizam as medições, e uma parte de *software*, que efetua as comparações com os dados previamente registados (Cortés Osorio et al., 2010, p. 99).

Para serem utilizados, devem ser verificados dois aspetos complementares, quanto aos sistemas de leitura biométrica, e são eles: o grau de desempenho (dependendo este aspeto da sua capacidade de resposta em termos de velocidade a identificar a pessoa em causa) e a taxa de precisão ou de erro que apresentam (o sistema deve ser capaz de rejeitar identidades falsas e, bem assim, não pode ser intrujado com facilidade) (Guerra, 2004, p. 194). Neste sentido, pretende-se que estes sistemas sejam fiáveis e que consigam assegurar que os dados pessoais sejam acedidos apenas por utilizadores e entidades legítimas.

Exemplos dos principais sistemas de leitura biométrica são a identificação das iris, a leitura de impressão digital (dados datiloscópicos), o reconhecimento facial, e o reconhecimento por voz.

[5] O modo de verificação responde à pergunta "Este dado biométrico pertence a João?", sendo representado pela expressão 1-n (um para muitos) (Guerra, 2004, pp. 185-186).

[6] O modo de identificação responde à pergunta "De quem é este dado biométrico?", e é representado pela expressão 1-1 (um para um) (Guerra, 2004, p. 186).

Cabe-nos ainda analisar a forma de aplicação dos sistemas biométricos, questão da qual aqui nos ocuparemos.

Como já se disse, os sistemas de leitura biométrica têm sido uma realidade crescente no espaço laboral. Estes são considerados mais seguros do que os métodos tradicionais, já que os códigos *pin* e os cartões podem ser copiados, roubados ou esquecidos facilmente, e os dados biométricos, à partida, não podem (Fernández Orrico, 2020, p. 302). De facto, o controlo biométrico assegura a impossibilidade de substituir um indivíduo por outro[7] (apesar de já se verificarem algumas possibilidades de contornar estes sistemas).

Assim, uma das maiores vantagens da utilização dos sistemas biométricos neste âmbito é o facto de o evento ficar associado a um indivíduo específico (um individuo não pode fazer-se passar por outro), não sendo como os códigos *pin* que são utilizáveis por várias pessoas. No entanto, outros benefícios são apontados por autores como Fernández Orrico (2020, p. 305), tais como: considera-se uma tecnologia conveniente, uma vez que não se tem de recordar uma chave; não é suscetível a perdas; a característica biométrica é a mesma, independentemente de onde o indivíduo se encontre; reforça a privacidade, pois protege contra acesso não autorizado a informação pessoal e pode ser um complemento a outros mecanismos de autenticação.

Contudo, não negando os benefícios evidentes associados a este modo de reconhecimento, a verdade é que, hoje em dia, o recurso a estes meios corresponde, não raras vezes, à adesão a uma moda e à "cedência a campanhas de marketing que prometem fiabilidade, segurança e rigor" (Guerra, 2004, p. 188).

E se, quando surgiram inicialmente, se podiam considerar uma tecnologia e um meio de identificação praticamente infalível e quase totalmente seguro, a verdade é que, com o passar dos anos e com o aumento da sua utilização (que começou por ser um "privilégio da polícia, das grandes empresas e poderes públicos"), os seus custos foram diminuindo, a utilização "universalizada" e a tendência para existirem burlas relacionadas com elas, aumentou (Guerra, 2004, p. 188). Para além destas "burlas", existem também problemas de eficiência a ter em conta, uma vez que os sistemas biométricos se baseiam em padrões de comparação que, aos dias de hoje, não garantem uma precisão infalível (Baz

[7] Tal como afirma um investigador francês e criador do sensor de impressões digitais *FingerPrint*, uma simples chave não prova que uma determinada pessoa que está a abrir o que seja com a chave, seja a pessoa que deve ter acesso àquele conteúdo ou aqueles dados, sendo que a biometria preenche (à partida) essa lacuna (Francois, 2006 *apud* Cortés Osorio et al., 2010, p. 99).

Rodríguez, 2019, p. 245). Ademais, tem-se estudado a possibilidade de alguns dos sistemas poderem causar danos à saúde do indivíduo (em especial, os dispositivos de identificação através da íris/retina) (Fernández Orrico, 2020, p. 305 e Guerra, 2004, p. 206). De referir ainda que os dados biométricos "roubados ou perdidos" apresentam riscos extremos para os seus titulares, uma vez que, ao contrário dos outros códigos (como *pins* e *passwords*), não podem ser alterados ou substituídos[8/9/10] (Guerra, 2004, p. 198).

É necessário ter também em conta que os riscos associados aos "erros dos sistemas biométricos" podem comportar graves consequências para o trabalhador em causa e, bem assim, consequências para a entidade empregadora, como a interdição indevida de pessoas autorizadas e a admissão indevida de pessoas não autorizadas (Guerra, 2004, p. 215).

Estes riscos são agravados quando os dados pessoais são armazenados em bases de dados centralizadas (que podem levar a um desvio da sua utilização ou ao roubo e ciberataques, perdendo o controlo dos dados), em vez de objetos ou dispositivos que possam permanecer sob o controlo exclusivo do titular dos dados (Baz Rodríguez, 2019, p. 245).

Assim, um dos maiores riscos inerente a estes sistemas, a nosso ver, é a possibilidade de chegarem à posse de pessoas não autorizadas e mal intencionadas, e que sejam por elas geridas, uma vez que se trata de informações/dados que não podem ser modificados, em caso de roubo ou falsificação de identidade (ao contrário de um código *pin*). Neste sentido, estes sistemas, podem, hipoteticamente, servir para a elaboração de perfis ou para o tratamento automatizado de dados biométricos para fins decisórios, o que pode levar a ações, comportamentos ou efeitos discriminatórios sendo que, não menos importante, a reutilização de dados biométricos *stricto sensu* para fins incompatíveis com a finalidade principal para a qual foram recolhidos, pode abrir o caminho a consequências prejudiciais

[8] Fernández Orrico (2020, pp. 306-307) refere que é necessário começar a tornar mais eficazes os sistemas, sendo que, por exemplo, no tocante aos sistemas de leitura de impressão digital, deve conjugar-se a leitura da impressão com a medição da temperatura aquando a captura para garantir que a mesma pertence a um ser humano vivo.

[9] Sobre as vantagens e desvantagens do uso dos sistemas biométricos aconselhamos a leitura de INCIBE (2016, pp. 21-28) que apresenta quadros-resumo, a nosso ver, muito interessantes.

[10] A *BioStar 2*, uma ferramenta de *software* desenvolvida por uma empresa líder de segurança, que permitia identificar uma pessoa através da sua impressão digital ou reconhecimento facial, foi indevidamente acedida em 2019, tendo sido armazenados 27,8 milhões de registos de forma insegura, e tendo sido expostos os dados de mais de um milhão de pessoas, incluindo senhas e informações biométricas, tais como impressões digitais ou informações de reconhecimento facial, que foram utilizadas para aceder a contas e instalações (Marrero Blanco & Mulero Fernández, 2020, p. 8). Estas informações biométricas, como é claro, não puderam ser posteriormente alteradas pelos seus titulares.

inaceitáveis para o titular destes dados (Baz Rodríguez, 2019, pp. 245-246). Para o tema que nos ocupa, quando falamos do controlo de entradas e saídas (quer seja para registo de assiduidade ou para o controlo a certos locais reservados), os sistemas mais utilizados são os que recorrem às características morfológicas, físicas ou fisiológicas, nomeadamente os sistemas de reconhecimento da impressão digital, da íris ou da retina, da geometria da mão ou do rosto (Guerra, 2004, p. 199).

Um outro sistema biométrico muito adotado devido aos baixos custos associados à sua implementação, é o reconhecimento pela assinatura. A digitalização da mesma é analisada de dois pontos de vista: a própria assinatura e a forma como está executada. É necessário apenas uma tábua de escrever ligada ao computador e os dados armazenados incluem a velocidade, pressão, direção, comprimento do curso e as áreas onde a caneta é levantada. O maior inconveniente deste método é que uma pessoa nunca assina duas vezes de forma exatamente igual, pelo que este método pode ser falível (Cortés Osorio et al., 2010, p. 99).

Antes de implementar qualquer sistema biométrico, a entidade empregadora deve ter em conta vários fatores como o "conforto na utilização, a precisão, a relação qualidade/preço e o grau de segurança" (Relatório da Assembleia Nacional Francesa[11] *apud* Guerra, 2004, p. 199) e deve também procurar obter o consenso dos trabalhadores[12]. Salvo melhor opinião, infelizmente, muitas vezes, o critério do empregador na eleição do sistema biométrico é o puramente economicista.

Os sistemas que recorrem à identificação através da impressão digital são, por enquanto, dos mais utilizados em diversas situações, entre as quais, no âmbito laboral. A sua aplicação apresenta vantagens, como as suprarreferidas, aliadas ao baixo custo da sua instalação. No entanto, têm-se também verificado desvantagens mais "específicas", relacionadas com a alteração/dificuldade de recolha decorrentes de humidade, suor, ou alguma eventualidade como uma queimadura ou um corte, o que pode dificultar a leitura da impressão digital do trabalhador e, por conseguinte, a sua recolha ou a qualidade (Fernández Orrico, 2020, p. 307).

[11] Este relatório pode ser consultado em https://www.assemblee-nationale.fr/12/pdf/rap-off/i0938.pdf.
[12] Tal facto (a obtenção do consenso por parte dos trabalhadores), ainda que não decorra de qualquer ordem jurídica que imponha a referida circunstância, deve verificar-se a fim de garantir a paz social e promover a boa relação entre as partes.

A verdade é que, em consequência da pandemia que o mundo tem vindo a atravessar, tem sido aconselhado o uso de sistemas de reconhecimento facial/da íris, em alternativa aos sistemas de impressão digital[13/14]. Assim seria ultrapassada a dificuldade de recolha de impressões digitais em profissões que utilizam luvas, ou que trabalham sob grande exposição de calor, por exemplo.

Guerra (2004, p. 215) considera ainda que a impressão digital não é, de entre os dados dos sistemas biométricos, a que maiores perigos apresenta para a privacidade do indivíduo, justificando que, para que a impressão digital seja recolhida, é necessário que a pessoa adira a esta recolha ou, pelo menos, que tenha conhecimento da mesma. Pelo contrário, essa adesão ou conhecimento, não é necessariamente verificado quando falamos do reconhecimento da voz ou da geometria facial que pode não pressupor a colaboração do titular, e pode dar origem a tratamentos ainda mais invasivos, especialmente quando utilizados com o desconhecimento e sem o controlo do seu titular (Guerra, 2004, p. 216). Entendemos, no entanto, que a recolha de dados pessoais, é sempre possível de ser feita de forma ilícita. Aliás, sempre que tocamos em algum objeto, deixamos, inevitavelmente, a nossa impressão digital.

Contudo, a doutrina tem apontado no sentido de a leitura da íris ser, especialmente na primeira fase de recolha, o sistema mais invasivo e o mais "lesivo" para os direitos fundamentais dos trabalhadores, uma vez que com a leitura da íris é possível obter certos dados sensíveis relativos à saúde do trabalhador (como revelar o consumo de álcool e drogas ou o sofrimento de doenças como a hipertensão ou diabetes), que pode levar a ações discriminatórias contra certos trabalhadores (Fernández Orrico, 2020, pp. 312-313).

1.2. Os dados biométricos como dados pessoais sensíveis

Em 24 de outubro de 1995 foi publicada a Diretiva 95/46/CE relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação

[13] Para além da maior facilidade de recolha da íris (nos dias de hoje, por exemplo, a utilização da máscara não prejudica a sua recolha), o controlo através desta é considerado o mais fiável de entre os sistemas biométricos, uma vez que utiliza cerca de 266 pontos únicos, quando a maioria dos restantes tem apenas cerca de 13 a 60 pontos (Cortés Osorio et al., 2010, p. 99). Cada olho é único (tanto de pessoa para pessoa, como também de um olho para o outro, de cada indivíduo) e permanece estável ao longo do tempo e em ambientes climáticos diferentes (Fernández Orrico, 2020, p. 312).

[14] Veja-se https://ordemdosmedicos.pt/covid-19-ordem-recomenda-abolicao-do-registo-biometrico-atraves-de-impressao-digital/ , medida esta que foi contemplada no Plano de Contingência da Assembleia da República, último acesso em 28/02/2022.

desses dados (doravante abreviadamente designada por Diretiva). Conscientes da necessidade de realizar uma análise aprofundada do conceito de dados pessoais, dadas as incertezas e diferentes interpretações dos Estados-Membros no que toca a aspetos importantes do conceito, que poderiam afetar o que se pretendia que fosse um correto funcionamento do quadro da proteção de dados vigente, o então denominado Grupo de Trabalho de Proteção de Dados do artigo 29.º[15] (doravante abreviadamente designado por GT29) emitiu o Parecer 4/2007[16]. Este tinha como objetivos principais a adoção de um entendimento comum acerca do conceito de dados pessoais, assim como fornecer orientações sobre como as regras nacionais de proteção de dados deveriam ser aplicadas, a que situações e de que forma (Parecer 4/2007, p. 3). Pretendia-se, acima de tudo, contribuir para uma aplicação uniforme dessas mesmas normas, o que constituía uma função central do GT29[17/18].

Assim, o conceito de dados pessoais que foi objeto de estudo pelo GT29 constava do art. 2.º, al. a), 1.ª parte da Diretiva e podia ler-se que era considerado dado pessoal "qualquer informação relativa a uma pessoa singular identificada ou identificável («pessoa em causa»)".

Esta noção não coincide integralmente com a que resulta da redação dada pelo Regulamento Geral da Proteção de Dados[19] agora em vigor, onde os dados pessoais são definidos como sendo a "informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»)" (art. 4.º, 1) do RGPD).

---

[15] Inicialmente, começou por se designar por Grupo de Trabalho de Proteção de Dados do artigo 29.º, que foi instituído ao abrigo do art. 29.º da Diretiva 95/46/CE, e que foi um órgão consultivo europeu independente em matéria de proteção de dados e privacidade (não refletindo a posição da Comissão Europeia). Este deixou de existir a partir do dia 25 de maio de 2018, tendo sido substituído pelo Comité Europeu de Proteção de Dados (doravante abreviadamente designado por CEPD), que assumiu como seus os pareceres/posições daquele grupo (considerando 139 do RGPD). Assim, faremos referência ao GT29 quando os pareceres/orientações sejam anteriores a 25 de maio de 2018, e ao CEPD, quando sejam posteriores a esta data.

[16] Este parecer, sobre o conceito de dados pessoais, pode ser consultado, em português, em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_pt.pdf.

[17] Esta necessidade devia-se, em grande parte, ao facto de os dados pessoais serem utilizados em vários Estados (por exemplo, no controlo das fronteiras), tornando-se necessária a adoção de regras jurídicas compatíveis entre eles (Guerra, 2004, p. 189).

[18] Parece-nos, no entanto, que esta tentativa de uniformizar não logrou efeitos. Assim, sendo necessária uniformidade legislativa nesta matéria, esta seria apenas alcançável por via de Regulamento, o que se veio a confirmar mais tarde, e deu lugar ao RGPD.

[19] Na verdade, em geral, podemos dizer que o RGPD veio a manter os conceitos constantes da Diretiva, embora com algumas alterações, ainda que não muito significativas.

Verifica-se, através da comparação das duas noções, que deixou de constar a palavra "qualquer" que se referia à "informação". Será que, com esta alteração, o legislador europeu pretendeu que a noção fosse mais restrita, que abrangesse menos informações do que aquela que era abrangida anteriormente? Ou será apenas uma questão de redação, não pretendendo alterar o âmbito de aplicação, apesar da mudança de redação? O mesmo questionamos quanto à última parte do mencionado artigo, em que no lugar de "pessoa em causa" passou a constar "titular dos dados". Parece-nos que, em ambos os casos, estará em causa apenas uma questão terminológica, não pretendendo o legislador abarcar menos situações e tencionando, sim, tornar mais clara a interpretação do artigo.

Assim, o GT29 analisou o conceito constante da Diretiva (e agora de forma idêntica do Regulamento) tratando-o com maior detalhe, através do referido Parecer 4/2007. Esta análise continua a ser utilizada e tem vindo a ser entendimento unânime que o conceito de dado pessoal se decompõe em quatro elementos, que estão relacionados entre si, mas que devem ser tratados separadamente, dada a complexidade subjacente — elementos estes que, juntos, determinam se uma informação deverá ou não ser considerada como "dado pessoal". Trata-se, então, dos seguintes elementos: (i) qualquer informação, (ii) relativa a, (iii) pessoa singular, (iv) identificada ou identificável. Vejamo-los de forma mais pormenorizada[20]:

i. Qualquer informação

Para efeitos de aplicação do Direito da Proteção de Dados, toda a informação é considerada relevante (Cordeiro, 2020, p. 107), e a expressão "qualquer informação" indica precisamente essa intenção – a de prever um conceito alargado de dado pessoal[21].

O GT29 analisou este elemento de três perspetivas: da perspetiva da natureza da informação, da perspetiva do conteúdo da informação e da perspetiva do formato em que a informação é apresentada.

[20] A nossa abordagem quanto a estes elementos não será exaustiva, uma vez que o âmbito do nosso trabalho não necessita de grandes desenvolvimentos relativamente aos mesmos, pelo que aconselhamos, para maiores esclarecimentos, a leitura de Cordeiro (2020, pp. 107-129), Pinheiro, et al. (2018, pp. 121-130) e, bem assim, do Parecer 4/2007 do GT29.

[21] No entanto, o GT29 também ressalva que "o âmbito das regras de proteção de dados não deverá ser inadequadamente ampliado" (Parecer 4/2007, p. 5).

Do ponto de vista da natureza da informação, segundo a análise do GT29, o conceito inclui qualquer tipo de declarações (que não necessitam de ser verdadeiras ou comprovadas) – tanto informações objetivas (por exemplo, a presença de determinada substância no sangue de uma pessoa), como informações, opiniões e avaliações subjetivas (por exemplo, que determinada pessoa é um bom trabalhador, e por isso merece ser promovido) (Parecer 4/2007, p. 6).

Já do ponto de vista do conteúdo da informação, o conceito de "dados pessoais" inclui qualquer tipo de informação, o que abrange tanto informações pessoais que são consideradas "dados sensíveis" atenta a sua natureza especial de risco, como tipos mais gerais de informação (Parecer 4/2007, p. 7). Tal inclui informações sobre pessoas singulares, tanto da sua vida privada como profissional[22] e social[23].

Finalmente, analisa-se o conceito do ponto de vista do formato, sendo que o conceito de "dados pessoais" inclui informação disponível em qualquer formato (por exemplo, alfabético, numérico, gráfico, fotográfico) e em qualquer suporte (em papel ou num computador) (Portaria 4/2007, p. 8).

ii. Relativa a

A informação é considerada "relativa a" uma pessoa quando é sobre essa pessoa[24].

Em muitos casos, esta relação é estabelecida com facilidade. No entanto, existem várias situações em que não é tão direta assim essa ligação.

Num documento emitido em 2005, o GT29 pronunciou-se no sentido de considerar que "os dados referem-se a uma pessoa se se referirem à identidade, características ou

[22] Veja-se, neste sentido, os arts. 9.º, n.º 2, al. h), 77.º, n.º 1 e 88.º do RGPD, em que se faz referência a dados pessoais dos trabalhadores.

[23] Neste sentido, veja-se o Acórdão do TFUE (Segunda Secção) de 16 de julho de 2015, C-615/13 P, EU:C:2015:489, em que se pode ler "o facto de essa informação se inscrever no contexto de uma atividade profissional não lhe pode retirar a qualificação de conjunto de dados pessoais", disponível em https://curia.europa.eu/jcms/jcms/j_6/pt/.

[24] Tal inclui também informações relativas a objetos, quando conjugadas com informações respeitantes a pessoas (por exemplo, que determinado telemóvel pertence a A), bem como informações factuais que permitam recolher algum elemento que identifique um sujeito (imagine-se que, numa sala de reuniões se faz referência à pessoa que usa um casaco cor de rosa, sendo a única que veste um casaco dessa cor) ou, ainda, quando essas informações factuais sejam armazenadas nesses termos, ou seja, identificando o seu titular *ab initio* (Cordeiro, 2020, p. 110).

comportamento de uma pessoa ou se tal informação for utilizada para determinar ou influenciar a forma como essa pessoa é tratada ou avaliada"[25]. Assim, o GT29 propõe que a expressão "relativa a" abranja um dos seguintes elementos: conteúdo, finalidade ou resultado – e são estes três elementos alternativos que o parecer vem apresentar (Parecer 4/2007, pp. 10-11).

Neste sentido, será tratada como "dado pessoal" toda a informação que incida sobre a pessoa, ou seja, quando a própria pessoa é objeto de análise (conteúdo)[26]; toda a informação que, embora não seja a própria pessoa o objeto de análise, permita "avaliar, tratar de determinada forma ou influenciar o estatuto ou o comportamento de determinada pessoa" (finalidade)[27]; ou ainda, que apesar de não existir nenhum dos elementos anteriores, seja provável que o uso dos dados tenha um impacto nos direitos e interesses dessa determinada pessoa (resultado)[28] (Cordeiro, 2020, pp. 111-112, e Parecer 4/2007, p. 11).

iii. Pessoa singular

Neste ponto, mais importante a frisar é o facto de que o RGPD apenas se aplica a pessoas singulares, independentemente da sua nacionalidade ou local de residência (considerando 14 e art. 1.º, n.º 1 do RGPD). E apesar de a relação dos n.ºs 1 e 3 do art. 1.º apontar para a circulação dos dados, retira-se do n.º 1 que o objeto do RGPD é o tratamento de dados pessoais, independentemente das circunstâncias em que se verifique (Pinheiro et al., 2018, p. 100).

Já as informações sobre pessoas coletivas apenas estarão sujeitas ao RGPD, se disserem respeito, direta ou indiretamente, a pessoas singulares (Cordeiro, 2020, p. 113).

[25] Este documento pode ser consultado em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp105_en.pdf.
[26] Por exemplo, os resultados de análises clínicas são relativos ao doente em causa (Parecer 4/2007, p. 11).
[27] Por exemplo, o registo de chamadas de um telefone no escritório de uma empresa (Parecer 4/2007, p. 11).
[28] Por exemplo, controlo do posicionamento dos táxis para otimizar os serviços, com impacto nos motoristas (Parecer 4/2007, pp. 11-12).

iv. Identificada ou identificável

Dos quatro elementos, apenas a expressão "identificável" é clarificada no texto do RGPD — "é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular" – art. 4.º, 1) do RGPD.

Este elemento trata especialmente das condições para que uma pessoa seja considerada como "identificável" e também dos "meios suscetíveis de serem razoavelmente utilizados" pelo responsável pelo tratamento dos dados (Parecer 4/2007, p. 27).

Aqui chegados, importa concluir que todo o tipo de dados pessoais que preencha os elementos acima descritos, merece proteção jurídica[29]. Não obstante, existem dados que, pela sua natureza, merecem uma proteção reforçada. Assim, estas regras sobre a proteção de dados pessoais foram criadas para acautelar situações em que os dados de pessoas singulares possam ser violados ou lesados e que, por isso, necessitem de tutela.

Na primeira parte do considerando 51 do RGPD, pode ler-se que "[m]erecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais" – os quais intitula de "dados especiais" ou "dados sensíveis". Não consta do Regulamento uma definição de dados pessoais especiais. No entanto, o legislador europeu optou por elencar no art. 9.º, n.º 1 do RGPD, de forma taxativa, os dados que são considerados especiais. Neste sentido, Cordeiro (2020, p. 133) considera que o referido artigo consagra dois blocos de dados que são merecedores desta especial tutela, sendo eles, por um lado, os dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou a filiação sindical (que respeita a resultados

[29] Pelo contrário, quando a informação tratada não preencha algum dos elementos identificados, não deve ser tratada segundo as regras relativas à proteção de dados pessoais.

decorrentes do tratamento) e por outro, os dados genéticos, os dados biométricos e os dados relativos à saúde (que respeita a categorias de dados).

Atualmente, com a evolução tecnológica, os sistemas de leitura biométrica estão a tornar-se numa tecnologia de maior recurso, sendo-lhes dadas as mais diversas finalidades. São cada vez mais as empresas que utilizam dispositivos de reconhecimento biométrico como meio de identificação e de autenticação. Com isto, e dada a especial sensibilidade dos dados que estão abrangidos, é importante existir uma proteção mais rigorosa no que ao tratamento destes dados diz respeito, e o legislador europeu teve a especial atenção de introduzir o tratamento destes dados como merecedores dessa proteção reforçada. Baz Rodríguez (2019, p. 246) afirma mesmo que o RGPD veio representar um verdadeiro ponto de viragem na regulamentação do processamento de dados biométricos, pretendendo harmonizar a questão a nível europeu e, bem assim, responder às dúvidas até então existentes sobre se os dados biométricos devem ou não ser considerados dados pessoais e, em particular, se devem ser considerados sensíveis.

Ora, para o GT29 (e para o CEPD, na medida em que assumiu como seus os Pareceres do GT29), os dados biométricos podem ser definidos como "propriedades biológicas, características fisiológicas, traços físicos ou acções reproduzíveis, na medida em que essas características e/ou acções 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" (Parecer 4/2007, p. 9)[30].

Nos termos do art. 4.º, 14) do RGPD, e agora claramente qualificados como dados pessoais sensíveis, são dados biométricos os "dados 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 os dados dactiloscópicos".

Estes, por permitirem a identificação única de pessoas singulares são, muitas vezes, propícios a abusos e discriminações, sendo também por isso, na esmagadora maioria das vezes, considerados dados particularmente sensíveis (Cordeiro, 2020, p. 140).

Importa ainda, antes de avançar, perceber se os algoritmos que derivam dos dados biométricos ou de parte deles, podem ser considerados dados pessoais e a eles deve ser

[30] Embora a Diretiva fosse omissa quanto aos dados biométricos, o GT29 considerava que estes já se encontravam abrangidos pela mesma.

aplicada a regulamentação relativa à proteção de dados pessoais, ou se esta apenas se deve aplicar aos dados biométricos *stricto sensu* (Garrote Crespo, 2021, p. 4).

Isto porque, por exemplo, as impressões digitais são recolhidas e armazenadas e, como vimos, esse armazenamento pode ser feito de duas formas, ou digitalizado (guardada a imagem), ou transformado num *template* [*template* este que, idealmente não deverá permitir a reversão dos dados[31] (Guerra, 2004, p. 193)]. Aliás, é este "processo de algoritmização" que gera uma chave, denominada de "assinatura biométrica", e que vai ser associada a uma pessoa e, posteriormente, por comparação, vai permitir que o sistema identifique, por reconhecimento, o respetivo utilizador (Guerra, 2004, p. 192) . E tal como refere a Agência Espanhola de Proteção de Dados (doravante abreviadamente designada por AEPD), se é certo que a impressão digital completa permite a identificação do seu titular, certo é também que essa identificação é passível de ser feita através da recolha de amostras de partes da impressão digital, transformadas num modelo, através do algoritmo que, quando processadas, permitirão a identificação do titular. Assim, na nossa opinião, aos algoritmos que derivam dos dados biométricos, devem aplicar-se as disposições em matéria de proteção de dados pessoais[32/33].

Note-se ainda que a sensibilidade dos dados deve ter em conta a sua capacidade de identificar indivíduos e, bem assim, o tipo de informações que são suscetíveis de ser reveladas (pois podem ser intrusivas na vida privada ou comportar o risco de decisões discriminatórias), ou não (Pinheiro et al., 2018, p. 320).

Para concluir, o GT29 salienta que a informação biométrica apenas constitui um dado pessoal após o tratamento tecnológico que sobre ela incide, o que significa que as fontes dos dados biométricos não são dados pessoais (Parecer 4/2007, p. 9). Ora, significa isto

[31] É dada grande importância a este elemento pelas entidades competentes. Aliás, como iremos ver mais adiante, antes da entrada em vigor do RGPD era necessário notificar a CNPD antes do início do tratamento de dados, devendo aquela avaliar a legitimidade daquele tratamento. Neste sentido, a título de exemplo, na Autorização 2559/2007 da CNPD, relativa à instalação de sistemas biométricos para controlo de assiduidade, pode ler-se o seguinte: "(…) o sistema biométrico que, através do processo de algoritmização, gerou o *template* que representa a característica biométrica captada, não permite fazer a reversão, isto é, descodificar e reproduzir a imagem da característica biométrica. Este aspeto é fundamental no âmbito de protecção da privacidade uma vez que o responsável do tratamento não dispõe de uma base de dados das características biométricas de cada trabalhador". Esta autorização pode ser consultada em https://www.cnpd.pt/.

[32] Pelo contrário, se não for possível identificar o titular, não serão reconduzidos ao conceito de dados pessoais.

[33] Dizem-nos Marrero Blanco & Mulero Fernández (2020, p. 4) que a obrigação do cumprimento de todas as garantias inerentes ao tratamento de dados biométricos, muitas vezes é ultrapassada pelas entidades empregadoras, "desculpando-se" estas com a justificação de que apenas utilizam algoritmos, assumindo que não está a ser efetuado qualquer tratamento/processamento de dados pessoais propriamente ditos.

que, até que a amostra biométrica seja submetida ao tratamento tecnológico que permite a identificação do titular, ela é apenas uma informação e não uma informação pessoal[34] (Pinheiro, 2018, pp. 179-180, 187).

1.3. O contrato de trabalho, a posição das partes e os dados pessoais

Nos termos do art. 11.º do CT, o "[c]ontrato de trabalho é aquele pelo qual uma pessoa singular se obriga, mediante retribuição, a prestar a sua actividade a outra ou outras pessoas, no âmbito de organização e sob a autoridade destas" (definição esta, similar à prevista no art. 1152.º do CC).

Assim, no contrato (individual) de trabalho, a identificação dos sujeitos não levanta dúvidas: tem-se, por um lado, o trabalhador e, por outro, a entidade empregadora. Tal como decorre do suprarreferido artigo, o trabalhador é aquele que presta uma atividade a outra(s) pessoa(s), sob autoridade e direção daquela(s). Neste sentido, o contrato de trabalho pressupõe a existência de uma subordinação do trabalhador em relação à entidade empregadora, subordinação esta que é essencialmente jurídica, mas também, muitas vezes, económica.

A subordinação jurídica consiste no facto de o trabalhador estar sujeito à autoridade da entidade empregadora e ter de prestar trabalho por conta e risco daquela, e sob sua orientação (Lambelho & Gonçalves, 2021, p. 78). Assim, a prestação de trabalho é realizada segundo ordens e direção da entidade empregadora, tendo o trabalhador o dever de obediência relativamente às ordens daquela (art. 128.º, n.º 1, al. e) do CT).

As evoluções tecnológicas e as novas formas de trabalho, trazem consigo muitas mais-valias para as relações laborais, mas também acarretam novas inseguranças no âmbito laboral e novas ameaças para os trabalhadores.

[34] A este respeito, a título de exemplo, não são abrangidas pelas regras aplicáveis ao tratamento de dados biométricos as mais comuns fotografias, mas apenas as fotografias biométricas (por exemplo, as que constam do cartão de cidadão), conforme decorre de um exemplo constante do considerando 51 do RGPD, onde se pode ler que "[o] tratamento de fotografias não deverá ser considerado sistematicamente um tratamento de categorias especiais de dados pessoais, uma vez que são apenas abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular".

E tal como acontece com os indivíduos em geral que, no âmbito do seu direito de personalidade[35], gozam de uma expetativa jurídica quase absoluta de proteção e tutela da sua privacidade e inviolável esfera da vida privada, também os trabalhadores, na sua qualidade de pessoas singulares, merecem semelhante proteção, ainda que adaptada às exigências da relação laboral (Henriques & Luís, 2019, pp. 14-15).

A realidade é que, como bem sabemos, o Direito do Trabalho surgiu como um ramo do Direito que pretendia proteger o trabalhador, a parte mais fraca na relação laboral, perante os arbítrios do empregador – uma vez que a aplicação do Direito Civil às relações laborais mostrava ser insuficiente, e em que a igualdade das partes era meramente formal (Moreira, 2020, p. 46). Neste sentido, as normas do Direito do Trabalho vêm proteger o trabalhador na sua inferioridade no contrato de trabalho, salvaguardando a sua pessoa, na sua dignidade, na sua vida familiar e na sua vida privada, relativamente aos seus dados pessoais (Castro, 2018, p. 276).

No que toca à proteção de dados, questão que nos importa particularmente, bem sabemos que, nos termos do art. 17.º do CT, as condições de recolha de informações sobre dados pessoais dos trabalhadores são restritas, e podemos desde já adiantar que, em termos gerais, tem de se ter em conta o princípio da necessidade. Para além disso, o trabalhador que haja fornecido informações de índole pessoal, goza do direito ao controlo dos respetivos dados pessoais, podendo tomar conhecimento do seu teor e dos fins a que se destinam, bem como exigir a sua retificação e atualização (entre outros direitos dos titulares, que vamos adiante analisar) (art. 17.º, n.º 3 do CT).

Apela-se, neste sentido, a uma compatibilização dos interesses dos intervenientes. Isto porque, se é certo que, por um lado, o Direito do Trabalho permite à entidade empregadora o controlo de determinados aspetos/momentos dos trabalhadores enquanto tais, por outro, o legislador também é claro quanto à exigência da proibição da entrada abusiva, quando desnecessária, na esfera privada dos trabalhadores e, por isso, torna-se imperioso saber se no dia a dia, nos locais de trabalho, são respeitados os direitos

[35] Os direitos de personalidade são, nas palavras de Moreira, "aqueles sem os quais as pessoas não são tratadas como tais" e, encontrando-se estes direitos ligados à dignidade da pessoa humana justifica-se a sua consagração ao nível do Direito do Trabalho (Amado et al., 2019, p. 106). Os direitos de personalidade, "penetram", assim, na relação de trabalho, constituindo-se como um importante limite aos poderes do empregador e, ao mesmo tempo, como uma garantia do exercício de vários direitos fundamentais dos trabalhadores, sendo que o ordenamento jurídico deve garantir esses direitos do trabalhador enquanto pessoa (Amado et al., 2019, p. 106).

fundamentais e de privacidade dos trabalhadores (Henriques & Luís, 2019, p. 15 e Guerra, 2004, p. 39).

É, neste sentido, de fundamental importância o Regulamento Geral de Proteção de Dados.

Cumpre ainda definir "tratamento" e "responsável pelo tratamento", uma vez que vão ser conceitos bastante utilizados ao longo do presente estudo.

Na aceção do RGPD, entende-se por tratamento "uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição" (art. 4.º, 2) do RGPD). Esclarece Pinheiro (2018, p. 131) que nem todas as fases são necessariamente aplicáveis a todos os tratamentos, sendo que é frequente que a maioria se baseie, sobretudo, na recolha, registo e conservação, como, aliás, é o caso do tratamento de dados biométricos, como iremos ver.

A proteção das pessoas singulares conferida pelo 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 (considerando 15 e art. 2.º, n.º 1 do RGPD).

Conforme dispõe o art. 4.º, 7) do RGPD, o responsável pelo tratamento é "a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro". A respeito do responsável pelo tratamento, note-se que, em regra, para o que nos importa em particular, este responsável será a entidade empregadora sendo, em contrapartida, o trabalhador o titular dos dados objeto de tratamento.

2. Evolução Histórica – da privacidade à proteção de dados pessoais

Nem sempre se falou da necessidade de proteção de dados pessoais, tendo começado por se falar do direito à privacidade.

O direito à privacidade enquanto tal foi, pela primeira vez reconhecido, em 1890, com a publicação de um artigo na *Harvard Law Review* por Samuel D. Warren e Louis D. Brandeis, intitulado de "The right to privacy", em que se falava do direito à privacidade como um direito à "não-intrusão", ou seja, o direito a não ser perturbado ou o direito a ser deixado só – "the right to be let alone", destinado a proteger as pessoas "da curiosidade popular" (Castro, 2005, p. 17).

Em 1948, no art. 12.º da Declaração Universal dos Direitos Humanos[36] (doravante DUDH) podia ler-se "[n]inguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a protecção da lei.". Foram, assim, pela primeira vez consagrados como direitos fundamentais, os direitos à privacidade e à reserva da intimidade da vida privada[37] (Alves, 2020, p. 13).

A Convenção Europeia dos Direitos do Homem, aprovada em 1950 pelo Conselho da Europa, veio a prever, no seu art. 8.º, que "1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros".

A primeira Lei de proteção de dados pessoais no mundo surgiu em 1970, no Estado de *Hesse*, na Alemanha, tendo sido este o primeiro país a introduzir uma legislação de proteção de dados pessoais (Alves, 2020, p. 14).

Fala-se, no entanto, de que terá sido a Constituição da República Portuguesa de 1976 a Lei Fundamental pioneira no que toca ao reconhecimento de alguma proteção constitucional aos titulares de dados pessoais (Lopes, 2016, p. 15). Previa (e continua a

[36] Aprovada pela Assembleia Geral das Nações Unidas, a 10 de dezembro de 1948.
[37] Considera Castro (2005, pp. 22-23) que o direito à reserva da intimidade da vida privada é um direito especial de privacidade e não um direito geral de privacidade.

prever de forma semelhante), no seu art. 35.º, n.º 1, que "[t]odos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam".

Mais tarde, em 1981, o Conselho da Europa adotou, a 28 de janeiro, a Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais[38], que tinha como objetivo principal "garantir, no território de cada Parte, a todas as pessoas singulares, seja qual for a sua nacionalidade ou residência, o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal que lhes digam respeito («protecção dos dados»)." (art. 1.º da Convenção 108) (Alves, 2020, p. 14). Nesta Convenção foram consagrados alguns princípios fundamentais e garantias que, mais tarde, vieram integrar a Diretiva 95/46/CE (Castro, 2005, p. 40).

Decorridos 15 anos, Portugal apresentou a primeira Lei dedicada à proteção de dados pessoais - a Lei n.º 10/91, de 29 de abril (Lei da Proteção de Dados Pessoais face à Informática), tendo-se seguido a Lei n.º 28/94 de 29 de agosto (que aprovou medidas de reforço da proteção de dados pessoais)[39].

Em 1995, foi aprovada a já mencionada Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais. Esta "visou harmonizar em todos os Estados-Membros o nível de proteção dos direitos e liberdades das pessoas no que diz respeito ao tratamento de dados pessoais, e teve por objetivo garantir um elevado nível de proteção na União e uma harmonização das referidas legislações nacionais – e não se limitava a uma harmonização mínima, mas antes conduzia a uma harmonização que era, em princípio, completa" (Alves, 2020, pp. 14-15). Esta Diretiva foi transposta para o ordenamento jurídico português pela Lei n.º 67/98, de 26 de outubro.

[38] Convenção esta que pode ser consultada em português em https://gddc.ministeriopublico.pt/sites/default/files/documentos/instrumentos/convencao_protecao_pessoas_tratamento_automatizado_dados_caracter_pessoal.pdf, último acesso em 25-09-2021.

[39] *in* https://www.cnpd.pt/cnpd/o-que-somos-e-quem-somos/historico-da-cnpd/, último acesso em 25-09-2021.

Com o Direito da União Europeia, foram surgindo inúmeros diplomas legais e outros textos (como recomendações) relativos à matéria de proteção de dados pessoais[40], tendo em 2009, com a entrada em vigor do Tratado de Lisboa, sido introduzida uma base legal para a proteção de dados pessoais na União Europeia, nomeadamente o art. 16.º do Tratado sobre o Funcionamento da União Europeia (doravante abreviadamente designado por TFUE), podendo nele ler-se que "1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. O Parlamento Europeu e o Conselho, deliberando de acordo com o processo legislativo ordinário, estabelecem as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controlo de autoridades independentes". Assim, a proteção de dados pessoais tornou-se um direito fundamental nos termos da legislação da União Europeia, consagrado no TFUE e, mais tarde, na Carta dos Direitos Fundamentais da União Europeia (doravante abreviadamente designada por CDFUE), dispondo assim, a partir desse momento, a UE de uma base jurídica para adotar legislação destinada à proteção deste direito[41].

Finalmente, surge o Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho (RGPD), a mais completa base jurídica europeia a tutelar os dados pessoais dos cidadãos, que inclui e reforça requisitos da Diretiva, mas também introduz novas obrigações para os responsáveis pelo tratamento de dados (Parecer 2/2017, p. 10). Este Regulamento revogou a Diretiva 95/46/CE, tendo como objetivo principal garantir uma efetiva aplicação uniforme das normas na matéria de proteção de dados.

Como já se referiu, foi com o RGPD que os dados biométricos passaram a ser tratados como categoria de dados especiais. A primeira utilização de sistemas biométricos para uso comercial remonta ao início dos anos 70, em que *Shearson Hamil*, uma empresa de *Wall Street*, instalou um sistema de identificação automática baseado em impressões digitais, e que utilizava para controlo de acesso às instalações (INCIBE, 2016, p. 4).

Ainda que, nos termos do art. 288.º do TFUE os regulamentos não careçam de transposição e, assim sendo, o RGPD seja diretamente aplicável a todos os Estados-

[40] Para maiores referências e esclarecimentos sobre estes Diplomas/documentos, aconselhamos a leitura de Castro (2005, pp. 62 e 63).
[41] *In* https://www.consilium.europa.eu/pt/policies/data-protection-reform/.

Membros, é-lhes dada a liberdade para definir um conteúdo complementar para inúmeras cláusulas que não estão totalmente concretizadas ou que podem deixar margem para dúvidas. Assim, cada Estado-Membro, para uma melhor proteção no que toca à matéria de proteção de dados pessoais, deve, se assim o entender, complementar o RGPD com uma lei interna.

Ora, o RGPD foi aprovado em 2016 e passou a ser aplicável em todos os Estados-Membros a 25 de maio de 2018 (art. 99.º, n.º 2 do RGPD), tendo, pois, os Estados-Membros uma *vacatio legis* de cerca de dois anos para se adaptarem às novas condições.

Decorrido mais de um ano da data da sua aplicação, foi publicada a lei que assegura a execução na ordem jurídica portuguesa — a Lei n.º 58/2019, de 8 de agosto.

3. Necessidade de regulação dos dados pessoais no ordenamento jurídico português

As primeiras necessidades de regulação da matéria de proteção de dados pessoais, fizeram-se sentir perante o impacto significativo na vida das pessoas singulares, resultado dos progressos tecnológicos (Calvão, 2018, p. 29). Esta crescente inovação tecnológica e, consequentemente, a utilização das novas tecnologias nos locais de trabalho, não poderiam passar à margem do Direito do Trabalho. Considerando a exposição dos dados dos trabalhadores nesta nova realidade é, hoje em dia, recorrente a expressão "nudez tecnológica" do trabalhador, pois existe uma autonomização de dados sobre o trabalhador que podem incidir sobre aspetos que fazem parte da sua privacidade[42], tornando-se necessário protegê-los e tutelá-los juridicamente (Moreira, 2020, p. 43).

A verdade é que, a par do que considera Calvão (2018, p. 26), visão com a qual concordamos, não existe, quer a nível nacional quer a nível internacional, doutrina suficiente para auxiliar a compreensão do Direito da Proteção de Dados. E é precisamente pela inexistência de suficiente abordagem sobre esta temática, que podemos dizer que a grande motivação para a consagração legal da proteção de dados no quadro jurídico nacional, se centra na necessidade de tutela dos trabalhadores nesta matéria, uma vez que a proteção das pessoas singulares relativamente aos dados pessoais é um direito fundamental, e é tendo em conta a recente e crescente evolução tecnológica, que criou novos desafios em matéria de proteção de dados pessoais, que se exige uma proteção sólida e unânime na União Europeia.

Nos dias de hoje, e tendo em conta as relações cada vez mais digitais, também no âmbito laboral, a utilização de tecnologias eletrónicas e digitais, deve respeitar os princípios da proteção de dados pessoais.

No entanto, na opinião de Rodríguez-Piñero Royo (2020, p. 275), os princípios do Direito do Trabalho e os princípios dos dados pessoais nem sempre coincidem, sendo por vezes necessário aplicar-se uns em detrimento de outros. Não obstante, na era em que nos encontramos, cada vez mais se torna imperioso aplicar os princípios da proteção de dados à relação laboral "tradicional". O ideal seria atingir um equilíbrio entre as normas do

[42] Pois o trabalhador, antes de ser trabalhador, é uma pessoa singular, não se podendo dissociar de si próprio só porque está a prestar trabalho a uma entidade.

Direito do Trabalho (na sua vertente digital, focando-nos sobretudo nos sistemas informáticos de recolha de dados sensíveis, a saber, dados biométricos, sendo nesta sede que a contradição se torna especialmente evidente) e o Direito da Proteção de Dados.

Também na senda de Calvão (2018, p. 32), o estudo da proteção de dados pessoais, deveria ser feito "no âmbito de uma disciplina jurídica especializada, voltada exclusivamente para a compreensão dos tratamentos de dados e para a problematização e subsequente elaboração de respostas aos desafios colocados".

A verdade é que, verifica-se que a informação pessoal do trabalhador, cada vez mais diversificada e em maior quantidade, é acessível ao empregador, face a estas "novas" tecnologias, tornando-se difícil estabelecer uma "fronteira" entre a vida privada e a vida profissional (Castro, 2018, p. 274).

Consideramos ainda que a regulamentação existente no CT se revela manifestamente insuficientemente face à realidade atual, criando constantemente a necessidade de se recorrer ao RGPD, ficando ainda assim matérias por tratar (deparando-nos efetivamente com lacunas legislativas). Aliás, a legislação sobre esta temática encontra-se dispersa[43], tornando difícil para o trabalhador e para a entidade empregadora o efetivo conhecimento da regulamentação destas matérias.

[43] Vamos perceber, ao longo do nosso trabalho, que vamos ter de alternar entre vários diplomas, como o CT, o RGPD, a Lei de Execução do RGPD, tendo ainda de consultar diversos pareceres, devido às temáticas não estavam suficientemente claras e desenvolvidas na legislação existente.

CAPÍTULO II – Os dados biométricos na relação laboral

1. Licitude do tratamento dos dados pessoais em geral

Defende Cordeiro (2020, p. 165) que o ponto de partida para qualquer análise da licitude do tratamento de dados pessoais deve ser o já referido art. 8.º, n.º 2 da CDFUE. Nos termos deste artigo, o tratamento de dados pessoais só pode ocorrer com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Assim, para que o tratamento dos dados pessoais por parte do responsável pelo tratamento seja considerado lícito, é necessário que assente num dos seguintes fundamentos de licitude previstos no art. 6.º, n.º 1 do RGPD, a saber: (i) consentimento válido do titular para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas [al. a)]; (ii) necessidade do tratamento 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 [al. b)]; (iii) necessidade do tratamento para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito [al. c)]; (iv) necessidade do tratamento para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular [al. d)]; (v) necessidade do tratamento para o exercício de funções de interesse público ou para o exercício da autoridade pública de que está investido o responsável pelo tratamento [al. e)]; (vi) necessidade do tratamento para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança [al. f)].

Estes fundamentos devem ser analisados e interpretados com rigor, tornando-se verdadeiramente importante a real compreensão dos mesmos, pois uma vez mal interpretados/aplicados, poderão ser considerados ilícitos (Magina, 2020, p. 51), e, em consequência, à aplicação das sanções previstas no art. 58.º, n.º 2 do RGPD.

Neste artigo são enumerados taxativamente os fundamentos para o tratamento lícito de dados pessoais, tratando-se, nas palavras de Cordeiro (2019, p. 3) de um preceito densificador do princípio da licitude *stricto sensu*, previsto no art. 5.º, n.º 1, al. a) do RGPD. Dizemos "taxativamente" pois o conteúdo contido nos restantes números do art. 6.º não dá abertura no sentido de permitir que os Estados-Membros adotem outros fundamentos de licitude para o tratamento de dados.

Percebemos ainda que os requisitos plasmados nas diferentes alíneas do artigo em análise são distintos entre si. Não obstante, é possível dividir os fundamentos em dois grupos: por um lado, temos os casos em que a licitude fica dependente de uma manifestação de vontade do titular dos dados [al. a)] e, por outro, os casos em que a licitude do tratamento pressupõe que o mesmo seja necessário num determinado contexto, sendo que este segundo se mostra independente de qualquer manifestação de vontade do titular [als. b) a f)] (Magina, 2020, p. 58).

1.1. Princípios do tratamento de dados pessoais no RGPD

A verdade é que apesar da já falada intromissão na vida privada, não se pode negar que, no âmbito laboral, existe uma necessidade de recolha de diversas informações dos trabalhadores para a correta execução do contrato de trabalho, considerando-se este tratamento uma "consequência quase natural" destas relações (Moreira, 2020, p. 51). Não obstante, e para que tudo seja mais seguro e que o tratamento não seja feito sem limites e de forma discricionária, esta recolha deve sempre ter em conta diversos princípios orientadores, que estão previstos no art. 5.º do RGPD, e são eles: o princípio da licitude, lealdade e transparência, o princípio da limitação da finalidade, o princípio da minimização dos dados, o princípio da exatidão, o princípio da limitação da conservação, os princípios da integridade e confidencialidade e o princípio da responsabilidade.

Nas palavras de Santos (2019, p. 29), estes princípios relativos ao tratamento de dados pessoais são considerados uma "chave de leitura do RGPD", sendo que os mesmos se encontram concretizados noutras disposições do Regulamento, sobretudo nas obrigações que recaem sobre os responsáveis pelo tratamento e nos direitos dos titulares dos dados. Assim, antes de mais, torna-se imprescindível compreender estes princípios para a correta interpretação do regime da proteção de dados pessoais.

Começando pelo princípio da licitude, lealdade e transparência, este dita que os dados pessoais devem ser objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados (art. 5.º, n.º 1, al. a) do RGPD). A respeito do referido princípio, quanto à licitude, esclarece Magina (2020, p. 53) que, em sentido estrito, o princípio da licitude faz depender o tratamento de dados pessoais da verificação de um dos fundamentos

previstos nos arts. 6.º, 9.º e 10.º[44] do RGPD e, em sentido amplo, pressupõe que o tratamento de dados seja conforme à legislação em vigor (RGPD e demais legislação aplicável)[45]. Em segundo lugar, o tratamento deve efetuar-se de maneira leal, com respeito por uma relação de equilíbrio entre as partes, devendo o titular dos dados ser informado sobre os riscos, com o objetivo de assegurar que o tratamento não tem efeitos imprevisíveis e negativos (Pinheiro et al., 2018, p. 206). Já a transparência exige que as informações e comunicações que têm que ver com o tratamento dos dados sejam facilmente acessíveis e compreensíveis, devendo ser prestado esclarecimento ao respetivo titular, na fase da inscrição, sobre os fins a que os dados se destinam (considerando 39 do RGPD) (Pinheiro et al., 2018, pp. 206, 323).

O princípio da limitação da finalidade vem previsto no art. 5.º, n.º 1, al. b) do RGPD, e significa que os dados pessoais devem ser recolhidos para um fim determinado, explícito e legítimo, e apenas podem ser utilizados para esse fim. Não podem, por isso, ser utilizados posteriormente de forma incompatível com aquela finalidade[46/47]. Este princípio pretende estabelecer limites para o tratamento de dados pessoais e impor a necessidade de fundamentação legítima para o mesmo (Pinheiro et al., 2018, p. 208). Na opinião de Moreira (2020, p. 54), o princípio da limitação da finalidade constitui-se como um princípio cardinal da proteção de dados, na medida em que se apresenta como um pilar em relação aos demais. Já Pinheiro (2018, p. 313) considera que este princípio desempenha um elemento fiscalizador da legitimidade do tratamento.

O princípio da minimização dos dados (muitas vezes denominado por princípio da proporcionalidade), significa que os dados devem ser adequados, pertinentes e limitados ao que é estritamente necessário relativamente às finalidades para as quais são tratados (art. 5.º, n.º 1, al. c) do RGPD). Por outras palavras, é necessário que se procure

[44] Sendo certo que este art. 10.º é uma norma especial, que se refere às condições de licitude do tratamento de dados pessoais relacionados com contraordenações penais e infrações, cujo âmbito material de aplicação se encontra limitado às operações de tratamento da mencionada tipologia de dados pessoais (Magina, 2020, p. 53) – e que não nos importa aprofundar.

[45] Este princípio da licitude, para além de assegurar um tratamento lícito dos dados pessoais no âmbito do RGPD, assegura também o cumprimento das exigências previstas no art. 52.º da CDFUE (Pinheiro, et al., 2018, p. 206).

[46] Não são considerados incompatíveis, e por isso, excetuam-se, os casos em que o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o art. 89.º, n.º 1 do RGPD.

[47] Apesar disso, admite-se o tratamento de dados para finalidade distinta daquela para a qual os dados foram recolhidos, mas não incompatível com aquela (considerando 50 do RGPD). Neste caso, importa refletir, não encontrando resposta doutrinária em sentido contrário, se podem ser utilizados fundamentos jurídicos distintos que não sejam "necessários" (Pinheiro et al., 2018, p. 209).

estabelecer um equilíbrio entre as obrigações do trabalhador (decorrentes do seu contrato de trabalho) e a sua privacidade (como direito constitucionalmente protegido) e que a "violação" deste direito seja realizada na medida do estritamente necessário, sendo este princípio fundamental, considerado por Moreira (2020, p. 58) um "mecanismo de equilíbrio" entre direitos. Ainda segundo este princípio, deve também ser assegurado que o prazo de conservação dos dados tratados seja o mínimo possível, de forma a estarem na "posse" do responsável pelo tratamento pelo período estritamente necessário (Pinheiro et al., 2018, p. 209), estando assim este interligado com o princípio da limitação da conservação.

Já o princípio da exatidão prevê que os dados sejam exatos e atualizados sempre que necessário, devendo ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora (art. 5.º, n.º 1 al d) do RGPD)[48].

Segundo o princípio da limitação da conservação, 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"[49] (art. 5.º, n.º 1 al e) do RGPD).

Quanto ao princípio da integridade e confidencialidade, este dita que os dados pessoais devem ser "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" (art. 5.º, n.º 1, al. f) do RGPD).

Finalmente, segundo o princípio da responsabilidade, incumbe ao responsável pelo tratamento o cumprimento dos princípios referidos e a prova desse mesmo cumprimento[50]

[48] Este princípio relaciona-se com o direito à retificação dos dados e com o direito ao seu apagamento, previstos nos arts. 16.º e 17.º do RGPD, respetivamente.

[49] Também neste caso "os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.º, n.º 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados" (art. 5.º, n.º 1, al. e), *in fine*, do RGPD).

[50] Na senda de Magalhães & Pereira (2018, p. 35), a entidade empregadora deve: comprovar o referido cumprimento por evidência, e, por conseguinte, que o tratamento dos dados é realizado em conformidade com o RGPD, devendo, para o efeito, demonstrar que os dados são legítimos e limitados ao estritamente necessário, estão atualizados, em segurança e que só lhes acede quem necessita efetivamente de os tratar (garantindo assim a sua confidencialidade); ser detentora de políticas, procedimentos, códigos de conduta e regulamentos internos disponíveis para acesso aos trabalhadores e, bem assim, às entidades competentes no caso de uma fiscalização; por último, possuir sistemas que permitam garantir que as políticas e os procedimentos estão a ser adotados (Magalhães & Pereira, 2018, p. 35).

(art. 5.º, n.º 2 do RGPD). Este Regulamento acarreta um "novo" princípio da responsabilidade, na medida em que se passa de uma filosofia de avaliação preventiva por parte das autoridades de proteção de dados[51] para uma atividade fiscalizadora *aposteriori*, devendo as entidades empregadoras assegurar *apriori* a o cumprimento das normas e leis estabelecidas.

O respeito pelos princípios suprarreferidos traz uma segurança associada, uma vez que, mesmo tendo sido prestado consentimento por parte do titular dos dados ou assentando o tratamento noutro dos fundamentos de licitude previstos no n.º 1 do art. 6.º do RGPD, se o referido tratamento não os respeitar, será sempre ilícito (Moreira, 2020, p. 52).

Em suma, e como vamos ter oportunidade de perceber melhor, o tratamento de dados pessoais dos trabalhadores apenas será permitido se estiver legitimado por um de três fundamentos. No entanto, seja qual for o fundamento jurídico para esse tratamento, o empregador está sempre obrigado a garantir que nenhum dos princípios é violado e, bem assim, a comprová-lo.

1.2. Direitos dos titulares dos dados previstos no RGPD

No considerando 11 do RGPD pode ler-se que "[a] proteção eficaz dos dados pessoais na União exige o reforço e a especificação dos direitos dos titulares dos dados (…)".

Assim, o RGPD veio conferir aos titulares dos dados pessoais objeto de tratamento mais direitos e reforçar os já existentes, que devem ser salvaguardados pelo responsável pelo seu tratamento (Magalhães & Pereira, 2018, p. 24).

Podemos, assim, dizer que os direitos dos titulares dos dados previstos atualmente são: o direito de acesso, o direito de retificação, o direito de apagamento, o direito à limitação do tratamento, o direito de portabilidade dos dados, o direito de oposição a decisões individuais automatizadas.

[51] Antes da entrada em vigor do RGPD, na vigência da Diretiva, o responsável pelo tratamento tinha o dever de fazer a notificação do tratamento dos dados pessoais à CNPD, devendo, no requerimento de notificação, ser indicadas as condições do tratamento e outras condições que permitissem à entidade apreciar o pedido em termos de necessidade e de proporcionalidade. No que toca ao tratamento de dados sensíveis, para além da necessidade de notificar a CNPD, era também necessária uma autorização. Neste sentido, a entidade empregadora devia não só notificar a CNPD, como aguardar pela autorização da mesma antes de dar início ao tratamento. Aconselhamos a leitura de um documento da CNPD, sobre os "Princípios sobre a utilização de dados biométricos no âmbito do controlo de acessos e de assiduidade" de 2004.

Encontra-se previsto no art. 15.º do RGPD o direito de acesso[52] do titular de dados, que prevê que o "titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto e tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais" e também a outras informações[53] que se relacionam com esse tratamento. Este direito consagra-se como um direito basilar relativamente aos restantes, porquanto é aquele que permite que sejam posteriormente exercidos outros direitos (tais como o direito da retificação ou o direito de apagamento, por exemplo) (Gonçalves, 2018, p. 359). No entanto, no caso objeto do nosso estudo, parece ser difícil o acesso pleno a este direito, uma vez que as características biométricas, como já se disse, estarão, à partida (e preferencialmente), representadas por um *template*, que não pode ser descodificado, podendo, neste caso, a informação apenas ser prestada na medida de se saber se ou que a característica se encontra, de facto, armazenada na base de dados, podendo essa comprovação ser feita através da autenticação (parece-nos que esta comprovação se consubstancia apenas numa tentativa de autenticação[54]) (Guerra, 2004, p. 209).

É também assegurado aos titulares dos dados pessoais o direito de obterem a retificação dos mesmos quando estes estejam desatualizados, incorretos ou incompletos (arts. 16.º do RGPD e 35.º da CRP).

O direito de apagamento consiste no direito de o titular dos dados, dentro das limitações impostas por lei, solicitar ao responsável pelo tratamento o apagamento dos seus dados, devendo este fazê-lo com a maior brevidade possível (art. 17.º do RGPD). O titular pode exercer este poder apenas nas circunstâncias elencadas nas alíneas do n.º 1 do art. 17 do

[52] Princípio este também previsto no art. 35.º da CRP.

[53] As diversas als. do art. 15.º, n.º 1 enumeram as restantes informações que devem ser prestadas: "a) As finalidades do tratamento dos dados; b) As categorias dos dados pessoais em questão; c) Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais; d) Se for possível, o prazo previsto de conservação dos dados pessoais, ou, se não for possível, os critérios usados para fixar esse prazo; e) A existência do direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação do tratamento dos dados pessoais no que diz respeito ao titular dos dados, ou do direito de se opor a esse tratamento; f) O direito de apresentar reclamação a uma autoridade de controlo; g) Se os dados não tiverem sido recolhidos junto do titular, as informações disponíveis sobre a origem desses dados; h) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.º, n.ºs 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados".

[54] Neste sentido, veja-se o considerando 26 da CNPD, onde se pode ler que "[o] titular tem o direito de saber se a sua característica biométrica se encontra armazenada e obter a respectiva comprovação, nomeadamente através do desencadeamento da operação de reconhecimento ou de autenticação" (CNPD, 2004).

RGPD, não se podendo, pelo contrário, aplicar este direito nas situações previstas no seu n.º 3.

O titular dos dados tem ainda o direito a exigir a limitação do tratamento dos seus dados pessoais nas situações previstas no art. 18.º, n.º 1 do RGPD. Este direito "consiste na inserção de uma marca nos dados pessoais conservados, visando a posterior limitação do seu tratamento e na obrigação que impende sobre o responsável de responder ao pedido do titular, sem demora injustificada, no prazo de um mês, de acordo com o n.º 3 do art. 12.º e expor as suas razões quando indeferir o pedido do exercício deste direito" (Gonçalves, 2018, p. 371).

Nos termos do art. 20.º do RGPD, o titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, podendo transmiti-los a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir quando se verifique, cumulativamente, o seguinte: o tratamento for baseado no consentimento dado nos termos do art. 6.º, n.º 1, al. a), ou do art. 9.º, n.º 2, al. a), ou ainda num contrato referido no artigo 6.º, n.º 1, al. b) e o tratamento seja realizado por meios automatizados. No exercício deste direito, o titular dos dados pessoais tem o direito a que os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento, sempre que tal seja tecnicamente possível ou, em alternativa, que lhe sejam entregues (art. 20, n.º 2 do RGPD).

A lei confere ao titular dos dados o direito de oposição (art. 21.º do RGPD) a decisões individuais automatizadas, de forma a não ficar sujeito a uma decisão que afete ou produza efeitos significativos na sua esfera jurídica, tomada com base no tratamento automatizado dos seus dados (art. 22.º, n.º 1 do RGPD).

2. Fundamentos de licitude do tratamento de dados pessoais na relação laboral

O empregador deve assegurar que são respeitados os direitos dos titulares dos dados sobre o tratamento efetuado no contexto laboral (Duarte, 2018, p. 179). Assim, o tratamento de dados pessoais dos trabalhadores apenas poderá ser feito com respeito pelos princípios

fundamentais já previstos no CT (arts. 14.º a 22.º), princípios estes que foram agora clarificados e reforçados pelo RGPD (Moreira, 2020, p. 54).

No âmbito da licitude do tratamento de dados pessoais em sede de um contrato de trabalho importa, em particular, o estudo dos fundamentos previstos nas als. a), b) e f) do art. 6.º, n.º 1 do RGPD[55], como veremos de seguida.

2.1. O consentimento do trabalhador

Neste primeiro fundamento de licitude do tratamento de dados pessoais, previsto no art. 6.º, n.º 1, al. a) do RGPD[56], cabe aos titulares dos dados decidir se autorizam que os seus dados sejam tratados, centrando-se este fundamento de legitimidade na autodeterminação da pessoa em causa (Magina, 2020, p. 58).

O RGPD veio trazer uma alteração importante para as relações laborais – veio retirar "o acento tónico" do consentimento como fundamento jurídico válido para o tratamento de dados pessoais quando, conforme dita o seu considerando 43 "exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento", como acontece, no caso sob estudo, entre o trabalhador e a entidade empregadora (Moreira, 2020, pp. 48-49). Tem, assim, vindo a ser bastante debatida a questão do consentimento do trabalhador como fundamento de licitude para o tratamento de dados pessoais, sendo que, na esteira de Moreira (2020, p. 49), para que o tratamento de dados pessoais seja válido, terá de assentar noutros princípios que não o mero consentimento do trabalhador.

Ainda antes da entrada em vigor do RGPD, o GT29, no seu Parecer 15/2011[57] sobre a definição de consentimento, havia entendido que "[o] consentimento apenas será válido se a pessoa em causa puder exercer uma verdadeira escolha e não existir nenhum risco de fraude, intimidação, coacção ou consequências negativas importantes se o consentimento for recusado" e que "(…) a proibição de tratamento de categorias especiais de dados pessoais não pode ser ultrapassada pelo consentimento da pessoa em causa".

---

[55] Há autores, como Moreira (2020, p. 54), que entendem que o único fundamento que pode legitimar o tratamento de dados pessoais numa relação laboral é a prossecução de interesses legítimos da entidade empregadora atendendo a cada caso concreto, quando o tratamento for necessário para a execução do contrato, nos termos do art. 6.º, n.º 1, al. b) do RGPD.

[56] Não iremos abordar o regime específico da obtenção do consentimento dos titulares de dados que sejam menores (considerando 38 e art. 38.º do RGPD), porquanto não se mostra relevante para o estudo em causa.

[57] Que pode ser consultado em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf.

Segundo o art. 4.º, 11) do RGPD, entende-se por consentimento do titular dos dados "uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento".

Moreira (2020, p. 50) defende que a noção de consentimento é um conceito de difícil concretização e de difícil preenchimento no contexto de uma relação de trabalho. Neste sentido, tem-se considerado que a definição de consentimento merece uma apreciação particular de cada um dos seus elementos (elementos estes que devem ser todos verificados para que o consentimento seja considerado lícito), a saber: manifestação de vontade (o que significa que "não existe a figura do consentimento obrigatório"); livre; específica; informada e explícita[58].

Pode ainda ler-se no considerando 32 do RGPD que "[o] silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento. O consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins."

Ora, em termos gerais, como se disse, o consentimento é uma das condições para o tratamento de dados pessoais ser legítimo, sendo mencionado e desenvolvido por diversos artigos do RGPD[59].

No entanto, como já se aludiu, várias têm sido as manifestações da doutrina[60/61] no sentido de se considerar que, no âmbito da relação laboral, em regra, seja obrigatório as entidades empregadoras prestarem informação completa aos trabalhadores sobre o tratamento dos seus dados pessoais e sobre a forma como este é feito, não sendo exigido o consentimento daqueles[62]. A verdade é que, por norma, o consentimento no contexto laboral não é

[58] Para maiores desenvolvimentos sobre estes elementos, veja-se o que entendem Cordeiro (2020, pp. 72 e ss.), Pinheiro et al. (2018, pp. 166 e ss.) e o GT29 no Parecer 15/2011.
[59] Vejam-se, a propósito do consentimento, os considerandos 32, 33, 42 e 43 e arts. 4.º, n.º 11, 6.º, n.º 1, al. a), 7.º, 8.º e 9.º, n.º 2 al. a) e ainda o art. 49.º, n.º 1, al. a) do RGPD. Também a Lei de Execução faz, diversas vezes, referência ao consentimento, nomeadamente nos seus arts. 16.º, 28.º, n.º 3 (artigo que foi desaplicado pela CNPD), 31.º, n.º 4, 37.º, 48.º, 51.º e 61.º.
[60] Também pela leitura e interpretação aprofundada dos artigos do RGPD, se depreende que o consentimento não é fundamento válido para o tratamento de dados pessoais no âmbito da relação laboral.
[61] Veja-se, neste sentido, por exemplo, Rodríguez-Piñero Royo (2020, p. 283) e González Biedma (2017, p. 223).
[62] Utilizando o exemplo de Henriques & Luís (2019, pp. 23 e 33), a entidade empregadora terá de prestar informação ao trabalhador sobre a forma como a informação recolhida será tratada, a razão da necessidade do tratamento e, bem assim, os direitos que assistem ao trabalhador para proteção da sua privacidade.

considerado fundamento válido para o tratamento de dados pessoais, uma vez que o trabalhador está numa posição de dependência e subordinação perante o empregador. E, ainda que se admita que a eficácia e o bom funcionamento do sistema estão dependentes, em grande medida, da cooperação por parte do trabalhador, afasta-se o consentimento como condição de legitimidade, devido à posição em que o trabalhador se encontra.

Pode dizer-se que as informações sobre o tratamento de dados são, de certa forma, constitutivas do consentimento como fundamento de tratamento de dados pessoais (quando possa ser considerado fundamento válido). Na realidade, o trabalhador deve obter a maior quantidade de informação possível, por forma a ser capaz de avaliar os riscos, benefícios e prejuízos relacionados com aquele tratamento de dados, bem como a própria necessidade do mesmo, nomeadamente no que concerne à qualidade de dados recolhidos e à extensão do tratamento (Pinheiro et al., 2018, p. 323).

Ora vejamos: como já se disse, o consentimento deve ser uma manifestação de vontade e deve ser livre. Como bem sabemos, o trabalhador, por se encontrar numa posição débil face à da entidade empregadora, teme-se que a sua manifestação de vontade não seja verdadeiramente livre. Imagine-se que o trabalhador não queria prestar o seu consentimento para o tratamento dos seus dados pessoais. Na prática, isto poderia acarretar-lhe consequências negativas, podendo, no limite, a entidade empregadora pôr fim à relação laboral (Alves, 2020, pp. 59-60). Assim, o consentimento prestado pelo trabalhador no âmbito da relação laboral não se pode considerar efetivamente como sendo uma manifestação de vontade dada de forma livre, como o RGPD pretende que seja e, por conseguinte, regra geral, não deverá ser considerado como um fundamento de licitude para o tratamento dos seus dados pessoais.

Aliás, Moreira (2020, p. 49) afirma mesmo que o elemento "livre" referente à manifestação de vontade é um elemento que está em falta nas relações laborais, que são um exemplo paradigmático de relações privadas e desiguais, não só no plano factual (porque os contraentes não dispõem da mesma liberdade no que toca à celebração do contrato de trabalho e à estipulação das suas cláusulas) como no plano jurídico (uma vez

Portanto, no caso da instalação de sistemas de leitura biométrica, importa que o trabalhador seja informado, por exemplo, sobre as finalidades desse tratamento, que informação é guardada e durante quanto tempo, os direitos dos trabalhadores perante a circunstância de tratamento dos seus dados.

que "a conclusão do contrato de trabalho coloca o trabalhador numa situação de subordinação face ao empregador").

Acresce que, conforme dita o considerando 43 do RGPD, o consentimento não deve constituir 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". Este considerando, apesar de se referir ao tratamento de dados por uma autoridade pública, poderia ele também estar redigido, no mesmo sentido, no âmbito da relação de trabalho, atendendo a que existe também um claro desequilíbrio entre o trabalhador e o empregador (parece-nos que, atendendo à relevância desta matéria, poderia o legislador europeu ter referido também como exemplo a relação laboral, não deixando assim dúvidas nem margem para interpretações dúbias).

Entende Simitis (2014 *apud* Cordeiro, 2020, pp. 168-169) que o consentimento é uma ficção, pois o reconhecimento deste direito "traduz uma falsa ideia de controlo na esfera jurídica do titular" e que "a imposição do consentimento não restringe o uso dos dados pessoais, pelo contrário: representa antes uma chave para um acesso virtualmente ilimitado a um sem fim de informações". A verdade é que muitas pessoas (incluindo, naturalmente, os trabalhadores), consentem no tratamento dos seus dados pessoais com um grande desconhecimento do real alcance que isso lhes produzirá.

No quadro jurídico nacional, pode ler-se no n.º 3 do art. 28.º da Lei n.º 58/2019, de 8 de agosto[63] que, salvo norma legal em contrário, o consentimento do trabalhador não constitui requisito de licitude do tratamento dos seus dados pessoais: se do tratamento resultar uma vantagem[64] jurídica ou económica para o trabalhador ou se esse tratamento estiver abrangido pelo disposto na alínea b) do n.º 1 do art. 6.º do RGPD, ou seja, se o tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte (no caso, o contrato de trabalho).

[63] Adiante designada apenas Lei de Execução.
[64] Levanta-se também a questão de saber o que é considerado uma vantagem, uma vez que o legislador também não confere uma noção desta nem dá, pelo menos, algum exemplo.

Note-se que, e a par do que considera Moreira (2020, p. 52), segundo o art. 28.º, n.º 3 da Lei de Execução, a base jurídica para o tratamento de dados pessoais no contexto laboral seria, essencialmente, o consentimento, não sendo o mesmo necessário se o trabalhador tiver alguma vantagem jurídica ou económica (quando do RGPD decorre precisamente o contrário, ou seja, que o consentimento não deve ser condição e que é nos casos em que existe uma vantagem jurídica ou económica que devemos/podemos aceitar que o consentimento seja juridicamente relevante) e ainda, a al. b) parece estar a excluir outras condições para o tratamento – o que não nos parece fazer sentido.

Aliás, a opinião da suprarreferida autora tomou por base também o entendimento da CNPD que, na sua Deliberação/2019/494[65] (p. 5v), aprovada a 3 de setembro de 2019, entendeu que, ainda que se admita a "natureza não paritária da relação laboral", a verdade é que decorre do princípio da dignidade da pessoa humana a necessidade de se reconhecer ao indivíduo o mínimo de livre arbítrio para gozar do seu direito fundamental à autodeterminação informacional[66] - direito este reconhecido pelo art. 35.º da CRP e 8.º da CDFUE.

Neste sentido, a CNPD veio desaplicar algumas normas da Lei de Execução através da referida Deliberação. Entendeu a Comissão que o disposto na al. a) do n.º 3 do art. 28.º restringe excessivamente a relevância do consentimento do trabalhador, eliminando qualquer margem do denominado livre-arbítrio dos trabalhadores, mesmo quando não há razão para tal – considerando, por isso, ser 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". Conclui ainda que a referida disposição não cumpre os requisitos da al. b) do n.º 2 do art. 9.º e do n.º 2 do art. 88.º do RGPD, uma vez que "não corresponde a uma medida legislativa nacional adequada que salvaguarde a dignidade, os direitos fundamentais e os interesses legítimos do trabalhador" e que, por esta razão, e de forma a assegurar a plena efetividade do RGPD, a CNPD decide desaplicar a referida norma (Deliberação/2019/494 de 3 de setembro de 2019).

[65] Deliberação esta que pode ser consultada em https://www.cnpd.pt/decisoes/historico-de-decisoes/.
[66] Este traduz-se, nas palavras de Castro (2005, pp. 25, 44) "num conjunto de direitos relacionados com o tratamento automático das informações pessoais dos cidadãos, que visam, simultaneamente protegê-las perante ameaças de recolha e de divulgação, assim como de outras utilizações possibilitadas pelas novas tecnologias, e, também, assegurar aos respetivos titulares um conjunto de poderes de escolha nesse âmbito" e que "nasce, assim, para garantir um direito à intimidade privada no que ao tratamento de dados pessoais diz respeito".

Nesta linha de raciocínio, também o GT29 entendeu, embora na esmagadora maioria das vezes, não dando relevância jurídica ao consentimento prestado pelos trabalhadores para o tratamento dos seus dados pessoais, que em circunstâncias excecionais, o consentimento pode consubstanciar um fundamento lícito para o tratamento de dados, mas apenas quando seja possível à entidade empregadora demonstrar que o consentimento foi dado livremente e que o mesmo não produzirá quaisquer consequências negativas para o trabalhador (Orientações relativas ao consentimento na aceção do Regulamento (EU) 2016/690, p. 8). Temos, no entanto, sérias dúvidas de que esta "prova" por parte da entidade empregadora seja possível ou credível.

Cabe ainda fazer referência ao considerando 155 (semelhante ao art. 88.º, n.º 1 do RGPD), segundo o qual "[o] direito do Estado-Membro ou as convenções coletivas (incluindo «acordos setoriais») podem prever regras específicas para o tratamento de dados pessoais dos trabalhadores no contexto laboral, nomeadamente no que respeita às condições em que os dados pessoais podem ser tratados no contexto laboral, com base no consentimento do assalariado, para efeitos de recrutamento, execução do contrato de trabalho, incluindo o cumprimento das obrigações previstas por lei ou por convenções coletivas, de gestão, planeamento e organização do trabalho, de igualdade e diversidade no trabalho, de saúde e segurança no trabalho, e para efeitos de exercício e gozo, individual ou coletivo, dos direitos e benefícios relacionados com o emprego, bem como para efeitos de cessação da relação de trabalho"[67/68].

[67] No que toca à matéria e ao tratamento de dados biométricos, após a entrada em vigor do RGPD, verifica-se que várias convenções coletivas de trabalho passaram a fazer menção à utilização de dados biométricos. Veja-se, a este respeito, a título de exemplo, o acordo coletivo celebrado entre Águas do Norte, SA e outras e o SINDEL - Sindicato Nacional da Indústria e da Energia e outro que refere, na Cláusula 11.ª que "[a] empresa só pode proceder ao tratamento de dados biométricos se os dados a utilizar forem necessários, adequados e proporcionais aos objetivos a atingir e observando a regulamentação em cada momento em vigor no âmbito da proteção de dados pessoais e demais regulamentação aplicável", publicado no Boletim do Trabalho e Emprego, n.º 41, de 08-11-2018, disponível em http://bte.gep.msess.gov.pt/. No entanto, e salvo melhor opinião, parece-nos que estas menções, apenas reforçam o que já consta no art. 18.º, n.º 2 do CT, não acrescentando novas regras quanto ao tratamento de dados biométricos dos trabalhadores no contexto laboral.

[68] Também em alguns estatutos das comissões de trabalhadores, tem-se verificado a menção da obrigatoriedade de o tratamento de dados biométricos (entre outros atos de decisão das empresas) ser precedido de parecer escrito da comissão de trabalhadores. Veja-se, a este respeito, a título de exemplo, o art. 20.º dos estatutos da MGC - Acabamentos Têxteis, SA – Constituição, aprovados em 14-12-2020, publicados no Boletim do Trabalho e Emprego, n.º 3, de 22-01-2021, disponível em http://bte.gep.msess.gov.pt/.

Aquelas normas, devem, segundo o n.º 2 do art. 88.º do RGPD, incluir medidas adequadas e específicas[69] para salvaguardar a dignidade, os interesses legítimos e os direitos fundamentais do titular dos dados, com especial relevo para a transparência do tratamento de dados, a transferência de dados pessoais num grupo empresarial ou num grupo de empresas envolvidas numa atividade económica conjunta e os sistemas de controlo no local de trabalho. Alves (2019, p. 61) esclarece que, hoje em dia, os trabalhadores estão sujeitos a uma supervisão constante no local de trabalho, através de sistemas como os de videovigilância, de geolocalização, biométricos para o controlo de assiduidade, entre muitos outros.

Assim, para autores como Alves (2019, pp. 57-58), o consentimento apenas se considerará um fundamento lícito apropriado se ao titular dos dados for dada a oportunidade de controlo dos mesmos, e desde que exista a opção de aceitar ou recusar que os seus dados sejam tratados nos termos que lhe são apresentados – sempre com a opção de poder recusar o seu tratamento, sem ser prejudicado por essa decisão[70]. Consideramos, ainda assim, tal como já referimos supra, que no âmbito da relação laboral será difícil que exista para o trabalhador a opção de recusa do consentimento ou até que exista garantia/prova de que não acarretará pela decisão de recusa, prejuízos na sua relação laboral[71/72].

Atentar ainda no facto de que, a liberdade do consentimento, tanto no contexto laboral como noutros, está também dependente do facto de o consentimento dever ser dado separadamente para cada finalidade do tratamento (Magina, 2020, pp. 78-79). Ou seja,

---

[69] Tal como referimos, parece-nos que em Portugal, e no que toca ao tratamento de dados biométricos, esta liberdade que é concedida aos Estados-Membros não foi bem aproveitada, uma vez que não se estabeleceram medidas específicas e adicionais nos IRCT's, relativamente ao que já consta da lei.

[70] Aliás, pode ler-se num acórdão da Sala Social do Tribunal Superior de Justiça da Comunidade Valenciana que "no âmbito laboral, o consentimento do trabalhador passa, como regra geral, para segundo plano, pois o consentimento se entende implícito na relação negocial, sempre que o tratamento de dados pessoais seja necessário para a manutenção e cumprimento do contrato celebrado entre as partes" (*tradução nossa*). https://www.boe.es/diario_boe/txt.php?id=BOE-A-2016-3405

[71] Vejamos um exemplo em que seria lícita a aplicação do fundamento do consentimento, dado pelo GT29 nas "Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679". Estando a decorrer filmagens numa empresa, e pretendendo a equipa de filmagem filmar determinada parte de um escritório, cabe aos trabalhadores escolher aparecer em segundo plano nessa gravação ou até não aparecer, prestando, em caso afirmativo, o seu consentimento. Os trabalhadores que optarem por não ser filmados não deverão ser penalizados, uma vez que poderão estar noutra zona da empresa enquanto durar a filmagem. Neste caso, parece-nos que o GT29 considera o consentimento como fundamento lícito para o tratamento de dados pessoais por se tratar de uma gravação às instalações.

[72] Para Henriques & Luís (2019, p. 21), esta questão parece ser indiscutível, pois estes afirmam que "a existência de consentimento por parte do trabalhador não poderá constituir fundamento de legitimidade para o tratamento dos dados pessoais deste", não abrindo, para o efeito, qualquer exceção.

não será possível que seja dado um mesmo consentimento para um conjunto de finalidades.

No que toca ao tratamento de dados biométricos, diz-nos Duarte (Pinheiro et al., 2018, p. 244) que o consentimento constitui um requisito residual, nos casos em que não seja aplicável qualquer das demais exceções à proibição prevista no n.º 1 do art. 9.º do RGPD, assumindo-se este fundamento como a manifestação "mais perfeita" (relativamente às demais alternativas do mencionado artigo) do direito à autodeterminação informacional – trataremos desta questão com mais desenvolvimento adiante.

Neste sentido, podemos concluir que o consentimento, enquanto requisito de licitude do tratamento, não é aplicável a todos os tratamentos de dados. Deve verificar-se se o consentimento é condição de licitude adequada para o tratamento de dados em causa, ou se haverá outro fundamento que se deva aplicar.

Assim, o consentimento é um fundamento jurídico válido para o tratamento de dados pessoais, inclusive dos dados sensíveis. Contudo, não constitui fundamento de legitimidade quando se trata de dados sensíveis no âmbito laboral – por um lado, devido ao desequilíbrio existente entre as partes (que não garante que o consentimento seja prestado de forma efetivamente livre) e, por outro lado, porque o tratamento de dados relativos aos trabalhadores está, na esmagadora maioria das vezes, previsto e regulado por lei e/ou é necessários para a execução do contrato de trabalho[73].

2.2. O tratamento dos dados pessoais para a execução de um contrato de trabalho e para o cumprimento de obrigações jurídicas a que a entidade empregadora está adstrita

No âmbito da relação laboral, várias são as situações em que é necessário tratar dados pessoais dos trabalhadores. Não obstante, não se poderá aqui considerar uma qualquer situação, uma vez que "deve existir um vínculo direto, objetivo e substancial entre o contrato e o tratamento realizado" (Magalhães & Pereira, 2018, p. 32). Pense-se, a título de exemplo, nos dados recolhidos para efeitos da celebração do contrato de trabalho, dados financeiros (para efeitos de pagamento da remuneração), morada, dados de identificação, entre outros. Este fundamento de legitimidade é o mais imediato para o

[73] Veja-se, neste sentido, https://www.cnpd.pt/organizacoes/areas-tematicas/consentimento/.

desenvolvimento de operações de tratamento de dados pessoais dos trabalhadores, sendo também indissociável da gestão corrente de recursos humanos no seio empresarial (Henriques & Luís, 2019, p. 28).

No entanto, existem situações de manifesta dificuldade, no que diz respeito à aplicabilidade dos fundamentos do tratamento de dados pessoais, em situações laborais. Por exemplo, quando falamos da recolha de certos dados destinados à celebração do contrato de trabalho, é de fácil compreensão que tal recolha é legítima. No entanto, quando se fala do fundamento que é aplicável a esse tratamento, podem surgir dúvidas quanto à aplicabilidade, uma vez que parece haver uma linha ténue entre o fundamento da necessidade para execução do contrato de trabalho, e o interesse legítimo da entidade empregadora (Magina, 2020, p. 82).

O art. 6.º, n.º 1, al. b) permite também o tratamento de dados que seja necessário[74] para a realização de diligências pré-contratuais a pedido do titular de dados. Este, no âmbito laboral, assume especial relevância na fase de recrutamento ou possível recrutamento (referente aos dados contidos nos documentos que suportam as candidaturas ou os currículos)[75].

Nos termos do art. 28.º, n.º 3, al. b) da Lei de Execução, o consentimento do trabalhador não constitui requisito de legitimidade do tratamento dos seus dados pessoais se esse tratamento estiver abrangido pelo disposto no art. 6.º, n.º 1, al. b) do RGPD, ou seja, pelo fundamento que estamos a analisar. Magina (2020, p. 84) considera, pois, que "o único sentido útil desta norma – pese embora com técnica legislativa discutível —, é esclarecer que os dois fundamentos são distintos, e contrariar uma tendência infelizmente generalizada, de errada interpretação e aplicação dos preceitos do RGPD, que se traduz em indicar, nos contratos de trabalho, que o tratamento de dados pessoais do trabalhador se baseia no consentimento deste, quando tal tratamento se fundamenta, na maior parte dos casos, apenas e tão só no facto de o mesmo ser necessário para a execução do próprio contrato".

[74] Para Kühling/Buchner (2018 *apud* Cordeiro, 2019, p. 9) o tratamento será necessário nos termos da al. b) sempre que exista uma relação direta entre o próprio tratamento e o cumprimento das obrigações contratuais assumidas pelo responsável.

[75] Este tipo de tratamento de dados pessoais levanta questões como o período de conservação admissível. Para mais desenvolvimentos sobre o prazo de conservação, veja-se o que entende Magina (2020, pp. 83-84).

Acresce que, de forma intimamente relacionada com o fundamento da execução do contrato de trabalho, deriva para a entidade empregadora o cumprimento de determinadas obrigações jurídicas, nomeadamente quando, por exemplo, tem de fornecer à segurança social dados relativos aos salários dos seus trabalhadores. Assim, no contexto laboral, estes dois fundamentos estão, em certa medida, interligados.

Este segundo fundamento[76] exige o preenchimento de dois requisitos: a verificação do princípio da necessidade[77] e a existência de uma obrigação jurídica que impenda sobre o responsável pelo tratamento (Magina, 2020, p. 85).

Ora, sobre o empregador impende o dever de proceder ao registo dos tempos de trabalho dos seus trabalhadores (art. 202.º do CT), conforme teremos oportunidade de melhor abordar mais adiante. Embora o cumprimento desta obrigação se pudesse considerar necessário no âmbito da execução do contrato de trabalho (assentando, neste caso, o fundamento na al. b) do n.º 1 do art. 6.º do RGPD), parece-nos que a lógica subjacente a esta obrigação será essencialmente a de permitir a fiscalização do cumprimento, pela entidade empregadora, do regime legal de duração e organização do tempo de trabalho e, nessa medida, o fundamento para o tratamento de dados pessoais será o cumprimento de uma obrigação jurídica, ao abrigo da al. c) do n.º 1 do art. 6.º do RGPD (Duarte, 2018, p. 180).

O tratamento de dados baseado nestes fundamentos [art. 6.º, n,º 1, als. b) e c) do RGPD] fazem referência a interesses legítimos e concretos, ao contrário do previsto no fundamento constante da al. f) do art. 6.º, n.º 1 do RGPD.

2.3. A prossecução dos interesses legítimos da entidade empregadora

Ao contrário do que se disse relativamente aos fundamentos acima analisados, nomeadamente o tratamento dos dados pessoais para a execução de um contrato de trabalho e/ou para o cumprimento de obrigações jurídicas a que a entidade empregadora está adstrita, o fundamento mencionado na al. f) do art. 6.º, n.º 1 do RGPD, referente a

[76] Este que, para alguns autores como Henriques & Luís (2019, p. 30) constitui o principal fundamento de licitude para o tratamento de dados pessoais em contexto laboral.
[77] O tratamento para o cumprimento de obrigações jurídicas apenas será necessário na medida em que a Lei assim o determine, sendo o conceito de necessidade preenchido à luz do conteúdo da própria obrigação legal (Kühling/Buchner, 2018 *apud* Cordeiro, 2019, p. 9).

qualquer tipo de interesse legítimo prosseguido pelo responsável pelo tratamento ou terceiro, não tem em causa um interesse concreto. Assim, deve ser demonstrado o equilíbrio através da realização do teste de ponderação.

Bem sabemos que a relação laboral é uma relação desequilibrada e, neste sentido, existe um risco elevado de se verificar uma ou mais violações dos direitos de personalidade dos trabalhadores.

Na CRP estão previstos certos direitos fundamentais que são especificamente laborais, como é o caso do direito à greve (art. 57.º) e do direito ao trabalho (art. 58.º), e outros direitos que, embora não sendo especificamente laborais, podem ser exercidos pela parte mais débil da relação laboral, adquirindo dimensão laboral (Amadeu et al., 2019, p. 108).

No entanto, tornou-se essencial que também o CT viesse regular especificamente os direitos de personalidade do trabalhador[78/79], por forma a encontrar novas formas de conferir garantias reforçadas aos trabalhadores "perante as novas formas de trabalho", o que fez nos seus arts. 14.º e seguintes. Em particular, e para o que mais releva para os efeitos do presente trabalho, o CT veio, no seu art. 16.º prever o direito à reserva da vida privada, estabelecendo que se "devem respeitar os direitos de personalidade da contraparte, cabendo-lhes, designadamente, guardar reserva quanto à intimidade da vida privada" o que abrange "quer o acesso, quer a divulgação de aspectos atinentes à esfera íntima e pessoal das partes, nomeadamente relacionados com a vida familiar, afectiva e sexual, com o estado de saúde e com as convicções políticas e religiosas".

O suprarreferido direito vem previsto constitucionalmente como um direito fundamental (art. 26.º, n.º 1 da CRP) e, no CC, como um direito de personalidade (art. 80.º do CC), sendo, não raras vezes, de entre os vários direitos de personalidade, o mais suscetível de violação e, por isso, aquele sobre o qual incide maior tutela legal, nomeadamente em matéria de proteção de dados pessoais[80] (Ramalho, 2014, p. 7).

[78] Apesar desta regulamentação, não pode deixar de se considerar a regulamentação constitucional, devendo continuar a ser seguidos os artigos constantes da mesma, até porque o CT apenas enuncia alguns direitos de personalidade (Amadeu et al., 2019, p. 112). Assim, no que toca aos direitos de personalidade, deve ser feita uma conjugação de toda a legislação vigente porquanto, estando em causa a tutela geral da personalidade, impõe-se a conjugação entre os vários ramos do Direito (Martinez, 2019, p. 377).

[79] Ainda que o tenha feito de uma forma igualitária para o empregador e para o trabalhador em alguns artigos, nomeadamente, arts. 14.º, 15.º e 16.º do CT.

[80] Aliás, considerando-se o mais vulnerável dos direitos do trabalhador, é o mais desenvolvido no CT, em várias projeções específicas nos artigos que se seguem (art. 17.º a 22.º), constituindo estes direitos projeções do direito à reserva da vida privada do trabalhador (Ramalho, 2014, p. 7).

O princípio que releva neste domínio é, nas palavras de Ramalho (2014, p. 7), o da "irrelevância das matérias da esfera privada das partes (*verbi gratia*, a esfera privada do trabalhador) para o contrato de trabalho", princípio este que acompanha toda a vida do contrato de trabalho, isto é, a sua formação, execução e até mesmo para efeitos de cessação.

Ora, a al. f) do art. 6.º, n.º 1 admite que o tratamento de dados pessoais seja lícito quando seja necessário para a prossecução dos interesses legítimos do responsável pelo tratamento ou de terceiros, salvo se, em concreto, prevalecerem os interesses ou os direitos e liberdades fundamentais do respetivo titular dos dados. Como nos diz Cordeiro (2019, pp. 3-4) este é um fundamento distinto dos demais, uma vez que não tem por base o direito à autodeterminação informacional, nem outros direitos fundamentais, nem uma disposição legal expressa, mas sim, os interesses do responsável pelo tratamento ou de terceiros.

Parece-nos, pela interpretação deste artigo, que devemos começar por notar que, para a lícita invocação deste fundamento se exige, cumulativamente, o seguinte: que exista um interesse do responsável pelo tratamento ou de terceiro, o qual deverá ser passível de ser considerado legítimo; que o tratamento de dados seja necessário para a prossecução desse interesse[81]; e que esse interesse não prevaleça sobre os interesses ou direitos e liberdades fundamentais do respetivo titular. Na opinião de Cordeiro (2019, p. 11), o requisito da necessidade não é autonomizável, sendo "consumido" pelo núcleo do art. 6.º, n.º 1, al. f) do Regulamento, sendo certo que o tratamento nunca poderá ser descrito como necessário se os interesses do interessado puderem ser prosseguidos através de uma alternativa menos intrusiva da esfera jurídica do titular dos dados.

Assim, no âmbito da relação laboral, é necessário que a entidade empregadora proceda a uma ponderação dos seus interesses legítimos, em relação aos interesses ou direitos e liberdades fundamentais do trabalhador. Para isso, o interesse legítimo deve ser bem identificado, deve perceber-se em que medida esse interesse é presente e relevante e qual é o eventual prejuízo que pode ter para o trabalhador. Por fim, deve fazer um exercício de proporcionalidade, semelhante àquele que se faz a propósito da colisão de direitos (Cordeiro, 2019, p. 5). De notar ainda que não é suficiente a invocação de um interesse

[81] Esta segunda condição constitui um corolário do princípio da proporcionalidade, exigindo-se que exista uma ligação entre o tratamento que se pretende fazer e os interesses legítimos prosseguidos e ainda que não exista outro meio menos invasivo para alcançar a mesma finalidade (Magina, 2020, p. 61).

legítimo por parte da entidade empregadora; é necessário que a própria finalidade do tratamento seja ela também legítima e que o tratamento seja 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" (Henriques & Luís, 2019, p. 31).

Para compreender o requisito da existência de um interesse legítimo do responsável pelo tratamento ou de terceiro, importa identificar quem é o sujeito do interesse, apurar o conceito de interesse e clarificar em que casos é que o interesse poderá ser considerado legítimo.

Ora, o sujeito do interesse será o responsável pelo tratamento (quando não seja autoridade pública no exercício das suas atribuições) ou um terceiro. O terceiro é definido nos termos do art. 10.º, n.º 4 do RGPD como "a pessoa singular ou coletiva, a autoridade pública, o serviço ou organismo que não seja o titular dos dados, o responsável pelo tratamento, o subcontratante e as pessoas que, sob a autoridade direta do responsável pelo tratamento ou do subcontratante, estão autorizadas a tratar dados pessoais"[82]. Atentar no facto de que este conceito é aplicável no contexto da al. f) do n.º 1 do art. 6.° com a exceção de que o fundamento de licitude do interesse legítimo não poderá ser invocado por autoridades públicas na prossecução das suas atribuições (conforme art. 6.º, n.º 1, al. f), segundo parágrafo do RGPD). Terceiros, neste contexto, podem, pois, ser quaisquer entidades incluídas na definição supra, desde que titulares de um interesse legítimo no tratamento.

Quanto ao conceito de interesse, nem o legislador europeu, nem o CEPD tomam posição quanto ao preenchimento do mesmo, limitando-se a apresentar alguns exemplos. No entanto, a doutrina tem vindo a debruçar-se sobre este conceito. Assim, nas palavras de Magina (2020, pp. 63-64), o interesse pode ser definido como "o objetivo que se visa alcançar com o tratamento ou o benefício que dele se pretende retirar", devendo esse objetivo ou benefício ser real e atual[83] e ainda devendo ser formulado da forma mais precisa e exata possível[84]. Já para Cordeiro (2019, p. 12), o interesse pode ser definido

[82] Para mais desenvolvimentos sobre o conceito de "terceiro" aconselhamos a leitura do Parecer 1/2010 do GT29, pp. 33 e seguintes.
[83] Isto significa que o objetivo ou benefício a atingir não pode ser meramente especulativo e demasiado vago – deve ser espectável num futuro próximo e basear-se em aspetos concretos (Magina, 2020, p. 64).
[84] Para Magina (2020, p. 63), o conceito de interesse é próximo do conceito de finalidade do tratamento, presente no RGPD, apesentando-nos o seguinte exemplo para melhor compreensão: o tratamento de dados através da implementação de um sistema de controlo da identificação e atuação dos utilizadores de

"como uma vantagem, legal ou fática, obtida pelo responsável pelo tratamento ou por um terceiro, decorrente, direta ou indiretamente, do tratamento de dados pessoais".

Por fim, é também fundamental reforçarmos que o interesse do responsável ou do terceiro, para efeitos do art. 6.º, n.º 1, al. f) tem de ser legítimo, o que quer dizer que tem de estar em conformidade quer com a legislação em matéria de proteção de dados, como com a demais legislação em vigor.

Analisados os conceitos, exige-se, no artigo em análise (art. 6.º, n.º 1, al. f) do RGPD), que o interesse legítimo do responsável pelo tratamento ou do terceiro não seja ultrapassado pelos interesses ou direitos e liberdades fundamentais dos titulares dos dados. Para isso, deve ser feita uma apreciação, devendo realizar-se um teste de ponderação, colocando-se os valores em confronto e apreciar o seu peso relativo.

Ainda na vigência da Diretiva 95/46/CE, os Estados-Membros desenvolveram alguns critérios úteis a ter em conta na realização do teste da ponderação e, dadas as parecenças entre os regimes, também no que toca a esta temática, alguns autores têm continuado a considerar esta análise. Ora, os critérios de apreciação são quatro, a saber: (i) avaliação do interesse legítimo do responsável pelo tratamento[85/86], (ii) impacto nas pessoas em causa[87], (iii) equilíbrio provisório[88] e (iv) garantias complementares aplicadas pelo

determinado *software*, em que teríamos como finalidade do tratamento o conhecimento, pelo responsável pelo tratamento, da identidade e atuação das pessoas que acedem e utilizam um determinado *software*, e em que teríamos como interesse, a prevenção e controlo da fraude. Neste sentido, em termos comparativos, poderíamos definir a finalidade do tratamento como sendo o objetivo concreto, específico e imediato desse, sendo o interesse definido como objetivo geral, abstrato e mediato do mesmo (Magina, 2020, p. 63).

[85] Impõe-se, relativamente a este elemento, que aquele tratamento seja necessário para a prossecução do interesse legítimo e que pertença ao responsável pelo tratamento ou terceiro, sendo que este requisito deve assegurar que não existe um meio menos invasivo que permita prosseguir a mesma finalidade.

[86] A título de exemplo, o considerando 47 do RGPD, diz-nos que poderá haver um interesse legítimo, quando exista uma relação relevante e apropriada entre o titular dos dados e o responsável pelo tratamento, em situações como aquela em que o titular dos dados é cliente ou está ao serviço do responsável pelo tratamento.

[87] Deve também ser apreciado o impacto que o tratamento terá nas pessoas em causa e aqui, importa atender duas noções: a avaliação da probabilidade de verificação do risco e a avaliação da gravidade das suas consequências – devendo estas avaliações corresponder a um exercício discricionário e ter em consideração todas as circunstâncias que envolvem o tratamento. Por regra, quanto mais alto ou incerto for o impacto, mais improvável é que o tratamento seja considerado lícito, em termos gerais (Magina, 2020, pp. 69-70).

[88] O objetivo, relativamente a este ponto, será o de contrapor os resultados obtidos nos dois pontos que antecedem e avaliar se os interesses, direitos e liberdades fundamentais do titular dos dados (trabalhador) não ultrapassam os do responsável pelo tratamento (empregador), sendo que, não ultrapassando, poderá ser efetuado o tratamento (Magina, 2020, p. 71).

responsável pelo tratamento para evitar qualquer impacto indevido nas pessoas em causa[89].

É por isto que tal como sempre acontece no caso de colisão de direitos, também aqui o interesse legítimo da entidade empregadora, como veremos, deve ser sopesado perante outros elementos relevantes (nos quais são de incluir os direitos fundamentais dos trabalhadores), num juízo de proporcionalidade (Henriques & Luís, 2019, p. 16).

Neste sentido, podemos aqui concluir que os interesses legítimos da entidade empregadora podem constituir um fundamento de licitude para o tratamento de dados pessoais (incluindo dados biométricos), desde que esses interesses não prevaleçam indevidamente sobre os direitos e liberdades fundamentais dos trabalhadores, tomando em conta as expetativas razoáveis destes, baseadas na relação com o responsável pelo respetivo tratamento. Deve, assim, este tratamento ter como base uma compatibilização dos interesses das partes.

3. O tratamento de dados biométricos no contexto laboral

3.1. Os poderes da entidade empregadora

A CRP consagra os direitos de livre iniciativa económica privada e de liberdade da empresa [arts. 61.º, n.º 1 e 80.º, al. c)], sendo eles que constituem o fundamento para os poderes que a entidade empregadora tem no âmbito da relação laboral. É, nomeadamente, o contrato de trabalho que se constitui como fonte dos poderes do empregador, uma vez que os mesmos apenas são relevantes quando o sujeito económico assume essa posição (Lambelho & Gonçalves, 2021, p. 165), podendo ser exercidos enquanto o mesmo vigorar. Assim, as entidades empregadoras têm diversos poderes que se podem dividir em três, a saber: poder de direção, poder regulamentar e poder disciplinar.

[89] No caso de não se verificar o pressuposto do equilíbrio provisório, como referido no ponto anterior, poderá ponderar-se a pertinência da adoção de medidas complementares destinadas a alterar o equilíbrio. Essas medidas poderão, dependendo do caso concreto, consistir, por exemplo, na limitação do volume de dados recolhidos, na eliminação imediata de dados, entre outros. Depois, a entidade empregadora deverá, novamente, proceder à ponderação. O suporte documental do teste de ponderação deverá ser conservado e apresentado, caso seja solicitado por algum interessado (Magina, 2020, p. 73).

O poder regulamentar consiste no poder que o empregador tem de elaborar um regulamento interno de empresa sobre a organização e disciplina do trabalho (art. 99.º, n.º 1 do CT)[90].

Já o poder disciplinar, consiste na faculdade de poder sancionar o trabalhador pela prática de infrações laborais, devendo este reger-se pelo disposto nos arts. 328.º e ss. do CT.

Finalmente, e sendo o que mais nos importa para o presente estudo, o poder de direção atribui à entidade empregadora a faculdade de dirigir a atividade desenvolvida pelo trabalhador e determinar em que termos é que "o trabalho deve ser prestado, dentro dos limites decorrentes do contrato e das normas que o regem" (art. 97.º do CT) (Lambelho & Gonçalves, 2021, p. 166). Este poder de direção tem, naturalmente, limites derivados do seu próprio conteúdo e dos direitos dos trabalhadores, razão pela qual o trabalhador não deve obediência à entidade empregadora quando as ordens ou instruções se mostrem contrárias aos seus direitos e garantias (Martinez, 2019, p. 650).

Neste sentido, os direitos de personalidade do trabalhador têm sempre de ser conjugados com os direitos fundamentais da entidade empregadora e, uma vez que os direitos em confronto são "da mesma espécie" (direitos reconhecidos na Parte I da Constituição), encontramo-nos perante a figura da colisão de direitos, devendo as partes encontrar um equilíbrio para que se produzam os efeitos necessários, mas com o menor prejuízo para qualquer das partes (Martinez, 2019, p. 650).

Para o que nos importa em particular, vamos perceber que a finalidade legítima do tratamento de dados biométricos assenta na necessidade de agilizar o cumprimento de um objetivo que a lei reconhece integrar-se no âmbito dos poderes de controlo da entidade empregadora (Guerra, 2004, p. 209).

3.1.1. Da determinação de horário de trabalho, controlo de assiduidade e controlo de acesso a instalações

Nos termos do art. 200.º, n.º 1 do CT, o horário de trabalho corresponde à determinação das horas de início e termo do período normal de trabalho diário e dos intervalos de

[90] Para mais desenvolvimentos sobre o poder regulamentar, aconselhamos a leitura de Lambelho (2020, pp. 223-251).

descanso. Esta determinação depende de uma decisão da entidade empregadora (art. 212.º, n.º 1 do CT), cabendo no respetivo poder de direção.

Estando delimitado o horário de trabalho o trabalhador deve "[c]omparecer ao serviço com assiduidade e pontualidade" (art. 128.º, n.º 1, al. b) do CT). A falta de assiduidade e de pontualidade deriva da negligência no exercício da atividade, o que consubstancia um cumprimento defeituoso do contrato de trabalho (Martinez, 2019, p. 521).

Assim, uma das atividades da entidade empregadora consiste no controlo da assiduidade do trabalhador, sendo um dos seus principais direitos e decorrendo também do poder de direção que lhe é conferido por lei.

A orientação da CNPD sobre os "Princípios sobre a utilização de dados biométricos no âmbito do controlo de acessos e de assiduidade" confere à entidade empregadora o poder de utilizar os sistemas biométricos para o controlo de assiduidade. No entanto, e salvo melhor opinião, cabe aqui fazer uma interpretação extensiva e considerar que o "controlo de assiduidade" que é permitido, se estende e se aplica também aos registos de tempos de trabalho. Até porque a intensão de que a nova obrigatoriedade de registos de trabalho produza efeitos, sendo muitas vezes utilizados sistemas biométricos para assegurar tal cumprimento, é levada a cabo e tem utilidade se forem registados os tempos de trabalho, e não apenas para controlar a assiduidade dos trabalhadores (se assim fosse, seria apenas uma vantagem para o empregador e não acautelava os trabalhadores que fariam, por exemplo, horas extra — o que nos parece incorreto[91]).

3.1.2. Do registo obrigatório dos tempos de trabalho

O Código do Trabalho, nomeadamente o seu art. 202.º, n.º 1, prevê que "o empregador deve manter o registo dos tempos de trabalho, incluindo dos trabalhadores que estão isentos de horário de trabalho, em local acessível e por forma que permita a sua consulta

[91] Aliás, acreditamos que muitas entidades empregadoras não vêm este método como uma vantagem, pois isso implicaria, muitas vezes, o pagamento de horas extra, questão que, com os métodos tradicionais de controlo, pode ser ultrapassada.

imediata". Esta obrigação surgiu no CT de 2003[92/93/94], e prevê uma obrigação genérica de os empregadores registarem os tempos de trabalho de todos os seus trabalhadores, tendo, mais tarde, o CT de 2009 acrescentado que esses registos devem ser guardados durante 5 anos. No entanto, tem-se entendido que a redação deste artigo levanta diversas questões, uma vez que utiliza dois conceitos indeterminados, e ainda não especifica a forma como esse registo deve ser feito[95].

Conforme decorre do art. 202.º, n.º 2 do CT, o registo deve ser diário e "deve conter a indicação das horas de início e de termo do tempo de trabalho, bem como das interrupções ou intervalos que nele não se compreendam, por forma a permitir apurar o número de horas prestadas por trabalhador".

Esta obrigação, apesar de servir para cumprir obrigações por parte das entidades empregadoras, a verdade é que acaba por proteger inevitavelmente os trabalhadores, na medida em que existe um maior e mais preciso controlo, que pode evitar certos abusos praticados por parte das entidades empregadoras (por exemplo, sobre as horas extraordinárias que possam ser prestadas e não pagas, ou a não existência de dias de descanso). O legislador espanhol acrescenta que a introdução desta obrigatoriedade, deve servir para contribuir para corrigir a situação de precariedade, baixos salários e pobreza que tem vindo a afetar muitos dos trabalhadores que sofrem abusos na relação laboral (Garrote Crespo, 2021, p. 3). Para além disso, a nosso ver, esta obrigatoriedade serve também para garantir a segurança e saúde do trabalhador, na medida em que, comprovadamente, o excesso de horas de trabalho coloca em causa o referido direito[96/97].

---

[92] Entretanto revogado pela Lei n.º 7/2009, de 12 de fevereiro, o atual Código do Trabalho.

[93] Nomeadamente, no seu artigo 162.º, no qual podia ler-se: "[o] empregador deve manter um registo que permita apurar o número de horas de trabalho prestadas pelo trabalhador, por dia e por semana, com indicação da hora de início e de termo do trabalho".

[94] Muitos países da União Europeia têm também esta obrigatoriedade consagrada nos seus ordenamentos jurídicos, como Alemanha, Espanha, Países Baixos, sendo que a par do que acontece no nosso ordenamento, não existem grandes requisitos específicos no que toca a este registo (García Coca, 2020, pp. 332-335). Pelo contrário, França, por exemplo, não tem esta obrigatoriedade legal.

[95] Para maiores desenvolvimentos sobre os conceitos indeterminados a que se faz referência, consultar Sousa (2018, pp. 129-140).

[96] Veja-se, a este respeito, Campos (2021), a propósito de um estudo realizado pela Organização Internacional de Trabalho, e que mostrou que cerca de 745 mil pessoas morreram em 2016 de derrames ou doenças cardíacas causadas por longos horários de trabalho, concluindo que "trabalhar 55 horas ou mais por semana estava associado a um risco 35% maior de acidente vascular cerebral e 17% maior de morrer de doença cardíaca quando comparado a uma semana de trabalho de 35 a 40 horas". Esta notícia pode ser consultada em https://www.jn.pt/mundo/longas-horas-de-trabalho-matam-745-mil-pessoas-por-ano-13730609.html.

[97] Já no decorrer do período pandémico, foi publicado um artigo no *Eurofound*, que relaciona o aumento do teletrabalho, com o aumento de horas de trabalho semanais. No âmbito de um estudo citado por este

No entanto, para além de uma obrigação, parece-nos, que também se mostra como uma vantagem e proteção para as entidades empregadoras, que conseguem controlar, com mais rigor, os horários efetivos dos trabalhadores, mostrando-se útil para prevenir alguns abusos praticados por parte daqueles (Fernandes, 2018, p. 121).

Por fim, esta obrigatoriedade facilita do controlo por entidades fiscalizadoras como a ACT e a Segurança Social.

No entanto, autores como Sousa (2018, p. 140) têm vindo a considerar que não se tem dado grande relevância a esta norma, nem tão pouco a doutrina se tem debruçado sobre esta questão, levantando assim ainda diversas dúvidas.

O referido art. 202.º, n.º 2 do CT, parecendo ser tão abrangente, coloca a questão de saber se se deverão considerar quaisquer interrupções (como pausas para lanche de dez minutos) ou apenas pausas consideráveis (como por exemplo o tempo de refeição). Parece-nos que serão de considerar apenas as pausas consideráveis, isto é, as de tempo igual ou superior a meia hora.

Acresce que o suprarreferido artigo indica apenas que este registo deve ser feito, não especificando a forma de o fazer[98]. Desta forma, cada entidade empregadora emprega o modo de registo que melhor lhe convier (seja economicamente, seja para que lhes seja mais "flexível", recorrendo a meios tecnológicos ou "manuais").

Ora, quando se fala desta obrigação, é imprescindível não se falar de dados pessoais. Isto porque, o registo de tempos de trabalho é um dado pessoal, uma vez que se trata de uma informação relativa a uma pessoa identificada (o trabalhador). Aliás, no contexto laboral, todas as informações do trabalhador que são arquivadas, acedidas e analisadas pelo empregador - tais como o *currículo vitae*, as notas de entrevista, elementos relativos ao tempo de trabalho (quer seja em sistemas de controlo de assiduidade ou de acesso a

artigo, verificou-se que dos trabalhadores que trabalhavam, semanalmente, entre 41 a 60 horas em casa, 20% se sentiam isolados e 39% se sentiam emocionalmente esgotados pelo trabalho sempre ou na maior parte do tempo (Predotova, 2021). Este artigo pode ser consultado em https://www.eurofound.europa.eu/pt/publications/article/2021/workers-want-to-telework-but-long-working-hours-isolation-and-inadequate-equipment-must-be-tackled.

[98] Para Aragüez Valenzuela (2019, pp. 7-8), poderia adotar-se como forma de registo de tempos de trabalho qualquer sistema tecnológico que se demonstre um sistema "transparente, aberto e verdadeiro" e desde que proporcione informação viável, imodificável e insuscetível de manipulação posterior, quer seja pelo empresário ou pelo próprio trabalhador. Acrescenta ainda o referido autor que, sendo o registo feito com recurso à tecnologia, o empregador deve salvaguardar que tanto os trabalhadores como as entidades competentes possam ter acesso a esses dados, através de transferência para um formato legível e tratável (Aragüez Valenzuela, 2019, p. 7).

instalações, como registos especificamente preparados), entre outros – são, como já vimos, dados pessoais do trabalhador e as operações sobre eles, operações de "tratamento" (Duarte, 2019, p. 179).

É certo que existem muitas questões que vieram a ser colocadas com a consagração legal desta nova obrigação. Mas quanto ao que nos interessa para a temática em estudo, e uma vez que não está regulada na lei a forma de fazer o registo, qualquer sistema pode ser válido, desde a assinatura num papel, como através de cartões magnéticos, fazendo *log in* numa plataforma interna da empresa, ou, finalmente, através dos sistemas biométricos aqui falados (Fernández Orrico, 2020, p. 315). No entanto, parece-nos que os métodos tradicionais, para além de desatualizados, tornam-se propícios a conduzir a práticas fraudulentas, porquanto outros trabalhadores podem simular a entrada e/ou saída de trabalhadores que ainda não se encontram na empresa, pelo que não se cumpre o critério de fiabilidade e veracidade que se deseja que este registo cumpra (García Coca, 2020, p. 337).

A verdade é que muitas entidades empregadoras têm vindo a recorrer aos sistemas de controlo biométrico para proceder ao registo dos tempos de trabalho[99], e fazem-no, sobretudo, através da recolha de impressões digitais ou de reconhecimento facial ou da íris. E, ainda que os controlos através de sistemas biométricos não sejam uma novidade no âmbito laboral, a verdade é que a sua análise do ponto de vista da proteção de dados é uma realidade recente (Rodríguez-Piñero Royo, 2020, p. 277). Pode, aliás, esta prática ser muito invasiva para a esfera privada dos trabalhadores. Verifica-se, assim, uma possível desproteção da pessoa do trabalhador com o acesso aos dados biométricos para registo dos tempos de trabalho, por ser um sistema que acede a dados pessoais íntimos e particularmente sensíveis (Aragüez Valenzuela, 2019, p. 9).

O sistema de registo deve, por isso, ser adaptado às circunstâncias e necessidades de cada empresa, devendo idealmente ser decidido pelos seus representantes em negociações coletivas ou pelas entidades empregadoras, sempre bem fundamentado (Fernández Orrico, 2020, p. 316).

[99] Nas palavras de Aragüez Valenzuela (2019, p. 7), o modo de registo de tempos de trabalho deve garantir que os dados recolhidos sejam objetivos, que garantam a veracidade e, sobretudo, a não alteração dos dados recolhidos, e ainda que estes registos sejam documentados, devendo ser mantidos pela entidade empregadora durante 5 anos.

Assim, o regime dos registos de tempos de trabalho deve ser analisado tendo também em conta o RGPD, cuja aplicabilidade direta no ordenamento jurídico português permite o prevalecimento das suas normas em detrimento de normas internas que com ele não coincidam (Marques, 2020, p. 38). Aliás, determina o art. 17.º, n.º 4, do CT que "os ficheiros e acessos informáticos utilizados pelo empregador para tratamento de dados pessoais do candidato a emprego ou trabalhador ficam sujeitos à legislação em vigor relativa à protecção de dados pessoais", isto é, ao RGPD e à Lei de Execução.

Uma vez que o RGPD clarifica estes dados como especialmente sensíveis, para que se possa realizar o seu tratamento é necessário manter um rigoroso juízo de proporcionalidade, não sendo válido qualquer acesso injustificado (Aragüez Valenzuela, 2019, p. 10).

Assim, esta "nova" obrigação de registo de tempos de trabalho, também parece ser uma base de legitimação à utilização dos sistemas biométricos, na medida em que permite que esta obrigação seja efetivada através de um método fiável.

3.2. Da utilização lícita dos dados biométricos do trabalhador

O art. 28.º, n.º 6 da Lei de Execução veio legitimar o tratamento de dados biométricos dos trabalhadores exclusivamente para fins de controlo de acesso às instalações da entidade empregadora ou para fins de controlo de assiduidade dos trabalhadores[100].

Tal como afirma Magina (2020, p. 91), opinião com a qual concordamos, esta norma, apesar de ter terminado com o vazio legal existente até então, a mesma não está isenta de críticas, especialmente no que diz respeito às limitações do seu âmbito de aplicação e às dúvidas que se podem colocar a esse respeito. E é isso que procuraremos abordar/concretizar neste ponto.

Uma vez que, antes da entrada em vigor do RGPD, os dados biométricos não eram considerados dados sensíveis (pelo menos de forma expressa/clara), o seu tratamento não estava, à partida, proibido. Assim, bastava o responsável pelo tratamento submeter um pedido fundamentado à CNPD, e uma vez aprovado, poderia implementar o sistema de registo de dados biométricos no local de trabalho. Neste sentido, antes da entrada em

[100] Esta norma encontra suporte nos arts. 9.º, n.º 4 e 88.º do RGPD.

vigor do RGPD, o tratamento de dados biométricos era feito segundo o princípio de heterorregulação, competindo à CNPD, enquanto autoridade de controlo, registar ou autorizar o tratamento desses dados (Monjardino, 2018, p. 6).

Atualmente, com a consagração dos dados biométricos como dados pessoais sensíveis[101], este tratamento passou a ser, por regra, proibido. A razão desta proibição, que consta no art. 9.º, n.º 1 do RGPD, não está justificada na lei, mas deve ser entendida como uma salvaguarda de direitos fundamentais dos trabalhadores face ao tratamento dos seus dados pessoais, por serem dados que permitem a confirmação da identidade de um indivíduo de forma inequívoca, estando essas características intrinsecamente ligadas a uma determinada pessoa, e podendo ser-lhes dados diversos usos inapropriados[102] (Pinheiro et al., 2018, p. 237). No caso dos dados biométricos, o direito fundamental a proteger parece ser a reserva da intimidade da vida privada.

A entrada em vigor do RGPD mudou, assim, o anterior paradigma de regulação, sendo que vigora agora um sistema de autorregulação, não dependendo o tratamento destes dados de qualquer autorização prévia, sendo o responsável pelo tratamento encarregue por assegurar um tratamento correto, leal e lícito dos dados pessoais (Monjardino, 2018, p. 7).

Esta consagração implicou também uma grande mudança na medida em que, hoje em dia, não é possível tratar categorias especiais de dados com o fundamento do interesse legítimo do responsável pelo tratamento. Parece resultar da lei, havendo também entendimento da doutrina, no sentido de considerar que o único fundamento para o tratamento legítimo de dados biométricos é, de momento, quando "o tratamento for necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, de segurança social e de proteção social, na medida em que esse tratamento seja permitido pelo direito da União ou dos Estados-Membros ou ainda por uma convenção coletiva nos termos do direito dos Estados-Membros que preveja

[101] A par de outros dados que passam também a ser considerados sensíveis, a saber: os dados pessoais que revelem origem racial ou ética, as opiniões políticas, as convicções religiosas ou filosóficas e a filiação sindical do titular e ainda os dados genéticos, os dados relativos à saúde e os dados relativos à vida sexual ou orientação sexual de uma pessoa (art. 9.º, n.º 1 do RGPD).

[102] Também neste sentido, veja-se Marrero Blanco & Mulero Fernández (2020, p. 5), para quem esta proibição também se deve ao facto de estarmos perante tratamentos cujo mau uso pode gerar tratamentos discriminatórios, como já terá acontecido historicamente, o que requer que o tratamento dos mesmos seja submetido a um controlo de legitimidade mais rigoroso.

garantias adequadas dos direitos fundamentais e dos interesses do titular dos dados" (fundamento este previsto no art. 9.º, n.º 2, al. b) do RGPD).

Antes de entrar na abordagem particular da questão, importa referir algumas questões prévias abordadas pela doutrina.

3.2.1. Generalidades

A 26 de fevereiro de 2004, a CNPD emitiu a já referida orientação denominada "Princípios sobre a utilização de dados biométricos no âmbito do controlo de acessos e de assiduidade". E embora as legislações vigentes à data da referida orientação fossem a Diretiva 95/46/CE e a Lei n.º 67/1998, não tendo a mesma ainda sido revogada pela CNPD, continua a ser tida em consideração, dada a sua relevância, sendo as nossas referências, naturalmente, adaptadas às legislações agora em vigor (RGPD e Lei de Execução).

A questão central da temática em estudo prende-se com a questão de saber em que termos o empregador pode utilizar dados biométricos para controlar a atividade do trabalhador, seja no que respeita ao registo dos tempos de trabalho, ao controlo dos acessos a instalações e/ou a equipamentos, como eventual mecanismo de prevenção de acidentes de trabalho ou de controlo da produtividade do trabalhador.

Tal como vimos no ponto anterior deste trabalho, a utilização dos dados biométricos pode consubstanciar uma vantagem, mas também é extremamente invasiva dos direitos de personalidade do trabalhador e a sua utilização comporta riscos não despiciendos.

Assim, importa começar por referir que os dois artigos de partida para a análise deste regime especial são, por um lado, o art. 6.º do RGPD que, como vimos, se refere à generalidade dos dados pessoais, ditando que o tratamento que tenha por fundamento um dos critérios nele expostos, será lícito e, por outro, o art. 9.º do RGPD que regula o tratamento de categorias especiais de dados, estando, no seu n.º 1 prevista uma proibição genérica de tratamento destas categorias, sendo essa proibição levantada sob certas condições previstas no n.º 2.

De acordo com Pinheiro parece haver interpretação de que os dados biométricos nem sempre serão dados sensíveis[103], sendo que para que se possa avaliar a concreta sensibilidade destes dados, é necessário fazer-se uma avaliação da quantidade e qualidade dos dados recolhidos (essencialmente no que ao seu potencial identificativo diz respeito), da finalidade do seu tratamento, da forma de armazenamento dos dados e das características do sistema biométrico[104] (Pinheiro et al., 2018, p. 321). Não obstante, perante o art. 9.º do RGPD, parece-nos claro que os dados biométricos se inserem na categoria de dados pessoais especiais. Aliás, a consagração dos dados biométricos como dados pessoais especiais foi uma das grandes novidades trazidas pelo RGPD.

No âmbito do presente trabalho, importa, em particular, tratar dos dados biométricos no contexto laboral. Sobre estes dados recai, como vimos, uma proibição geral, que apenas conhece exceções nos casos especificamente previstos no art. 9.º, n.º 2 do RGPD, e ao que nos parece, é o fundamento da al. b) o que maioritariamente é chamado a legitimar o tratamento de dados neste contexto.

Importa, ainda, refletir também sobre uma questão colocada por Magina (2020, p. 55) que é a de saber se, relativamente aos dados sensíveis, se deve articular o preceituado nestes dois artigos (arts. 6.º e 9.º do RGPD), ou se bastará respeitar apenas o disposto no art. 9.º do RGPD, sendo este suficiente para cumprir o princípio da licitude — questão esta que se mostra particularmente interessante. Parece-nos que deve sempre fazer-se uma ponderação casuística que permita apurar se se justifica a cumulação dos dois artigos, sendo certo que a maioria dos fundamentos previstos no art. 9.º se limita a concretizar os previstos no art. 6.º e, quando assim for, pensa-se que o art. 9.º será suficiente. Acima de tudo, importa assegurar que em caso algum a proteção conferida aos dados sensíveis seja inferior à proteção conferida aos restantes (Magina, 2020, pp. 55-56).

Por outro lado, relativamente ao recurso aos sistemas biométricos, têm surgido opiniões em dois sentidos diversos: por um lado, os que estão entusiasmados e confiantes com as potencialidades que estes sistemas apresentam e que não veem nenhum inconveniente na

[103] Cumpre esclarecer que o autor não faz distinção entre dados sensíveis e dados especiais, interpretação essa também por nós acolhida.

[104] O autor esclarece que se impõe que, no âmbito do tratamento dos dados e antes do mesmo, o responsável pelo tratamento faça uma análise casuística e pondere se os dados biométricos são dados sensíveis naquele preciso contexto. Quando se mostre evidente o caráter sensível dos dados, o tratamento dependerá da verificação de uma das alíneas previstas no n.º 2 do art. 9.º do RGPD. Por seu turno, quando os mesmos não sejam considerados sensíveis, os dados biométricos poderão ser tratados ao abrigo dos fundamentos do art. 6.º, n.º 1 do RGPD.

sua utilização[105]; por outro, aqueles a quem esta utilização suscita preocupações pelas várias razões que já fomos elencando ao longo do trabalho (Guerra, 2004, p. 209). Compreendemos as duas posições, no entanto, na nossa modesta opinião, na perspetiva do trabalhador (que é a que mais dúvidas levanta, pois são os dados pessoais deste que estão a ser utilizados), a utilização de sistemas biométricos nas relações de trabalho, apresenta também, em certos casos, vantagens significativas. Até porque vejamos: nos dias de hoje, diariamente, as pessoas enquanto consumidores, celebram contratos em que o produto lhes é fornecido não a troco de uma prestação pecuniária, mas sim a troco de dados pessoais[106/107] (Narciso, 2019, p. 129). Assim, os consumidores não terão acesso a plataformas como, por exemplo, o *Facebook*, a *Netflix*, ou o *WhatsApp* se não consentirem no tratamento dos seus dados pessoais, sendo que, muitas vezes, consentem neste tratamento, sem ter a plena consciência de que os seus dados vão ser tratados e que, muitas vezes, poderão ser utilizados para outros diversos fins. A título de exemplo, um utilizador que instale a aplicação *WhatsApp* e aceite os termos e condições de privacidade sem as ler previamente (como maior parte das vezes acontece), está a aceitar, por exemplo, fornecer ao *Facebook* e suas empresas associadas o seu número de contacto, a sua foto de perfil, para fins ainda não detalhados (Velencoso & López, 2018, p. 16). É certo que alguns destes tratamentos não são lícitos e, por isso, não deveriam verificar-se. No entanto, a realidade é que acontecem e que, de facto, as pessoas enquanto consumidores, muitas vezes, não ponderam sobre as consequências do risco que estão a correr.

Pelo exposto, importa refletir: se corremos o risco de renunciar à nossa privacidade, enquanto consumidores, para ter acesso a uma conta *Facebook*, não será também justificável que os nossos dados pessoais sejam tratados enquanto trabalhadores, para benefício dos mesmos? Sendo certo até que, enquanto trabalhadores, a tutela do tratamento dos dados pessoais será maior – pois, como vimos, são preferencialmente aceites os sistemas biométricos que utilizem uma base de dados interna, que não permite

[105] Veja-se, a este respeito, Fernández Orrico (2020, p. 310).
[106] A este respeito, aconselhamos a leitura de Narciso (2019, pp. 129-147) e Martínez Velencoso & Sancho López (2018), que explicam a problemática dos dados pessoais como contraprestação, pondo-nos a par do facto de que os dados pessoais são muito "valiosos" em termos económicos, havendo inclusive empresas a ganhar exclusivamente dinheiro com os dados pessoais dos utilizadores de diversas redes sociais.
[107] Vários são os exemplos destes contratos, tais como: os contratos entre o utilizador de redes sociais e as plataformas de redes sociais (por exemplo, *Facebook, Instagram*), contratos de *download* de aplicações móveis "gratuitas" (como a aplicação do *Google Maps*) ou contratos de utilização de *websites* (por exemplo, navegação no *Youtube*) (Narciso, 2019, p. 130).

que os dados pessoais sejam acessíveis por outros, e sistemas que não permitam a reversão dos dados. Nestes casos, pensamos então existir um benefício para os trabalhadores que, a título de exemplo, não poderão ver lesados os seus direitos no que diz respeito, por exemplo, ao pagamento de horas suplementares, e ao respeito pelos tempos de descanso, uma vez que os verdadeiros tempos de trabalho serão registados[108].

O já referido art. 28.º, n.º 6 da Lei de Execução determina que "[o] tratamento de dados biométricos dos trabalhadores só é considerado legítimo para controlo de assiduidade e para controlo de acessos às instalações do empregador". Relativamente à questão do controlo da assiduidade, já explicámos supra que consideramos estender-se também aos registos de tempos de trabalho.

A este respeito, Moreira (Amado et al., 2019, p. 155), com a qual concordamos, considera que também poderia ser justificável que o acesso a dispositivos móveis e informáticos fosse feito através de sistemas biométricos, não parecendo, contudo, que a lei tenha dado "abertura" para tal, afastando como finalidade legítima esta última hipótese. No entanto, pensamos que, no futuro, e quando a lei fosse revista, se justificasse que esta possibilidade fosse também ela regulada, uma vez que, com as evoluções tecnológicas, esta atualização seria útil e atual.

A verdade é que esta temática não está muito fundamentada nem clara na lei. Mesmo na abordagem da doutrina, quer nacional, quer estrangeira, surgem dúvidas, devido às diferentes interpretações desta questão.

A Lei de Execução decidiu regular num artigo autónomo, por exemplo, a videovigilância. No entanto, optou por não o fazer quanto aos sistemas biométricos, tendo-os apenas incluído no art. 28.º, onde também não acrescentou muito. Sendo uma realidade cada vez mais aplicada nas empresas, parece-nos que também seria merecedora de uma regulamentação específica.

[108] Com isto, importa reforçar que não deixamos de compreender a posição da doutrina a quem esta utilização de sistemas biométricos causa sérias preocupações. Consideramos, aliás, que os dados pessoais deveriam ser mais protegidos, o que infelizmente não acontece, especialmente no mundo digital. No entanto, pensamos ser mais vantajoso e mais "justificável" que os dados pessoais sejam tratados no âmbito laboral, cumprindo todas as obrigações legais que as entidades empregadoras devem respeitar e sendo (em princípio) utilizados apenas para fins determinados, em relação ao tratamento de dados dos consumidores, dados estes que são, muitas vezes, utilizados para diversos fins não conhecidos ao consumidor no momento que aceita o tratamento.

O art. 88.º do RGPD, com a epígrafe "Tratamento no contexto laboral" resulta, na opinião de Moreira (Amado et al., 2019, p. 113), da consciencialização das inúmeras possibilidades de controlo através das novas tecnologias e, bem assim, das diferenças em matéria de proteção laboral relativamente ao tratamento de dados pessoais dos trabalhadores nos diferentes Estados-Membros, pelo que dificilmente será conseguida uma harmonização máxima nesta temática, atentas as inúmeras especificidades e sensibilidades de certas matérias, tentando conseguir-se uma harmonização mínima.

O suprarreferido artigo dispõe que "[o]s 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" incluindo nestas normas "medidas adequadas e específicas para salvaguardar a dignidade, os interesses legítimos e os direitos fundamentais do titular dos dados, com especial relevo para a transparência do tratamento de dados, a transferência de dados pessoais num grupo empresarial ou num grupo de empresas envolvidas numa atividade económica conjunta e os sistemas de controlo no local de trabalho" (art. 88.º, n.os 1 e 2 do RGPD). No nosso ordenamento jurídico, optou o legislador por não estabelecer muito mais do que aquilo que já constava no RGPD quanto aos dados biométricos sendo, no entanto, neste artigo (e também no art. 9.º, n.º 4), que o n.º 6 do art. 28.º da Lei de Execução, encontra suporte.

3.2.2. Tratamento de dados biométricos no âmbito laboral

Afirma a CNPD que "[a] operação de recolha das características biométricas com a finalidade de controlo do horário de trabalho não envolve, em si mesmo, uma violação da integridade física do trabalhador, do seu direito à privacidade ou da sua intimidade". Isto será verdade, se a finalidade for estritamente prosseguida pelo responsável pelo tratamento (Pinheiro et al., 2018, p. 326).

Também a AEPD considera que, o tratamento da impressão digital para controlo de horário não consubstancia nenhuma violação dos direitos de personalidade, porquanto a informação contida neste dado biométrico não contém nenhum aspeto concreto da personalidade do trabalhador em questão, não olvidando o facto de ser por eles aconselhado o uso de meios menos invasivos de armazenamento (Fernández Orrico, 2020, p. 307).

E se, por exemplo, os dados forem recolhidos por reconhecimento da íris para controlo de assiduidade de um trabalhador, e sendo cumpridas todas as regras e princípios por parte da entidade empregadora, à partida, não parece existir qualquer risco de violação da integridade física do trabalhador ou dos seus direitos de personalidade[109]. No entanto, rapidamente poderá o caso mudar de figura, quando, através destes mecanismos, seja possível aceder a outras informações sobre o trabalhador que não sejam necessárias para cumprir o objetivo para o qual foram inicialmente recolhidos, e podendo-se tornar conhecidas informações, tais como dados relativos à saúde do trabalhador através da leitura da íris, podendo a entidade empregadora utilizar estas informações para levar a cabo práticas discriminatórias e até comprometer a carreira profissional do trabalhador (García Coca, 2020, p. 343).

O art. 18.º do CT, que se refere especificamente aos dados biométricos, regulamenta o tratamento destes dados em contexto laboral ainda à luz da Diretiva 95/46/CE de 24 de outubro, não tendo acompanhado o RGPD. Nos n.os 1 e 4 deste artigo faz-se referência à notificação prévia à Comissão Nacional de Proteção de Dados, normas que devem ser tidas por revogadas pelo RGPD. Segundo o considerando 89 do Regulamento, a obrigação geral de notificação estabelecida pela Diretiva 95/46/CE, além de originar encargos administrativos e financeiros, nem sempre contribuiu para a melhoria da proteção dos dados pessoais.

Assim, ainda segundo o referido considerando, entende-se que a obrigação de notificação deve ser suprimida e substituída por regras e procedimentos eficazes, tendo em conta o que faz mais sentido para cada tratamento em específico que seja suscetível de resultar num elevado risco para os direitos e liberdades das pessoas singulares, devido à sua natureza, âmbito, contexto e finalidades. Nestes casos, o responsável pelo tratamento deverá, antes, proceder a uma avaliação do impacto sobre a proteção de dados (doravante designada por AIPD), a fim de avaliar a probabilidade ou gravidade particulares do elevado risco, tendo em conta a natureza, o âmbito, o contexto e as finalidades do

[109] Também neste sentido, Fernández Orrico (2020, pp. 309-310) considera que estes sistemas não constituem uma violação da intimidade e integridade pessoal protegidos constitucionalmente, uma vez que se resume apenas a um algoritmo digitalizado de uma imagem (trata-se de uma "versão digital" da impressão digital ou da geometria da mão, e que não expressa nenhum aspeto concreto da personalidade da pessoa), não tendo assim os dados biométricos mais impacto do que outros dados relativos à informação pessoal, por exemplo. Contudo, devemos atentar no facto de que esta opinião é emitida no contexto legal e jurisprudencial do regime jurídico espanhol.

tratamento e as fontes do risco[110] (considerando 90 do RGPD). Neste sentido, à data de hoje, não existe uma obrigatoriedade de notificação prévia à CNPD.

A AIPD trata-se de um processo que se resume no seguinte: quando um determinado tratamento em particular que utilize novas tecnologias, tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades dos trabalhadores, a entidade empregadora procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais (art. 35.º, n.º 1 do RGPD). Como se depreende da leitura do preceito, no âmbito laboral, esta avaliação será efetuada antes do início do tratamento, pelo empregador. Esta avaliação parece remeter-nos para o princípio da minimização dos dados, segundo o qual se pretende que os dados sejam adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados (art. 5.º, n.º 1, al. c) do RGPD).

Dispõe o art. 35.º, n.º 3 do RGPD que a realização de uma avaliação de impacto sobre a proteção de dados é obrigatória nos seguintes casos:

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

Ainda a este respeito, a CNPD publicou o Regulamento n.º 1/2018 relativo à lista de tratamentos de dados pessoais sujeitos a Avaliação de Impacto sobre a Proteção de Dados[111], lista esta em complemento à supra identificada, e que apresenta tratamentos

[110] Acrescenta o mesmo considerando que "[e]ssa avaliação do impacto deverá incluir, nomeadamente, as medidas, garantias e procedimentos previstos para atenuar esse risco, assegurar a proteção dos dados pessoais e comprovar a observância do presente regulamento".
[111] Este regulamento pode ser consultado em https://www.cnpd.pt/decisoes/regulamentos/, última consulta a 07-03-2022.

que também preenchem os pressupostos do art. 35.º, n.º 1 do RGPD. No próprio regulamento, a CNPD ressalva que a lista não é exaustiva, e que poderão surgir, em função do desenvolvimento tecnológico, outras situações em que se justifique realizar obrigatoriamente a AIPD[112].

No âmbito laboral, e quando a entidade empregadora tratar dados biométricos dos trabalhadores, mesmo que em pequena escala, aquela fica obrigada a realizar uma AIPD, por o tratamento recair sobre titulares de dados de grupos vulneráveis (os trabalhadores)[113]. Pelo contrário, se o empresário pretender utilizar dados biométricos para o controlo da entrada de clientes, parece não ser necessário, por regra, proceder à AIPD.

Em suma, e tal como nos explica Magina (2020, p. 69), quanto mais alto e incerto for o impacto do tratamento, mais improvável é que o tratamento venha a ser considerado, em termos gerais, lícito.

Já o n.º 2 do art. 18.º refere que o tratamento de dados biométricos só é permitido se os dados a utilizar forem necessários, adequados e proporcionais aos objetivos a atingir. Ora, esta regulação reforça alguns dos princípios de tratamento de dados pessoais consagrados no RGPD. Desta redação constam apenas três dos princípios elencados no RGPD, no entanto, é claro que devem ser respeitados todos os princípios que já acima analisámos. Por outro lado, a regulação deste artigo, é mais ampla em comparação com aquilo que regula a Lei de Execução, parecendo permitir, nomeadamente, a utilização de dados biométricos para acesso a equipamentos eletrónicos[114]. Contudo, certo é que, tal como referimos na primeira parte do nosso trabalho, devemos conjugar toda a legislação vigente sobre a matéria de proteção de dados, pelo que não nos parece, a par do que já referimos, que seja, pelo menos para já, intenção do legislador permitir tal tratamento.

[112] Também aqui é notória a importância que é dada aos dados biométricos, sendo por diversas vezes referidos ao longo da lista.
[113] A este respeito, veja-se o referido Regulamento n.º 1/2018 e também o Parecer 18/2018 sobre o projeto de lista da autoridade de controlo competente de Portugal respeitante às operações de tratamento de dados pessoais sujeitas a avaliação de impacto sobre a proteção de dados, disponível em https://edpb.europa.eu/sites/default/files/files/file1/edps-2018-00017-00-14_pt.pdf, última consulta a 28-03-2022.
[114] Moreira (2021, p. 234) considera mesmo que se deverá fazer uma interpretação extensiva desta norma, uma vez que lhe parece ser, também esta, uma finalidade legítima.

Finalmente, o n.º 3 do art. 18.º dita que "[o]s dados biométricos são conservados durante o período necessário para a prossecução das finalidades do tratamento 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"[115], constituindo a violação do disposto neste número uma contraordenação grave, nos termos do n.º 5 do mesmo artigo. A este respeito, e "[a] fim de assegurar que os dados pessoais sejam conservados apenas durante o período considerado necessário, o responsável pelo tratamento deverá fixar os prazos para o apagamento ou a revisão periódica" (considerando 39 do RGPD). Assim, também este n.º 3 do art. 18.º do CT, reforça o princípio da limitação da conservação, um dos princípios relativos ao tratamento de dados pessoais, previsto no art. 5.º, n.º 1, al. e) do RGPD.

Relativamente ao art. 28.º, n.º 6 da Lei de Execução "[o] tratamento de dados biométricos dos trabalhadores só é considerado legítimo para controlo de assiduidade e para controlo de acessos às instalações do empregador, devendo assegurar-se que apenas se utilizem representações dos dados biométricos e que o respetivo processo de recolha não permita a reversibilidade dos referidos dados", e tal como já referimos, o mesmo não comporta nenhuma novidade. Devemos fazer a interpretação extensiva de que falámos, no sentido de entender que o controlo de assiduidade se estenda também ao registo de tempos de trabalho, até porque, consideramos que o registo de tempos de trabalho feito desta forma rigorosa, é benéfico para o trabalhador, sendo que, como bem sabemos, a proteção do trabalhador constitui um dos objetivos principais do Direito do Trabalho.

Para Baz Rodríguez, a primeira avaliação a fazer-se deve ser a de perceber se o tratamento de dados biométricos é necessário para alcançar o objetivo a que se propõe, na medida em que parece ser essencial para se satisfazer essa necessidade e não apenas porque é a forma mais conveniente para a entidade empregadora de o fazer (2019, p. 251).

Na senda de Duarte (Pinheiro et al., 2018, p. 665), as atividades e entidades que pressuponham tratamento de dados pessoais sensíveis deveriam regulamentar o

[115] Aqui, parece fazer-se referência ao princípio da limitação da conservação (previsto no art. 5.º, n.º 1, al. e) do RGPD) e consagra o direito automático ao apagamento dos dados quando o trabalhador seja transferido ou quando cesse o seu contrato de trabalho (art. 17.º do RGPD).

tratamento de dados, nomeadamente em sede de instrumento de regulamentação coletiva[116].

As exceções à proibição do tratamento de dados pessoais constituem o resultado de ponderações do legislador europeu entre direitos ou interesses juridicamente relevantes e o risco que o tratamento destas categorias especiais de dados implica, sendo que, quando resolvidas a favor do tratamento de dados, constituem-se como causas de exclusão da ilicitude[117], devendo ser preenchida uma das finalidades admissíveis constantes do art. 9.º, n.º 2 do RGPD (Pinheiro et al., 2018, p. 238, 244). No entanto, como já se disse nem todos os fundamentos constantes das alíneas do art. 9.º, n.º 2 serão fundamento válido no âmbito laboral[118].

O tratamento de dados biométricos é, então, à partida, permitido se os dados forem necessários, adequados e proporcionais aos objetivos a atingir. Conforme o considerando 27 da orientação da CNPD "[a] finalidade do tratamento assenta na necessidade de agilizar o cumprimento de um objectivo que a lei reconhece integrar-se no âmbito dos poderes de controlo da entidade responsável pelo tratamento: a fixação do horário de trabalho, o controlo da assiduidade e o registo do tempo de trabalho" (2004, p. 4). Sendo assim, o tratamento de dados biométricos, quando necessário, é permitido para fins de controlo de acessos e assiduidade. Neste sentido, sendo os dados biométricos recolhidos exclusivamente para essa finalidade, à partida, não haverá problema quanto ao tratamento de dados, desde que esse tratamento seja adequado e proporcional aos objetivos a atingir, encontrando este tratamento fundamento no art. 9.º, n.º 2, al. b) do RGPD.

[116] Como já se disse supra, e salvo melhor opinião, destacamos quanto a esta matéria, o caráter pouco inovador da nossa contratação coletiva, que nos apresenta muito poucos IRCT's que prevejam o tratamento de dados biométricos, sendo que os existentes, não comportam nenhuma novidade.

[117] Sendo que o conceito de licitude se reporta à hierarquia de valores vigente num ordenamento jurídico, que serve base às ponderações que os casos concretos exijam (Pinheiro et al., 2018, p. 244).

[118] Como já se disse, o consentimento explícito do trabalhador tem também sido afastado do "leque" de fundamentos de legitimidade para o tratamento de dados pessoais dos trabalhadores e, em particular, para o tratamento de dados biométricos, tal como entende grande parte da doutrina. Já a CNPD, muito antes da entrada em vigor do RGPD ditou no mesmo sentido que "[s]erá de afastar o consentimento como «condição de legitimidade», em face da posição em que o trabalhador se encontra" (CNPD, 2004, p. 5, considerando 35). Neste sentido, o consentimento do trabalhador para o processamento da monitorização biométrica, não é necessário, uma vez que a base legal para o tratamento em causa será outro dos fundamentos constantes no art. 9.º, n.º 2 do RGP, não olvidando da obrigatoriedade da entidade empregadora de prestar informações completas ao trabalhador. E o dever de informação deve ser considerado cumprido, porquanto a informação teve de ser prestada ao trabalhador (mesmo que tenha sido, excecionalmente, prestada verbalmente) pelo simples facto de a impressão digital ter sido recolhida com tecnologia infravermelha, e a finalidade do processamento ter sido indicada (Fernández Orrico, 2020, p. 319).

O fundamento de licitude mais aceite pela doutrina era, antes da entrada em vigor do RGPD, o tratamento de dados para a prossecução de interesses legítimos da entidade empregadora, plasmado no art. 6.º, n.º 1, al. f) do RGPD. Alguns autores entendiam, tendo a CNPD (2004, considerando 39) se pronunciado também neste sentido, que a legitimidade para o tratamento de dados com a finalidade de controlo do horário de trabalho (assiduidade), só poderia ter como fonte a previsão do artigo 6.º al. f) do RGPD, uma vez que o tratamento é feito na "prossecução de interesses legítimos do responsável". Neste sentido também se pronunciou o Comité de Ministros dos Estados-Membros[119], que entendeu que a recolha e o posterior tratamento de dados biométricos apenas devem ser efetuado quando for "necessário proteger os interesses legítimos dos empregadores, empregados ou terceiros, e apenas se não existirem outros meios menos intrusivos e apenas se for acompanhado de salvaguardas apropriadas, incluindo as salvaguardas adicionais previstas em princípio" (tradução nossa). No entanto, e não podendo à data de hoje, os dados pessoais ser tratados com base nos fundamentos do art. 6.º, e não fazendo o fundamento para a "prossecução de interesses legítimos do responsável" parte do "leque" dos fundamentos legítimos para o tratamento da categoria de dados sensíveis, esta leitura, apesar de nos parecer fazer algum sentido, encontra-se desatualizada, face à legislação agora vigente e face à elevação dos dados biométricos à categoria de dados especiais sensíveis.

Moreira (2021, p. 235) ressalva ainda a importância de realizar a ponderação de interesses em confronto, a fim de aferir da licitude da utilização dos dados biométricos sendo, na opinião da Autora, preferível adotar uma postura cuidadosa e realista em relação à utilização e generalização destes meios de controlo para evitar, tanto quanto possível, os riscos para os titulares dos dados. É neste procedimento que se aplica o princípio da proporcionalidade, não devendo o tratamento ser feito quando se revele injustificado por ser desajustado e excessivo ou quando, pela sua falta de fiabilidade, comprometa a finalidade determinante do tratamento[120] – constituindo-se este princípio como o critério

[119] Na sua Recomendação CM/Rec(2015)5 adotada a 1 de abril de 2015, sobre o tratamento de dados no contexto laboral, que pode ser consultada em https://www.apda.ad/sites/default/files/2018-10/cm-rec-2015-5-en.pdf.

[120] Castro (2005, p. 86) indica dois exemplos para melhor compreensão deste princípio no contexto que importa: por um lado, foi autorizado o controlo de acessos a determinadas áreas do Louvre através de controlos biométricos de leitura da impressão digital; por outro lado, a utilização de sistemas de identificação através da impressão digital numa cantina escolar foi considerada excessiva, e não foi autorizada, uma vez que não respeitava o princípio da proporcionalidade. Ora, facilmente se percebe que o museu do Louvre poderá ser propício a diversas tentativas de assalto, tratando-se de uma galeria de arte, com algumas das mais importantes obras a nível mundial, sendo lugares desta importância várias vezes

determinante das decisões relativas ao tratamento de dados biométricos (CNPD, 2004, considerandos 41, 42 e 43).

Assim, impõe-se, segundo o princípio da proporcionalidade, "que qualquer tratamento de dados pessoais, atenta a sua finalidade concreta, deva ser avaliado em termos de idoneidade e de intervenção mínima", o que envolve uma ponderação, em cada caso particular, entre a finalidade pretendida e o sacrifício ou limitação de direitos ou interesses dos trabalhadores que ela implica[121] (considerando 51, 2004, CNPD).

Neste sentido, a eventual "invasão da privacidade" deverá ser abordada em duas fases do tratamento: por um lado, na fase da captura[122/123] das características e do subsequente armazenamento no sistema e, por outro lado, na fase da identificação, aquando do registo dos movimentos do trabalhador no local de trabalho (Guerra, 2004, p. 210).

Assim, consideram Cunha & Santos (2021, p. 9) que, na relação laboral, os dados biométricos poderão ser alvo de tratamento por serem parte do contrato, mas apenas se a sua finalidade for a do controlo de tempos de trabalho do trabalhador ou dos acessos às instalações da empresa, sempre com a ressalva de que não pode existir forma menos invasiva de prosseguir esses objetivos. Os dados recolhidos para determinado fim, não poderão ser utilizados para outra finalidade que não para a qual foram inicialmente recolhidos.

Importa ainda ter em conta que a obrigação de registo de tempos de trabalho pode, na nossa opinião, proporcionar uma base regulamentar que justifique a necessidade de implementação dos sistemas biométricos para este fim, com o objetivo de cumprimento de obrigações do responsável pelo tratamento em matéria de legislação laboral, desde que

alvo de tentativas de ataques terroristas, exigindo um maior controlo de entradas e para além do controlo, é importante que não haja falhas quanto à entrada de pessoas apenas autorizadas. Já no seguindo caso, é fácil perceber que é exagerado submeter as crianças a um controlo biométrico para acesso à cantina.

[121] Em relação ao princípio da proporcionalidade, a AEPD tem vindo a entender que os sistemas de controlo biométrico não superam, por regra, o "teste" de proporcionalidade, pelo que as autoridades devem sempre provar que não existe um sistema de menor impacto ou menos invasivo nos direitos das pessoas afetadas (Rodríguez-Piñero Royo, 2020, p. 294).

[122] A operação de captação de dados biométricos que implica, naturalmente, a cooperação do trabalhador, não pode ser realizada com violação da sua identidade pessoal (art. 26.º da CRP), com lesão da sua integridade física (art. 25.º, n.º 1 da CRP) ou com intromissão na intimidade privada (art. 26.º da CRP), não afetando esta operação o direito à identidade pessoal e da intimidade da vida privada, garantidas constitucionalmente pelo art. 26.º da CRP (considerando 47, 2004, CNPD).

[123] Para o autor (Rodríguez-Piñero Royo, 2020, p. 277), o grau de intrusão na fase da captura varia também conforme o mecanismo utilizado sendo, para ele, menos intrusivo verificar, a título de exemplo, o rosto de uma pessoa (que se faz à distância) do que a sua impressão digital (que existe um contacto físico com o aparelho).

a entidade empregadora justifique a proporcionalidade e a adequação da sua utilização, face ao caso concreto[124]. Em todo o caso, a entidade empregadora deve fornecer garantias adicionais adequadas de respeito pelos direitos e interesses fundamentais do trabalhador, garantias essas que devem incluir, entre outras, a informação prévia, o diálogo e a adoção de medidas técnicas e organizacionais na empresa sobre o processamento de dados (Baz Rodríguez, 2019, pp. 248-250).

Moreira (2021, pp. 235-236) resume, assim, o tratamento de dados biométricos no âmbito laboral nos seguintes princípios:

i) Tem de ocorrer uma ponderação da idoneidade e da necessidade daquele meio e da conformidade dos motivos apresentados com o princípio da proporcionalidade;
ii) Para fins de controlo de acessos, devem ser utilizados, sobretudo, sistemas de reconhecimento que não deixem vestígios ou que os deixem, mas não em bases de dados centralizadas;
iii) O empregador não pode (ou não deve) encarar estes sistemas como sendo instrumentos infalíveis;
iv) Os dados biométricos são obrigatoriamente eliminados aquando da transferência do trabalhador para outro local de trabalho, ou no caso de cessação do contrato de trabalho;
v) Os dados biométricos apenas devem ser utilizados se a sua utilização for adequada, pertinente e não excessiva, o que implica que deve haver uma avaliação rigorosa da necessidade da proporcionalidade dos dados tratados.

3.2.3. Finalidades do tratamento

A verdade é que, em Portugal, nas relações laborais, a finalidade do tratamento de dados biométricos assenta na necessidade de agilizar o cumprimento de um objetivo que a lei reconhece integrar-se no âmbito dos poderes de controlo da entidade responsável pelo

[124] Sendo certo que, em alguns casos, não se revelará proporcional e necessário o tratamento de dados biométricos para este fim. Pense-se, a título de exemplo, numa empresa onde colaboram apenas cinco trabalhadores, todos com horário laboral compreendido entre as 09h00 e as 18h00. Por outro lado, uma empresa com 800 trabalhadores que recorre ao trabalho por turnos, parece-nos que já poderá "superar" o teste da proporcionalidade.

tratamento: a fixação do horário de trabalho, o controlo da assiduidade e o registo do tempo de trabalho (CNPD, 2004, considerando 27), poderes estes que já desenvolvemos supra. E, por isso, o fundamento para a licitude do tratamento dos dados biométricos será, a nosso ver e de acordo com o que tem vindo a ser exposto, o tratamento dos dados pessoais para a execução de um contrato de trabalho e para o cumprimento de obrigações jurídicas a que a entidade empregadora está adstrita (art. 9.º, n.º 2, al. b) do RGPD).

Refere ainda o art. 9.º, n.º 4 do RGPD que "[o]s Estados-Membros podem manter ou impor novas condições, incluindo limitações, no que respeita ao tratamento de dados genéticos, dados biométricos ou dados relativos à saúde". O legislador português optou por não acrescentar novas condições, apesar de o RGPD permitir fazê-lo.

3.2.4. Breves notas sobre as entidades de supervisão e o regime sancionatório dos dados pessoais

A consagração de um regime contraordenacional comum para todos os países da União Europeia, foi uma das várias novidades que surgiu com o RGPD, porquanto a Diretiva previa apenas que os Estados-Membros deviam tomar as medidas adequadas para assegurar a plena aplicação do diploma, tendo liberdade total para, eles próprios, determinar as sanções a aplicar[125] (Cordeiro, 2020a, p. 194).

No considerando 11 do RGPD pode ler-se que "[a] proteção eficaz dos dados pessoais na União exige o reforço e a especificação dos direitos dos titulares dos dados e as obrigações dos responsáveis pelo tratamento e pela definição do tratamento dos dados pessoais, bem como poderes equivalentes para controlar e assegurar a conformidade das regras de proteção dos dados pessoais e sanções equivalentes para as infrações nos Estados-Membros".

Atualmente, o regime sancionatório, encontra-se previsto essencialmente no art. 83.º do RGPD e nos arts. 37.º e ss. da Lei de Execução.

O art. 83.º do RGPD, com os elevados montantes das coimas que veio consagrar, alertou as entidades empregadoras e os cidadãos para a seriedade do tema dos dados pessoais e para as obrigações decorrentes do seu tratamento. O referido artigo estabelece,

[125] Este anterior regime, determinou uma diversidade de quadros sancionatórios, uma vez que cada legislador de cada Estado-Membro, podia fazer as suas escolhas (Pinheiro et al., 2018, p. 640).

atualmente, os critérios que devem ser tidos em conta aquando da determinação da medida da coima e tipifica as condutas que constituem contraordenações, estabelecendo as respetivas coimas (Pinheiro et. al., 2018, p. 640).

É ao CEPD que cabe elaborar diretrizes dirigidas às autoridades de controlo dos diferentes Estados-Membros em matéria de aplicação das medidas a que se refere o art. 58.º, n.ºs 1, 2 e 3 e fixar as coimas nos termos do art. 83.º (art. 70.º, n.º 1, al. k) do RGPD). Isto, mostra a intenção do legislador de assegurar uma aplicação uniforme, também nesta matéria, no espaço europeu.

Às autoridades de controlo de cada EM cabe "[i]mpor uma coima nos termos do artigo 83.º, para além ou em vez das medidas referidas no presente número, consoante as circunstâncias de cada caso" (art.º 58.º, n.º 2, al. i) do RGPD), cabendo, no nosso caso, esse poder à CNPD. Devem as autoridades aplicar as coimas fazendo sempre uma análise casuística e assegurando que a aplicação das mesmas seja efetiva, proporcionada e dissuasiva (art.º 83.º, n.º 1 do RGPD)[126]. Apesar da discricionariedade concedida à CNPD, esta é reduzida, na medida em que é condicionada pelos princípios que devem ser respeitados, nomeadamente e especialmente, o princípio da proporcionalidade (Cordeiro, 2020a, pp. 199-200).

No artigo 58.º estão previstos os poderes de supervisão da CNPD, enquanto autoridade de controlo, e estes podem dividir-se em 3: poderes de investigação (art.º 58.º, n.º 1 do RGPD), poderes de correção e de sanção (art.º 58.º, n.º 2 do RGPD) e poderes consultivos e de autorização (art.º 58.º, n.º 3 do RGPD).

Ora, a aplicação das coimas, como em qualquer ramo do Direito, deve ser adequada à situação em concreto. Dispõe, neste sentido, o art.º 83.º, n.º 1 que a aplicação das coimas deve ser "em cada caso individual, efetiva, proporcionada e dissuasiva". Assim, devem ser respeitados os princípios da efetividade, proporcionalidade e dissuasão, para além dos princípios da especificidade e da equivalência ou igualdade (Cordeiro, 2020a, p. 199).

O art. 83.º, n.º 3 estabelece um princípio em matéria de fixação do montante da coima a aplicar em caso de concurso de contraordenações (Coelho, 2018, p. 642).

[126] Segundo o Considerando 148 do RGPD, pode ainda, em caso de infração menor, ou se o montante da coima suscetível de ser imposta constituir um encargo desproporcionado para uma pessoa singular, ser feita uma repreensão em vez de aplicada uma coima.

Por sua vez, o art. 39.º, n.º 1 da Lei de Execução acrescenta três critérios aos constantes do art. 83.º, n.º 2, sendo que, também quanto a este aspeto, a CNPD veio desaplicar essas normas, alegando que a alínea k) permite que as autoridades de controlo valorizem outros fatores mas não que os fatores sejam determinados pelos legisladores nacionais (Parecer n.º 20/2018).

Em matéria de categorias especiais de dados, as sanções a aplicar em caso de infração ou incumprimento das normas seriam as que se aplicam no art. 83.º, n.º 5, al. a) do RGPD.

PÁGINA DEIXADA PROPOSITADAMENTE EM BRANCO

Conclusão

As evoluções tecnológicas trouxeram inovações para as relações laborais e, para além dos benefícios relacionados com a modernização das empresas, verificam-se alterações positivas no dia a dia das mesmas. Estes avanços, exigem novas respostas da legislação em todas as áreas pelo que deve (ou deveria) o Direito do Trabalho acompanhá-las, surgindo, na verdade, constantes desafios a este nível, uma vez que, esse acompanhamento nem sempre se revela tão célere como desejado.

Recentemente, têm surgido novas formas de monitorização dos trabalhadores, que passam a ser utilizadas pelos empregadores com fundamento (essencialmente) no seu interesse legítimo, mas que, muitas vezes, se constituem como uma forma abusiva de controlo sobre os trabalhadores.

De entre os desafios colocados às entidades empregadoras, apresentam-se dois interesses divergentes: por um lado, a vontade de manter a segurança nos locais de trabalho (ou de tentar fazer um registo justo das horas de trabalho) e, por outro, a necessária proteção da vida privada dos trabalhadores (Amadeu et al., 2019, p. 154).

Os sistemas biométricos começaram a surgir como forma de controlo para diversas finalidades das entidades empregadoras no âmbito laboral e, com a entrada em vigor do RGPD passaram a ser consideradas categorias especiais de dados pessoais, sendo merecedoras, em certas situações, de tutela reforçada. No âmbito laboral, o tratamento deve ter por base um fundamento válido que garanta a licitude do tratamento, encontrando suporte nos arts. 6.º ou 9.º do RGPD.

O registo de tempos de trabalho dos trabalhadores, que se tornou obrigatório em 2003, veio ser uma "chamada de atenção" para as entidades empregadoras, e veio a aumentar o recurso a sistemas biométricos para o efetivo cumprimento desta obrigação. Isto porque, a regulamentação sobre esta obrigatoriedade, não determina qual o método de controlo mais apropriado para este cumprimento, permitindo à entidade empregadora a escolha deste sistema de controlo, devendo apenas garantir a fiabilidade e veracidade dos dados registados nestes dispositivos, e exigindo o cumprimento do princípio da boa-fé, e a obrigatoriedade de informar o trabalhador da existência dos mesmos (García Coca, 2020, p. 340). Bem sabemos que os métodos tradicionais de autenticação são falíveis e suscetíveis de serem manipulados ou roubados. E os sistemas biométricos, apesar de se revelarem, para alguma doutrina, como sistemas "intrusivos" na esfera privada dos

trabalhadores, a verdade é que aqueles métodos tradicionais, que são menos intrusivos, se revelam também menos fiáveis e menos precisos, pelo que não cumprem (parece-nos a nós) com o objetivo primordial daquela obrigação – o registo das horas efetivas de trabalho.

Para o tratamento de dados biométricos no contexto de uma relação laboral, o fundamento de licitude a aplicar será a execução do contrato de trabalho, tendo em conta que a finalidade para o tratamento desses dados será o controlo de acessos às instalações da entidade empregadora e o controlo de assiduidade.

Assim, deve a entidade empregadora, antes da utilização dos sistemas biométricos, adotar medidas organizativas adequadas destinadas a aplicar com eficácia todos os princípios da proteção de dados dos trabalhadores (ou candidatos) e incluir as garantias necessárias no tratamento, para que o pretendido registo cumpra os requisitos do RGPD e proteja os direitos dos titulares dos dados (Duarte, 2018, pp. 181-182).

Por se tratar de uma operação de tratamento que pode implicar um elevado risco para os direitos e liberdades dos trabalhadores, deve ainda a entidade empregadora, antes de iniciar o tratamento, proceder a uma Avaliação de Impacto sobre a Proteção de Dados (Cunha & Santos, 2021, p. 10).

O equilíbrio entre os direitos dos trabalhadores e o poder de controlo eletrónico da entidade empregadora não constitui uma tarefa fácil. Deve, acima de tudo, ter-se em conta que "nem tudo o que é tecnicamente possível é juridicamente admissível", pelo que o respeito pelos princípios fundamentais de tratamento de dados pessoais é elementar (Moreira, 2017, pp. 33-34).

Em matéria de proteção de dados pessoais, continuarão a surgir dúvidas e novas questões se vão levantar, uma vez que as tecnologias estão em constante desenvolvimento, e o Direito, como se disse, não consegue "responder" em tempo útil.

Bibliografia

Alves, L. D. (2020). *Proteção de Dados Pessoais no Contexto Laboral. O Direito à Privacidade do Trabalhador*. Coimbra: Edições Almedina, S. A..

Amado, J. L., Rouxinol, M. S., Vicente, J. N., Santos, C. G., Moreira, T. C. (2019). *Direito do trabalho: relação individual*. Edições Almedina, S. A.

Aragüez Valenzuela, L. (2019). *Los sistemas biométricos de registro de jornada y la (des) protección jurídica de la persona del trabajador*. Disponível em https://www.juntadeandalucia.es/empleo/carl/portal/c/document_library/get_file?uuid=77ad7ac7-da0f-47e2-976d-60e78c0a46db&groupId=10128, consultado a 04-08-2021.

Baz Rodríguez, J. (2019). El tratamiento de datos biometricos de los trabajadores, como categoria especial de datos personales: el RGPD como respuesta frente a la segunda generación de técnicas biométricas. *Privacidad y protección de datos de los trabajadores en el entorno digital*, pp. 243-259.

Campos, M. (2021). Longos horários de trabalho matam 745 mil pessoas por ano. *Jornal de Notícias*, de 17 de maio de 2021, disponível em https://www.jn.pt/mundo/longas-horas-de-trabalho-matam-745-mil-pessoas-por-ano-13730609.html, última consulta a 30-03-2022.

Carvalho, M. J. & Lopes, P. S. (2019). Da Privacidade à Proteção de Dados, de 16 de dezembro de 2019, disponível em https://www.uc.pt/protecao-de-dados/protecao_dados_pessoais/da_privacidade_a_protecao_de_dados, consultado a 17-06-2021.

Castro, C. S. e (2005). *Direito da informática, privacidade e dados pessoais*. Coimbra: Almedina.

Castro, C. S. e. (2018). Novas tecnologias e relação laboral – alguns problemas: tratamentos de dados pessoais, novo regulamento geral de proteção de dados e direito à desconexão. *Revista do CEJ*, Lisboa, n.º 1 (1.º Semestre 2018), pp. 271-299.

Comissão Nacional de Proteção de Dados, *Princípios sobre a utilização de dados biométricos no âmbito do controlo de acessos e de assiduidade*, de 26 de

fevereiro de 2004, disponível em https://www.cnpd.pt/media/uqunywgn/principios-biom-assiduidade-acesso.pdf, consultado a 20-03-2022.

Comissão Nacional de Proteção de Dados, *Regulamento n.º 1/2018 relativo à lista de tratamentos de dados pessoais sujeitos a Avaliação de Impacto sobre a Proteção de Dados*, de 16 de outubro de 2018, disponível em https://www.cnpd.pt/decisoes/regulamentos/, consultado a 20-03-2022.

Comité Europeu para a Proteção de Dados. *Parecer 18/2018 sobre o projeto de lista da autoridade de controlo competente de Portugal respeitante às operações de tratamento de dados pessoais sujeitas a avaliação de impacto sobre a proteção de dados*, de 25 de setembro de 2018, disponível em https://edpb.europa.eu/sites/default/files/files/file1/edps-2018-00017-00-14_pt.pdf, consultado a 28-03-2022.

Comité Europeu para a Proteção de Dados. *Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679*, de 4 de maio de 2020, disponível em https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pt.pdf , consultado a 28-03-2022.

Cordeiro, A. B. M. (2019). O tratamento de dados pessoais fundado em interesses legítimos. *Revista de Direito e Tecnologia, Vol. 1* (n.º 1), pp. 1-31. Disponível em https://blook.pt/publications/publication/29c85b840a65/, consultado a 10-03-2022.

Cordeiro, A. B. M. (2020). *Direito da proteção de dados: à luz do RGPD e da Lei n.º 58/2019*. Coimbra: Edições Almedina, S. A.

Cordeiro, A. B. M. (2020a). O Direito Sancionatório da Proteção de Dados. *Revista de Direito e Tecnologia, Vol. 2* (n.º 2), pp. 193-217. Disponível em https://blook.pt/publications/publication/5c39f7a8d388/, consultado a 09-03-2022.

Cortés Osorio, J. A., Medina Aguirre, F. A. & Muriel Escobar, J. A. (2010). Sistemas de seguridad basados en Biometría. *Scientia et Technica*, XVII (46), pp. 98-102. Disponível em https://www.redalyc.org/articulo.oa?id=84920977016, consultado a 10-10-2021.

Cunha, J. F. S. R., Santos, P. B. (2021). *O tratamento de dados biométricos no contrato de trabalho*. Artigo apresentado no XIII Congresso Europeu da Sociedade Internacional de Direito do Trabalho e da Segurança Social, que decorreu online de 5 a 7 de maio de 2021 em Lisboa.

Dicionário Priberam da Língua Portuguesa [em linha] (2008-2021), consultado pela última vez a 6 de fevereiro de 2022 em https://dicionario.priberam.org/.

Duarte, D. P. (2018). Registo dos Tempos de Trabalho e Proteção de Dados Pessoais. In M. R. P. Ramalho & T. C. Moreira (Coord.), *Tempo de Trabalho e Tempos de não Trabalho. O Regime Nacional do Tempo de Trabalho à luz do Direito Europeu e Internacional – Estudos APODIT 4* (pp. 173-183). Lisboa: AAFDL Editora.

Fernandes, F. L. (2018). *O trabalho e o tempo: comentário ao Código do Trabalho*. Universidade do Porto. Centro de Investigação Jurídico-Económica. Reitoria. (Online)

Fernández Orrico, J. (2020). Límites a la biometria como medio de identificación y control de los trabajadores: necesidad de su regulación. In Rodríguez-Piñero Royo, M. & Todolí Signes, A. (Dir.), *Vigilancia y controle en el Derecho del Trabajo Digital* (1.ª Ed., pp. 301-326). Navarra, España: Aranzadi.

García Coca, O. (2020). El registro de la jornada laboral y la privacidade de los trabajadores. In Rodríguez-Piñero Royo, M. & Todolí Signes, A. (Dir.), *Vigilancia y controle en el Derecho del Trabajo Digital* (1.ª Ed., pp. 301-326). Navarra, España: Aranzadi.

Garrote Crespo, P. (2021). *El uso de datos biométricos en el control del registro de la jornada laboral de los trabajadores*. Diario La Ley, n.º 48, Sección Ciberderecho, 28 de Febrero de 2021, Wolters Kluwer. Disponível em http://www.diariolaley.es, consultado a 26-10-2021.

González Biedma, E. (2017). Derecho a la información y consentimiento del trabajador en materia de protección de datos. *Temas laborales. Revista andaluza de trabajo y bienestar social*, núm. 138, pp. 223-247. Disponível em https://dialnet.unirioja.es/metricas/documentos/ARTREV/6552394, consultado a 02-12-2021.

Grupo de Trabalho de Proteção de Dados do Artigo 29.º. *Opinion 1/2010 on the concepts of "controller" and "processor"*, de 16 de fevereiro de 2010, 00264/10/EN, WP 169, disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf, consultado a 12-09-2021.

Grupo de Trabalho de Proteção de Dados do Artigo 29.º. *Opinion 15/2011 on the definition of consent*, de 13 de julho de 2011, 01197/11/EN, WP187, disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf, consultado a 15-01-2022.

Grupo de Trabalho de Proteção de Dados do Artigo 29.º. *Parecer 4/2007 sobre o conceito de dados pessoais*, de 20 de junho de 2007, 01248/07/PT, WP 136, disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_pt.pdf, consultado a 15-01-2022.

Grupo de Trabalho de Proteção de Dados do Artigo 29.º. *Working document on data protection issues related to RFID technology*, de 19 de janeiro de 2005, 10107/05/EN, WP 105, disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp105_en.pdf, consultado a 12-09-2021.

Guerra, A. (2004). *A privacidade no local de trabalho. As novas tecnologias e o controlo dos trabalhadores através de sistemas automatizados: as alterações do Código do Trabalho.* Coimbra: Almedina.

Henriques, S. C., & Luís, J. V. (2019). Consentimento e outros fundamentos de licitude para o tratamento de dados pessoais em contexto laboral. *Anuário de Proteção de Dados*, pp. 13-36. Disponível em https://cedis.novalaw.unl.pt/wp-content/uploads/2021/03/ANUARIO-2019-Eletronico_compressed.pdf, consultado a 04-11-2021.

Instituto Nacional de Ciberseguridad (2016). *Tecnologías biométricas aplicadas a la ciberseguridad: : una guía de aproximación para el empresario*. Madrid: INCIBE. Disponível em https://www.incibe.es/protege-tu-empresa/guias/tecnologias-biometricas-aplicadas-ciberseguridad-guia-aproximacion-el, consultado a 16-01-2022.

Jain, A. K., Prabhakar S., Ross, A. (2004). *An introduction to biometric recognition*. IEEE Transactions on Circuits and Systems for Video Technology, Volume 14, pp. 4-12. Disponível em https://www.researchgate.net/publication/3308596_An_Introduction_to_Biometric_Recognition#fullTextFileContent, consultado a 07-08-2021.

Lambelho, A. & Gonçalves, L. A. (2021). *Direito do Trabalho – Da Teoria à Prática* (2.ª Ed.). Lisboa: Rei dos Livros.

Lambelho, A. (2020). O poder regulamentar do empregador. *Prontuário do Direito do Trabalho*, 2020 – I, pp. 223-251.

Lopes, B. (2018). *O que é a biometria*. Disponível em https://bioglobal.pt/o-que-e-a-biometria/, consultado a 05-12-2021.

Lopes, J. d. S. (2016). O artigo 35.º da Constituição: da génese à atualidade e ao futuro previsível in *Fórum de Proteção de Dados*, n.º 2, janeiro de 2016, pp. 14-51, CNPD, Disponível em https://www.cnpd.pt/media/kjspegob/forum_2_af_web_low.pdf, consultado a 05-12-2021.

Magalhães, F. M. & Pereira, M. L. (2018). *Regulamento Geral de Proteção de Dados – Manual Prático* (2.ª Ed.). Vida Económica – Editorial SA.

Magina, J. (2020). Fundamentos de Licitude do Tratamento de Dados Pessoais em Contexto Laboral *In* M. R. P. Ramalho & T. C. Moreira (Coord.), *O Regulamento Geral de Proteção de dados e as relações de trabalho – Estudos APODIT 6 (pp. 49-97)*. Lisboa: AAFDL Editora.

Marques, H. A. A. V. (2020). *Os deveres de controlo do empregador em matéria de tempo de trabalho*. Universidade Católica Portuguesa, Faculdade de Direito, Escola do Porto.

Marrero Blanco, D., Mulero Fernández, J. M.. (2020). *Los sistemas de control de la jornada laboral basados en datos biométricos. Un análisis crítico desde la privacidade*. Disponível em http://www.diariolaley.es, consultado a 01-06-2021.

Martínez Velencoso, L. M. & Sancho López, M. (2018). El nuevo concepto de onerosidad en el mercado digital. ¿Realmente es gratis la App?. *InDret*, Vol. 1, 2018. Disponível em https://indret.com/el-nuevo-concepto-de-onerosidad-en-el-mercado-digital-realmente-es-gratis-la-app/, consultado a 12-03-2022.

Monjardino, J. P. (2018). A recolha de dados biométricos no contexto laboral. *E-Report* (outubro 2018), páginas 6-7, disponível em https://www.sociedadeadvogados.eu/xms/files/wax_news/e-report-outubro18.pdf, consultado a 20-03-2022.

Moreira, T. C. (2017). Algumas Implicações Laborais do Regulamento Geral de Proteção de Dados Pessoais no Trabalho 4.0. *Revista Questões Laborais* (a. 24, n.º 51, julho/dezembro 2017) , páginas 9-34. Edições Almedina S. A.

Moreira, T. C. (2020). Dados pessoais: breve análise do art. 28.º da lei n.º 58/2019, de 8 de agosto. *Revista Questões Laborais* (Ano XXVI, n.º 55, julho/dezembro 2019) , páginas 41-62. Edições Almedina S. A.

Moreira, T. C. (2021). *Direito do Trabalho na Era Digital*. Edições Almedina, S. A.

Mota, J. & Pedral, A. S. (2019). Regulamento Geral de Proteção de Dados em Portugal – alguns apontamentos à sua lei de execução. *Actualidad Jurídica Uría Menéndez*, 53, pp. 142-148. Disponível em https://www.uria.com/documentos/publicaciones/6855/documento/port01.pdf?id=9341, consultado a 11-08-2021.

Narciso, M. (2019). Dados Pessoais como Contraprestação em Contratos de Consumo – Breve Reflexão. *Anuário do NOVA Consumer Lab, Ano 1* (*pp. 129-147*). Disponível em http://novaconsumerlab.novalaw.unl.pt/anuario-nova-consumer-lab/, consultado a 12-03-2022.

Ordem dos Médicos (2020). *COVID-19: Ordem recomenda abolição do registo biométrico através de impressão digital*, de 5 de março de 2020, disponível em https://ordemdosmedicos.pt/, consultado a 20-03-2022.

Pinheiro, A. S. (2018). Apresentação do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016: Regulamento Geral de Proteção de Dados (RGPD). *Revista do CEJ*, Lisboa, n.º 1 (1.º Semestre 2018), pp. 303-327.

Pinheiro, A. S. (Coord.), Coelho, C. P., Duarte, T., Gonçalves, C. J. & Gonçalves, C. P. (2018). *Comentário ao Regulamento Geral de Proteção de Dados.* Coimbra: Edições Almedina, S.A.

Predotova, K., Vargas Llave, O. (2021). Working conditions and sustainable work. Workers want to telework but long working hours, isolation and inadequate equipment must be tackled. *Eurofound*, de 06-09-2021, disponível em https://www.eurofound.europa.eu/pt/publications/article/2021/workers-want-to-telework-but-long-working-hours-isolation-and-inadequate-equipment-must-be-tackled.

Ramalho, M. R. P. (2014). *Tutela da personalidade e equilíbrio entre interesses dos trabalhadores e dos empregadores no contrato de trabalho. Breves notas.* Apresentada no VI Colóquio do Supremo Tribunal sobre Direito do Trabalho. Disponível em https://www.stj.pt/wp-content/uploads/2014/10/prof_maria_rosario_ramalho.pdf, consultado a 06-02-2022.

Rodríguez-Piñero Royo, M. (2020). Registro de jornada mediante controles biométricos: un caso de incoherencia en el Derecho del Trabajo Digital. In M. R. P. Royo & A. T. Signes (Dir.), *Vigilancia y controle en el Derecho del Trabajo Digital* (1.ª Ed., pp. 273-300). Navarra, España: Aranzadi.

Sousa, D. A. e (2018). Registo dos Tempos de Trabalho e Proteção de Dados Pessoais. In M. R. P. Ramalho & T. C. Moreira (Coord.), *Tempo de Trabalho e Tempos de não Trabalho. O Regime Nacional do Tempo de Trabalho à luz do Direito Europeu e Internacional – Estudos APODIT 4* (pp. 117-156). Lisboa: AAFDL Editora.