POLITÉCNICO DE LEIRIA | ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

Dissertação

Mestrado em Solicitadoria de Empresa

A Monitorização do Trabalhador e o RGPD

Carolina Sofia Mendes Ferreira

Leiria, setembro de 2019

Esta página foi intencionalmente deixada em branco

Dissertação

Mestrado em Solicitadoria de Empresa

A Monitorização do Trabalhador e o RGPD

Carolina Sofia Mendes Ferreira

Dissertação de Mestrado realizada sob a orientação do Doutor Jorge Barros Mendes, Professor da Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria.

Leiria, setembro de 2019

Esta página foi intencionalmente deixada em branco

Originalidade e Direitos de Autor

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

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

Esta página foi intencionalmente deixada em branco

Agradecimentos

Ao meu orientador, o Dr. Jorge Barros Mendes, por mesmo tendo mil outras coisas para fazer conseguir dispensar um pouco do seu escasso tempo comigo nesta dissertação e por ser a minha maior referência em matéria de proteção de dados pessoais.

Aos meus pais, por me ensinarem que a liberdade e a independência se conjugam com trabalho e responsabilidade.

À Patrícia, por tudo o que sempre fez por mim e por desde cedo me ter proporcionado a oportunidade de ter uma melhor amiga para brincar, desabafar, aconselhar, chatear e fazer as pazes, a quem chamo de irmã.

Ao meu namorado, por ser o meu suporte diário de felicidade, apoio e motivação. Aquele que me ouve quando estou irritada e está comigo a festejar as vitórias. Aquele que me aguenta nos dias maus e nos dias bons. Aquele que faz parte do meu passado, presente e futuro. O nosso futuro!

A todos os meus amigos, colegas de curso e colegas de trabalho que comigo privaram e tornaram estes 5 anos de mudança e superação, mais leves e fáceis de ultrapassar.

A todos os professores, não só da Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria, mas também do Colégio Dr. Luís Pereira da Costa, por todos os conhecimentos que me transmitiram e por serem um suporte base da nossa sociedade que nem sempre é devidamente reconhecido.

Obrigada, do fundo do coração, a todos os que comigo percorreram este caminho!

Esta página foi intencionalmente deixada em branco

Resumo

A relação laboral inerente à realização de um contrato de trabalho acarreta inúmeros direitos e deveres, tanto para o trabalhador como para a entidade empregadora. A recolha e tratamento de dados pessoais é uma consequência desse contrato.

Sendo o trabalhador a parte mais frágil da relação, visto estar em situação de inferioridade relativamente à entidade para a qual presta a sua atividade, deve ter mecanismos legais para reivindicar os seus direitos e cumprir os seus deveres, o que ocorre por determinação do Código do Trabalho.

Com a instituição do Regulamento Geral de Proteção de Dados esclareceram-se algumas questões relativas à proteção de dados pessoais dos trabalhadores, visto que uma monitorização do trabalhador deve ser realizada com ponderação e no cumprimento de normas legais.

Mais recentemente, Portugal transpôs para a sua ordem jurídica a Lei nº 58/2019, de 8 de agosto, que assegura a execução a nível nacional do Regulamento Geral de Proteção de Dados.

Deste modo, com a presente dissertação de mestrado pretendeu-se analisar as várias vertentes da relação laboral, desde a procura de emprego, a plena execução do contrato de trabalho e a sua cessação. Problematizando o sistema da monitorização do trabalho e o impacto do Regulamento Geral de Proteção de Dados nas relações laborais.

Palavras-chave: “dados pessoais”, “RGPD”, “trabalhador”, “monitorização”, “entidade empregadora”

Esta página foi intencionalmente deixada em branco

Abstract

The labour relationship involved in an employment contract entails countless rights and duties, both for the employee as for the employer. The gathering and processing of personal data is a consequence of such a contract.

Considering employees as the weakest link in the relationship, once there is a position of inferiority towards the employers they work for, employees should have access to legal mechanisms to claim their rights and comply with their duties, as determined by the Labour Code.

When the General Data Protection Regulation was issued, some questions were raised regarding the protection of employees' personal data, since employee monitoring should be performed thoughtfully and considering legal regulations.

Recently, Portugal enacted Law nº 58/2019, of 8th of August, assuring the national enforcement of the General Data Protection Regulation.

Thus, this Master's Thesis intends to examine the diverse angles in a labour relationship, from searching for a job vacancy to the full enforcement of an employment contract and its termination, questioning the labour monitoring system and the impact of the General Data Protection Regulation.

Keywords: "personal data", "GDPR", "employee", "monitoring", "employer"

Esta página foi intencionalmente deixada em branco

Lista de siglas e acrónimos

Ac. – Acórdão

ACT – Autoridade para as Condições do Trabalho

AIPD – Avaliação de Impacto sobre a Proteção de Dados

Al./Als. – Alínea/Alíneas

ARCO – Acceso, Rectificación, Cancelación y Oposición

Art./Arts. – Artigo/Artigos

BYOD – Bring Your Own Device

CC – Código Civil

CDFUE – Carta dos Direitos Fundamentais da União Europeia

CEDH – Convenção Europeia dos Direitos do Homem

CNPD – Comissão Nacional de Proteção de Dados

CPC – Código de Processo Civil

CRCivil – Código do Registo Civil

CRP – Constituição da República Portuguesa

CT – Código do Trabalho

DPO – Encarregado de Proteção de Dados, em inglês "Data Proteccion Officer"

ETT – Empresa de Trabalho Temporário

GT29 – Grupo de Trabalho do Artigo 29º

IEFP – Instituto de Emprego e Formação Profissional

IRCT – Instrumento de Regulamentação Coletiva de Trabalho

MDM – Mobile Device Management

NIF – Número de Identificação Fiscal

NISS – Número de Identificação de Segurança Social

Nº/Nºs – Número/ Números

P./PP. – Página/Páginas

RGPD – Regulamento Geral de Proteção de Dados

UE – União Europeia

WP243 rev.01 – Orientações sobre os encarregados da proteção de dados (EPD)

WP259 rev.01 – Orientações relativas ao consentimento na aceção do Regulamento (EU) 2016/679

WP260 rev.01 – Orientações relativas à transparência na aceção do Regulamento 2016/679

Índice

1. Introdução

Hoje em dia estamos na era digital!

A era em que estamos omnipresentes sem estarmos presentes. A comunicação tornou-se mais simples e impessoal, já que o contacto físico facilmente é substituído pela utilização de meios de comunicação à distância, como *smartphones*.

Por conseguinte, as relações laborais também sofreram alterações. O que antes era realizado em papel, hoje é realizado digitalmente. Noutros tempos, o direito à desconexão não existia por não se revelar necessário. Afinal ao terminar a jornada laboral não existia outro meio de comunicação entre entidade empregadora e trabalhador. Atualmente, a realidade revela-se díspar, nomeadamente com a existência de *smartphones*. Também a comunicação entre trabalhador e entidade empregadora se tornou mais acessível, mas também mais intrusiva da vida pessoal do trabalhador.

O quotidiano laboral também sofreu alterações. Anteriormente, o registo dos tempos de trabalho era realizado pela aposição da assinatura do trabalhador de forma a confirmar o horário de trabalho desempenhado, sendo mais fácil colmatar atrasos e, bem assim, excesso de período normal de trabalho. Atualmente, na maioria das empresas, este registo dos tempos de trabalho não é realizado tendo por base a confiança no trabalhador, mas sim em sistemas biométricos, que funcionam através da impressão digital, da íris ou formato do rosto. Estes sistemas são mais fidedignos, mas também mais invasivos da esfera privada do trabalhador que vê um dado pessoal seu, como a impressão digital, a íris, a constar de uma base de dados da entidade empregadora, motivo pelo qual o trabalhador não se pode desvincular da sua monitorização.

O trabalhador é a parte mais fraca da relação laboral, visto ser subordinado juridicamente da entidade empregadora. Deste modo, a proteção da monitorização dos seus dados pessoais deve ser uma constante diária de todos os que lidam diariamente com os mesmos. Atento o disposto no art. 4º do Regulamento Geral de Proteção de Dados, doravante RGPD, dados pessoais são *toda a informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação,*

dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular. Quer isto dizer que, sendo o trabalhador sujeito a subordinação jurídica por parte de uma entidade empregadora que lida com os seus dados pessoais para o cabal cumprimento do contrato de trabalho, este deve ter especial proteção da sua monitorização desmedida.

Deste modo, o objetivo da presente dissertação passa por uma análise exaustiva da monitorização do trabalhador, problematizando as suas diversas vertentes, em harmonia com o RGPD, a Lei nº 58/2019, de 8 de agosto, o Código do Trabalho, doravante CT, na sua Lei nº 7/2009, de 12 de fevereiro e demais legislação específica.

Esclarecemos que na falta de indicação de norma legal aplica-se o RGPD.

2. Considerações gerais relativas à proteção de dados pessoais dos trabalhadores

O Direito ao Trabalho está consagrado constitucionalmente no art. 58º da Constituição da República Portuguesa, doravante CRP, referindo que todos têm direito ao trabalho. Esse mesmo direito é regulado por normas legais e contratuais, regidas pelo princípio da boa fé de ambas as partes.

O trabalhador por conta de outrem celebra com a sua entidade empregadora um contrato de trabalho escrito. De forma a que a entidade empregadora cumpra o dever de informação que recaí sobre si. Contrato de trabalho *é aquele pelo qual uma pessoa singular se obriga, mediante retribuição, a prestar a sua atividade a outra ou outras pessoas, no âmbito de organização e sob a autoridade destas*, conforme dispõe o art. 11º do CT.

No que ao nosso tema concerne, iremos focar-nos, embora de forma não exaustiva e sem o intuito de os esgotar, nos três grandes pilares do CT português que fazem a ligação ao RGPD, a saber: 1) o direito à reserva da intimidade da vida privada; 2) a subordinação jurídica e; 3) o direito à desconexão.

2.1. Direito à reserva da intimidade da vida privada

O direito à reserva da intimidade da vida privada encontra-se consagrado nos arts. 26º, nº 3 da CRP, 80º, nº 1 do Código Civil, doravante CC, 164º, nº 1, 417º, nº 3, al. b) ambos do Código de Processo Civil, doravante CPC e, em termos laborais, no art. 16º, nº 1 do CT.

Pela invocação destes artigos apercebemo-nos que desde o Direito Constitucional até ao Direito Laboral, o legislador português tem em apreço que a vida privada do cidadão português deve ser objeto de normas específicas, que evidenciem a sua proteção. Neste sentido, o artigo 17º, nº 1, al. a) do CT refere, expressamente, *que o empregador não pode exigir a candidato a emprego ou a trabalhador que preste informações relativas à sua vida privada*, exceto *quando estas sejam estritamente necessárias e relevantes para avaliar da respetiva aptidão no que respeita à execução do contrato de trabalho e seja fornecida por escrito a respetiva fundamentação*.

Neste sentido, podemos concluir que o direito em análise é um direito fundamental e de personalidade. De acordo com o Acórdão do Supremo Tribunal de Justiça[1] "a tutela do direito à intimidade da vida privada desdobra-se em duas vertentes: a protecção contra a intromissão na esfera privada e a proibição de revelações a ela relativas".

No entanto, não estamos perante um direito absoluto, como facilmente compreenderemos analisando o caso de figuras públicas. Vejamos: uma figura pública que prescindiu do seu direito à imagem, isto é, a um direito de personalidade, pode invocar posteriormente que quer ver cumprido o direito à reserva da intimidade da vida privada, quando foi a própria pessoa que o violou? Os direitos de personalidade gozam desta dicotomia, que deve ser analisada casuisticamente.

Em termos laborais, a violação deste direito pode ocorrer de diversas formas, por exemplo, o controlo do uso do telefone e e-mail da empresa para fins pessoais.

2.2. Direito à desconexão

Vivemos na era digital, em que o trabalhador, não raras as vezes, para ser considerado competente tem de estar disponível 24 sobre 24 horas. Precisamente no sentido oposto encontramos o direito à desconexão, que é a faculdade que assiste ao trabalhador de se abstrair do trabalho quando está fora dele.

Este direito não está consagrado expressamente na lei, porém encontramos diversos indícios dele no nosso ordenamento jurídico. A CRP no art. 59º, nº 1, als. b) e d) refere que *todos os trabalhadores, sem distinção de idade, sexo, raça, cidadania, território de origem, religião, convicções políticas ou ideológicas, têm direito a organização do trabalho em condições socialmente dignificantes, de forma a facultar a realização pessoal e a permitir a conciliação da atividade profissional com a vida familiar* e *ao repouso e aos lazeres, a um limite máximo da jornada de trabalho, ao descanso semanal e a férias periódicas pagas*. Assim, podemos concluir que há uma preocupação do legislador em desarticular a vida pessoal da vida profissional.

[1] Ac. com o processo nº 03B2361 (Relator Oliveira Barros), de 25 de setembro de 2002, disponível em: www.dgsi.pt/jstj.nsf/0/0e0db401e6e9d5dc80256dea004e8bba?OpenDocument (consultado pela última vez a 25/03/2019 pelas 21:54)

De igual modo, o CT apresenta vários indícios deste direito, nomeadamente, a limitação temporal do período de trabalho em 8 horas diárias e 40 horas semanais (203º, nº 1), a distinção tácita entre período de descanso e de trabalho (199º) e a atribuição de, pelo menos, um dia de descanso semanal (232º, nº 1). Por outro lado, a lei prevê mecanismos para a entidade empregadora garantir que o trabalhador se mantém disponível mesmo fora do seu período normal de trabalho como, o trabalho suplementar (226º, nº1).

De acordo com Teresa Coelho Moreira, existe a "*divisão tripartida* do dia em 8 horas para trabalhar, 8 horas para dormir e 8 horas para a realização social do trabalhador enquanto pessoa" (Moreira, 2017, p. 7). Este seria o cenário ideal, porém não realista. Se assim o fosse o direito à desconexão seria supérfluo.

A maioria dos trabalhadores acede ao e-mail e ao telefone do trabalho fora do mesmo. Instintivamente haverá a curiosidade de verificar se chegou algum e-mail que pode preocupar e perturbar as ditas "8 horas para a realização social do trabalhador enquanto pessoa".

Esta é a realidade de algumas categorias profissionais. Exceto as que laboram numa fábrica, por exemplo, em que os trabalhadores cumprem o objetivo do dia, tal como encomendas, regressam a casa no final do dia e não têm a preocupação de receber um e-mail ou uma chamada visto que isso não são funções desempenhadas durante o período normal de trabalho.

De acordo com Francisco Liberal Fernandes (2017, p. 15):

> o direito à desconexão significa que o trabalhador deixa de estar (e de sentir) obrigado a permanecer ligado ou disponível durante os seus períodos de descanso para responder às ordens ou solicitações de serviço que lhe são enviadas através dos meios eletrónicos. Porém, para produzir os efeitos que pretendem, este direito não pode limitar-se às relações entre o empregador ou superiores hierárquicos e o trabalhador (dimensão vertical), mas deve ser igualmente oponível aos colegas de trabalho, clientes, fornecedores ou subcontratantes (dimensão horizontal).

No mesmo sentido, Teresa Coelho Moreira refere (Moreira, 2017, p. 12):

> o trabalhador tem direito a não ser incomodado permanentemente na sua vida privada e no seu tempo privado, criando-se um direito ao 'isolamento', à *desconexão*, a um repouso 'efetivo'. Trata-se de uma desconexão técnica que, segundo Jean-Emmanuel Ray é favorável pois os trabalhadores que não têm um tempo livre não se tornam mais produtivos, nem mais *fiéis* à empresa.

Contudo, estamos perante um costume cada vez mais enraizado nos trabalhadores portugueses, isto é, ter hora de entrada, mas não hora de saída. O que deveria ser a exceção tornou-se a regra. Na maioria das situações são realizadas horas extras que não são contabilizadas porque "na maior parte dos casos, não há uma ordem expressa do empregador neste sentido" (Moreira, 2017, p. 14).

Na opinião de Teresa Coelho Moreira, com a qual concordamos, "não podemos deixar de atender que realizar diferentes tarefas simultaneamente pode necessitar de mais tempo e conduzir a mais erros na medida em que existem limites ao processamento mental do Homem" (Moreira, 2017, p. 13). Para além disso, pode desenvolver a Síndrome de *Burnout* que "pode surgir como resposta a um *stress* laboral crónico, perante o qual a pessoa sente que não tem estratégias adaptativas para lidar"[2].

O Acórdão do Tribunal da Relação do Porto[3] refere que "o momento limite entre o 'tempo de trabalho' e o 'tempo de descanso' é aquele em que o trabalhador adquire o domínio absoluto e livre da gestão da sua vida privada". O predito Acórdão vai mais longe e condena a entidade empregadora a uma indemnização por danos não patrimoniais:

> a desorganização da vida pessoal e familiar do trabalhador, os danos causados à sua saúde, por interrupção ou falta de dormir o tempo necessário (num período de 3 anos e 5 meses), e a falta de privacidade, constituem o direito a ser indemnizado por danos não patrimoniais, no montante de €30.000,00.

Face ao exposto concluímos que, a maioria das fontes do direito se encontra em consonância, nomeadamente, a lei, a jurisprudência e a doutrina. No entanto, os usos e costumes parecem sobrepor-se pelas partes mais interessadas no direito à desconexão, os próprios trabalhadores. Não quer isto dizer que, por vezes, não seja a própria entidade empregadora que incentive, pelo exemplo, a trabalhar para além do período normal de trabalho.

[2] Para mais informações ver https://www.saudecuf.pt/mais-saude/artigo/sindrome-de-burnout-os-7-tipos-de-sinais-de-alerta-a-que-deve-estar-atento (consultado pela última vez a 14/08/2019 pelas 21:24)
[3] Ac. com o processo nº 2066/15.0T8PNF.P1 (Relator Domingos Morais), de 24 de janeiro de 2018, disponível em: http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/6cd2c4a6745adb2a8025822e00407c51?OpenDocument (consultado pela última vez a 01/04/2019 pelas 16h40)

2.3. Subordinação jurídica

A subordinação jurídica é típica de um contrato de trabalho subordinado e consiste no poder da entidade empregadora de vincular a prestação de trabalho do trabalhador através de diretivas, ordens e instruções. Em harmonia com o Acórdão do Tribunal da Relação de Coimbra[4]:

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

A entidade empregadora no exercício do poder de direção que lhe é atribuído pode designar o trabalhador ao exercício de funções não compreendidas na atividade contratada, *desde que tal não implique modificação substancial da posição do trabalhador* (art. 120º, nº 1 CT). No entanto, a duração temporal da mobilidade funcional *não deve ultrapassar dois anos* (art. 120º, nº 3 CT) e *salvo disposição em contrário, o trabalhador não adquire a categoria correspondente às funções temporariamente exercidas* (120º, nº 5 CT).

Contudo, o CT no seu art. 119º prevê a mudança do trabalhador para uma categoria inferior àquela para que foi contratado *mediante acordo, com fundamento em necessidade premente da empresa ou do trabalhador, devendo ser autorizada pelo serviço com competência inspetiva do ministério responsável pela área laboral no caso de determinar diminuição da retribuição*, atualmente a Autoridade para as Condições de Trabalho, doravante ACT. Conforme refere Menezes Cordeiro citado no Acórdão do Supremo Tribunal de Justiça[5]:

> A categoria, em Direito do Trabalho, obedece aos princípios da efetividade (relevam as funções substancialmente prefiguradas e não os meros designações exteriores), da irreversibilidade (uma vez alcançada certa

[4] Ac. com o processo nº 5/13.1T4AGD.C1 (Relator Jorge Loureiro), de 3 de abril de 2014, disponível em: http://www.dgsi.pt/jtrc.nsf/8fe0e606d8f56b22802576c0005637dc/812bbe9f7644731c80257cb700486b6c?OpenDocument (consultado pela última vez a 01/04/2019 pelas 19h02)

[5] Ac. com o processo nº 518/14.8TTBRG.G1.S1 (Relator Ferreira Pinto), de 16 de março de 2017, disponível em: http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/02f9eba5bcb19203802580e90031f9e7?OpenDocument (consultado pela última vez a 02/04/2019 pelas 22h02)

> categoria, o trabalhador não pode ser despromovido) e do reconhecimento (através da classificação, a categoria-estatuto deve corresponder à categoria-função de maneira que a categoria estatuto assente nas funções efetivamente desempenhadas)" - (Menezes Cordeiro, Manual de Direito do Trabalho, pág. 669).

Isto é, o trabalhador é a peça móvel da relação laboral subordinada. Porém, o trabalhador goza de autonomia técnica, ou seja, *a sujeição à autoridade e direção do empregador não prejudica a autonomia técnica do trabalhador inerente à atividade prestada, nos termos das regras legais ou deontológicas aplicáveis*, nos termos do art. 116º CT.

De acordo com Júlio Gomes (2007, pp. 320-321):

> é praticamente unânime o entendimento segundo o qual o empregador goza da faculdade de controlar a correta execução da prestação de trabalho. Essa faculdade é, na nossa opinião, um corolário da subordinação jurídica e uma faceta ou aspecto instrumental do poder de direcção, não sendo necessário extraí-la (ou extraí-la também) de um qualquer poder organizativo. O que se passa é que não faria sentido um poder de dar ordens ou instruções desprovido da possibilidade de conferir se essas ordens ou instruções foram efectivamente acatadas.

A subordinação jurídica encontra o seu contraste no poder de direção, sendo esta um corolário da realização de um contrato de trabalho. Concordamos que de outra forma não faria sentido a realização de um contrato de trabalho propriamente dito. Conforme suprarreferido, "não faria sentido um poder de dar ordens ou instruções desprovido da possibilidade de conferir se essas ordens ou instruções foram efectivamente acatadas".

Por último, consideramos que a subordinação jurídica e o poder de direção são duas realidades que devem estar em sintonia para possibilitar a configuração de uma relação laboral saudável. Não devem existir abusos de nenhuma das partes. Porém, a monitorização dos trabalhadores é uma realidade que tem o seu expoente máximo precisamente devido à subordinação jurídica. No entanto, devem ser avaliados os limites do direito da personalidade e da proteção de dados pessoais, sendo que ambos não devem ser violados. Esse é precisamente o mote para a realização da presente dissertação.

3. Princípios do Regulamento Geral de Proteção de Dados e sua aplicabilidade na relação laboral

Desde o dia 4 de maio de 2016[6] que a União Europeia, doravante UE, tem um novo quadro normativo para a proteção de dados pessoais, contrariamente ao que existia até então, em que nos confrontávamos com 28 legislações diferentes, que dificultavam o exercício de direitos por parte dos titulares dos dados. Deste modo, desde 25 de maio de 2018[7], todo o espaço da UE passou a ter um ordenamento jurídico comum nesta matéria.

O Regulamento 2016/679 da UE, designado por RGPD, vem definir o regime jurídico da proteção de dados pessoais, estabelecendo novas obrigações e responsabilidades para todas as entidades, públicas e privadas e foi diretamente aplicável a partir de 25 de maio de 2018, conforme dispõe o art. 99º, nº 2 do predito regulamento.

O RGPD é dirigido a todos aqueles que entram em contacto com dados pessoais, por exemplo, diretores de sistemas de informação, técnicos de informática, auditores internos, empresários, administradores e diretores de empresas, responsáveis de recursos humanos, juristas e todos os profissionais com tarefas que impliquem a recolha e posterior tratamento de dados pessoais.

Contudo, a proteção de dados pessoais já era uma realidade com a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, agora revogada pelo RGPD. Portugal também legislou nesta matéria com a Lei nº 67/98, de 26 de outubro, que foi recentemente revogada pelo art. 66º, nº 1 da Lei nº 58/2019, de 8 de agosto.

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

[6] Data de publicação e entrada em vigor do RGPD.
[7] Data da produção de efeitos do RGPD.

De acordo com a Comunicação da Comissão ao Parlamento Europeu e ao Conselho citado na obra "Comentário ao Regulamento Geral de Proteção de Dados" (Pinheiro, Coelho, Duarte, Gonçalves, & Gonçalves, 2018, p. 9):

> "Os dados são algo cada vez mais valioso para a economia atual e são fundamentais para a vida quotidiana dos cidadãos. As novas regras constituem uma oportunidade única tanto para as empresas como para o público. As empresas, em especial as de menor dimensão, poderão beneficiar de um conjunto de regras único e inovador e «pôr as suas casas em ordem» em termos de dados pessoais para reconquistar a confiança dos consumidores e usar isso como vantagem competitiva na UE. Os cidadãos poderão beneficiar de uma maior proteção em matéria de dados pessoais e conseguir maior controlo sobre a forma como os dados são tratados pelas empresas.
>
> **Num mundo moderno com uma economia digital em crescimento, a União Europeia, os seus cidadãos e as suas empresas devem estar totalmente preparados para colher os benefícios e compreender as consequências da economia de dados. O novo regulamento oferece os instrumentos necessários para preparar a Europa para o século XXI.**"

No entanto, já existiam instrumentos para proteger os dados pessoais, previstos em vários diplomas legais. A Carta dos Direitos Fundamentais da União Europeia, doravante CDFUE, prevê no seu art. 8º que *todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito*. A CRP dispõe no art. 35º que *todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam.*

No âmbito da proteção de dados pessoais de trabalhadores, o CT refere no art. 17º que *o candidato a emprego ou o trabalhador que haja fornecido informações de índole pessoal goza do direito ao controlo dos respetivos dados pessoais, podendo tomar conhecimento do seu teor e dos fins a que se destinam, bem como exigir a sua retificação e atualização.*

Neste sentido, encontramos vários direitos relativos à proteção de dados pessoais, anteriores ao RGPD, que assistem aos trabalhadores na vigência de um contrato de trabalho subordinado: conhecer a finalidade e o direito à sua retificação e atualização. Com a entrada em vigor do RGPD o trabalhador tem acesso a novos direitos que serão abordados de seguida.

3.1. A licitude, finalidade e proporcionalidade da recolha de dados pessoais

Com a entrada em vigor do RGPD tipificaram-se novos fundamentos legais para tornar a recolha de dados e o seu tratamento legítimos.

No art. 6º do RGPD são enumerados os casos em que o tratamento de dados é lícito, este é-o *na medida em que se verifique*m determinadas condições:

> a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;
>
> b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;
>
> c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;
>
> d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;
>
> e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;
>
> f) O tratamento for necessário 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.

No nosso caso em concreto, o contexto laboral, aplicamos a al. b) do predito artigo. Visto que, estamos perante a execução de um contrato de trabalho e "este fundamento pode permitir, por exemplo, o tratamento das informações relativas ao salário e dos dados relativos à conta bancária para que os salários possam ser pagos" (Pinheiro et al., 2018, p. 216). Para não falar da inscrição na Segurança Social, no Fundo de Compensação do Trabalho, no Fundo de Garantia de Compensação do Trabalhado, na Folha de Férias, na apólice do seguro de Acidentes de Trabalho e no processamento de salários pela contabilidade. Contudo, este pode não ser o único fundamento para o tratamento de dados em contexto laboral. Afinal, algumas das situações referidas anteriormente como a inscrição na Segurança Social e o Seguro de Acidentes de Trabalho constituem obrigações jurídicas da entidade empregadora, pelo que nestes casos

aplicamos a al. c). Pese embora poder ser realizada a recolha e o tratamento de dados pessoais com fundamento no consentimento, constante na al. a)[8].

De acordo com o art. 5º, nº 1, al. a) os dados pessoais são *objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados*. Assim, o trabalhador na vigência do contrato de trabalho disponibiliza os seus dados pessoais à entidade empregadora para as finalidades acima elencadas que são legítimas para a plena execução do contrato de trabalho.

Este entendimento é também elencado no considerando 44 do RGPD[9] que refere que *o tratamento deverá ser considerado lícito caso seja necessário no contexto de um contrato ou da intenção de celebrar um* contrato. Face ao exposto, concluímos que o tratamento de dados no contexto de uma relação de trabalho para as finalidades expostas acima é lícito.

Em harmonia com o considerando 4 *o tratamento dos dados pessoais deverá ser concebido para servir as pessoas. O direito à proteção de dados pessoais não é absoluto; deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade.*

O princípio da finalidade previsto na al. b) do nº 1 do art. 5º refere que os dados pessoais são *recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89º, nº 1 («limitação das finalidades»)*. Ou seja, os dados pessoais recolhidos na vigência de um contrato de trabalho apenas são válidos para essa finalidade e todas as outras inerentes à boa execução do mesmo.

De acordo com Alexandre Sousa Pinheiro no Comentário ao Regulamento Geral de Proteção de Dados (Pinheiro et al., 2018, p. 207):

> "o espaço do princípio da finalidade no direito a proteção de dados pessoais é crucial, na medida em que funciona como a primeira justificação para a realização de um tratamento de dados, impondo-se até ao consentimento. A realização de escolha de informação pessoal – ou qualquer outra operação de

[8] Esta matéria será abordada em profundidade no ponto seguinte.
[9] De ora em diante na falta de indicação da origem do considerando aplica-se o RGPD.

> tratamento – deve estar respaldada numa razão-finalidade para, em função dela, se determinar a natureza necessária e não excessiva da informação pessoal recolhida."

Portanto, um dado pessoal que foi recolhido com uma finalidade certa e determinada apenas deve ser utilizado com essa finalidade. De igual modo, "é entendimento doutrinário que julgamos correto considerar que não podem ser armazenados dados pessoais para 'finalidades futuras que ainda não estão previstas no momento da recolha'" (Pinheiro et al., 2018, p. 208).

O considerando 50 vai mais longe e estabelece que *o tratamento para outros fins que não aqueles para os quais os dados pessoais tenham sido inicialmente recolhidos apenas deverá ser autorizado se for compatível com as finalidades para as quais os dados pessoais tenham sido inicialmente recolhidos. Nesse caso, não é necessário um fundamento jurídico distinto do que permitiu a recolha dos dados pessoais*. Isto é, a entidade empregadora celebra um seguro de acidentes de trabalho com determinada seguradora, à qual disponibiliza os dados pessoais dos seus trabalhadores. A entidade empregadora cessa o vínculo com a seguradora e estabelece novo contrato de seguro com uma seguradora distinta. Estamos perante a mesma finalidade pelo que nos parece legítimo que a entidade empregadora transmita os dados pessoais dos seus trabalhadores à nova seguradora. Uma vez que, é compatível com as finalidades para as quais os dados pessoais foram previamente recolhidos. "A questão que se pode colocar corresponde a saber se podem ser utilizados fundamentos jurídicos distintos, não se 'são necessários'." (Pinheiro et al., 2018, p. 209).

No nosso entendimento, consideramos que se os dados pessoais foram recolhidos com a finalidade e o fundamento jurídico da plena execução de um contrato de trabalho, não lhes pode ser dada outra finalidade. Não seria legítimo à luz do RGPD, utilizar os dados recolhidos no âmbito de um contrato de trabalho para fins de marketing e publicidade, por exemplo.

O princípio da proporcionalidade não tem uma definição expressa no RGPD, no entanto, o art. 5º, nº 1, al. c) refere que os dados pessoais são *adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («minimização dos dados»)*.

De acordo com este princípio apenas devem ser recolhidos os dados necessários e suficientes para a finalidade concreta. O considerando 39 refere que *os dados pessoais deverão ser adequados, pertinentes e limitados ao necessário para os efeitos para os quais são tratados.*

Sendo os dados pessoais recolhidos no âmbito de um contrato de trabalho, importa analisar o momento da recolha. Com a entrevista de emprego e sem, *a priori*, saber se o trabalhador ingressará na empresa, parece-nos que apenas faz sentido recolher o número de telemóvel e/ou o e-mail, que normalmente constam do currículo enviado pelo trabalhador. Isto porque, na eventualidade de ser o escolhido para a vaga de emprego tem de existir algum meio de comunicar com o futuro trabalhador. No caso oposto, isto é, não ser a pessoa a preencher a vaga, informar o trabalhador disso mesmo será um ato cordial que concordamos que se enquadre no princípio da proporcionalidade.

No início do contrato de trabalho cabe à entidade empregadora cumprir determinadas obrigações jurídicas como, por exemplo: inscrever o trabalhador na Segurança Social, no Fundo de Compensação do Trabalho e no Fundo de Garantia de Compensação do Trabalho, no seguro de acidentes de trabalho e realizar a consulta de medicina no trabalho.

Durante o contrato de trabalho a entidade empregadora deve realizar as prestações contributivas obrigatórias para a Segurança Social, enviar a folha de férias e as informações relativas ao salário para a contabilidade, preencher o Relatório Único e eventuais inquéritos estatísticos que sejam disponibilizados pelo Instituto Nacional de Estatística.

No término do contrato de trabalho, a entidade empregadora pode conservar os dados pessoais do trabalhador *enquanto não decorrer o prazo de prescrição dos direitos correspetivos*, de forma a *comprovar o cumprimento de obrigações contratuais ou de outra natureza*, ao abrigo do disposto no art. 21º, nº 3 da Lei nº 58/2019, de 8 de agosto. Relativamente aos dados referentes à carreira contributiva para efeitos de reforma, o nº 6 do mesmo artigo não estabelece um limite de prazo.

3.2. O consentimento

De acordo com o Dicionário da Língua Portuguesa,[10] "consentimento" é um substantivo masculino, que exprime a ***manifestação*** (nosso negrito) *que autoriza algo*.

O consentimento é um dos fundamentos legais que possibilita o tratamento de dados pessoais, quando este não é realizado devido a um contrato (art. 6º, nº 1, al. b), uma obrigação jurídica (art. 6º, nº 1, al. c), a interesses vitais (art. 6º, nº 1, al. d), interesse público ou ao exercício da autoridade pública (art. 6º, nº 1, al. e), ou interesses legítimos (art. 6º, nº 1, al. f).

O tratamento baseado no consentimento é lícito em harmonia com o art. 6º, nº 1, al. a). Deste modo, esgotadas todas hipóteses possíveis de tratamento suprarreferidas aplica-se o consentimento, se a este houver lugar.

O art. 4º, nº 11 define consentimento do titular dos dados como *uma **manifestação*** (nosso negrito) *de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco* (nosso sublinhado), *que os dados pessoais que lhe dizem respeito sejam objeto de tratamento*. Desta definição estabelecemos as formalidades que a manifestação de vontade que é o consentimento necessita para ser válido, ou seja, este tem de ser: livre, específico, informado e explícito.

No entanto, em harmonia com o Parecer 15/2011 do Grupo de Trabalho do Artigo 29º[11], doravante GT29, sobre a definição de consentimento (p. 7):

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

[10] https://dicionario.priberam.org/consentimento (consultado pela última vez a 23/04/2019 pelas 16h10)
[11] Grupo instituído ao abrigo do art. 29º da revogada Diretiva 95/46/CE, foi órgão consultivo europeu independente em matéria de proteção de dados e privacidade. Este deu lugar, após 25 de maio de 2018 com a eficácia plena do RGPD, ao Comité Europeu para a Proteção de Dados.

Podemos concluir que, pelo menos, desde 2011 os Estados Membros da UE têm-se esforçado, ainda no âmbito da Diretiva 95/46/CE ora revogada, em definir o conceito de consentimento, que *é comum a outras áreas do direito, em particular do direito das obrigações*, em harmonia com o Parecer 15/2011. Vejamos, em harmonia com o art. 1682º, nº 1 do CC, *a alienação ou oneração de móveis comuns cuja administração caiba aos dois cônjuges carece do* ***consentimento*** (nosso negrito) *de ambos, salvo se se tratar de ato de administração ordinária*. Estando definido no art. 1684º, nº 2 do mesmo diploma que *a forma do consentimento é a exigida para a procuração*, isto é, *instrumento público, por documento escrito e assinado pelo representado com reconhecimento presencial da letra e assinatura ou por documento autenticado*, conforme dispõe o art. 116º, nº 1 do Código do Notariado.

Para além de todas as formalidades acima referidas torna-se evidente que é necessário ocorrer uma **manifestação** expressa por parte do titular dos dados, ou seja, não basta o mero assentimento[12], tem de ocorrer uma "declaração ou ato positivo inequívoco" por parte do titular dos dados, seja uma assinatura, um clique no rato do computador, entre outros. O consentimento não pode ser presumido tem de ser dado sem margem para dúvidas. Assim também o entende Borja Adsuara Varela (2016, p. 152) ao referir as formas de expressar o consentimento: "a) mediante uma declaração e b) mediante uma ação. Logo não há lugar ao (mal) chamado *consentimento tácito*".

De acordo com o GT29, nas "Orientações relativas ao consentimento na aceção do Regulamento (EU) 2016/679"[13], doravante WP259 rev.01, "o elemento «livre» implica uma verdadeira escolha e controlo para o titular dos dados. Regra geral (nosso sublinhado), o RGPD prevê que se o titular dos dados não puder exercer uma verdadeira escolha, se sentir coagido a dar o consentimento ou sofrer consequências negativas caso não consinta, então o consentimento não é válido".

O elemento "livre" em contexto laboral é difícil de comprovar "atendendo à dependência (subordinação jurídica) que resulta da relação empregador/trabalhador. É improvável que o titular dos dados possa recusar ao seu empregador o consentimento para o tratamento dos dados sem que haja medo ou risco real de consequências negativas

[12] Ato de assentir. Anuência. https://dicionario.priberam.org/assentimento (consultado pela última vez a 23/04/2019 pelas 16h18)

[13] Cfr. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 (consultado pela última vez a 22/10/2018 pelas 10:20)

decorrentes da recusa", conforme dispõe o WP259 rev.01 (p. 7). Assim, no âmbito laboral "ou o tratamento é necessário à execução de um contrato, ou deverá ser obtido o consentimento (livre)", de acordo com o Parecer 15/2011 (p. 9).

Em harmonia com Carlos Domènech (2017, p. 157) "o recurso ao consentimento deve limitar-se aos casos em que o trabalhador pode expressar-se de forma totalmente livre e tenha a possibilidade de retificar posteriormente sem ser prejudicado por isso". Vejamos o exemplo 5 do WP259 rev.01 (p. 8):

> Uma equipa de filmagem pretende filmar determinada parte de um escritório. O empregador solicita o consentimento de todos os trabalhadores que se sentam nessa zona do escritório para serem filmados, uma vez que podem aparecer em segundo plano nas filmagens do vídeo. Os trabalhadores que não quiserem ser filmados não serão de forma alguma penalizados, uma vez que serão colocados noutro local de trabalho equivalente numa outra zona do edifício enquanto durar a filmagem.

No exemplo acima, o consentimento é dado de forma totalmente livre. Afinal não existe nenhuma consequência para quem não o der. Simplesmente serão colocados noutro local de trabalho enquanto decorrer a filmagem, o que nos parece legítimo. Diferente seria se a entidade empregadora ao solicitar o consentimento, informasse que quem não o prestasse sofreria uma penalização na remuneração desse mês, aí estaríamos perante uma pressão por parte da entidade empregadora. Esta posição é apoiada pelo WP259 rev.01 (p.8) que refere que "o consentimento não será dado livremente nos casos em que exista qualquer elemento de obrigatoriedade, pressão, incapacidade de exercício da livre vontade".

Importa ainda avaliar *com a máxima atenção* se *a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato*, conforme dispõe o art. 7º, nº 4. De acordo com o considerando 43:

> **presume-se** (nosso negrito) que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução.

Assim, "o RGPD assegura que o tratamento dos dados pessoais relativamente ao qual se solicita o consentimento não pode ser direta ou indiretamente uma contrapartida da execução de um contrato", isto é "procura assegurar que a finalidade do tratamento dos dados pessoais não está camuflada nem agregada à execução de um contrato ou à prestação de um serviço para os quais esses dados pessoais não são necessários", conforme dispõe o WP259 rev.01 (p. 8).

O Parecer 1/2017 do GT29 sobre a proposta de regulamento relativo à privacidade e às comunicações eletrónicas (2002/58/CE)[14] (p. 10) saúda a clarificação que "**o acesso e a telefonia (móvel) são serviços essenciais e que os prestadores desses serviços não podem «<u>obrigar</u>» os seus clientes a dar o seu consentimento para quaisquer operações de tratamento de dados desnecessárias para a prestação do serviço essencial em si**". Esse parecer remete-nos para o considerando 18 que refere que o RGPD não se aplica a atividades exclusivamente pessoais ou domésticas. Todavia, aplica-se aos responsáveis pelo tratamento e subcontratantes que forneçam os meios para o tratamento dos dados pessoais dessas atividades pessoais ou domésticas.

Resumindo, o GT29 no WP259 rev.01 (p. 9) refere que:

> o artigo 7º, nº 4, só é aplicável se os dados solicitados **não** forem necessários para a execução do contrato (incluindo a prestação de um serviço) e a execução desse contrato ficar subordinada à obtenção desses dados com base no consentimento. Em contrapartida, se o tratamento **for** necessário para a execução do contrato (incluindo a prestação de um serviço), então o art. 7º, nº 4, não é aplicável

No contexto laboral, de acordo com o WP259 rev.01 (p. 9):

> este fundamento pode permitir, por exemplo, o tratamento das informações relativas ao salário e dos dados relativos à conta bancária para que os salários possam ser pagos. Tem de existir uma relação direta e objetiva entre o tratamento dos dados e a finalidade da execução do contrato.

Vejamos o exemplo 6 do mesmo parecer (pp. 9 – 10):

> Um banco solicita aos clientes consentimento para que terceiros possam utilizar os seus dados de pagamento para fins de comercialização direta. Esta atividade de tratamento não é necessária para a execução do contrato nem para a prestação dos serviços bancários normais. Se a recusa do cliente em consentir o tratamento para estes fins implicar a não prestação dos serviços

[14]Cfr. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610140 (consultado pela última vez a 25/04/2019 pelas 17:32)

> bancários, o encerramento da conta bancária ou, dependendo do caso, um aumento de comissões, o consentimento não pode ser dado livremente.

Isto quer dizer que o consentimento para o tratamento de dados pessoais é prestado livremente quando o portador dos dados não sofre nenhum tipo de consequência se não o prestar. "A final, não existem consentimentos obrigatórios", conforme refere Alexandre Sousa Pinheiro (2018, p. 167).

Esclarece ainda o Parecer 1/2017 do GT29 (p. 33) que as normas do RGPD "são igualmente aplicáveis aos utilizadores finais que sejam pessoas coletivas. No entanto, "o empregador não pode, na maioria dos casos, dar o seu consentimento em nome dos seus trabalhadores (…) dada a relação de poder desigual (…) esse consentimento não será válido na medida em que não foi prestado de forma livre".

O WP259 rev.01 (p.10) estabelece que:

> Em todo o caso, o ónus da prova no artigo 7º, nº 4 recai sobre o responsável pelo tratamento. Esta norma reflete o **princípio geral da responsabilização** (nosso negrito) que permeia todo o RGPD. Contudo, quando o artigo 7º, nº 4, for aplicável, será mais difícil para o responsável pelo tratamento provar que o consentimento foi dado de livre vontade pelo titular dos dados.

Deste modo, o responsável pelo tratamento no momento da recolha dos dados pessoais tem de estabelecer uma forma de o consentimento ser prestado pelo titular dos dados de forma inequívoca e irrepreensível. De forma a comprovar a qualquer momento que o consentimento foi prestado livremente e sem qualquer tipo de pressão, invocação de qualquer tipo de prejuízo, entre outros. Deste modo, de acordo com o mesmo parecer (p. 10):

> o consentimento não pode ser considerado livre se o responsável pelo tratamento alegar que existe uma escolha entre o seu serviço que inclui consentimento para a utilização dos dados pessoais para **fins complementares** (nosso negrito), por um lado, e um serviço equivalente oferecido por um responsável pelo tratamento diferente, por outro.

Em harmonia com o suprarreferido, podemos concluir que o consentimento não seria prestado livremente e, por conseguinte, de harmonia com o RGPD.

De acordo com Alexandre Sousa Pinheiro (2018, p. 167):

> O titular dos dados não pode ficar numa posição de coação na celebração de contratos ou de qualquer outra forma de aceder a bens ou serviços.
>
> Ou seja, não pode ficar privado do acesso a um bem ou serviço se não consentir no tratamento de dados para finalidades distintas daquelas que estão a ser prosseguidas com a sua aquisição originária.

Retomemos o exemplo 5[15] do WP259 rev.01. Nesse caso não há qualquer prejuízo para os trabalhadores que decidem ir para outra sala, e consequentemente, não serem filmados. Os que optaram por ficar não serão beneficiados, nem prejudicados, assim como os que decidiram ir para outra sala. No entanto, tendo em conta que o ónus da prova recai sobre o responsável pelo tratamento, o consentimento deveria ser prestado através de um formulário escrito, de forma a futuramente ser possível comprovar que o consentimento foi efetivamente prestado livremente.

Todavia, "o RGPD não deve ser interpretado de forma a colocar em crise comportamentos sociais habituais que moldam a vida nas comunidades que compõem os Estados-Membros", isto é, o RGPD não deve ser um "elemento bloqueador da informalidade social" (Pinheiro et al., 2018, p. 169). Assim, na opinião deste autor, com a qual concordamos, a prestação de consentimento por escrito "dependerá da ocasião social em que for exigida". Sendo que, "no caso do consentimento oral, o elemento testemunhal pode substituir a necessidade de gravar declarações, o que só por si já constitui um tratamento de dados com caráter significativo e sensível" (Pinheiro et al., 2018, p. 169).

O consentimento deve ainda beneficiar de granularidade, pois "um serviço pode envolver múltiplas operações de tratamento para mais do que uma finalidade. Nestes casos, os titulares dos dados devem poder escolher quais são as finalidades que aceitam e não ter de dar consentimento para um conjunto de finalidades de tratamento", em harmonia com o parecer em análise (p. 11). Isto quer dizer, que não é admissível um pedido de consentimento genérico para todo e quaisquer fins.

De acordo com Alexandre Sousa Pinheiro (2018, p. 168), "a especificidade do consentimento apresenta uma relação muito clara com a finalidade ou o conjunto de finalidades prosseguido. Neste sentido concretiza de forma mais próxima do princípio da

[15] Ver pág. 17.

finalidade a característica de 'liberdade' do consentimento". Reparemos no exemplo 7 do WP259 rev.01 (p. 11):

> Num mesmo pedido de consentimento, o retalhista solicita aos clientes consentimento para utilizar os dados destes para lhes enviar publicidade via correio eletrónico e também para partilhar esses dados com outras empresas do grupo. Este consentimento não é granular, uma vez que não separa os consentimentos para estas duas finalidades distintas; por conseguinte, o consentimento não é válido. Neste caso, deve ser recolhido um consentimento específico para enviar os dados de contacto dos clientes para os parceiros comerciais. Esse consentimento específico será considerado válido para cada parceiro (…), cuja identidade tem de ser fornecida ao titular dos dados aquando da recolha do seu consentimento, desde que lhes seja enviado com a mesma finalidade (neste exemplo: a finalidade é a publicidade).

Isto é, "esta granularidade está estritamente relacionada com a necessidade de o consentimento ser específico". Deste modo "quando o tratamento dos dados for realizado procurando alcançar várias finalidades, a solução para satisfazer as condições inerentes a um consentimento válido passa pela granularidade, ou seja, a separação dessas finalidades e a obtenção de consentimento para cada uma das delas", em harmonia com o parecer suprarreferido.

O art. 6º, n.º 1, al. a) refere que o tratamento só é lícito se *o titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades* ***específicas*** (nosso negrito). De acordo com o WP259 rev.01 (p. 13):

> Este requisito (…) permanece estreitamente ligado ao requisito de «consentimento informado». Ao mesmo tempo, deve ser interpretado em consonância com o requisito de «granularidade» aquando da obtenção de consentimento «livre». Resumindo, para cumprir o elemento «específico», o responsável pelo tratamento deve aplicar:
>
> i) Especificidade em função da finalidade como salvaguarda contra o desvirtuamento da função,
> ii) Granularidade nos pedidos de consentimento, e
> iii) Separação clara entre as informações relacionadas com a obtenção de consentimento para atividades de tratamento de dados e as informações sobre outras questões.
>
> (…)
>
> Em consonância com o conceito de *limitação da finalidade*, com o artigo 5.º, n.º 1, alínea b), e com o considerando 32, o consentimento pode abranger operações diferentes, desde que essas operações sirvam a mesma finalidade.

Assim, se posteriormente à recolha dos dados pessoais para uma finalidade específica surgir uma nova finalidade, deverá ser obtido novo consentimento para essa

finalidade, "exceto se existir outro fundamento legal que reflita melhor a situação", em harmonia com o mesmo parecer.

No âmbito da retirada/revogação do consentimento o RGPD é claro *o consentimento deve ser tão fácil de retirar quanto de dar*, conforme dispõe o art. 7º, nº 3. Assim, o titular dos dados não pode ser prejudicado pela retirada do consentimento, caso contrário não podemos considerar que o consentimento foi prestado de livre vontade. Assim, em harmonia com o considerando 42 "não se deverá considerar que o consentimento foi dado de livre vontade se o titular dos dados não dispuser de uma escolha verdadeira ou livre, ou não puder **recusar** (nosso negrito), nem **retirar** (nosso negrito) o consentimento sem ser prejudicado".

Para melhor compreensão, vejamos o exemplo 8 do WP259 rev.01 (p. 12):

> Ao descarregar uma aplicação para telemóvel relativa a hábitos de vida, a aplicação solicita consentimento para aceder ao acelerómetro do telefone. Não se trata de algo necessário para a aplicação funcionar, mas é útil para os responsáveis pelo tratamento que pretendem saber mais acerca dos movimentos e dos níveis de atividade dos utilizadores. Posteriormente, se a utilizadora revogar esse consentimento, descobre que a aplicação só funciona parcialmente. Estamos perante um exemplo de prejuízo na aceção do considerando 42, o que significa que o consentimento **nunca foi obtido validamente** (nosso negrito) (e logo, o responsável pelo tratamento tem de apagar todos os dados pessoais acerca dos movimentos dos utilizadores recolhidos desta forma).

Com este exemplo concluímos que, o consentimento deve ser retirado sem prejuízos e "sem ter que alegar ou provar a existência de uma causa justificativa, do mesmo modo que não teve nem de alegar nem de provar uma causa ao interessado para prestar o seu consentimento", (Mañas et al., 2016, p. 161). No entanto, a retirada do consentimento não tem efeitos retroativos. Esta "não compromete a licitude do tratamento efetuado com base no consentimento previamente dado", em harmonia com o art. 7º, nº 3.

Assim, "regra geral, se o consentimento for retirado, todas as operações de tratamento de dados baseadas nesse consentimento e que ocorreram antes da retirada do consentimento (…) permanecem lícitas". Por conseguinte, "o responsável pelo tratamento deve parar as ações de tratamento em causa". No entanto, "a retirada do consentimento não significa que o responsável pelo tratamento tenha de apagar os dados

tratados para uma finalidade que se baseia na execução do contrato celebrado com o titular dos dados", em harmonia com o WP259 rev.01 (p. 25).

Relativamente às condições aplicáveis ao consentimento, podemos resumir em cinco pontos elencados por Alexandre Sousa Pinheiro (2018, p. 172):

> a. Compete ao responsável pelo tratamento provar a prestação do consentimento pelo titular dos dados (n.º 1);
> b. Os pedidos de consentimento devem encontrar-se formulados de um modo claro e simples, distinguindo-se as solicitações de consentimento de outras matérias eventualmente contidas em declarações escritas (n.º 2);
> c. O titular dos dados pode retirar o consentimento, a qualquer momento, considerando-se lícitos os tratamentos até aí feitos com base nesta condição de legitimidade (n.º 3);
> d. O consentimento deve ser tão fácil de retirar quanto de fornecer (n.º 3);
> e. Deve verificar-se se a prestação de certo serviço está dependente da recolha de atos de consentimento que respeitem a dados pessoais que não sejam necessários para a execução desse contrato (n.º 4).

3.3. Os novos direitos dos titulares dos dados estabelecidos no RGPD

O RGPD estabeleceu novos direitos aos titulares dos dados nomeadamente: direito de informação sobre o tratamento de dados (arts. 13º e 14º); direito de acesso (art. 15º) e o procedimento equitativo para tal acesso (art. 12º/2 e ss.); direito de retificação, limitação e apagamento (arts. 16º, 18º, 17º + 19º); direito de portabilidade de dados (art. 20º + 12º/3 e ss.). Para além disso, o RGPD incluiu o princípio da transparência que consuma o exercício dos direitos referidos.

O princípio da transparência não se encontra definido no RGPD, no entanto o considerando 39 estabelece como deve ser cumprido o tratamento de dados de forma transparente, que passamos a citar:

> Deverá ser transparente para as pessoas singulares que os dados pessoais que lhes dizem respeito são recolhidos, utilizados, consultados ou sujeitos a qualquer outro tipo de tratamento e a medida em que os dados pessoais são ou virão a ser tratados. O princípio da transparência exige que as informações ou comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples.

O direito de informação sobre o tratamento de dados coaduna-se em verdadeiras "*checklists*" a cumprir e a renovar, quando assim for necessário. Este direito subdivide-

se em *informações a facultar quando os dados pessoais: são recolhidos junto do titular* **ou** *não são recolhidos junto do titular*, arts. 13º e 14º, respetivamente.

Deste modo, o art. 13º refere, de forma taxativa, as informações que o responsável pelo tratamento tem de facultar ao titular dos dados aquando da recolha desses dados, que passamos a citar:

> a) A identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante;
>
> b) Os contactos do encarregado da proteção de dados, se for caso disso;
>
> c) As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;
>
> d) Se o tratamento dos dados se basear no artigo 6º, nº 1, alínea f), os interesses legítimos do responsável pelo tratamento ou de um terceiro;
>
> e) Os destinatários ou categorias de destinatários dos dados pessoais, se os houver;
>
> f) Se for caso disso, o facto de o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação adotada pela Comissão ou, no caso das transferências mencionadas nos artigos 46º ou 47º, ou no artigo 49º, nº 1, segundo parágrafo, a referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas.
>
> (…)
>
> a) Prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse prazo;
>
> b) A existência do direito de solicitar ao responsável pelo tratamento acesso aos dados pessoais que lhe digam respeito, bem como a sua retificação ou o seu apagamento, e a limitação do tratamento no que disser respeito ao titular dos dados, ou do direito de se opor ao tratamento, bem como do direito à portabilidade dos dados;
>
> c) Se o tratamento dos dados se basear no artigo 6º, nº 1, alínea a), ou no artigo 9º, nº 2, alínea a), a existência do direito de retirar consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado;
>
> d) O direito de apresentar reclamação a uma autoridade de controlo;
>
> e) Se a comunicação de dados pessoais constitui ou não uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o titular está obrigado a fornecer os dados pessoais e as eventuais consequências de não fornecer esses dados;
>
> f) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22º, nºs 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.

> 3. Quando o responsável pelo tratamento de dados pessoais tiver a intenção de proceder ao tratamento posterior dos dados pessoais para um fim que não seja aquele para o qual os dados tenham sido recolhidos, antes desse tratamento o responsável fornece ao titular dos dados informações sobre esse fim e quaisquer outras informações pertinentes, nos termos do nº 2.

Por sua vez, quando os dados *não são recolhidos junto do titular* para além das informações suprarreferidas, acrescem as seguintes alíneas aos nºs 1 e 2, respetivamente:

> d) As categorias dos dados pessoais em questão;
>
> (…)
>
> b) A origem dos dados pessoais e, eventualmente, se provêm de fontes acessíveis ao público.

Os artigos em análise são unânimes quando referem que nenhuma destas alíneas se aplica *quando e na medida em que o titular dos dados já tenha conhecimento das informações*. No entanto, o art. 14º diverge e refere que as alíneas referidas também não se aplicam quando *se comprove a impossibilidade de disponibilizar a informação, o esforço envolvido seja desproporcionado, seja suscetível de tornar impossível ou prejudicar gravemente a obtenção dos objetivos desse tratamento, a obtenção ou divulgação esteja expressamente prevista no direito da União ou do Estado-Membro, os dados devam permanecer confidenciais em virtude de uma obrigação de sigilo profissional*.

Em Portugal, a atividade do Solicitador é objeto de sigilo profissional ao abrigo do disposto nos arts. 127º e 141º do Estatuto da Ordem dos Solicitadores e dos Agentes de Execução. Como tal, à atividade do Solicitador é dispensada a aplicação do art. 14º.

Em harmonia com Alexandre Sousa Pinheiro (2018, p. 348), "o direito à informação pressupõe uma posição ativa por parte do responsável pelo tratamento e não uma ação indagatória por parte do titular dos dados". Quer isto dizer, que a iniciativa de ver cumprido o direito de informação tem de partir do responsável pelo tratamento, afinal é a ele que incumbe o ónus da prova, em matéria de consentimento, e aqui consideramos que o legislador pretendeu obter a mesma finalidade, a responsabilização do responsável pelo tratamento.

Apesar de o consentimento e o direito de informação serem duas realidades distintas, são frequentemente confundidas, pelo que importa distinguir ambas: o

consentimento é uma das finalidades possíveis de tratamento; por sua vez, o direito de informação "figura como uma posição ativa dos titulares dos dados que não carece, por natureza, de qualquer consentimento" (Pinheiro et al., 2018, p. 349).

Podemos considerar o direito de informação simultaneamente como um dever, como já acontece nas Cláusulas Contratuais Gerais, nomeadamente no art. 6º. Isto porque o titular dos dados tem o direito de informação sobre o modo de tratamento dos seus dados e, simultaneamente, sobre o responsável pelo tratamento impende o dever de informação ao titular dos dados sobre o tratamento que será efetuado. Este direito e dever é a simbiose perfeita da recolha de dados pessoais, independentemente de serem, ou não, recolhidos junto do titular.

O art. 13º, nº 3 admite a possibilidade do tratamento de dados *para um fim que não seja aquele para o qual os dados tenham sido* (inicialmente) *recolhidos*. Conforme já admitia o art. 5º, nº 1, al. b), isto é "o tratamento de dados com finalidades não incompatíveis com a finalidade originária do tratamento" (Pinheiro et al., 2018, p. 349). Por sua vez, o considerando 61 esclarece que ***antes*** (nosso negrito) *desse tratamento o responsável pelo tratamento deverá fornecer ao titular dos dados informações sobre esse fim e outras informações necessárias*.

No entanto, quando os dados não são recolhidos junto do titular, o art. 14º, nº 3 difere, referindo que as informações suprarreferidas devem ser comunicadas ao titular dos dados *num prazo razoável após a obtenção dos dados pessoais, mas o mais tardar no prazo de um mês* (al. a)), ou *o mais tardar no momento da primeira comunicação ao titular dos dados* (al. b)), ou ainda, *o mais tardar aquando da primeira divulgação desses dados* (al. c)). O GT29 nas "Orientações relativas à transparência na aceção do Regulamento 2016/679"[16], doravante WP260 rev.01, esclarece que "em todo o caso, o prazo-limite máximo no qual as informações relativas ao artigo 14.º devem ser comunicadas a um titular dos dados é um mês". Contudo, o GT29 (p. 18) alerta os responsáveis pelo tratamento que devem ser consideradas:

> as expectativas razoáveis dos titulares dos dados, os efeitos que o tratamento possa vir a ter sobre eles e a capacidade dos titulares dos dados para exercerem os seus direitos em relação a esse tratamento quando decidem o momento em que comunicam as informações relativas ao artigo 14º.

[16] Cfr. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 (consultado pela última vez a 06/05/2019 pelas 16:51)

Assim, e de forma racional, o WP260 rev.01 (p. 18) refere que "a responsabilidade exige que os responsáveis pelo tratamento demonstrem a lógica subjacente à sua decisão e justifiquem por que razão as informações foram comunicadas no momento em que foram". Deste modo, concluímos que, pode ser livremente fixado, desde que não ultrapasse um mês, o prazo para o cumprimento do direito de informação, que deve ser analisado casuisticamente, até porque o titular dos dados já pode ter conhecimento das informações e aí já não se aplica, conforme refere o art. 14º, nº 5, al. a).

De seguida vamos analisar o direito de acesso do titular dos dados, que se encontra no art. 15º e estipula 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 de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais e às seguintes informações:
>
> a) As finalidades do tratamento dos dados;
>
> b) As categorias dos dados pessoais em questão;
>
> c) Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais;
>
> d) Se for possível, o prazo previsto de conservação dos dados pessoais, ou, se não for possível, os critérios usados para fixar esse prazo;
>
> e) A existência do direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação do tratamento dos dados pessoais no que diz respeito ao titular dos dados, ou do direito de se opor a esse tratamento;
>
> f) O direito de apresentar reclamação a uma autoridade de controlo;
>
> g) Se os dados não tiverem sido recolhidos junto do titular, as informações disponíveis sobre a origem desses dados;
>
> h) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.o, 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.

Isto é, o direito de informação e o direito de acesso estão intrinsecamente relacionados. Embora o primeiro esteja previsto constitucionalmente no art. 35º, nº 1 que dispõe que *todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito*. Sendo que o nº 7 do predito artigo esclarece que *os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica*.

O direito de acesso é a porta de entrada para outros direitos fundamentais ao nível da proteção de dados pessoais. De acordo com Carlos Jorge Gonçalves (Pinheiro et al., 2018, p. 359)

> O direito de acesso do titular dos dados queda-se a montante de outros direitos, tornando-se basilar no exercício de direitos consignados sistematicamente nos artigos subsequentes (…) é aquele que permite o exercício posterior de outros direitos, tais como o direito de retificação, o direito de apagamento, o direito à limitação do tratamento, o direito de portabilidade e o direito de oposição.

Dado o mote para a análise de outros direitos, comecemos pelo direito de retificação previsto no art. 16º que se coaduna com a possibilidade conferida ao titular dos dados de retificar os dados pessoais inexatos que lhe digam respeito, *sem demora injustificada*. Esta retificação pode ser efetuado *por meio de uma declaração adicional*.

No entanto, não podemos interpretar este direito somente no âmbito da existência de dados pessoais inexatos. Afinal ao titular dos dados deve ser admitida a possibilidade de ”que os dados pessoais a seu respeito sejam corretos, exatos, completos e atuais”, (Pinheiro et al., 2018, p. 363). Isto é, “o exercício do direito de retificação em sentido amplo, atenta a evolução quotidiana da situação do respetivo titular, deverá abranger o direito de atualização de dados pessoais, tais como: morada, telefone, endereço de correio eletrónico, habilitações académicas, experiência profissinal, etc.”, em consonância com a mesma obra (p. 365).

O considerando 59 estabelece que o responsável pelo tratamento deve possibiliar ao titular dos dados o exercício desse direito por via eletrónica, “em especial quando os dados sejam também tratados por essa via”. Sendo obrigado a responder ao pedido de retificação “sem demora injustificada e o mais tardar no prazo de um mês e expor as suas razões quando tiver intenção de recusar o pedido”.

Em harmonia com Carlos Jorge Gonçalves, “em caso de deferimento do pedido, o responsável, na resposta ao titular, deverá identificar, clara e inequivocamente, quais os dados objeto de retificação, completação ou atualização”. Por outro lado, se existir a possibilidade do indeferimento do pedido de retificação, o responsável pelo tratamento deverá “notificar o respetivo titular desse projeto de indeferimento para facultar a possibilidade de correção do pedido formulado”. Na inércia do responsável pelo tratamento, este “informa-o sem demora e, o mais tardar, no prazo de um mês a contar da data de receção do pedido, das razões que o levaram a não tomar medidas e da

possibilidade de apresentar reclamação a uma autoridade de controlo e intentar ação judicial", (Pinheiro et al., 2018, pp. 363-364).

Em caso de demora ou, inclusive, recusa por parte do responsável pelo tratamento em satisfazer o pedido do titular dos dados, deverá ser indicado, por forma a ser aceite, um justo impedimento. De acordo com o art. 140º do CPC, considera-se «justo impedimento»: *o evento não imputável à parte nem aos seus representantes ou mandatários que obste à prática atempada do ato*; devendo logo ser oferecida a prova respetiva.

Outro direito que assiste ao titular dos dados é o «direito à limitação do tratamento» que consiste na "inserção de uma marca nos dados pessoais conservados com o objetivo de limitar o seu tratamento no futuro". O art. 18º admite a limitação do tratamento a pedido do titular dos dados nas seguintes situações:

> a) Contestar a exatidão dos dados pessoais, durante um período que permita ao responsável pelo tratamento verificar a sua exatidão;
>
> b) O tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização;
>
> c) O responsável pelo tratamento já não precisar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial;
>
> d) Se tiver oposto ao tratamento nos termos do artigo 21º, nº 1, até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados.

O pedido de limitação do tratamento pode ser indeferido com os seguintes fundamentos: "(i) impossibilidade de verificar a identidade do requerente (cfr. nº 6 do artigo 12º)), (ii) falta de junção de procuração ou junção de documento sem poderes suficientes para a prática deste ato e (iii) falta de concretização do pedido, isto é, dos dados pessoais sobre os quais pretende o exercício do direito", (Pinheiro et al., 2018, p. 372).

Todavia, apesar da possibilidade do tratamento dos dados ser limitado, e disso ser informado pelo responsável pelo tratamento o titular dos dados (nº 3). Existem circunstâncias previstas no nº 2 e somente essas, já que "a anteposição do advérbio 'só' (…) indica que tal elenco é taxativo", (Pinheiro et al., 2018, p. 372), em que os dados pessoais podem ser tratados em momento posterior ao exercício do direito à limitação do

tratamento, nomeadamente: *com o consentimento do titular*; *para efeitos de declaração, exercício ou de defesa de um direito num processo judicial*, *de defesa dos direitos de outra pessoa singular ou coletiva; ou por outros motivos ponderosos de interesse público da União ou de um Estado-Membro*.

O RGPD prevê ainda o «direito a ser esquecido», que na era contemporânea se trata de um verdadeiro luxo, na real aceção da palavra. Afinal, estamos na era digital, na qual a facilidade com que se acede a dados pessoais é enorme. Costuma-se, inclusive, dizer, vulgarmente, que o que vai para a Internet fica na Internet, para sempre.

No entanto, o art. 17º estabelece o «direito ao apagamento dos dados» que se resume ao *apagamento dos seus dados pessoais, sem demora injustificada*, por parte do responsável pelo tratamento a pedido do titular dos dados. Este "deverá ser realizada pelo responsável sem demora injustificada, salvo, porventura, o justo impedimento ou a deficiente formulação do pedido. Em qualquer caso, o responsável deverá responder (…) no prazo de um mês (…) e fundamentar a sua decisão se o pedido for indeferido", (Pinheiro et al., 2018, p. 367).

O exercício do direito em análise terá de ser fundamentado nas alíneas do nº 1 do art. 17º, que são:

> a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento;
>
> b) O titular retira o consentimento em que se baseia o tratamento dos dados nos termos do artigo 6º, nº 1, alínea a), ou do artigo 9º, nº 2, alínea a) e se não existir outro fundamento jurídico para o referido tratamento;
>
> c) O titular opõe-se ao tratamento nos termos do artigo 21º, nº 1, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21º, nº 2;
>
> d) Os dados pessoais foram tratados ilicitamente;
>
> e) Os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito;
>
> f) Os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8º, nº 1.

Em todos estes casos existe a possibilidade do exercício do direito ao apagamento. Porém, este direito não é tão linear como até aqui se deu a entender. Afinal, tornar-se-ia muito fácil não pagar, por exemplo, a conta da luz, bastaria solicitar à entidade prestadora

do serviço o apagamento dos seus dados na altura da faturação da eletricidade, que a fatura nunca chegaria à posse do titular dos dados e, por conseguinte, nunca entraria em mora. Celebrar-se-ia um novo contrato de fornecimento de eletricidade todos os meses e nunca se entraria em mora. Ora, o legislador europeu precaveu-se em relação a essas situações e elencou uma série de situações em que o suprarreferido não se aplica, isto é, em que não se pode exercer o direito a ser esquecido, na medida em que o tratamento se revela necessário.

Estes casos estão previstos no nº 3 e são: o exercício da liberdade de expressão e de informação (al. a)); o cumprimento de uma obrigação legal, o exercício de funções de interesse público, o exercício da autoridade pública de que esteja investido o responsável pelo tratamento (al. b)); por motivos de saúde pública (al. c)); fins de arquivo de interesse público, investigação científica, histórica ou fins estatísticos (al. d)); e, por último, para efeitos de declaração, exercício ou defesa de um direito num processo judicial (al. e)).

No âmbito laboral, com o término do contrato de trabalho e o pagamento de todos os créditos salariais a entidade empregadora deverá conservar os dados do trabalhador até à entrega do Relatório Único, previsto na Portaria nº 55/2010, de 21 de janeiro. Trata-se, portanto, de uma obrigação legal, que deverá ser cumprida durante o período de 16 de março a 15 de abril, ao abrigo do disposto no art. 4º, nº 1 da referida portaria. Quer isto dizer, que um trabalhador que cesse funções a 30 de abril só no ano seguinte é que poderá ver os seus dados apagados da base de dados da entidade empregadora.

Sendo que, a iniciativa de apagar os dados do (ex-) trabalhador deverá ser da entidade empregadora, visto que *os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento*, conforme prevê o nº 1, al. a).

Na via eletrónica, *quando o responsável pelo tratamento tiver tornado público os dados pessoais e for obrigado a apagá-los nos termos do nº 1, toma as medidas que forem razoáveis, incluindo de caráter técnico, tendo em consideração a tecnologia disponível e os custos da sua aplicação, para informar os responsáveis pelo tratamento efetivo dos dados pessoais de que o titular dos dados lhes solicitou o apagamento das ligações para esses dados pessoais, bem como das cópias ou reproduções dos mesmos*, conforme prevê o nº 2 e o considerando 66. Quer isto dizer que estamos perante o "direito a ser esquecido em linha, que se consubstancia na adoção de medidas técnicas, por parte do responsável

pelo tratamento, para informar outros sítios web de que determinado titular requereu o apagamento dos seus dados pessoais", (Pinheiro et al., 2018, p. 368).

O Acórdão do Tribunal de Justiça[17], em que Manni é o administrador único da "Italiana Construzioni Srl", à qual foi adjudicado um contrato para a construção de um complexo turístico em Itália. Instaurou um processo judicial contra a Câmara de Comércio de Lecce, "alegando que os imóveis desse complexo não se vendiam por resultar do registo das sociedades que ele tinha sido o administrador único e o liquidatário da Immobiliare e Finanziaria Salentina Srl (a seguir «Immobiliare Salentina»), cuja falência tinha sido declarada em 1992". Posteriormente, argumentou que a sociedade tinha sido cancelada a seu pedido, no entanto invoca que a Câmara de Comércio de Lecce não procedeu ao respetivo cancelamento. Portanto, os seus dados pessoais continuavam acessíveis e relacionados ao processo de liquidação, do qual fez parte.

Assim, Manni pediu, que:

> por um lado, que seja ordenado à Câmara de Comércio de Lecce que cancele, torne anónimos ou bloqueie os dados que o associam à falência da Immobiliare Salentina e, por outro, que essa Câmara de Comércio seja condenada a reparar o prejuízo por ele sofrido pelo facto de a sua reputação ter sido prejudicada.

De facto, o tribunal julgou procedente aquele pedido e solicitou à Câmara de Comércio que agisse em conformidade. O primeiro entendeu que "as inscrições que associam o nome de uma pessoa singular a uma fase crítica da vida da empresa (como a falência) não podem ser perenes, na falta de um interesse geral específico na respetiva conservação e divulgação". Mais ainda, "após concluída a falência da sociedade em causa e o seu cancelamento do registo das sociedades, a necessidade e a utilidade (…) da indicação do nome do antigo administrador único dessa sociedade no momento da falência desta desaparece".

A Primeira Diretiva do Conselho de 9 de março de 1968, a Diretiva 68/151/CEE estabelece a publicidade obrigatória por parte das sociedades, nomeadamente, no art. 2º, que *in casu*, se aplica o nº 1, als. d) e j), referente às pessoas que vinculam a sociedade e

[17] Ac. (Segunda Secção) com o processo nº C-398/15, de 9 de março de 2017, disponível em: http://curia.europa.eu/juris/document/document_print.jsf?docid=188750&text=&dir=&doclang=PT&part=1&occ=first&mode=req&pageIndex=1&cid=21%E2%80%A6 (consultado pela última vez a 08/05/2019 pelas 18:11)

a representam, bem como aos seus liquidatários. O acórdão em questão aplicou a antiga diretiva, ora revogada pelo RGPD, por ser lei vigente na prática dos atos em questão, mormente os arts. 6º, nº 1, al. e) e 12º, al. b).

O acórdão invoca também a CDFUE, que detém duas normas que, *in casu*, entram em conflito, mormente o art. 7º que refere que "todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações" e o art. 8º que estabelece o seguinte "todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito".

Aplicando o RGPD ao caso concreto, estamos perante o art. 5º, nº 1, al. e), 17º, nº 1, al. a) e 18º, nº 1, al. a), e concordamos com o juiz também em matéria de RGPD, já que "não conduz a uma ingerência desproporcionada nos direitos fundamentais das pessoas". Uma vez que, a publicidade suprarreferida existe porque:

> As sociedades anónimas e as sociedades por quotas apenas oferecem como garantia perante terceiros o seu património social, o que represente um risco acrescido para estes (…) justifica-se que as pessoas singulares que optem por participar nas trocas comerciais por intermédio dessa sociedade sejam obrigadas a disponibilizar ao público os dados que se referem à sua identidade e às suas funções nesta, tanto mais que estão conscientes dessa obrigação no momento em que decidem exercer tal atividade.

Para além disso, para lá dos dados pessoais em questão prevalecem "a necessidade de proteger os interesses de terceiros em relação às sociedades (…) garantir a segurança jurídica (…) a lealdade das transações comerciais e o bom funcionamento do mercado interno". Assim, "a mera circunstância de que, supostamente, os imóveis de um complexo turístico (…) de que S. Manni é atualmente administrador único, não se vendem porque os potenciais adquirentes desses imóveis têm acesso a esses dados no registo das sociedades não basta para configurar tal razão, tendo em conta, designadamente, o interesse legítimo destes de disporem dessas informações".

Concluímos que o caso em apreço consubstancia uma exceção ao direito a ser esquecido, por interesses superiores de terceiros, que têm o direito de ter conhecimento sobre as pessoas que gerem determinada empresa, sendo ainda o motivo invocado para o exercício do direito ao apagamento incoerente.

No entanto, consideramos que o registo obrigatório da declaração de insolvência previsto art. 1º, nº 1, al. l) do Código do Registo Civil, doravante CRCivil, é lícito, sendo

este realizado por averbamento ao assento de nascimento (art. 69º, nº 1, al. i) CRCivil). Mais ainda, concordamos com o legislador português quando este admite a eliminação do averbamento referida decorridos cinco anos (art. 81º-A, nº 1, al. b) CRCivil). Afinal, um julgamento *ad eternum* não seria correto. Relativamente à Conservatória do Registo Comercial, consideramos que se deveria aplicar igualmente o prazo de 5 anos.

Por último, iremos analisar o direito de portabilidade dos dados, que está previsto no art. 20º este divide-se em dois direitos: *o de receber os dados pessoais que lhes digam respeito e que tenha fornecido a um responsável pelo tratamento* **e** *o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possam impedir*. Acresce ainda "o direito a que os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento", (Pinheiro et al., 2018, p. 376), sempre que seja tecnicamente possível. Em harmonia com Alexandre Sousa Pinheiro e Carlos Jorge Gonçalves (Pinheiro et al., 2018, p. 377):

> Em qualquer caso, se não se revvelar tecnicamente possível a transmissão direta dos dados pessoais entre os responsáveis, o responsável transmissor deverá comunicar tal impossibilidade ao titular dos dados e enviar-lhe, em anexo a esta comunicação, cópia dos seus dados pessoais que são objeto de tratamento. Resta saber se (…) o titular pode obtar pelo exercício do direito de, ele próprio, receber os dados pessoais que tenha fornecido a um responsável pelo tratamento e, sequencialmente, exercer o direito de transmitir esses dados pessoais ao novo responsável (…). Se for tecnicamente possível a transmissão direta, o titular terá à sua disposição o exercício do direito de receber os dados ou o direito de solicitar a transmissão direta entre responsáveis.

O considerando 68 clarifica a interpretação do artigo em análise, referindo que o direito à portabilidade dos dados "deverá aplicar-se também se o titular dos dados tiver fornecido os dados pessoais com base no seu consentimento ou se o tratamento for necessário para o cumprimento de um contrato". Por outro lado, explica que fora dessses fundamentos jurídicos não é aplicável. Assim como em relação aos responsáveis pelo tratamento que o façam na prossecução das suas atribuições públicas e quando o tratamento for necessário para o cumprimento de uma obrigação jurídica, atribuições de interesse público, ou o exercício da autoridade pública de que esteja revestido o responsável pelo tratamento.

Para além do exposto, o considerando 68 esclarece ainda que o direito à portabilidade dos dados "não deverá prejudicar o direito dos titulares dos dados a obter o

apagamento dos dados pessoais nem as restrições a esse direito" e, bem assim "não deverá implicar o apagamento dos dados pessoais relativos ao titular que este tenha fornecido para a execução de um contrato, na medida em que e enquanto os dados pessoais forem necessários para a execução do referido contrato".

Portanto, perante um contrato de trabalho, em caso de mudança de entidade empregadora, aplica-se o direito à portabilidade dos dados. No entanto, conforme referimos acima, após a cessação do contrato de trabalho será necessário preencher o Relatório Único. Assim, aplica-se o direito à portabilidade dos dados, sem, no entanto, se configurar o apagamento dos dados da anterior entidade empregadora, na medida em que os dados pessoais ainda serão necessários para a execução do contrato de trabalho.

Por último, relativamente à retificação, apagamento ou limitação, o art. 19º prevê a obrigatoriedade de notificação dos destinatários a quem os dados pessoais tenham sido transmitidos por parte do responsável pelo tratamento e, se o titular dos dados o solicitar, o responsável pelo tratamento deverá informá-lo sobre esses mesmos destinatários. Relativamente à notificação, esta não é obrigatória se tal notificação *se revelar impossível ou implicar um esforço desproporcionado*.

Consideramos as duas obrigações legítimas ao abrigo do princípio da transparência que medeia todo o tratamento de dados. Porém, o artigo consagra duas exceções à obrigatoriedade imposta, acima referidas. Relativamente à segunda, isto é, *implicar um esforço desproporcionado,* Carlos Jorge Gonçalves enuncia que "estamos perante um conceito jurídico indeterminado", deixando a sua determinação para uma análise casuística, afirmando que "de qualquer forma, as hipóteses de impossibilidade da comunicação deverão ser residuais. Com o desenvolvimento tecnológico a que assistimos apenas se o responsável pelo tratamento desconhecer alguns destinatários a comunicação se revela, obviamente, impossível", (Pinheiro et al., 2018, p. 374).

Sobre o titular dos dados recai ainda o direito de oposição ao tratamento, previsto no art. 21º. Este direito pode ser exercido *a qualquer momento*, devendo o responsável pelo tratamento terminar o tratamento dos dados pessoais em questão. Exceto se apresentar *razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial*. Isto é, o titular dos dados tem sempre o direito de se opor ao tratamento, mesmo estando perante o exercício de funções

de interesse público ou o exercício de autoridade pública, caberá ao responsável pelo tratamento "provar que os seus interesses legítimos imperiosos prevalecem sobre os interesses ou direitos e liberdades fundamentais do titular dos dados", conforme explana o considerando 69.

Por úlitmo, de forma sumária, iremos explanar o art. 22º que trata as *decisões individuais automatizadas, incluindo a definição de perfis*. O nº 1 do artigo em questão refere expressamente que o titular dos dados *tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar*. Quer isto dizer que, qualquer decisão automatizada que afete, por exemplo, o cálculo das horas extras de determinado trabalhador, que consequentemente afeta a sua esfera jurídica não é legítimo à luz do RGPD. Vejamos, o controlo das entradas e saídas dos trabalhadores é legítimo, como iremos explanar no próximo capítulo. *In casu*, estamos perante uma exceção ao art. 22º, prevista no nº 2, al. a), que refere que o nº 1 não se aplica *se a decisão for necessária para a celebração ou execução de um contrato entre o titular dos dados e um responsável pelo tratamento*. No entanto, o art. 22º não deve ser interpretado como uma proibição, se assim fosse os responsáveis pelo tratameneto não poderiam tomar decisões automatizadas, exceto se estivessemos perante as exceções do nº 2. Por outro lado, assim "os titulares dos dados não precisam de se precaver contra as decisões automatizadas mas, pelo contrário, estão protegidos por defeito", (Wachter, Mittelstadt, & Floridi, 2017, p. 95).

3.4. Tratamento de dados sensíveis

O RGPD refere que os dados pessoais que são considerados sensíveis e que portanto estão sujeitos a condições de tratamento específicas são[18]:

- dados pessoais que revelem a origem racial ou étnica, opiniões políticas e convicções religiosas ou filosóficas;
- filiação sindical;

[18] Cfr. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_pt (consultado pela última vez a 26/08/2019 pelas 22:20)

- dados genéticos, dados biométricos tratados simplesmente para identificar um ser humano;
- dados relacionados com a saúde;
- dados relativos à vida sexual ou orientação sexual da pessoa.

O considerando 10 prevê expressamente a possibilidade de cada Estado-Membro determinar as condições em que o tratamento de dados pessoais sensíveis é lícito. Em ambas as situações com garantias de não discriminação.

Importa analisar o interesse público que pode estar na finalidade do tratamento de dados sensíveis. Na indústria farmacêutica, por exemplo, em que são produzidos medicamentos para uso nacional e internacional, é conveniente que um trabalhador com uma doença infeciosa informe um superior do seu estado de saúde, sendo que o mesmo deve estar obrigado a manter sigilo profissional.

Quer isto dizer que, a finalidade não é, de todo, limitar o acesso a profissões por pessoas portadoras de doenças infeciosas, mas ter em atenção a sua condição e adotar medidas de forma a evitar a contaminação dos produtos farmacêuticos e, consequentemente, de toda a população nacional e internacional, isto é, por motivos de saúde pública. Como assim o determina o considerando 54 "o tratamento de categorias especiais de dados pessoais pode ser necessário por razões de interesse público nos domínios da saúde pública, sem o consentimento do titular dos dados."

A Ordem dos Médicos no seu Regulamento sobre os Profissionais Médicos Seropositivos e a Prática de Procedimentos Invasivos[19] refere que:

> 1. Os médicos devem usar os mais altos padrões de controlo da infecção, recorrendo às melhores barreiras estéreis conhecidas, às precauções universais e às práticas cientificamente aceites do controlo da infecção. Estas medidas devem ser extensíveis a todos os locais onde se praticam procedimentos invasivos cirúrgicos e a todos os doentes que sejam objecto desses procedimentos.
> 2. Os médicos, nomeadamente especialistas em áreas cirúrgicas, seropositivos para o V.I.H. podem continuar a praticar procedimentos invasivos e intervenções cirúrgicas.
> 3. São excepções ao disposto no número anterior:
> a) A demonstrada incapacidade do médico para cumprir os procedimentos básicos de controlo da infecção; ou
> b) O médico estar, comprovadamente, incapaz funcionalmente para tratar os seus doentes.

[19] https://ordemdosmedicos.pt/estatutos-e-regulamentos/regulamento-sobre-os-profissionais-medicos-seropositivos/ (consultado pela última vez a 22/08/2019 pelas 22:46)

Posto isto, concluímos que o controlo de dados sensíveis não é, nem deve ser, limitador do acesso ao mundo do trabalho, não é essa a finalidade do RGPD. Antes pelo contrário, o mesmo pretende salvaguardar a privacidade dos trabalhadores. Se não fosse essa a finalidade do regulamento, o legislador não previa que o tratamento deste tipo de dados apenas pudesse ser realizado por profissionais abrangidos pelo dever do segredo profissional.

4. A monitorização do trabalhador

4.1. O registo dos tempos de trabalho

O registo dos tempos de trabalho está abrangido pelo conceito de dados pessoais previsto no art. 4º, nº 1 e de acordo com o Acórdão do Tribunal de Justiça[20] "a recolha, o registo, a organização, a conservação, a consulta e a utilização desses dados por um empregador assim como a sua transmissão por este às autoridades nacionais com competência para a fiscalização das condições de trabalho são, portanto, características de um «tratamento de dados pessoais»".

O registo dos tempos de trabalho é uma obrigação legal ao abrigo do art. 202º do CT. De acordo com este artigo 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 imediata*. Relativamente ao local onde o registo deverá ser mantido, consideramos que deve ser no local de trabalho. No entanto, depende da forma como o registo dos tempos de trabalho é efetuado. Vejamos, sendo o registo efetuado manualmente, em papel, por cada um dos trabalhadores, o registo deverá ser mantido num local de fácil acesso por parte dos trabalhadores, por exemplo, num dossier mantido na sala de refeições. Por outro lado, sendo o registo dos tempos de trabalho efetuado através de sistemas biométricos, por exemplo, íris, impressões digitais, o seu registo reflete-se através de um software de controlo de assiduidade. Neste caso, "o local onde deverá obrigatoriamente ser acedido será na sede do empregador por ser aí que se cumprem as suas obrigações", (Sousa, 2018, p. 134).

Relativamente à disponibilidade do registo dos tempos de trabalho, que o art. 202º, nº 1 indica a sua *consulta imediata, "*acontece que esta norma está construída partindo do pressuposto que o registo ainda é efetuado em papel (…) todavia, os empregadores já pouco usam os registos em papel". Assim, consideramos que se aplica o princípio da proporcionalidade, para além disso "tem sido reconhecido que o acesso a estes registos não tem de ser instantâneo", (Sousa, 2018, p. 138-139). Perante uma inspeção da ACT, o

[20] Ac. (Terceira Secção) com o processo nº C-342/12, de 30 de maio de 2013, disponível em: http://curia.europa.eu/juris/document/document_print.jsf?docid=137824&text=&dir=&doclang=PT&part=1&occ=first&mode=lst&pageIndex=0&cid=909%E2%80%A6 (consultado pela última vez em 21/05/2019 às 15:08)

acesso instântaneo ao registo dos tempos de trabalho teria de ser realizado através do responsável pelos mesmos. Ora perante a ausência do mesmo, o cumprimento do acesso instântaneo implicaria que mais pessoas do que as necessários tivessem acesso ao registo dos tempos de trabalho, o que não se coaduna com o princípio da proporcionalidade.

Posto isto, concordamos com Duarte Abrunhosa e Sousa quando este refere que "é legítimo que apenas trabalhadores com responsabilidades específicas, tais como chefias ou profissionais de recursos humanos tenham acesso ao registo dos tempos de trabalho de uma determinada organização", (2018, p. 145).

Para além disso, o empregador, *in casu*, o responsável pelo tratamento deverá, em harmonia com o considerando 78, implementar "medidas técnicas e organizativas adequadas" de forma a permitir o acesso ao menor número de pessoas possíveis por exemplo, aplicando a técnica de pseudominização. Isto é, a entidade empregadora remete ao departamento de recursos humanos somente uma lista com algarismos e letras que servem de base à atividade desse departamento. Assim, o departamento, em vez de analisar os dados com os nomes respetivos, analisa-os com uma lista que não permite identificar os trabalhadores em questão. Como tal, somente a entidade empregadora, por exemplo, na pessoa do gerente, é que teria acesso à descodificação das letras e algarismos. A questão levantar-se-ia aquando da entrada de um novo trabalhador, no entanto, bastaria alterar toda a codificação.

Deste modo, o departamento de recursos humanos ao verificar o registo dos tempos de trabalho não saberia a quem pertencem. Em todo o caso, não sendo possível a implementação deste sistema inovador, concordamos que "o acesso ao registo de tempos de trabalho apenas deverá ser feito por pessoas envolvidas no processamento dos tempos de trabalho ou com funções de gestão dos modelos de duração e organização de tempos de trabalho na empresa", (Duarte, 2018, p. 182). Contudo, em harmonia com Mike Hintze, "outro benefício de reconhecer explicitamente um espectro de identificabilidade é que ele pode ajudar a aliviar a ansiedade de uma hipérbole que domina muitas discussões sobre o escopo dos 'dados pessoais'", (2018, p. 101).

Quanto ao exercício de direitos relativos ao RGPD, o direito de acesso e retificação, previstos nos arts. 15º e 16º, respetivamente, estes são legítimos "na medida em que estes direitos incluem também os dados que sejam tratados no cumprimento de

obrigações legais", (Duarte, 2018, p. 183), sendo o registo dos tempos de trabalho uma obrigação legal decorrente do supracitado art. 202º, nº 1 do CT.

Todavia, Filipa Calvão, Presidente da CNPD, é da opinião que o tratamento de dados biométricos em contexto laboral necessita do consentimento do trabalhador, (Calvão, 2019, p. 69)[21], o que, por sua vez, permitiria o exercício do direito ao apagamento. O tratamento de dados biométricos de 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*, de acordo com o art. 28º, nº 6 da Lei nº 58/2019, de 8 de agosto.

Os sistemas biométricos podem tratar dados de vários tipos desde a impressão digital, geometria do rosto, íris do olho, palma da mão, entre outros. Estes surgiram em substituição dos métodos convencionais como o cartão de ponto, código e a palavra-passe. Porém, são menos fidedignos na medida em que possibilitam a sua transmissão a outrem o que, por sua vez, não ocorre com os sistemas biométricos.

Ora, estando nós na era digital, como também refere o considerando 6, ("a rápida evolução tecnológica e a globalização criaram novos desafios em matéria de proteção de dados pessoais"), os sistemas biométricos evoluiram nesse sentido, de forma a facilitar o trabalho dos recursos humanos e cumprir a obrigação legal do registo dos tempos de trabalho. Se o consentimento para a utilização de sistemas biométricos em contexto laboral fosse necessário, este não seria dado livremente tendo em conta a subordinação jurídica inerente à relação laboral. Tal como refere o Parecer 2/2017 do GT29 sobre o tratamento de dados no local de trabalho[22] (p. 4): "é muito improvável que o consentimento possa constituir uma base jurídica para o tratamento de dados no local de trabalho, a menos que os empregados possam recusar, sem consequências adversas".

Assim, a utilização de sistemas biométricos deve realizar-se da mesma forma para todos os trabalhadores. Isto é, deve ter-se em conta os usos e os costumes da empresa em questão. Sendo que, o *software* utilizado pela empresa não deve permitir a visualização

[21] Ver nota de rodapé nº 4.

[22] Cfr. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169 (consultado pela última vez a 23/05/2019 pelas 19:08)

do dado biométrico tratado, apenas deve registar os tempos de trabalho de cada trabalhador.

Por outro lado, prevendo o art. 202º, nº 4 do CT a obrigação legal de manter o registo dos tempos de trabalho durante cinco anos, como poderia o trabalhador exercer o direito ao apagamento? Que relembramos só ser possível em sede do fundamento jurídico do consentimento. Estariamos perante um conflito de fundamentos jurídicos em sede de RGPD, sendo o próprio a solucionar esta temática no seu art. 88º ao afirmar que *os Estados-Membros podem estabelecer, no seu ordenamento jurídico ou em convenções coletivas, normas mais específicas para garantir a defesa dos direitos e liberdades no que respeita ao tratamento de dados pessoais dos trabalhadores no contexto laboral*. Isto é, Portugal estabeleceu o prazo de conservação de 5 anos do registo dos tempos de trabalho de forma a garantir "a defesa dos direitos e liberdades" dos trabalhadores em contexto laboral, o que nos parece legítimo e proporcional.

Posto isto, concordamos com Diogo Pereira Duarte quando este afirma, relativamente ao exercício de direitos sobre dados pessoais, "uma vez que o seu fundamento não é o consentimento, fica afastada a possibilidade de exigir o apagamento", (2018, pp. 182-183), aplicando-se a mesma lógica ao exercício do direito à portabilidade dos dados. Assim, só será permitido o exercício dos direitos de acesso e retificação.

4.2. Instrumentos de trabalho sujeitos a controlo pela entidade empregadora

Neste subcapítulo trataremos da análise da possibilidade e legitimidade do acesso por parte da entidade empregadora à grande quantidade de dispositivos eletrónicos que atualmente se encontram à disposição do trabalhador. Estes, não raras as vezes, fazem parte do seu material de trabalho como, por exemplo, a "geolocalização, controlo das comunicações eletrónicas, controlo através das redes sociais, das mensagens instantâneas, dos dados biométricos, do reconhecimento facial, da crescente utilização da *Inteligência Artificial*, que permitem monitorizar", (Moreira, 2017a, p. 9). Falamos portanto de dispositivos como o telemóvel, carro de serviço, e-mail, o uso da Internet, que consubstanciam a realidade laboral de muitos cidadãos portugueses.

De acordo com Teresa Coelho Moreira (2017a, p. 10):

> (…) hoje estamos perante uma verdadeira revolução digital, associada à internet, ao *cloud computing* e a novas formas de prestar trabalho. Com esta surge também o denominado trabalho digital na economia colaborativa, em plataformas digitais, e um novo tipo de trabalhador o que origina um novo tipo de subordinação reforçada por "um espaço sem distâncias e um tempo sem demoras".

Portanto, face ao suprarreferido importa "encontrar a justa composição entre o direito à privacidade dos trabalhadores e a liberdade de gestão e organização que é conferida pela lei aos empregadores, para o que importa considerar o artigo 22º do CT", em harmonia com a Deliberação nº 1638/2013[23] da CNPD. O art. 22º do CT protege as mensagens de caráter não pessoal que o trabalhador possa enviar através do correio eletrónico durante a jornada laboral. Não obstante, o nº 2 dota a entidade empregadora da possibilidade de estabelecer regras de utilização dos meios de comunicação eletrónicos da empresa, por exemplo, o e-mail.

No mesmo sentido, o Parecer 2/2017 (p. 4) estabelece que "os empregadores devem ter sempre em conta os princípios fundamentais da proteção de dados, independentemente da tecnologia utilizada (…) os empregados devem receber informações eficazes sobre a realização da monitorização". Isto é, a monitorização pode existir, desde que o trabalhador tenha conhecimento e não seja excessiva.

O referido parecer (p. 15) invoca as tecnologias modernas como "riscos" para o trabalhador na medida em que "permitem que os empregados sejam objeto de um acompanhamento ao longo do tempo, nos seus locais de trabalho e nos seus domicílios, através de diversos dispositivos, tais como telemóveis inteligentes, computadores de secretária, *tablets*, veículos e tecnologia usável". Impondo que deve existir um limite ao tratamento, que deve ser pautado pelo princípio da transparência, o pilar da proteção de dados. Caso contrário "existe um risco elevado de que o interesse legítimo dos empregadores na melhoria da eficiência e da proteção do património de uma empresa se transforme numa **monitorização intrusiva e injustificável** (nosso negrito)".

Esta "monitorização intrusiva e injustificável" traduzir-se-á em trabalhadores "robots" e infelizes visto que "a monitorização das comunicações e do comportamento

[23] Ver https://www.cnpd.pt/bin/orientacoes/Delib_controlo_comunic.pdf (consultado pela última vez a 23/05/2019 pelas 16:06)

exercerá pressão sobre os empregados para a conformidade, a fim de evitar a deteção daquilo que pode ser considerado como anomalia", de acordo com o parecer aqui analisado. Na medida em que, os trabalhadores se sentirão inibidos de agirem naturalmente. Daí que, ainda que a monitorização possa existir, deve ser ponderada e refletida e não colocada à disposição do livre arbítrio da entidade empregadora.

Para além disso, não podemos deixar de concordar com a CNPD na sua Deliberação nº 1638/2013 (p. 1) quando refere que:

> As tecnologias de comunicação, e o incremento da sua utilização, constituem um fator determinante para a modernização, a organização, o aumento da produtividade e competitividade das empresas, que simultaneamente podem ser utilizadas para potenciar um maior controlo dos trabalhadores em matéria de produtividade, na verificação do grau de eficiência e na apreciação da sua competência no desempenho das funções, e até na aferição do cumprimento das ordens e instruções da entidade empregadora.

No entanto, importa delimitar o controlo exercido por parte da entidade empregadora. Importa destacar que "a vida já não é o que era, destacando-se um segmento digital que se deve à combinação ousada entre a inata sociabilidade humana e as tecnologias de informação e comunicação disponíveis", (I. P. de Sousa, 2018, p. 64). Tradicionalmente, antes da era digital, ao nos pronunciarmos relativamente à monitorização falaríamos do uso do telefone, do e-mail e do uso da Internet. Atualmente, a realidade é díspar, com a introdução do trabalho 4.0, dado que estamos constantemente conetados ao trabalho. Se antes desligar o computador significava terminar o dia de trabalho, hoje em dia a realidade pode não ser essa, com a existência das referidas *clouds* e redes VPN torna-se "fácil" terminar um relatório, por exemplo. Para além destes, existem várias formas de monitorização como aliás constam do Parecer 2/2017 (pp. 15-16):

> - as ferramentas de prevenção de perda de dados (PPD), que realizam a monitorização das comunicações enviadas, a fim de detetar potenciais violações de dados;
> - as barreiras de segurança de próxima geração («Next-Generation Firewalls - NGFWs») e os sistemas de gestão unificada de ameaças («Unified Threat Management - UTM»), que podem proporcionar várias tecnologias de monitorização, incluindo a inspeção profunda de pacotes de dados, a interceção de TLS, a filtragem de sítios *Web*, a filtragem de conteúdos, a comunicação integrada de soluções de segurança, as informações da identidade do utilizador (como descrito supra) e a prevenção de perda de

> dados. Tais tecnologias podem também ser implantadas individualmente, dependendo do empregador;
>
> - as aplicações e as medidas de segurança que envolvem o acesso do empregado para a entrada nos sistemas do empregador;
> - a tecnologia *eDiscovery*, que se refere a qualquer processo em que os dados eletrónicos são pesquisados com o objetivo de os utilizar como prova;
> - o acompanhamento da aplicação e a utilização do dispositivo através de *software* invisível, quer no computador de secretária, quer na computação em nuvem;
> - a utilização de aplicações de escritório no local de trabalho fornecidas como um serviço de computação em nuvem, o que, em teoria, permite a entrada bastante pormenorizada das atividades dos empregados;
> - a monitorização de dispositivos pessoais (por exemplo, computadores pessoais, telemóveis, *tablets*), que os empregados fornecem para os seus trabalhos, em conformidade com uma política de utilização específica, tal como a «Bring-Your-Own-Device (BYOD)» (Traga o seu próprio dispositivo), bem como a tecnologia «Mobile Device Management (MDM)» (gestão de dispositivos móveis), que permite a distribuição de aplicações, dados e definições de configuração e correções para dispositivos móveis; e
> - a utilização de tecnologia usável (por exemplo, dispositivos relacionados com a saúde e a condição física).

Quer isto dizer que, atualmente a prestação de trabalho está mais fácil e acessível ao trabalhador, mas menos privada. Portanto é fulcral estabelecer normas e procedimentos internos nas empresas de forma a potenciar o direito à reserva da intimidade da vida privada e o direito à desconexão, em conjugação com o direito à proteção de dados pessoais. Assim, torna-se imperativo a implementação de medidas técnicas e organizativas que possibilitem que *por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento*, em harmonia com o art. 25º. Isto é, "a prevenção deve ter muito mais peso do que a deteção", de acordo com o Parecer 2/2017 (p. 19).

Daí que, o GT29, no aqui já analisado Parecer 2/2017 (pp. 19-25) estabeleça algumas orientações que importa ter em consideração:

- Ao utilizar *clouds*[24] deve garantir-se que os trabalhadores podem designar determinados espaços como privados;
- Deve ter-se em atenção o requisito da subsidiariedade, que *in casu*, significa que a **monitorização não pode ser realizada em caso algum**. Exemplo: "se for possível o bloqueio de sítios *Web*, em vez de a monitorização contínua de todas

[24] Computação em nuvem.

as comunicações, o bloqueio deve ser escolhido". Isto é, aplicando-se o método de *privacy by default*, previsto no art. 25º;

- Relativamente ao método BYOD[25], devem limitar-se as fronteiras entre a utilização para fins privados e fins profissionais;
- Quanto ao método MDM[26], o parecer sugere a realização de uma Avaliação de Impacto sobre a Proteção de Dados, doravante AIPD, antes da implementação dessas tecnologias, sendo que os trabalhadores devem ser plenamente informados de que o acompanhamento está a ser realizado e as consequências respetivas;
- Surge a figura da tecnologia usável que pode consistir, por exemplo, na contagem dos passos realizados por um trabalhador, sendo que esta tecnologia só pode ser utilizada com o consentimento do trabalhador. No entanto, "os empregados não são, na sua essência, «livres» para dar tal consentimento de antemão", conforme analisámos no ponto 2.2;
- O tratamento de dados biométricos relacionados com a pontualidade e assiduidade pode ser utilizado, desde que unicamente com essa finalidade e não, por exemplo, controlar o tempo de uso de instalações sanitárias;
- Por último, relativamente ao uso de veículos de serviço existe um interesse legítimo da entidade empregadora em ter conhecimento da localização dos seus veículos. No entanto, se este também for utilizado para fins pessoais do trabalhador, em caso de controlo a tempo real da sua localização deve existir a opção de exclusão da monitorização, isto é, temporariamente desligar o sistema de localização.

Para além destas orientações importa ter em consideração a Deliberação nº 1638/2013 (p. 7) que explana que "a escolha dos meios de controlo por parte do empregador tem de obedecer aos princípios da necessidade, da proporcionalidade e da boa-fé, devendo este demonstrar que escolheu as formas de controlo com menor impacto sobre os direitos fundamentais dos trabalhadores". Sendo que, de acordo com o Acórdão

[25] Sigla para Bring Your Own Device, refere-se ao uso de dispositivos eletrónicos pessoais no local de trabalho para fins profissionais.

[26] Sigla para Mobile Device Management. "A gestão de dispositivos móveis permite aos empregadores localizar dispositivos à distância, implantar configurações e/ou aplicações específicas e eliminar dados mediante pedido. O próprio empregador pode utilizar esta funcionalidade, ou recorrer a um terceiro para fazer isso. Os serviços de gestão de dispositivos móveis permitem também aos empregadores registar ou acompanhar o dispositivo em tempo real, caso não seja comunicado o seu furto.", Parecer 2/2017 (p. 22).

do Tribunal da Relação do Porto[27], "em qualquer caso, o acesso e tratamento de correio eletrónico (emails, anexos e dados de tráfego) pelo empregador tem que observar os princípios consagrados na Lei 67/98, designadamente os princípios da finalidade, da transparência".

Em termos de RGPD, importa primordialmente aplicar o princípio da minimização da recolha dos dados, isto é, limitar a recolha de dados pessoais ao estritamente necessário. De seguida, deve permitir-se aos trabalhadores o direito de aceder aos seus dados pessoais e informá-los das finalidades do tratamento dos dados. Por exemplo, a utilização de sistemas de localização numa viatura da entidade empregadora com a finalidade de saber a sua localização em caso de roubo parece-nos uma finalidade legítima. Portanto, a tónica da proteção de dados pessoais nestes casos impõe-se relativamente "aqueles dados de tráfego que são reveladores de aspetos da vida privada do trabalhador, como sejam o número de telefone chamado, o endereço de correio eletrónico do destinatário ou a identificação do sítio da Internet visitado", em harmonia com a Deliberação nº 1638/2013 da CNPD. O Acórdão do Tribunal da Relação do Porto, converge com o suprarreferido referindo que:

> IV - Pelo menos nas situações em que o empregador, ao abrigo do disposto nos citados arts. 22º, nº 2, e 106º, nº 1, não haja regulamentado e proibido a utilização de contas de correio eletrónico pessoais, o controlo dos dados de tráfego dos emails enviados ou rececionados em tais contas é sempre inadmissível.
> V - No que se reporta a contas de correio eletrónico profissionais com utilização indistinta para fins profissionais e pessoais, o empregador pode tomar conhecimento da data e hora do envio do email, dos dados externos dos anexos (que não do seu conteúdo), mas não do remetente e/ou destinatário do email que seja terceiro

A mesma deliberação refere ainda que, aquando da cessação da atividade de um trabalhador lhe deve ser dado um prazo razoável para eliminar o conteúdo de cariz pessoal dos arquivos do seu correio eletrónico, decorrido o qual a entidade empregadora deve proceder à eliminação da respetiva conta. Além disso, "o empregador deve assegurar que

[27] Ac. com o processo nº 208/14.1TTVFR-D.P1 (Relator Paula Leal de Carvalho), de 15 de dezembro de 2016, disponível em: http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/df89d957d1942212802580a70058cc70?OpenDocument (consultado pela última vez a 28/05/2019 pelas 17:56)

o mesmo endereço eletrónico não será ulteriormente atribuído a outro trabalhador (*email heritage*)".

A entidade empregadora pode implementar regras de utilização da Internet (Wi-Fi), delimitando os períodos em que autoriza a utilização da Internet através dos meios da empresa, por exemplo, pausas para lanche, horas de almoço. Em casos extremos pode, inclusive, bloquear o acesso fora desses períodos a sítios na Internet definidos como não profissionais. No entanto, em harmonia com a deliberação da CNPD "a entidade empregadora não deve fazer um controlo permanente e sistemático do acesso à Internet. O controlo dos acessos à Internet – a ser decidido – deve ser feito de modo global devidamente parametrizado, a fim de poder detetar eventuais desvios ou abusos à norma estabelecida". Porém, "em particular, poderá ser necessário verificar as horas de conexão (início e fim) para comprovar que o acesso para fins privados ocorreu fora do horário de trabalho".

Por fim, importa ter em conta o «**triplo juízo de proporcionalidade»**, de forma que, (Mañas et al., 2016, p. 635):

- Não exista outra medida mais moderada ou menos lesiva para satisfazer o interesse da entidade empregadora com a mesma eficácia (**juízo de necessidade**);
- Se demonstre a idoneidade do meio escolhido, isto é, que o meio de controlo seja efetivamente apto a satisfazer o interesse que justifica a sua implementação (**juízo de idoneidade**);
- Seja proporcional ao meio escolhido em relação ao sacrifício que representa para os direitos fundamentais dos trabalhadores (**juízo de proporcionalidade** em sentido estrito).

Posto isto, a utilização de dispositivos móveis por parte do trabalhador deve ser ponderada e limitada ao estritamente necessário. Do mesmo modo, que o controlo exercido pela entidade empregadora deve limitar-se ao mínimo possível, tendo em conta o princípio da proporcionalidade e o princípio da minimização da recolha dos dados, bem como o tripo juízo de proporcionalidade suprarreferido. Isto é, a monitorização de instrumentos de trabalho como o e-mail, o telemóvel, o uso da Internet pode existir, desde que com conta, peso e medida.

No entanto, não podemos deixar de concluir que estamos perante uma evolução tecnológica constante, surgem cada vez mais novas tecnologias. Pelo que se torna importante adaptar a implementação do RGPD às novas realidades que possam surgir, pelo que nunca será só um processo com início, meio e fim. Deste modo o tratamento de

dados pessoais deverá ser sempre realizado em harmonia com o princípio basilar da proteção de dados pessoais, o princípio da transparência.

4.3. Os meios de vigilância à distância e o teletrabalho

O CT prevê no seu art. 21º, nº 1 a utilização de meios de vigilância à distância no local de trabalho sendo que até 25 de maio de 2018 esta vigilância estava "sujeita a autorização da Comissão Nacional de Protecção de Dados". Trata-se, portanto, de "uma das alterações introduzidas pelo RGPD é o fim do controlo prévio exercido pela Autoridade Nacional, no caso português, a CNPD. Assim, o tratamento de dados pessoais, onde naturalmente se inclui a videovigilância, deixa de ter a obrigatoriedade de autorização prévia", (Alves, 2019). De todo o modo, o empregador "não pode utilizar meios de vigilância à distância no local de trabalho (…) com a finalidade de controlar o desempenho profissional do trabalhador", conforme dispõe o art. 20º do mesmo diploma. Esta utilização com a finalidade prevista no predito artigo, seria incorreta pois, o trabalhador ao saber que estava a ser filmado alteraria a sua conduta, tanto poderia ficar mais inibido, como poderia dar a falsa impressão de bastante produtividade. Ainda mais limitador do direito à privacidade, seria a utilização de câmaras de vigilância a fim de controlar o número de vezes e o tempo que um trabalhador dispensa nas utilizações sanitárias.

Assim, o legislador no art. 19º da Lei nº 58/2019, de 8 de agosto, estipula os locais sobre os quais as câmaras de vigilância não podem incidir:

> a) *Vias públicas, propriedades limítrofes ou outros locais que não sejam do domínio exclusivo do responsável, exceto no que seja estritamente necessário para cobrir os acessos ao imóvel;*
> b) *A zona de digitação de códigos de caixas multibanco ou outros terminais de pagamento ATM;*
> c) *O interior de áreas reservadas a clientes ou utentes onde deva ser respeitada a privacidade, designadamente instalações sanitárias, zonas de espera e provadores de vestuário;*
> d) *O anterior de áreas reservadas aos trabalhadores, designadamente zonas de refeição, vestiários, ginásios, instalações sanitárias e zonas exclusivamente afetas ao seu descanso.*

O referido artigo explana a utilização de câmaras de vigilância nos estabelecimentos de ensino referindo que estas *só podem incidir sobre os perímetros*

externos e locais de acesso, e ainda sobre espaços cujos bens e equipamentos requeiram especial proteção, como laboratórios ou salas de informática. Por último, no seu nº 4 estabelece a proibição de captação de som, *exceto no período em que as instalações vigiadas estejam encerradas ou mediante autorização prévia da CNPD*.

Porém, a realidade pode não ser tão linear como o desejado. Imaginemos que na zona de cargas e descargas de uma empresa, se encontram presentes instalações sanitárias. A videovigilância dessa zona é importante para controlar eventuais furtos, no entanto ao captar imagens da zona de cargas e descargas também se estará a captar imagens da entrada das instalações sanitárias e, consequentemente, de forma involuntária, a entidade empregadora poderá controlar o tempo e o número de vezes que cada trabalhador utiliza nas referidas instalações.

De outro modo, se as câmaras de videovigilância podem captar laboratórios e salas de informática de estabelecimentos de ensino, os docentes que lecionam nessas instalações poderão estar constantemente, ainda que involuntariamente, a ver o seu desempenho profissional controlado, o que não é permitido pelo art. 20º, nº 1 do CT.

A utilização de meios de vigilância à distância "é lícita sempre que tenha por finalidade a protecção e segurança de pessoas e bens ou quando particulares exigências inerentes à natureza da actividade o justifiquem", conforme dispõe o art. 20º, nº 2 do CT. Neste caso, a entidade empregadora deve informar o trabalhador sobre os requisitos previstos no art. 20º, nº 3 do CT:

> (…) a existência e finalidade dos meios de vigilância utilizados, devendo nomeadamente afixar nos locais sujeitos os seguintes dizeres, consoante os casos: «Este local encontra-se sob vigilância de um circuito fechado de televisão» ou «Este local encontra-se sob vigilância de um circuito fechado de televisão, procedendo-se à gravação de imagem e som», seguido de símbolo identificativo.

De todo o modo, a utilização de câmaras de vigilância é lícita com a finalidade da *proteção e segurança de pessoas e bens ou quando particulares exigências inerentes à natureza da actividade o justifiquem*, em harmonia com o art. 20º, nº 2 do CT. Não obstante os casos em que a lei impõe ou admite a possibilidade de utilização de câmaras de vigilância, como por exemplo o art. 11º da Lei nº 38/98, de 4 de agosto[28].

[28] O artigo refere que "os recintos desportivos onde se disputem competições profissionais devem dispor de um sistema de vigilância e controlo por circuito fechado de televisão a fim de permitir o controlo visual

Como o art. 88º refere, os Estados-Membros podem estabelecer normas no seu ordenamento jurídico destinadas a *salvaguardar a dignidade, os interesses legítimos e os direitos fundamentais do titular dos dados*, em contexto laboral, estabelecendo assim uma "margem de manobra" à utilização de câmaras de vigilância. No entanto, a palavra-chave será "ponderação". Ponderação entre os "interesses e direitos em oposição, das circunstâncias do caso concreto e, ainda, da importância dos direitos previstos nos artigos 7º e 8º da CDFUE, e, acrescentaríamos, das normas constitucionais e do artigo 8º da Convenção Europeia dos Direitos do Homem, doravante CEDH, para uma 'garantia da proteção efetiva da vida privada e de não discriminação'", (I. P. de Sousa, 2018, p. 66).

A utilização de câmaras de vigilância no local de trabalho coloca em confronto o direito à reserva da intimidade da vida privada e a proteção e segurança de pessoas e bens, "ou quando devido à natureza da atividade desempenhada se justifique o seu uso"[29]. A título de exemplo, consideramos o uso de câmaras de vigilância em ourivesarias legítimo com a finalidade da proteção de pessoas e bens. Os arts. 7º e 8º da CDFUE confrontam precisamente o respeito pela vida privada e familiar e a proteção de dados pessoais, respetivamente. Relativamente a normas constitucionais, podemos aplicar o art. 35º que invoca o direito de acesso aos cidadãos dos dados informatizados que lhe digam respeito. E, bem assim, o art. 26º da CRP que reconhece o direito à reserva da intimidade da vida privada. Por último, o art. 8º da CEDH estabelece o direito ao respeito pela vida privada e familiar, referindo que *qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência*. Acrescentamos ainda o art. 7º do CT que enumera as condições de trabalho que devem ser cumpridas, não obstante a existência de regulamentação coletiva de trabalho específica para o caso concreto, nesse sentido, a alínea h) prevê a **segurança** e saúde no trabalho.

Resumindo o exposto, com os princípios relativos aos meios de vigilância à distância estabelecidos por António Menezes Cordeiro (2018, p. 572) e já aqui analisados, concluímos que:

> (a) o empregador não os pode utilizar para controlar o desempenho profissional dos trabalhadores (20º/1);
> (b) mas apenas para a proteção e segurança de pessoas e bens ou quando especiais exigências inerentes à natureza da atividade o justifiquem (20º/2);

---

de todo o recinto desportivo". Cfr. http://www.idesporto.pt/DATA/DOCS/LEGISLACAO/doc124.pdf (consultado pela última vez a 29/05/2019 pelas 17:13)

[29] Ac. do Tribunal da Relação do Porto com o processo nº 6909/16.2T8PRT.P1 (Relator Jerónimo Feitas), de 26 de junho de 2017, disponível em: http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/213e51a9c28137de80258169003b373d?OpenDocument (consultado pela última vez a 29/05/2019 pelas 15:22)

> (c) a existência de tais meios (normalmente câmaras de vídeo) deve ser publicitada no local (20º/3);
> (…)
> (e) o pedido deve ser acompanhado de parecer da comissão de trabalhadores ou, não estando este disponível 10 dias após a consulta, de comprovativo do pedido de parecer (21º/4).[30]

A jurisprudência já analisou casos de utilização de meios de vigilância à distância e a sua legitimidade, sendo aqui elaborada uma breve resenha de alguma dela. Como aqui já foi analisado, existem casos em que a própria lei obriga/impõe a instalação de câmaras de vigilância. Comecemos por um Acórdão do Tribunal da Relação do Porto[31] que teve a sua razão de ser através de um despacho que "autorizou/validou o visionamento de imagens de videovigilância no local de trabalho". Assim, em harmonia com o referido acórdão:

> C. Se a lei não permite – até proíbe – que se instale uma câmara para controlar o desempenho de um trabalhador, também não pode permitir que se instale uma câmara para proteger pessoas e bens e, depois, se utilizem, as imagens recolhidas para controlar o desempenho do trabalhador...;
> D. Seria "deixar entrar pela janela aquilo que a lei não permite que entre pela porta..."

No entanto, consideramos ponto assente que a utilização de meios de vigilância à distância com a finalidade de controlar o desempenho do trabalhador será sempre ilícita, em harmonia com o art. 20º, nº 1 do CT. Por outro lado, será lícita sempre que tenha como escopo a proteção de pessoas e bens ou quando particulares exigências inerentes à natureza da actividade o justifiquem, em harmonia com o nº 2 do mesmo artigo. Isto é, o que se pretende é limitar e regular, mas não impedir. Sendo a entidade empregadora obrigada a informar o trabalhador da utilização de câmaras de vigilância e a utilizar sinalética específica, conforme prevê o nº 3.

No caso dos autos em questão, a utilização de câmaras de vigilância "não se destinava a controlar o desempenho profissional da Recorrente, antes tendo uma finalidade genérica: a protecção de pessoas e bens". Essas câmaras eram do conhecimento do trabalhador que "sempre se conformou". Tendo em conta o exposto, "conclui-se que o visionamento das imagens captadas pelas câmaras de videovigilância (…) não serviu

[30] Todos os artigos aqui expostos são referentes ao Código do Trabalho, Lei nº 7/2009, de 12 de fevereiro.
[31] Ac. com o processo nº 402/14.5TTVNG.P1 (Relator Rui Penha), de 19 de outubro de 2015, disponível em:
http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/951c7f4a2a5d3c9680257efb003f2f6a (consultado pela última vez a 30/05/2019, pelas 15:27)

para controlar o desempenho profissional da Recorrente, sendo assim lícito o seu visionamento como meio de prova no âmbito quer do procedimento disciplinar, quer do processo judicial".

Mais recentemente, também no Tribunal da Relação do Porto, um acórdão[32] converge com o anterior, *in casu*, estamos perante um funcionário bancário, que exercia a função de caixa e se apropriou "ilicitamento do valor em numerário de €1.460,00, de um total de €3.000,00, em notas de €10,00 e €20,00, que recebeu das mãos de uma cliente que essas pretendia trocar por notas de €500,00". Independentemente do valor em causa, o comportamento do trabalhador é "doloso e grave". O trabalhador alega que "é ilícito o uso pelo Tribunal *a quo* das imagens referidas, em sede de fundamentação da decisão, já que as mesmas surgem num contexto jus-laboral de controlo da actividade do trabalhador, e fora do raio de incidência da lei penal". O uso de câmaras de vigilância na instituição de crédito estava autorizado pela CNPD, "a solicitação fundamentava-se na obrigatoriedade de 'adoptar um sistema de segurança privada', nos termos previstos no art. 5-1 do DL 231/98, de 22.07"[33]. A CNPD determinou que "o sistema agora notificado não pode ser utilizado para finalidades diversas das previstas no DL 231/98, em particular para o 'controlo da liberdade de movimentos de pessoas no interior das instalações', '**controle dos trabalhadores**' (nosso negrito) ou outras finalidades não especificadas ou concretizadas no pedido". Não obstante:

> São de admitir as imagens captadas por sistema de videovigilância como meio de prova em processo disciplinar e na subsequente ação judicial em que se discuta a aplicação de sanção disciplinar, assim de despedimento, desde que sejam observados os pressupostos que decorrem da legislação sobre a protecção de dados e se conclua que a finalidade da sua colocação não foi exclusivamente a de controlar o desempenho profissional do trabalhador.

Decisão da qual concordamos, afinal é expectável por parte da entidade empregadora um comportamento exemplar dos seus trabalhadores. Em ambos os

[32] Ac. com o processo nº 1119/13.3TTPRT.P2 (Relator Nelson Fernandes), de 5 de março de 2018, disponível em: http://www.dgsi.pt/jtrp.nsf/-/D0447DC12DC8048F8025826A00480362 (consultado pela última vez a 29/05/2019 pelas 15:32)

[33] O art. 5º, nº 1 do DL 231/98, de 22 de julho trata da "obrigatoriedade de adoção do sistema de segurança privada" referindo que: *O Banco de Portugal, as instituições de crédito e as sociedades financeiras, públicas e privadas, são obrigadas a adotar um sistema de segurança privada em conformidade com o disposto no presente diploma e em legislação especial*.

acórdãos analisados, os trabalhadores tinham conhecimento da existência e localização[34] de câmaras de vigilância. Abrindo o precedente de que a captação de imagens por câmaras de vigilância não surtia efeitos na esfera laboral, traduzir-se-ia num descrédito da justiça portuguesa. A Lei nº 58/2019, de 8 de agosto permite precisamente o uso das *imagens gravadas e outros dados pessoais registados através da utilização de sistemas de vídeo ou outros meios tecnológicos de vigilância à distância* utilizadas no *âmbito do processo penal* sejam também *utilizadas para efeitos de apuramento de responsabilidade disciplinar, na medida em que o sejam no âmbito do processo penal*, de acordo com os nºs 4 e 5 do art. 28º, respetivamente.

A relação entre trabalhador e entidade empregadora deve pautar-se pela boa-fé, confiança e respeito mútuo. Tendo o trabalhador, no caso analisado, violado esses princípios, mesmo sofrendo consequências a nível penal, a relação de boa-fé, confiança e respeito mútuo que se exige estaria debilitada *ad eternum*. Motivo pelo qual não se pode exigir que qualquer entidade empregadora volte a confiar na honestidade e idoneidade de um trabalhador nesta situação. A conduta lesiva dos trabalhadores aqui analisados foi ponderada e consciente, ainda que fortuita e isolada, tendo em conta a antiguidade dos mesmos. Posto isto, torna-se insustentável a manutenção da relação laboral.

Por último, cumpre analisar o prazo de conservação das imagens captadas através de câmaras de vigilância. A Lei nº 34/2013, de 16 de maio[35] refere no seu art. 31º nº 2 que: *as gravações de imagem obtidas pelos sistemas videovigilância são conservadas, em registo codificado, **pelo prazo de 30 dias** contados desde a respetiva captação, findo o qual são destruídas*. Por sua vez, o art. 21º, nº 3 do CT refere que: *os dados pessoais recolhidos através dos meios de vigilância a distância são conservados **durante o período necessário** para a prossecução das finalidades da utilização a que se destinam, devendo ser destruídos no momento da transferência do trabalhador para outro local de trabalho ou da cessação do contrato de trabalho*. Constituindo contra-ordenação grave a violação do disposto no referido nº 3. Assim, deve ser realizada uma ponderação na aplicação do prazo de conservação. No caso concreto do trabalhador da instituição de crédito, o prazo de conservação deve ser, na nossa opinião, pelo menos, até ao ao trânsito em julgado da decisão do Tribunal.

[34] A obrigatoriedade da afixação de informação relativa à "existência e localização" das câmaras de vigilância prevista na al. a), do nº 5, do art. 31º da Lei nº 34/2013, de 16 de maio foi revogada pelo art. 2º da Lei nº 46/2019, de 8 de julho.

[35] Regula o Regime do Exercício da Atividade de Segurança Privada.

Posto isto, concluímos que a instalação de câmaras de vigilância é uma realidade, quer por imposição da lei, quer pela finalidade essencial e última da instalação das mesmas, a "proteção de pessoas e bens". Não obstante, os acórdãos analisados que nos remetem para uma esfera, à partida diferente, da análise da instalação de câmaras de vigilância. Afinal, nada é linear no Direito, tudo deve ser ponderado e aplicado ao caso concreto. Assim, na monitorização de outros intrumentos de trabalho, como o e-mail, sugerimos a aplicação do método do "triplo juízo de proporcionalidade"[36], bem como o princípio da minimização da recolha de dados, inerente à aplicação do RGPD. Por último, "é verdade que a privacidade é um valor complexo e que as barreiras digitais já não correspondem aos limites do espaço íntimo e familiar". No entanto, deve ter-se em consideração "o respeito pelo fim-último da proteção de dados: a salvaguarda da vida privada do ser humano", (I. P. de Sousa, 2018, pp. 70-71).

A partir deste ponto, cumpre analisar o regime do teletrabalho, que de harmonia com o art. 165º do CT é *a prestação laboral realizada com subordinação jurídica, habitualmente fora da empresa e através do recurso a tecnologias de informação e de comunicação*. Isto é, temos duas realidades em confronto a subordinação jurídica do trabalhador e o poder de direção da entidade empregadora e, acima de tudo, o direito à reserva da intimidade da vida privada. O poder de direção é intrínseco à noção de contrato de trabalho prevista no art. 11º do CT[37].

Por outros palavras, um trabalhador em regime de teletrabalho realiza as suas funções, habitualmente, no seu domicílio, sob a tutela da subordinação jurídica e do poder de direção da entidade empregadora, pelo que importa defender o seu direito à reserva da intimidade da vida privada, inerente ao desempenho laboral no seu domicílio.

Primeiramente, importa enumerar as várias formas de prestar teletrabalho, em harmonia com Raquel Poquet Catala (2018, p. 116):

> Según el tipo de communicación con la empresa se distingue entre teletrabajo *off line*, *on line* y *two way line*. El teletrabajo *off line* o "desconectado" se produce cuando el teletrabajador trabaja con un equipo informático, pero recibe o envía las instrucciones de trabajo y el resultado por medios convencionales no telemáticos. El trabajo *on line* o "conectado" ocurre cuando para recoger las especificaciones del trabajo, para realizarlo o enviarlo se utilizan las comunicaciones telemáticas. El teletrabajo *two way line* o "en

[36] Ver pág. 48.

[37] O art. 11º do CT referente à noção de contrato de trabalho expõe que: *contrato de trabalho é aquele pelo qual uma pessoa singular se obriga, mediante retribuição, a prestar a sua atividade a outra ou outras pessoas, no âmbito de organização e sob a autoridade destas.*

> doble sentido"se da cuando el teletrabajador trabaja conectado a una red de comunicaciones telemáticas, mientras que en el *one way* line la conexión del ordenador del teletrabajador com el central de la empresa es muy rudimentaria.

Existe a presunção legal do art. 168º, nº 1 do CT, de que os instrumentos de trabalho respeitantes a informação e comunicação utilizados pelo trabalhador pertencem à entidade empregadora. Posto isto, esta poderá exercer o controlo da atividade laboral e dos instrumentos de trabalho sendo que, sempre que o teletrabalho seja realizado no domicílio do trabalhador, a visita ao domicílio/local de trabalho apenas poderá ser efetuada entre as 9 e as 19 horas, conforme prevê o art. 170º do CT.

De todo o modo, o art. 169º do CT prevê a igualdade de tratamento de trabalhadores em regime de teletrabalho, ou seja, iguais direitos e deveres dos trabalhadores convencionais. Até porque o teletrabalho é somente "um meio para modernizar a organização laboral da empresa e, ao mesmo tempo, uma forma de cumprir a jornada laboral que permite aos trabalhadores conciliar as suas vidas laboral e familiar, atribuindo-lhes uma maior autonomia organizativa", (Catala, 2018, p. 119).

Portanto, face ao exposto, um dos maiores obstáculos no âmbito da proteção de dados pessoais e direito à reserva da intimidade da vida privada prende-se com o exercício do poder de direção e a proteção de pessoas e bens, presumindo que os instrumentos de trabalhos utilizados pertencem à entidade empregadora. Assim, no âmbito da proteção de pessoas e bens é lícita a instalação de câmaras de vigilância ou outro meio de vigilância à distância, de acordo com o art. 20º, nº 2 do CT. No entanto, se em todos os restantes casos a instalação de câmaras de vigilância deve ser pautada pela ponderação, quando em regime de teletrabalho esta ponderação deve ser exponenciada, principalmente se o trabalhador exercer funções no seu domicílio.

Assim, sempre que possível a entidade empregadora deve exercer o seu poder de direção e o controlo da atividade profissional do trabalhador mediante as visitas referidas acima. No entanto, se existir um instrumento de trabalho valiosíssimo e/ou o trabalhador tratar dados sensíveis, sendo que "o objeto a proteger deve ser realmente valioso para legimitar a intromissão da intimidade do domicílio, e deverá limitar-se a filmar a zona em que se desempenhe o trabalho", (Catala, 2018, p. 121). Posto isso, também aqui sugerimos a aplicação do método do triplo juízo de proporcionalidade[38].

[38] Ver pág. 48.

Não obstante, na opinião da mesma autora, existindo suspeitas razoáveis da realização de irregularidades por parte do trabalhador, pode ser legitimado a nível disciplinar a instalação de câmaras de vigilância, a fim de comprovar a existência das referidas irregularidades. Logo, a instalação de câmaras de vigilância no local de trabalho de um trabalhador, sendo esse local o domicílio, deverá "limitar-se a uma zona da casa e por um período de tempo determinado, suficiente para comprovar que não era um ato isolado ou uma confusão", (Catala, 2018, p. 121).

Esta página foi intencionalmente deixada em branco

5. O papel do DPO em articulação com o responsável pelo tratamento nos RH[39] de uma empresa

Neste capítulo será analisada a nova figura presente na secção 4 do RGPD o Encarregado de Proteção de Dados, em inglês "Data Protection Officer", doravante DPO, esta figura será analisada de forma breve. Vamos tentar perceber a sua importância no tratamento de dados nos processos de recrutamento e em todas as fases de um contrato de trabalho, desde a contratação até à sua cessação.

De forma genérica, o DPO é designado com base em duas qualidades profissionais e, em especial, nos seus conhecimentos especializados no âmbito do direito da proteção de dados pessoais, em harmonia com o art. 37º, nº 5. O art. 9º, nº 1 da Lei nº 58/2019, de 8 de agosto estabeleceu que o exercício da função de DPO não carece de certificação profissional. Não obstante, considerarmos importante algum conhecimento prévio que se poderá adquirir com formação profissonal certificada. Ressalvamos que em Portugal não existe uma entidade certificadora, pelo que as formações profissionais que eventualmente existirem terão uma função meramente pedagógica.

Contudo, a designação de um DPO nem sempre é obrigatória, estabelecendo o nº 1 do art. 37º a obrigatoriedade de designação de um DPO, embora com conceitos indeterminados[40], nos seguintes casos: *autoridade ou um organismo público, excetuando os tribunais no exercício da sua função jurisdicional* (al. a)); *as atividades principais* que *consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala* (al. b)); *operações de tratamento em grande escala de categorias especiais de dados nos termos do art. 9º e de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10º* (al. c)).

O DPO é envolvido, *de forma adequada e em tempo útil, a todas as questões relacionadas com a proteção de dados pessoais* e está vinculado à *obrigação de sigilo ou confidencialidade no exercício das suas funções,* em harmonia com o art. 38º, nº 1 e nº 5,

[39] Recursos Humanos

[40] Para um melhor entendimento, cfr. "Orientações sobre os encarregados da proteção de dados (EPD)" em https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 (consultado pela última vez a 06/06/2019 pelas 19:10)

respetivamente e o art. 10º da Lei nº 58/2019, de 8 de agosto que declara que o dever de sigilo e confidencialidade "se mantém após o termo das funções que lhes deram origem".

O DPO é um ponto de contacto entre os titulares dos dados e o exercício dos direitos previstos no RGPD; por exemplo, o direito de acesso, conforme prevê o nº 4 do mesmo artigo. O DPO *não pode ser destituído nem penalizado pelo responsável pelo tratamento ou pelo subcontratante pelo facto de exercer as suas funções*, de acordo com o nº 3 do artigo em análise. Quer isto dizer, em harmonia com Cristina Pimenta Coelho (Pinheiro et al., 2018, p. 475),

> (…) que o que se pretende evitar é que o DPO seja condicionado no exercício das suas funções, pelo que não deve ser proibido de dar seguimento a uma queixa, nem ser obrigado a interpretar uma determinada norma legal com o sentido que o responsável pelo tratamento ou o subcontratante lhe pretendem dar. Tal não significa, porém, que o DPO tenha poderes decisórios mas antes que deve ser independente na forma como cumpre as obrigações que o Regulamento lhe impõe, bem como ser livre de expressar as suas opiniões e conselhos que, como é evidente, podem ou não ser seguidos por quem é responsável pelo cumprimento das normas de proteção de dados.

Assim, o exercício da função de DPO deve pautar-se pela imparcialidade na aplicação do RGPD. Pelo que, a sua integração e a aplicação de procedimentos no setor de recursos humanos de uma empresa, se revela importante para proteger os futuros, atuais e antigos trabalhadores de violações aos seus dados pessoais. O DPO deverá ser visto pelos trabalhadores como uma figura idónea, cumpridora e imparcial que praticará a aplicação do direito à proteção de dados pessoais, em confomidade com o RGPD e com a Lei nº 58/2019, de 8 de agosto. Não obstante, o DPO poder ser *um elemento do pessoal da entidade responsável pelo tratamento ou do subcontratante*, em harmonia com o nº 6 do art. 37º. Sendo que, nesse caso não poderá resultar num possível conflito de interesses, como refere o nº 6 do art. 38º. Em todo o caso, o exercício da função de DPO poderá ter por base um contrato de prestação de serviços, de acordo com o já referido art. 37º, nº 6, *in fine*. Nesse caso, em harmonia com as "Orientações sobre os encarregados da proteção de dados (EPD)"[41], doravante WP243 rev.01 (p. 25) do GT29, "um conjunto de pessoas que trabalham para essa entidade poderá exercer de modo eficaz as funções do EPD enquanto equipa, sob a responsabilidade de um contacto principal e «pessoa responsável»

[41] Cfr. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 (consultado pela última vez a 06/06/2019 pelas 19:09)

designado para o cliente. Neste caso, é essencial que cada membro da organização externa que exerça as funções de EPD cumpra todos os requisitos aplicáveis do RGPD".

Relativamente às funções a desempenhar pelo DPO, o RGPD no seu art. 39º elenca algumas dessas funções, embora o artigo não seja taxativo, são elas:

> *a)* ***Informa*** (nosso negrito) *e* ***aconselha*** (nosso negrito) *o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações nos termos do presente regulamento e de outras disposições de proteção de dados da União ou dos Estados-Membros;*
> *b)* ***Controla*** (nosso negrito) *a conformidade com o presente regulamento, com outras disposições de proteção de dados da União ou dos Estados-Membros e com as políticas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes;*
> *c) Presta aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controla a sua realização nos termos do artigo 35.o;*
> *d)* ***Coopera*** (nosso negrito) *com a autoridade de controlo;*
> *e) Ponto de contacto para a autoridade de controlo sobre questões relacionadas com o tratamento, incluindo a consulta prévia a que se refere o artigo 36º, e* ***consulta*** (nosso negrito)*, sendo caso disso, esta autoridade sobre qualquer outro assunto.*

Assim, face ao exposto, o exercício da função de DPO, a profissão do futuro, uma profissão, na nossa opinião, de grande prestígio, deve ser realizada de forma idónea e imparcial, no escopo do cumprimento em pleno do RGPD, da Lei nº 58/2019, de 8 de agosto e restante legislação nacional aplicável. Visto que, em harmonia com o considerando 97, "estes encarregados da proteção de dados, sejam ou não empregados do responsável pelo tratamento, deverão estar em condições de desempenhar as suas funções e atribuições com independência".

5.1. O estabelecimento da relação laboral

Em Portugal, quando se inicia uma prestação de trabalho subordinado, isto é, um contrato de trabalho, existem certos e determinados procedimentos a considerar antes, durante e depois. Assim, neste ponto serão analisados todos os requisitos necessários à celebração do mesmo, bem como a sua articulação com o RGPD de forma a evitar uma monitorização excessiva do trabalhador e salvaguardar os seus direitos relativos à proteção de dados pessoais.

5.1.1. Procura ativa de emprego e consequente processo de recrutamento

Na sociedade portuguesa, existe um percurso pessoal e académico que pode ser percorrido, que é a concretização dos "estudos", que tanto podem culminar no Ensino Secundário, como na Licenciatura e, inclusive ir mais além com um Mestrado e posterior Doutoramento. A opção é invidual e não existem opções certas, nem opções erradas. Um ponto comum à finalização dos "estudos" é a procura ativa de emprego. Não raras as vezes, essa procura ativa de emprego consiste no envio ou na entrega de um currículo, que se trata de um "documento que contém os dados biográficos e os relativos à formação, conhecimentos e percurso profissional de um pessoa"[42]. Assim, pelo art. 4º, nº 1 no currículo constam dados pessoais, que ao serem recolhidos consubstanciam um tratamento de dados, pelo nº 2 do mesmo artigo. Assim, importa analisar e proteger os dados pessoais dos cidadãos, que por estarem à procura de emprego e, portanto, numa situação vulnerável, ainda que não subordinados juridicamente, entregam e/ou o enviam a empresas. Iremos ainda analisar as várias vertentes da procura ativa de emprego, como o Instituto do Emprego e Formação Profissional, doravante IEFP, as empresas de trabalho temporário, as empresas de consultoria na área dos recursos humanos e, bem assim, a iniciativa própria.

Mais uma vez, não podemos deixar de referir que estamos na era digital e tudo se alterou com a introdução das novas tecnologias, a procura de emprego não é exceção. Tornou mais fácil a procura de emprego, mas também mais impessoal. O que em outros tempos se traduzia numa conversa com o possível gerente da empresa e posterior entrega de currículo. Hoje em dia é maioritariamente, realizada através do envio de um e-mail, sem qualquer tipo contacto pessoal com a outra parte. O que ocorre para evitar um desaproveitamento de tempo de ambas as partes, afinal se existir interesse da empresa esta contactará o possível futuro trabalhador para uma entrevista presencial.

Em outro sentido, importa analisar os casos em que um trabalhador empregado procura um novo projeto profissional e portanto, não quer criar conflitos internos com a atual entidade empregadora sem nada previamente definido. Assim, torna-se importante proteger todas as pessoas que procuram um novo emprego, independentemente da atual situação profissional.

[42] https://dicionario.priberam.org/curr%C3%ADculo (consultado pela última vez a 07/06/2019 pelas 16:54)

Não podemos deixar de referir os "Sistemas de Seleção 2.0" invocados por Olga García Coca (2016, p. 69), que se enquadram no âmbito da era digital. Basicamente, estes sistemas permitem a busca de candidatos a emprego e de emprego através de redes sociais ou de sites de pesquisa de empregos.

As redes sociais são um "modelo colaborativo e aberto à partipação de todos os usuários possíveis", (Coca, 2016, p. 71). Permitem uma interação à distância de um clique e uma inclusão, ou exclusão, de candidatos exclusivamente com base nas suas habilitações académicas e experiências, não consente *a priori* em juízos de valor[43]. Outra vantagem desta forma de seleção de trabalhadores prende-se com o facto de esta se poder, em harmonia com Olga García Coca (2016, p. 72):

> tornar uma tarefa de equipa em que não apenas o departamento de recursos humanos intervém, mas qualquer trabalhador da empresa que visualize o perfil de um candidato, porque anteriormente ele se registou como utilizador na rede social e, portanto, este trabalhador também pode fornecer informações àqueles que se dedicam à seleção de pessoal.

Por outro lado, pode existir um conhecimento por parte de um atual trabalhador da empresa, que pode nem sempre surtir bons resultados para o candidato a emprego, mas isso somente depende da conduta profissional de cada um e, bem assim, do profissionalismo e imparcialidade que regem a atividade profissional de determinado trabalhador.

Em Portugal, existe uma rede social profissional, que é a mais conhecida mundialmente[44], trata-se do *LinkedIn*. Esta permite a criação de um perfil profissional individual, com a indicação, a título exemplificativo, das seguintes informações: um resumo, que permite a cada pessoa indicar o que pretende a nível profissional e académico, se assim entender; a indicação das suas habilitações académicas, concluídas e/ou a frequentar; a experiência profissional; experiências de voluntariado; a indicação da frequência de formações, mediante a indicação dos certificados obtidos e a respetiva validade, se exitir; e, por último a indicação em título com grande destaque do seu título

[43] O art. 17º nº 1 do CT estabelece a proibição do empregador obter informações sobre o trabalhador relativas: *a) À sua vida privada, salvo quando estas sejam estritamente necessárias e relevantes para avaliar da respetiva aptidão no que respeita à execução do contrato de trabalho e seja fornecida por escrito a respetiva fundamentação; b) À sua saúde ou estado de gravidez, salvo quando particulares exigências inerentes à natureza da atividade profissional o justifiquem e seja fornecida por escrito a respetiva fundamentação.*

[44] "É considerada a rede social que mais se ajusta ao que se conhece como rede social profissional", (Coca, 2016, p. 73).

profissional e da região em que se estabelece, ou pretende estabelecer profissionalmente, incluindo ainda uma fotografia.

De acordo com o GT29, no aqui já referido "Parecer 2/2017 sobre o tratamento de dados no local de trabalho" (p. 13),

> a utilização dos meios sociais pelas pessoas é generalizada e relativamente comum para que os perfis de utilizador sejam acessíveis ao público, dependendo das definições escolhidas pelo titular da conta. Em consequência, os empregadores podem considerar que a inspeção dos perfis sociais de possíveis candidatos possa ser justificada durante o seu processo de recrutamento. Isto pode também ser o caso de outras informações publicamente disponíveis sobre o potencial empregado.

Assim, à primeira vista, parece-nos que um empregador pode analisar qualquer tipo de rede social do trabalhador. Porém, o mesmo parecer vem esclarecer que os empregadores "não devem pressupor que o simples facto do perfil de um utilizador estar publicamente disponível num meio social lhes permita proceder ao tratamento desses dados para os seus próprios fins". Afinal, tal não seria legítimo e, sendo-o, deveriam ser disponibilizadas as informações constantes no art. 14º por forma a cumprir o princípio da transparência.

Neste sentido, "o empregador deve, antes da inspeção do perfil no meio social, ter em conta se o perfil no meio social do candidato diz respeito a fins profissionais ou privados". Portanto, em certa medida, uma inspeção ao perfil do LinkedIn de um futuro possível trabalhador pode ser legítima, não esquecendo que "os empregadores apenas estão autorizados à recolha e ao tratamento de dados pessoais respeitantes aos candidatos a emprego, na medida em que a recolha desses dados é necessária e pertinente para o desempenho da função à qual estão a candidatar-se", de acordo com o mesmo parecer.

De todo o modo, é inquestionável que "a informação que se pode obter, por exemplo, nas redes sociais e nos sites de pesquisa de emprego é maior que a que se obteria se se utilizasse o método tradicional de receção física de CV's", (Coca, 2016, p. 101). Contudo, importa analisar os casos em que trabalhadores possuem conta numa rede social profissional somente por uma questão lúdica, não estando à procura de emprego. Nesse sentido, Olga García Coca denomina-os de "candidatos passivos", ou seja "não se encontram numa procura ativa de emprego", (Coca, 2016, p. 72). Neste caso, os seus dados pessoais são disponibilizados de forma pública pelo trabalhador de forma intencional, não devendo ser utilizados para outros fins, se o forem deve ser solicitado o

consentimento do trabalhador. Em qualquer caso, o Parecer 2/2017 (p. 13) esclarece que "não existe qualquer fundamento jurídico para um empregador exigir ao potencial empregado «ser amigo» do potencial empregador, ou por outras vias, facultar o acesso ao conteúdo dos seus perfis".

Para além disso, importa analisar o caso dos candidatos a emprego que se inscrevem em empresas de recursos humanos, especializadas em recrutamento. Visto que, o candidato a emprego quando se inscreve numa dessas empresas, presta o seu consentimento, ou realiza um contrato que legitima o tratamento de dados pessoais à empresa de recursos humanos. Pelo que, é nosso entendimento que a disponibilização dos seus dados pessoais, por parte da empresa de recursos humanos, a uma possível empresa não possa ser realizado sem o consentimento do candidato a emprego. Na medida em que este, enquanto titular dos dados, deve ter conhecimento pleno relativamente a que empresa os seus dados pessoais serão transmitidos. Afinal, o candidato a emprego quando se inscreveu na empresa de recursos humanos necessitava de emprego. No entanto, pode iniciar uma relação laboral sem o auxílio da empresa de recursos humanos e esta não ter conhecimento desse início. Pelo que, nos parece correto questionar o candidato a emprego se ainda se encontra à procura de emprego e, acima de tudo, se tem interesse na vaga que lhe apresentam.

Para além destas empresas privadas, existe um organismo público destinado a auxiliar pessoas desempregadas a procurar emprego, trata-se do IEFP. Este "é o serviço público de emprego nacional. Tem por missão promover a criação e a qualidade do emprego e combater o desemprego, através da execução de políticas activas de emprego, nomeadamente de formação profissional"[45]. Isto é, o IEFP cria um perfil de utilizador de cada cidadão de forma a selecionar as vagas mais adequadas a cada candidato em específico. Estando os colaboradores do IEFP sujeitos a um Código de Ética e de Conduta[46] que os remete no art. 30º à sujeição à *legislação vigente relativa à proteção das pessoas singulares, no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados*. Assim, os dados pessoais dos utilizadores do IEFP encontram-se protegidos, em termos de proteção de dados pessoais.

[45] Cfr. https://www.iefp.pt/instituicao (consultado pela última vez a 11/06/2019 pelas 10:50)
[46] Cfr. https://www.iefp.pt/documents/10181/702348/C%C3%B3digo+de+%C3%89tica+e+de+Conduta.pdf/662d2ef3-fd21-426a-a167-20674f82dacf (consultado pela última vez a 11/06/2019 pelas 11:07)

No entanto, o portal do IEFP permite também a publicação de ofertas de emprego por parte de empresas conforme as suas necessidades, somente com caráter informativo. Os candidatos a emprego têm acesso às ofertas de emprego publicadas e podem candidatar-se autonomamente, sem necessidade de auxílio por parte dos colaboradores do IEFP, desde que estejam devidamente registados no portal *iefponline*[47].

Face ao exposto, não só as empresas de consultoria de recursos humanos, mas também o IEFP são "conhecidos como 'zonas TIC[48]', que são aquelas que tentam melhorar os serviços aos cidadãos minimizando tempos e simplificando trâmites", (Coca, 2016, p. 76). Afinal, propicia uma economia de tempo tanto aos candidatos a emprego como às empresas, na medida em que só serão selecionados para um primeiro contacto as pessoas que efetivamente possuírem as competências necessárias para cada vaga em concreto.

No caso do IEFP, uma vez que se trata de um um serviço público, aplica-se a Lei nº 26/2016, de 22 de agosto, conforme expõe o art. 26º da Lei nº 58/2019, de 8 de agosto. O art. 5º da Lei nº 26/2016, de 22 de agosto refere que *todos, sem necessidade de enunciar qualquer interesse, têm direito de acesso aos documentos administrativos, o qual compreende os direitos de consulta, de reprodução e de informação sobre a sua existência e conteúdo.* A mesma lei distingue "documento administrativo" de "documento nominativo". O primeiro, elencado no art. 3º, nº 1, al. a) é: *qualquer conteúdo, ou parte desse conteúdo, que esteja na posse ou seja detido em nome dos órgãos e entidades referidas no artigo seguinte[49], seja o suporte de informação sob forma escrita, visual, sonora, eletrónica ou outra forma material, neles se incluindo, designadamente, aqueles relativos a;*

i) Procedimentos de emissão de atos e regulamentos administrativos;

ii) Procedimentos de contratação pública, incluindo os contratos celebrados;

iii) Gestão orçamental e financeira dos órgãos e entidades;

iv) Gestão de recursos humanos, nomeadamente os dos procedimentos de recrutamento, avaliação, exercício do poder disciplinar e quaisquer modificações das respetivas relações jurídicas.

[47] Disponível em: https://iefponline.iefp.pt/IEFP/authentication/loginUser.jsp (consultado pela última vez a 11/06/2019 pelas 11:43)

[48] Em português, Tecnologias de Informação e Comunicação.

[49] Elenca as situações de aplicação subjetiva. Cfr. art. 4º da Lei 26/2016, de 22 de agosto, disponível em http://www.pgdlisboa.pt/leis/lei_print_articulado.php?tabela=leis&artigo_id=&nid=2591&nversao=&tabela=leis (consultado pela última vez a 11/06/2019 pelas 12:27)

Por sua vez, "documento nominativo", que encontra a sua definição no art. 3º, nº 1, al. b), é *o documento administrativo que contenha dados pessoais, definidos nos termos do regime legal de proteção de dados pessoais*. Isto é, *informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular*, em harmonia com o art. 4º, nº 1. Assim, face ao exposto concluímos que o IEFP, que trata dados pessoais e, por conseguinte, documentos nominativos, *ad contratio* do art. 6º, nº 5 da Lei nº 26/2016, de 22 de agosto, não pode permitir o acesso a um terceiro.

Exceto se, de acordo com o artigo referido, um terceiro: *estiver munido de autorização escrita do titular dos dados que seja explícita e específica quanto à sua finalidade e quanto ao tipo de dados a que quer aced*er (al. a)); *demonstrar fundamentadamente ser titular de um interesse direto, pessoal, legítimo e constitucionalmente protegido suficientemente relevante, após ponderação, no quadro do princípio da proporcionalidade, de todos os direitos fundamentais em presença e do princípio da administração aberta, que justifique o acesso à informação* (al. b)).

Não obstante, o art. 65º da Lei nº 58/2019, de 8 de agosto inserir o nº 9 ao art. 6º da Lei nº 26/2016, de 22 de agosto, que tem a seguinte redação: *nos pedidos de acesso a documentos nominativos que não contenham dados pessoais que revelem a origem étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, dados genéticos, biométricos ou relativos à saúde, ou dados relativos à intimidade da vida privada, à vida sexual ou à orientação sexual de uma pessoa, **presume-se*** (nosso negrito), *na falta de outro indicado pelo requerente, que o pedido se fundamenta no direito de acesso a documentos administrativos.* Assim, em harmonia com a Lei nº 58/2019, de 8 de agosto, no caso do IEFP que não trata nenhum dos tipos de dados elencados acima, conclui-se que é permitido o acesso por qualquer pessoa dos dados dos candidatos a emprego que lá se encontram inscritos.

Importa ainda enunciar que os titulares dos dados, seja com o IEFP, seja com empresas de recursos humanos, têm o poder de exercer os direitos "ARCO"[50],

[50] Acrónimo espanhol para "**A**cceso, **R**ectificación, **C**ancelación y **O**posición".

(Domènech, 2017, p. 32). Quer isto dizer, que os titulares dos dados, *in casu*, candidatos a emprego podem exercer os direitos ARCO. Assim, no âmbito do IEFP, cuja inscrição é condição para a atribuição de subsídio de desemprego, o exercício do direito ao apagamento consubstanciará o término do pagamento das referidas prestações.

Por fim, é ponto assente pelo GT29 no seu Parecer 2/2017 (p. 13) que "os dados recolhidos devem, em geral, ser eliminados assim que se torne claro que uma oferta de emprego não será realizada ou não for aceite pela pessoa em causa". Em harmonia com a Recomendação CM/REC (2015) 5 do Comité de Ministros aos Estados-Membros[51] sobre o tratamento de dados pessoais no contexto laboral, que refere que:

> Os dados pessoais submetidos numa candidatura de emprego devem, normalmente, ser excluídos assim que ficar claro que uma oferta de emprego não será feita ou não será aceite pelo candidato a emprego. Quando esses dados são armazenados com vista a uma nova oportunidade de trabalho, o titular dos dados deve ser informado em conformidade e os dados devem ser apagados, se assim o solicitarem.

Portanto, os candidatos a emprego que enviem o seu currículo a uma empresa e não sejam selecionados, podem ver os seus currículos armazenados pela referida empresa com vista ao preenchimento de uma eventual oferta de emprego. O mesmo acontecendo no caso do envio de uma candidatura espontênea em que *a priori* o currículo já é armazenado com vista ao preenchimento de uma futura vaga. Para além de que, em harmonia com o art. 32º, nº 1 do CT *todas as entidades devem manter durante cinco anos o registo dos processos de recrutamento efetuados*. Não obstante os elementos conservados serem os seguintes: *a) convites para o preenchimento de lugares; b) anúncios de oferta de emprego; c) número de candidaturas para apreciação curricular; d) número de candidatos presentes em entrevistas de pré-seleção; e) número de candidatos aguardando impresso; f) resultados de testes ou provas de admissão e seleção; g) balanços sociais relativos a dados, que permitam analisar a existência de eventual discriminação de pessoas de um dos sexos no acesso ao emprego, formação e promoção profissionais e condições de trabalho*, de acordo com o mesmo artigo.

Opinião contrária à de Olga García Coca (2016, p. 107), que refere que após a outorga do contrato de trabalho "o resto dos CV's já não são necessários, pois a sua finalidade era a de fazer parte desse processo de seleção". De todo o modo, o candidato a

[51] Ver ponto 13.2 em https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a (consultado pela última vez em 11/06/2019 pelas 15:54)

emprego tem de ser informado da finalidade do armazenamento do seu currículo, do prazo de conservação do mesmo e a quem se deve dirigir para exercer os seus direitos ARCO.

De seguida, importa aplicar o exposto, na medida do possível, ao trabalho temporário[52]. Trata-se de uma relação triangular entre o trabalhador, a empresa de trabalho temporário, doravante ETT, e o utilizador, que será quem usufruirá da força laboral do trabalhador. Deste modo, o trabalhador realiza uma contrato de trabalho temporário com a ETT (contrato laboral) e, por sua vez, a ETT realiza um contrato de utilização de trabalho temporário com o utilizador (contrato comercial). Geralmente, a contratação dos serviços de uma ETT ocore "quando uma empresa necessita de cobrir temporariamente um posto de trabalho", (Coca, 2016, p. 67). Posto isto, importa analisar o tratamento de dados aquando da entrega de currículo à ETT, a utilização dos dados pessoais para efeitos de contratação e a sua transmissão à empresa utilizadora.

Relativamente, à entrega de currículos a ETT's aplica-se o acima exposto, ou seja, o trabalhador tem o poder de exercer os seus direitos ARCO, vendo sempre cumprido o princípio da transparência. Relativamente aos dados pessoais utilizados para efeitos de contratação, estamos perante uma obrigação legal, pelo que o tratamento será lícito no âmbito do art. 6º, nº 1, al. c). Uma vez realizado o contrato laboral e comercial, o tratamento de dados será lícito pelo art. 6º, nº 1, al. b). Pelo que se aplicam as disposições relativas a um contrato de trabalho comum, que serão analisadas de seguida.

Por último, terminada a fase da procura ativa de emprego com a realização de uma entrevista de emprego importa ter em consideração as informações que não podem ser prestadas em sede de entrevista. De acordo com Olga García Coca (2016, pp. 105-106), as entrevistas de emprego apresentam-se sobre uma dupla perspetiva:

> por um lado, podem servir para completar e inclusivamente realçar o CV; mas, por outro lado, também podem ser aproveitadas para recolher mais informações do que a realmente necessária para a seleção do trabalhador. Não obstante, o intermedidador incorrerá em **má fé** (nosso negrito) se estiver consciente da inexistência de relação entre essa informação e a valorização do perfil profissional do candidato pelo que, neste caso, se estará sem dúvida violando o princípio da qualidade do dados.

Neste sentido, o CT prevê no seu art. 17º a proibição da exigência ao candidato a emprego das informações relativas:

[52] Consultar o art. 172º e ss. do CT para maiores esclarecimentos.

> a) À sua vida privada, salvo quando estas sejam estritamente necessárias e relevantes para avaliar da respectiva aptidão no que respeita à execução do contrato de trabalho e seja fornecida por escrito a respectiva fundamentação;
> b) À sua saúde ou estado de gravidez, salvo quando particulares exigências inerentes à natureza da actividade profissional o justifiquem e seja fornecida por escrito a respectiva fundamentação.

Assim, um candidato a emprego que seja questionado sobre questões do foro pessoal pode recusar prestá-las, na medida em que não são necessárias, somente convenientes para a entidade empregadora, para o preenchimento da vaga de emprego.

Relativamente às informações relativas à saúde do candidato a emprego, estas só podem ser prestadas a um médico que informará a entidade empregadora se o trabalhador está apto, ou não, a desempenhar a função, conforme dispõe o nº 2 do mesmo artigo. Neste caso, estaremos em sede de contrato de trabalho em que é exigida a realização de uma consulta de medicina do trabalho[53].

Em Espanha, a LOPD[54] prevê o princípio da qualidade dos dados, que resumidamente explana que só devem ser recolhidos dados pessoais que sejam efetivamente necessários para determinada finalidade específica e concreto (Coca, 2016, pp. 101-102), *in casu*, o preenchimento de uma vaga de emprego. Assim, de acordo com a mesma autora, não devem ser recolhidos dados irrelevantes para comprovar a capacidade profissional do candidato a emprego, por exemplo, questionar o estado civil deste é irrelevante face ao real desempenho da função, o mesmo ocorre relativamente à filiação, quer da existência, quer da quantidade. "Em todo o caso, estão fora do conceito de averiguação proibida, aqueles factos ou dados que sejam do conhecimento geral ou que tenham uma divulgação pública", (Coca, 2016, p. 103).

Por último, ao trabalhador é permitido exercer o *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*, em harmonia com o nº 3 do predito artigo. Para além disso, *os ficheiros e acessos informáticos utilizados pelo empregador para tratamento de dados pessoais do candidato a emprego ou trabalhador ficam sujeitos*

[53] Ver o art. 44º do Regime Jurídico da Promoção da Segurança e Saúde no Trabalho, Lei nº 102/2009, de 10 de setembro, disponível em: http://www.pgdlisboa.pt/leis/lei_busca_assunto_diploma.php?buscajur=medicina&exacta=on&artigo_id=&pagina=1&ficha=1&nid=1158&tabela=leis&diplomas=&artigos=&so_miolo= (consultado pela última vez a 13/06/2019 pelas 18:54)

[54] Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, cfr. https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf (consultado pela última vez a 17/06/2019 pelas 22:14)

à legislação em vigor relativa à protecção de dados pessoais, de acordo com o nº 4. No entanto, "a obrigação de informar sobre o tratamento de dados pode-se excluir quando a mesma se deduza pelas circunstâncias em que se recolham os dados ou da sua própria natureza", (Coca, 2016, p. 109). No entanto, conforme já referido, o candidato a emprego deve ter conhecimento dos direitos que lhe assistem, nomeadamente os direitos ARCO, para a qualquer momento exigir o apagamento do seu currículo da base de dados de uma empresa, após ter sido contratado por outra, a título de exemplo.

Assim, concluímos que existem, pelo menos, dois momentos num processo de recrutamento a candidatura e a entrevista de emprego. Ambos regem-se pelos mesmos princípios. De referir que a entrevista de emprego pode ser realizada por videoconferência que consubstancia um tratamento de dados e assim deve ser respeitado o RGPD. Por último, a entrevista de emprego não deve ser utilizada para a obtenção de informação proibida, como por exemplo, a fé religiosa, mas sim para aprofundar as capacidades profissionais do candidato a emprego e explanar as condições de trabalho que lhe serão proporcionadas.

5.1.2. O início da relação laboral, seu desenvolvimento e término

Terminada a fase da procura ativa de emprego e da entrevista de emprego, inicia-se a relação laboral propriamente dita. Geralmente esta inicia-se com a redução de um contrato de trabalho a escrito, não obstante a regra geral seja a inexistência de forma, de acordo com o art. 110º do CT. No entanto, o art. 106º do CT estabelece o dever de informação que pende sobre a entidade empregadora. Este dever estabelece que o trabalhador deve ser informado sobre *aspetos relevantes do seu contrato de trabalho* (nº 1) e, bem assim, *sobre aspectos relevantes para a prestação da actividade laboral* (nº 2). O nº 3 estabelece um elenco mínimo de informações que devem ser prestadas obrigatoriamente ao trabalhador por parte da entidade empregadora, que passamos a indicar:

> *a) A respetiva identificação, nomeadamente, sendo sociedade, a existência de uma relação de coligação societária, de participações recíprocas, de domínio ou de grupo, bem como a sede ou domicílio;*
> *b) O local de trabalho ou, não havendo um fixo ou predominante, a indicação de que o trabalho é prestado em várias localizações;*
> *c) A categoria do trabalhador ou a descrição sumária das funções correspondentes;*
> *d) A data de celebração do contrato e a do início dos seus efeitos;*
> *e) A duração previsível do contrato, se este for celebrado a termo;*

f) A duração das férias ou o critério para a sua determinação;
g) Os prazos de aviso prévio a observar pelo empregador e pelo trabalhador para a cessação do contrato, ou o critério para a sua determinação;
h) O valor e a periodicidade da retribuição;
i) O período normal de trabalho diário e semanal, especificando os casos em que é definido em termos médios;
j) O número da apólice de seguro de acidentes de trabalho e a identificação da entidade seguradora;
l) O instrumento de regulamentação coletiva de trabalho aplicável, se houver.
m) A identificação do fundo de compensação do trabalho ou de mecanismo equivalente, bem como do fundo de garantia de compensação do trabalho, previstos em legislação específica.

O art. 107º, nº 1 do CT esclarece que a informação deve ser *prestada por escrito* o que, por uma questão de conveniência, ocorre num contrato de trabalho ou contrato-promessa de contrato de trabalho, de acordo com o nº 3 do mesmo artigo. Todavia, a lei permite que a informação conste de um ou vários elementos, por exemplo, uma adenda ao contrato de trabalho. A atualização da informação por parte da entidade empregadora deve ser realizada por escrito nos 30 dias subsequentes, sendo o mesmo prazo aplicável ao trabalhador, em harmonia com o art. 109º, nº 1 e nº 3, respetivamente.

Assim, esta é uma fase de "nascimento da relação laboral, (deste modo) o clausulado contratual é um espaço idóneo para o desenvolvimento do princípio da transparência; informando o trabalhador dos ficheiros, responsáveis, encarregados, fins e exercício de direitos ARCO", (Domènech, 2017, p. 196).

Porém, não obstante a importância da prestação em escrito da informação supra, a entidade empregadora tem de cumprir algumas obrigações legais para legitimar a contratação do trabalhador, nomeadamente relativamente a entidades externas, como por exemplo, a Segurança Social. Esta entidade externa, tanto ao trabalhador, como à entidade empregadora, regula a obrigatoriedade da *comunicação da admissão de trabalhadores*, sendo esta a epígrafe do art. 29º do Código dos Regimes Contributivos do Sistema Previdencial de Segurança Social[55]. O nº 1 do predito artigo elenca que a obrigatoriedade de comunicação de admissão de trabalhadores recaí sobre a entidade empregadora[56]. Nesta são comunicados o NISS[57] e se o contrato de trabalho é a termo ou sem termo e *os*

[55] Cfr. http://www.seg-social.pt/documents/10152/15009350/C%C3%B3digo_Contributivo/1e56fad5-0e2a-42c2-b94c-194c4aa64f74 (consultado pela última vez a 18/06/2019 pelas 14:58)
[56] Exceto os trabalhadores do serviço doméstico, de acordo com o art. 29º, nº 1, *in fine*, do diploma em questão.
[57] Número de Identificação de Segurança Social, que permite que a identificação perante a Segurança Social seja única, exata e rigorosa, a nível nacional. Ver http://www.seg-social.pt/pedido-de-niss1 (consultado pela última vez a 19/06/2019 pelas 12:42)

demais elementos necessários ao enquadramento do trabalhador, em harmonia com o nº 3 do mesmo artigo.

Para além da admissão na Segurança Social, com o início do contrato de trabalho é também obrigatória a realização de uma consulta de medicina do trabalho. Esta obrigatoriedade é imposta pelos arts. 281º a 284º do CT[58] e, bem assim, pelo art. 108º, nº 3, al. a) da Lei nº 102/2009, de 10 de setembro que legitima a obrigatoriedade da realização de um exame de admissão *antes do início da prestação de trabalho ou, se a urgência da admissão o justificar, nos 15 dias seguintes*. Para além do exame de admissão, o referido artigo prevê também a obrigatoriedade da realização de exames periódicos *anuais para os menores e para os trabalhadores com idade superior a 50 anos, e de 2 em 2 anos para os restantes trabalhadores* (al. b)); e exames ocasionais *sempre que haja alterações substanciais nos componentes materiais de trabalho que possam ter repercussão nociva na saúde do trabalhador, bem como no caso de regresso ao trabalho depois de uma ausência superior a 30 dias por motivo de doença ou acidente* (al. c)). Assim, cabe à entidade empregadora a responsabilidade de assegurar aos trabalhadores as condições necessárias à prevenção e promoção da saúde dos seus trabalhadores, em todos os aspetos relacionados com o trabalho.

Portanto, podemos desde já concluir que a realização de um contrato de trabalho torna lícito o tratamento de dados para esse fim, não obstante nesta fase estarmos perante obrigações impostas por lei que recaem sobre a entidade empregadora, que é a responsável pelo tratamento, portanto, é aplicável o art. 6º, nº 1, al. c). Assim sendo, por conseguinte, o titular dos dados é o trabalhador que deve ver respeitados os seus direitos aplicáveis em sede de RGPD. De referir que, como se trata de uma obrigação legal estamos perante uma exceção ao exercício do direito ao apagamento dos dados, pelo que não pode ser solicitado o apagamento dos dados por parte do titular dos dados, *in casu*, o trabalhador, em harmonia com o art. 17º, nº 3, al. b).

Para além destas obrigações impostas por lei, importa agora analisar os elementos necessários para a realização do contrato de trabalho como, por exemplo, a fotocópia do cartão de cidadão, que não raras as vezes é solicitada ao trabalhador para assim iniciar funções. Este, numa situação de subordinação jurídica, assente de forma a não ser prejudicado, quer seja pela perda do emprego, quer seja eventuais represálias no futuro.

[58] O art. 284º do CT faz uma remissão expressa para a legislação específica, *in casu*, a Lei nº 102/2009, de 10 de setembro, isto é, o Regime Jurídico da Promoção da Segurança e Saúde no Trabalho.

No entanto, a Lei nº 7/2007, de 5 de fevereiro[59] proíbe expressamente a *reprodução do cartão de cidadão em fotocópia ou qualquer outro meio sem consentimento do titular*, em harmonia com o art. 5º, nº 2 da referida lei. Assim, como o trabalhador é subordinado juridicamente da sua entidade empregadora, nunca prestará o consentimento de forma livre, pelo que o consentimento, em última instância, será nulo. De referir que a entidade empregadora pode recolher os elementos constantes no cartão de cidadão, sem necessidade de o fotocopiar.

Para além destas obrigações, impende ainda ao trabalhador o direito de livre filiação sindical, que é um corolário do *direito à igualdade no acesso a emprego e no trabalho*, conforme refere o art. 24º, nº 1 do CT. Deste modo, incumbe à entidade empregadora o *tratamento informático de dados pessoais dos trabalhadores referentes a filiação sindical, desde que, nos termos da lei, sejam exclusivamente utilizados para cobrança e entrega de quotas sindicais*, em harmonia com o art. 457º, nº 3 do CT. Não obstante o exposto por Carlos Hugo Preciado Domènech (2017, p. 215):

> (…) esta conclusão é em parte questionável, uma vez que a comunicação dos dados de afiliação ao empregador é exclusivamente para fins de desconto e pagamento ao sindicato, esta é uma obrigação questionável que deve ser assumida pelo principal, que deve pagar apenas as dívidas salariais, sem que haja qualquer preceito legal que imponha o desconto em caso de responsabilidade solidária.

Quer isto dizer que, a entidade empregadora tem a obrigação legal de cobrar e entregar as quotas sindicais. No entanto, não é solidariamente responsável pelo seu cabal pagamento, mas é ela quem procede à cobrança e entrega das quotas sindicais, pelo que nos encontramos perante uma situação triangular. Afinal, o trabalhador pode filiar-se sindicalmente, mas é à entidade empregadora que cumpre a cabal cobrança e entrega

Por último, concluímos que também a filiação sindical é um dado pessoal que pode ser tratado pela entidade empregadora de forma a cumprir uma obrigação legal prevista no código do trabalho, ou seja, o tratamento é realizado licitamente desde que somente com as finalidades acima expostas. Assim, ao trabalhador assistem os direitos de acesso, retificação, apagamento, limitação, portabilidade e oposição. Visto que, o próprio trabalhador pode realizar a cobrança e entrega de quotas sindicais por sua

[59] Regula a emissão e utilização do cartão de cidadão. Ver http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2807&tabela=leis&so_miolo= (consultado pela última vez a 19/06/2019 pelas 16:29)

iniciativa. No entanto, sendo da responsabilidade da entidade empregadora, por assim estar previsto em Instrumento de Regulamentação Coletiva de Trabalho, doravante IRCT, esta será a única responsável pela cobrança e entrega das quotas sindicais. Contrariamente ao que acontece em Espanha, em que a responsabilidade é solidária. Assim, neste caso, o trabalhador não poderá exercer o seu direito ao apagamento visto estar em causa o cumprimento de uma obrigação legal.

No âmbito da relação laboral podem ocorrer acidentes de trabalho que são protegidos por seguros de acidentes de trabalho. Esta matéria está prevista no art. 284º do CT que remete para legislação específica, mais concretamente a Lei nº 98/2009, de 4 de setembro[60] no seu art. 1º. Este diploma abrange *o trabalhador por conta de outrem de qualquer atividade, seja ou não explorada com fins lucrativos*, em harmonia com o seu art. 3º, nº 1. Isto é, o trabalhador subordinado juridicamente. Assim, a entidade empregadora deve cumprir o dever de informação previsto no art. 106º, nº 3, al. j) do CT, isto é, informar o trabalhador do *número da apólice de seguro de acidentes de trabalho e a identificação da entidade seguradora*. Deste modo, a entidade empregadora deve remeter à seguradora aos dados pessoais necessários à sua inserção na apólice do seguro de acidentes de trabalho, de forma a cumprir a obrigação legal de reparação de acidentes de trabalho. Assim, também a inserção do trabalhador na apólice do seguro de acidentes de trabalho consubstancia o cumprimento de uma obrigação legal, pelo que o trabalhador pode exercer os seus direitos de acesso, retificação, limitação, portabilidade e oposição. O apagamento não é possível visto que se trata de uma obrigação legal.

O corolário da prestação de trabalho é a retribuição, que o seu apuramento, não raras as vezes, é da responsabilidade de um serviço de contabilidade externo à entidade empregadora. Deste modo, a entidade empregadora celebra um contrato de prestação de serviços com o serviço de contabilidade, do qual o trabalhador é alheio, mas para o qual os seus dados pessoais são transmitidos para mensalmente se realizar o seu processamento salarial. O CT prevê somente o dever de informar o trabalhador do valor e da periodicidade da retribuição, de acordo com o art. 106º, nº 3, al. j).

Posto isto, cumpre desde já analisar a licitude da transferência de dados entre a entidade empregadora e a empresa de contabilidade. Ora, tendo as partes realizado um

[60] Este diploma regulamenta o Regime de Reparação de Acidentes de Trabalho e de Doenças Profissionais. Cfr. http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=1156A0001&nid=1156&tabela=leis&pagina=1&ficha=1&so_miolo=&nversao=#artigo (consultado pela última vez a 26/06/2019 pelas 12:02)

contrato de prestação de serviços, o tratamento de dados é lícito pois estamos perante uma obrigação contratual, ao abrigo do art. 6º, nº 1, al. b). Porém, a licitude do tratamento dos dados pessoais não afasta o exercício do direito à proteção de dados pessoais, ainda que em sede de subcontratação. Deste modo, a entidade empregadora deve privilegiar o estabelecimento de um vínculo contratual com *subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas de uma forma que o tratamento satisfaça os requisitos do presente regulamento e assegure a defesa dos direitos do titular dos dados*, em harmonia com o art. 28º, nº 1. A prestação de garantias depende do caso concreto, do local onde os dados serão tratados, se o serão com o uso de meios próprios, entre outros fatores. Assim, podemos concluir que esta "pode concretizar-se de modo diverso: quer quanto ao conteúdo, quer quanto à forma, consoante as caraterísticas específicas de cada relação de subcontratação", (Pinheiro et al., 2018, p. 420).

Esclarecemos que, "não se afiguraria compatível com o objeto, nem com os objetivos do RGPD que o responsável pelo tratamento, como figura central da imputação de obrigações no âmbito do RGPD pudesse desresponsabilizar-se por via do recurso à subcontratação do tratamento de dados", (Pinheiro et al., 2018, p. 419). Assim, em harmonia com o art. 24º, nº 1, *tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades*. Estas podem ser *a pseudominização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento*, de acordo com o art. 25º, nº 1. Deste modo, o responsável pelo tratamento, *in casu* a entidade empregadora, deve *assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento*.

Deste modo, ao serviço de contabilidade apenas devem ser disponibilizados os dados pessoais estritamente necessários para o correto processamento salarial. De acordo com o art. 25º, nº 2, em parte citado acima, *essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em especial, essas medidas asseguram que, por defeito, os dados*

pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares. Quer isto dizer, que a entidade empregadora quando transmite dados a subcontratantes deve realizá-lo com conta, peso e medida, em harmonia com as necessidades concretas. O mesmo ocorre com a medicina no trabalho e o seguro de acidentes de trabalho, visto que são também entidades externas à entidade empregadora. Deste modo, apenas devem ser transmitidos aos respetivos subcontratantes os dados pessoais que sejam realmente necessários ao caso concreto, evitando a transmissão de dados excessivos e não proporcionais ao tratamento de dados que será realizado, em harmonia com o princípio da minimização da recolha de dados. Por outro lado, não deve ser dado acesso aos dados pessoais em questão a "um número indeterminado de pessoas singulares".

Afinal, também os subcontratantes têm um responsável pelo tratamento que deve ser do conhecimento da entidade empregadora e do titular dos dados, assim como as pessoas singulares que irão tratar os dados pessoais que lhes forem transmitidos. Numa correlação tal que a entidade empregadora consiga saber, a todo o tempo, quem são as pessoas singulares que estão a tratar os dados pessoais e, bem assim, o responsável pelo tratamento.

Em outro sentido, o subcontratante pode *contratar outro subcontratante para a realização de operações específicas de tratamento de dados por conta do responsável pelo tratamento,* em harmonia com o art. 28º, nº 4. Sendo abrangido pelas mesmas normas relativas à proteção de dados pessoais que o subcontratante inicial e o responsável pelo tratamento. Quer isto dizer que toda a cadeia de subcontratação, assim como o principal responsável pelo tratamento, devem cumprir a matéria relativa ao RGPD, de forma a garantir que o titular dos dados saiba como e por quem os seus dados pessoais estão a ser tratados a todo o momento, numa estreita relação de confiança.

Não obstante o exposto no art. 28º, nº 2, que explana que *o subcontratante não contrata outro subcontratante sem que o responsável pelo tratamento tenha dado, previamente e por escrito, autorização específica ou geral. Em caso de autorização geral por escrito, o subcontratante informa o responsável pelo tratamento de quaisquer alterações pretendidas quanto ao aumento do número ou à substituição de outros subcontratantes, dando assim ao responsável pelo tratamento a oportunidade de se opor a tais alterações*. Não obstante o exposto no nº 4 do mesmo artigo *se esse outro subcontratante não cumprir as suas obrigações em matéria de proteção de dados, o subcontratante inicial continua a ser plenamente responsável, perante o responsável pelo*

tratamento, pelo cumprimento das obrigações desse outro subcontratante, "isto é, responde como se o incumprimento lhe fosse imputável", (Pinheiro et al., 2018, p. 421).

Em harmonia com Tatiana Duarte (Pinheiro et al., 2018, p. 422), para além disso existe a:

> necessidade de modelar os termos da responsabilidade de cada uma das partes à realidade subjacente a cada relação de subcontratação. Se o subcontratante inicial estiver vinculado a sujeitar uma subcontratação ulterior a autorização do responsável pelo tratamento, mas estiver incumbido de fiscalizar o cumprimento das obrigações daquele - não deverá responder pela escolha do responsável pelo tratamento, mas deverá responder pelo incumprimento das obrigações cujo cumprimento ficou adstrito de verificar. Se o responsável pelo tratamento quiser autorizar especificamente cada subcontratante ulterior, como ainda, pretender verificar o cumprimento das suas obrigações, afigura-se-nos desproporcional responsabilizar o subcontratante inicial, pela aplicação cega do nº 4 do artigo 28º do RGPD.

Isto é, não nos devemos limitar a uma aplicação taxativa do nº 4 do art. 28º, mas sim fazer uma análise casuística para melhor entender a cadeia de subcontratação em causa e as suas especificidades, nomeadamente através da análise da autorização do responsável pelo tratamento.

Deste modo, torna-se importante o estabelecimento de relações contratuais com entidades que também elas cumpram as normas do direito à proteção de dados pessoais, de forma a salvaguardar eventuais incumprimentos, e acima de tudo proteger os dados pessoais dos titulares dos dados, *in casu*, os trabalhadores de determinada entidade empregadora. Portanto, deve dar-se uso à figura da certificação[61] prevista no art. 42º, que apesar de voluntária (nº 3), deve ser encarada como um direito/dever das empresas. No sentido em que estas têm o direito de serem certificadas para assim serem consideradas instituições dignas e prestigiadas e, por outro lado, um dever, visto que os titulares dos dados sentir-se-ão mais seguros na recolha dos dados ao saberem que aquela empresa cumpre as normas relativas ao direito à proteção de dados pessoais.

No mesmo sentido, o já referido art. 88º estabelece que os Estados-Membros podem estabelecer normas mais específicas para o contexto laboral. Assim, a título de sugestão, sugerimos a implementação de códigos de conduta, como requisito para a certificação de empresas, de forma a que estas o cumpram sob pena de deixarem de ser elegíveis para a certificação. Os códigos de conduta estão previstos no art. 40º que recomenda a sua realização *tendo em conta as caraterísticas dos diferentes setores de*

[61] A Lei nº 58/2019, de 8 de agosto prevê no seu art. 14º que *a autoridade competente para a acreditação dos organismos de certificação em matéria de proteção de dados é o IPAC, I.P.*

tratamento e as necessidades específicas das micro, pequenas e médias empresas. A Lei nº 58/2019, de 8 de agosto remete essa competência para a CNPD, no seu art. 15º. Não obstante, aconselhamos o desenvolvimento e a implementação de um código de conduta próprio, como se de um manual de procedimentos se tratasse, sempre em harmonia com as normas relativas à proteção de dados pessoais. De forma a que, todos os trabalhadores tenham acesso ao mesmo e consigam saber como se processa o tratamento dos seus dados pessoais, em conformidade com o princípio da transparência que rege todos acontecimentos em matéria de proteção de dados pessoais. Os códigos de conduta podem ser cumpridos quer pelos responsáveis pelo tratamento ou os subcontratantes, quer pelos responsáveis ou subcontratantes que a ele não estão sujeitos, em harmonia com os nºs 2 e 3 do art. 40º. De referir que, de acordo com o art. 24º, nº 3, *o cumprimento de códigos de conduta* (…) *pode ser utilizado como elemento para demonstrar o cumprimento das obrigações do responsável pelo tratamento*, reforçando ainda mais a ideia de direito/dever.

Pese embora, de acordo com Carlos Jorge Gonçalves (Pinheiro et al., 2018, p. 485), a elaboração de códigos de conduta

> além de constituir uma **medida atenuante** (nosso negrito) no âmbito da aplicação de uma coima e de presunção de garantias de segurança dos dados e proteção dos respetivos titulares, a falta de elaboração de projetos de códigos de conduta nenhuma consequência desfavorável parece trazer para os responsáveis e subcontratantes. Aliás, a presunção das garantias de segurança e de proteção poderão ser facilmente ilididas.

Apesar do exposto, realçamos o facto da elaboração de códigos de conduta consubstanciar uma medida atenuante e, quanto mais não seja, uma forma de os responsáveis pelo tratamento e os subcontratantes saberem como agir em determinadas situações, daí que falemos em manual de procedimentos. Isto é, uma sistematização da tramitação a adotar aquando da recolha dos dados, quando for realizado um pedido de acesso, de apagamento, de retificação, entre outros. De modo que os profissionais que lidam diretamente com estas questões tenham um meio para se socorrerem em caso de dúvida. Afinal, a implementação das normas relativas à proteção de dados pessoais não é realizada somente pelo responsável pelo tratamento, mas sim por todos os trabalhadores, que não o sendo, têm acesso aos mesmos para cumprirem as suas funções laborais.

Deste modo, torna-se importante reforçar que uma empresa deve ser dominada pela cooperação entre todos os trabalhadores, de forma a que o tratamento de dados

realizado por ela seja realizado da forma mais lícita e controlada possível, com a aplicação de medidas técnicas e organizativas como por exemplo, "pseudominização e cifragem dos dados pessoais, tratamento apenas dos dados pessoais que sejam necessários para cada finalidade específica e a garantia de que os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares", (Pinheiro et al., 2018, p. 495).

No final de contas, "o processamento desses dados por parte da entidade empregadora tem que ser adequado, pertinente e não excessivo para a finalidade para que se solicitam", (Coca, 2016, p. 167), em harmonia com o princípio da minimização da recolha de dados.

Por último, cumpre analisar o que ocorre com o término da relação laboral, seja por caducidade, denúncia, entre outras causas, o que releva é que existiu uma relação laboral que, entretanto, terminou. Portanto, importa saber como a entidade empregadora deve agir relativamente aos dados pessoais que possui do ex-trabalhador. Afinal, não deve fazer um uso abusivo dos mesmos seja em que momento for. Deste modo, regra geral, a entidade empregadora deve eliminar os dados pessoais que já não serão necessários, isto é, em que não existe licitude para o tratamento, em harmonia com o princípio da proporcionalidade na recolha de dados. Visto que, terminando a relação laboral termina também a licitude para o tratamento dos dados pessoais de um determinado trabalhador.

Conforme analisado nos parágrafos acima, a licitude do tratamento de dados pessoais de trabalhadores baseia-se, maioritariamente, em obrigações legais. Assim, terminando o contrato, extinguem-se essas obrigações legais. No entanto, podem existir outras obrigações legais que se sobrepõem às analisadas. Vejamos, acima referimos que a entidade empregadora poderia contratar um serviço de contabilidade externo para realizar o processamento salarial, e não só, no entanto referimos ainda que a contabilidade também pode ser realizada internamente.

Deste ponto de vista, terminada a relação laboral todos os dados pessoais que tenham sido utilizados para efeitos de processamento salarial serão eliminados. Porém o Código Comercial[62] não se coaduna neste sentido, visto que o seu art. 40º prevê a obrigação de arquivar *a sua escrituração mercantil e os documentos a ela relativos, devendo conservar tudo pelo período de 10 anos*. Quer isto dizer que a entidade empregadora tem a obrigação legal de conservar os registos de contabilidade, incluindo

[62] Aprovado pela Carta de Lei de 28 de junho de 1888, contando atualmente com diversas alterações.

os relativos ao processamento salarial que, por sua vez, possuem dados pessoais, como NIF[63], NISS, estado civil e regime de tributação pelo prazo de 10 anos. No entanto, os dados pessoais acima mencionados não podem ser utilizados pela entidade empregadora com outra finalidade que não a existente num processo de inspeção, promovido, a título de exemplo, pela Segurança Social ou a ACT. Assim, concluído o prazo de 10 anos os dados pessoais devem ser destruídos. Afinal não existe nenhuma finalidade subjacente à sua conservação por um período superior. Da mesma forma o estipula a Deliberação 60/2000 da CNPD[64] no seu art. 3º nº 1 da sua autorização de isenção nº 1/99, que refere que *a informação não poderá ser conservada para além de 10 anos sobre a cessação da relação de trabalho*. Quanto ao conceito de "informação" o art. 2º do mesmo diploma elenca as categorias de dados às quais se refere e que passamos a citar:

> a) «Dados de identificação (nosso sublinhado)» — nome, data de nascimento, naturalidade, filiação, sexo, nacionalidade, morada e telefone, habilitações literárias, número de bilhete de identidade, número de contribuinte, número de segurança social, número de sócio do sindicato;
> b) «Situação familiar (nosso sublinhado)» — estado civil, nome do cônjuge, filhos ou pessoas a cargo e outras informações suscetíveis de determinar a atribuição de complementos de remuneração;
> c) «Sobre a atividade profissional (nosso sublinhado)» — horário e local de trabalho, número de identificação interno, data de admissão, antiguidade, categoria profissional, antiguidade na categoria, nível/escalão salarial, natureza do contrato;
> d) «Elementos relativos à retribuição (nosso sublinhado)» — retribuição base, outras prestações certas ou variáveis, subsídios, férias, assiduidade e absentismo, licenças, outros elementos relativos à atribuição de complementos de retribuição, montante ou taxa em relação aos descontos obrigatórios ou facultativos;
> e) «Outros dados (nosso sublinhado)» — grau de incapacidade do trabalhador ou de membro do agregado familiar, incapacidade temporária resultante de acidente de trabalho ou de doença profissional, local de pagamento, número de conta bancária, número de associado e identificação da entidade à ordem da qual devem ser efetuados descontos obrigatórios ou facultativos (sindicato, serviços sociais, grupo desportivo, etc.).

Por seu turno, a seguradora de acidentes de trabalho, um subcontratante da entidade empregadora, conforme explanado supra, tem previsto um prazo de prescrição superior. Assim, "até ao decurso do prazo legal de prescrição de todas as obrigações emergentes do contrato de seguro após o termo deste (em regra, 20 anos, art. 309º do CC),

[63] Número de Identificação Fiscal

[64] Cfr. https://dre.pt/web/guest/pesquisa-avancada/-/asearch/2028668/details/maximized?search= (consultado pela última vez a 18/07/2019 palas 15:50)

e no âmbito da Gestão de Sinistros - danos corporais, em Acidentes de Trabalho, pelo prazo de 20 anos"[65].

Portanto, reiteramos a importância da implementação de um manual de procedimentos, formalmente designado de código de conduta, elaborado em cooperação com o DPO e o responsável pelo tratamento de cada departamento de uma empresa. Este deve ser um elemento facilitador e fidedigno do cumprimento da legislação em matéria de proteção de dados pessoais. Deste modo, o *modus operandi* do tratamento de dados pessoais será claro e explícito para todos quanto os que diariamente lidam com eles. Por sua vez, os titulares de dados pessoais sentir-se-ão confiantes e protegidos ao revelá-los. Por último, a existência de certificação será uma garantia adicional para os titulares dos dados e, bem assim, para os responsáveis pelo tratamento que terão a aprovação de uma entidade externa e saberão que estão a proceder corretamente.

5.2. O armazenamento de dados pessoais

Por fim, os dados pessoais dos trabalhadores são armazenados, seja em suporte físico, seja em suporte digital. O suporte físico é o método tradicional de arquivo e este pode ser realizado em dossiers que posteriormente serão depositados em armários. O suporte digital pode comportar o arquivo de dados pessoais num ficheiro Excel, que posteriormente será confiado a uma *cloud*, afinal estamos na era digital. confinado

O armazenamento de dados pessoais de trabalhadores é uma realidade inerente ao desempenho de diversas funções, afinal a pessoa responsável pela emissão e entrega do recibo de vencimento tem de ter acesso aos dados pessoais dos respetivos trabalhadores. O responsável pela participação de um acidente de trabalho também o tem, assim como quem entrega os valores mensais às Finanças e à Segurança Social relativos ao vencimento. Quer isto dizer que o armazenamento de dados pessoais é lícito se servir somente o cabal desempenho das funções de determinado trabalhador ou grupo de trabalhadores, por exemplo, as descritas acima. Deste modo, ultrapassada a questão da licitude, importa implementar medidas técnicas e organizativas, de forma ao armazenamento de dados ser realizado em conformidade com o RGPD. Afinal, "cumpre

[65] Cfr. https://www.allianz.pt/protecao-dados/finalidade-e-fundamentos-do-tratamento (consultado pela última vez a 18/07/2019 pelas 17:22)

concluir que o RGPD se apresenta como um instrumento essencial para a modernização e harmonização das regras de proteção de dados na UE, baseando-se, essencialmente, na garantia dos direitos e liberdades fundamentais dos cidadãos, perante os novos desafios da era digital", (Lopes, 2018, p. 69).

Deste modo, o ficheiro, quer seja digital, quer seja físico, deve ser "criado com a justificação de cumprir uma série de finalidades e funções legítimas", ou seja, estamos perante "bases de dados necessárias", (Coca, 2016, p. 186). Estas bases de dados podem conter diversos tipos de informações, vejamos os seguintes exemplos (Domènech, 2017, p. 234):

> arquivos organizados em suporte de papel como historial clínico, faturas, gravações analógicas de som e vídeo de um sistema de videovigilância, negativos fotográficos organizados e classificados por datas, impressões digitais dos trabalhadores de uma empresa com a identificação do respetivo titular e sua digitalização para o seu processamento informático num sistema de controlo de acessos, etc.

Pese embora, estejamos perante bases de dados que contêm informações necessárias para o cabal desempenho de funções, estas bases de dados devem estar protegidas do acesso indevido às mesmas. Na prática, os dossiers que contenham dados pessoais devem estar organizados num armário com um cadeado. A chave do cadeado deve estar na posse do responsável pelo tratamento. Posteriormente, os colaboradores que necessitem de determinado dossier solicitam o mesmo ao responsável pelo tratamento, mediante a indicação da finalidade concreta. Deste modo, os dados pessoais estão sempre protegidos e somente têm acesso aos mesmos as pessoas que efetivamente deles necessitem, por exemplo, o controlo dos tempos de trabalho. Para além disso, recomendamos a implementação de um formulário em que é indicada a data e o trabalhador que teve acesso a determinado dossier. Em suporte digital, a proteção será realizada de forma diferente, com a atribuição de uma palavra-passe que somente o responsável pelo tratamento saberá, para além de que as alterações realizadas aos ficheiros deverão ser assinadas pelo trabalhador que as efetuou.

Desta forma, os dados pessoais estarão protegidos do acesso indevido e injustificado, que também será uma garantia para os titulares dos dados, *in casu*, os trabalhadores. Estas medidas técnicas e organizativas devem constar do manual de procedimentos, que posteriormente integrarão o código de conduta e serão uma mais-valia em qualquer empresa.

Esta página foi intencionalmente deixada em branco

6. Conclusão

Com a presente dissertação analisámos, numa primeira fase, as vertentes do CT diretamente relacionadas com o RGPD, nomeadamente o direito à reserva da vida privada, a subordinação jurídica e o direito à desconexão. Esclarecemos que o trabalhador é a parte mais débil da relação laboral pelo que merece especial proteção, nomeadamente no âmbito da proteção de dados pessoais. Até aqui, compreendemos que o trabalhador tem a sua vida privada que deve ser separada da vida profissional, não só em termos de horários, como também em comunicações.

De seguida, analisámos a criação do RGPD, com a revogação da anterior Diretiva, que teve uma aplicação direta em todos os Estados Membros da UE. O RGPD estabeleceu a forma como deve ser realizada a recolha e o tratamento de dados pessoais e que ambos devem ser realizados com um fundamento lícito para uma finalidade única e especificada. O fundamento pode ser, desde a execução de um contrato, o cumprimento de uma obrigação jurídica, o consentimento, entre outros.

O consentimento é uma matéria que pede especial cautela, pois este não pode ser solicitado sem a indicação do modo como os dados serão tratados e para que finalidade. Estes nunca podem ser tratados para uma finalidade diferente para a qual o consentimento foi prestado, nem para uma finalidade camuflada ou agregada à execução de um contrato, nem ser a contrapartida de algo. O consentimento deve ser prestado através de uma manifestação, quer seja uma assinatura ou uma ação. Este tem de ser prestado de forma expressa, livre e inequívoca.

Com a entrada em vigor do RGPD, os titulares dos dados encontram-se protegidos por novos direitos, mediados pelo princípio da transparência. Deste modo, os titulares dos dados, podem exercer os seus direitos de acesso, de informação, de retificação, de limitação, o direito ao apagamento e a portabilidade dos dados pessoais. Todos estes direitos encontram-se à disposição dos titulares dos dados. No entanto, o seu exercício só é possível de forma racional e acautelada, mediante uma análise casuística, tal como as decisões automatizadas e a definição de perfis.

O tratamento de dados pessoais sensíveis tem a sua tónica por se tornar revelador de aspetos da vida privada. Dentre os quais constam a convicção política e a fé religiosa, por exemplo. O tratamento destes não é totalmente proibido e o seu tratamento pode ser

permitido em situações concretas. Por exemplo, perante um interesse público, por exemplo, a saúde pública. No entanto, nos casos em que o tratamento de dados sensíveis é realizado, é conveniente que o mesmo o seja por profissionais vinculados ao dever de sigilo profissional.

A realidade laboral sofreu diversas alterações, desde o uso de dispositivos eletrónicos pessoais como ferramenta de trabalho e a gestão de dispositivos móveis. Afinal, estamos na era digital e, por conseguinte, na era do trabalho 4.0. O que torna o trabalho mais invasivo da esfera da vida privada dos trabalhadores, que por estarem subordinados juridicamente necessitam de proteção nesse sentido.

Desta forma, a utilização de ferramentas que permitam a monitorização do trabalhador, deve ser realizada, nos casos em que efetivamente é necessário, de acordo com o princípio da minimização da recolha dos dados. Isto é, o tratamento de dados pessoais obtidos através da monitorização das ferramentas de trabalho dos trabalhadores deve realizar-se de forma a não invadir a esfera da vida privada. No mesmo sentido, também os trabalhadores devem ter o cuidado de não utilizar os instrumentos de trabalho disponibilizados pela entidade empregadora para fins pessoais. Deste modo, tanto a entidade empregadora, como o trabalhador, convivem numa simbiose de interesses em termos de vinculação às normas da proteção de dados pessoais.

Uma das ferramentas que pode permitir a monitorização dos trabalhadores é a instalação de câmaras de vigilância, esta deve ser realizada com o intuito da proteção de pessoas e bens e nunca com a finalidade de controlar o desempenho profissional dos trabalhadores.

Na presente dissertação, foram analisados dois acórdãos que convergem: trabalhadores que sabendo que estavam a ser vigiados através de câmaras de vigilância, devido ao local em local em que exercem a sua atividade, desrespeitam o princípio da boa-fé e da confiança entre entidade empregadora e trabalhador, o que inviabiliza a continuidade da relação laboral. Deste modo, tornou-se importante possibilitar a licitude das gravações obtidas desta forma. Isto é, a instalação das câmaras de vigilância nunca teve como intuito controlar o desempenho profissional dos trabalhadores, mas sim a proteção de pessoas e bens. A captação das práticas dos atos ilícitos ocorreu por dolo dos trabalhadores, que sabendo da existência das câmaras de vigilância não ponderaram o peso dos seus atos. Assim, a não responsabilização destes atos por parte dos trabalhadores

por as provas terem sido obtidas com a finalidade da proteção de pessoas e bens abriria o precedente de que o poderiam realizar sem consequências a nível laboral.

Uma nova realidade é a realização de teletrabalho, o que permite aos trabalhadores uma maior autonomia na conciliação da vida pessoal e profissional. O teletrabalho resume-se, regra geral, a trabalhar a partir do seu domicílio em vez das instalações da entidade empregadora. Esta realidade levanta inúmeras questões. Afinal, o trabalhador encontra-se subordinado juridicamente e à entidade empregadora cabe o poder de direção.

Deste modo, o controlo do desempenho do trabalhador pode ser realizado mediante visitas ao domicílio do trabalhador, cujo horário de visitas se compreende entre as 9 e as 19 horas, o que se compreende também pelo facto de os instrumentos de trabalho serem da entidade empregadora e esta pretender a proteção dos seus bens. No entanto, se o trabalhador tratar dados sensíveis no desempenho das suas funções ou se tiver na sua posse um instrumento de trabalho muito valioso, a instalação de câmaras de vigilância pode ocorrer, não obstante as imagens captadas deverem limitar-se à zona em que o trabalhador exerça as funções. Por fim, nos casos em existam suspeitas de irregularidades por parte do trabalhador também pode ser realizada a instalação de câmaras de vigilância para comprovar a existência destas ou refutá-las.

Com o RGPD surgiu a figura do DPO, que se configura num responsável pelo cumprimento do mesmo. Este não é obrigatório em todas as empresas. O DPO tanto pode ser um trabalhador da empresa, como externo à mesma. Em qualquer dos casos, sobre ele recai o dever de sigilo e confidencialidade, inclusive após o termo do exercício das suas funções. O exercício das suas funções é realizado com autonomia técnica, imparcialidade e idoneidade, inclusive perante a entidade empregadora, se for trabalhador da empresa. Estes profissionais devem ser vistos como externos à empresa, mesmo sendo trabalhadores. No sentido em que, cumprem o estipulado no RGPD, na Lei nº 58/2019, de 8 de agosto e restante legislação nacional aplicável sem qualquer tipo de influências. De realçar que o DPO não pune a empresa na eventualidade de um incumprimento, mas sim evita a existência destes. Sendo a prevenção a melhor arma para os evitar.

A relação laboral é pautada pela existência de uma necessidade do trabalhador que assim inicia a sua procura ativa de emprego. Esta procura de emprego consiste hoje em dia, maioritariamente, no envio de um e-mail com o currículo. Ora, o currículo contém dados pessoais que devem ser protegidos em matéria de direito da proteção de dados pessoais. Deste modo, o seu prazo de conservação pode limitar-se ao tempo necessário

para o preenchimento da vaga, se outro candidato for selecionado, ou então, à sua conservação para o preenchimento de eventuais vagas que possam existir. De todo o modo, o candidato a emprego deve sempre ser informado do que irá ocorrer ao seu currículo, se será eliminado da base de dados ou se, pelo contrário, será conservado na base de dados da empresa. Não obstante as empresas deverem manter durante cinco anos o registo dos processos de recrutamento efetuados.

Para além da procura ativa de emprego por iniciativa própria do trabalhador, existem empresas que prestam consultadoria de recursos humanos, especializadas em recrutamento, as ETT's e o IEFP. Todas com a finalidade de auxiliar candidatos a emprego a encontrar emprego e as empresas a obterem o preenchimento das suas vagas em aberto. Em qualquer dos casos, para o preenchimento das vagas em aberto é realizada uma entrevista presencial ou por videoconferência com a finalidade de esclarecer eventuais dúvidas que se suscitaram com a análise do currículo e, bem assim, para a empresa explicar as condições de trabalho que serão proporcionadas ao candidato a emprego. A entrevista nunca deve ser realizada com a finalidade de obter informação pessoal não relevante para o preenchimento da vaga em aberto, mas sim para aprofundar e valorizar as habilitações académicas e a experiência profissional do trabalhador.

De seguida à entrevista de emprego pode ocorrer o início da relação laboral, esta pauta-se pela outorga de um contrato de trabalho e com ela a entidade empregadora vê-se obrigada a cumprir diversas obrigações legais, como a inscrição na Segurança Social, a inserção numa apólice de seguro de acidentes de trabalho, a realização de uma consulta de medicina no trabalho, a cobrança e entrega de quotas sindicais, se existirem, e o processamento salarial, que pode ser realizado por uma entidade externa à entidade empregadora.

Nesta matéria, estamos perante subcontratantes, deste modo a entidade principal deve garantir que o seu subcontratante apresenta as mesmas garantias em termos de proteção de dados pessoais. Existindo acreditação e certificação, como assim prevê o art. 14º, nº 1 da Lei nº 58/2019, de 8 de agosto, recomendamos o estabelecimento de um vínculo de subcontratação somente com entidades também certificadas. Para além disso, recomendamos a implementação de códigos de conduta, que se traduzem em verdadeiros manuais de procedimentos, de forma a que qualquer trabalhador, que não sendo responsável pelo tratamento e lide com dados pessoais no seu quotidiano profissional,

saiba como agir perante um pedido de informação, de acesso, de retificação, de oposição, entre outros.

Ocorrendo a cessação do contrato de trabalho, o Código Comercial prevê um prazo de conservação da "escrituração mercantil" de 10 anos. Por seu turno, as seguradoras de acidentes de trabalho preveem um prazo de prescrição de 20 anos. Findos estes prazos as entidades são obrigadas a eliminá-los visto que já não existe nenhuma finalidade para a sua conservação.

Por fim, o armazenamento dos dados pessoais dos trabalhadores deve ser realizado da forma mais confidencial possível. De forma a que se saiba, a todo o tempo, quem acedeu aos dados pessoais e se efetuou alterações. Se estivermos perante um armazenamento digital, esta verificação é fácil de realizar. Por conseguinte, se for um arquivo físico, pode-se implementar um cadeado que somente o responsável pelo tratamento possui a chave e realizar um registo das pessoas a quem disponibiliza a chave.

Face ao exposto, concluímos que a relação laboral apresenta inúmeras nuances em matéria de RGPD que aqui se analisaram. A monitorização do trabalhador tornou-se mais difícil com a chegada do RGPD e mais recentemente da Lei nº 58/2019, de 8 agosto. Assim, concluímos que o RGPD reforça os direitos dos trabalhadores, não sendo possível à entidade empregadora monitorizar o mesmo sem a observância dos limites impostos por lei. Ou seja, em determinadas situações pode existir uma monitorização do trabalhador, dentro dos limites da lei, o que por si só não consubstancia uma monitorização do trabalhador, mas sim o cumprimento de uma obrigação imposta por lei.

Esta página foi intencionalmente deixada em branco

Bibliografia

Alves, L. D. (2019). A videovigilância e a compressão da privacidade. In: *Anuário da Proteção de Dados 2019* (pp. 137–155). Lisboa: CEDIS.

Calvão, F. (2019). O RGPD e o papel da Comissão Nacional de Proteção de Dados. In: *Revista de Direito Administrativo n.º 4*, 68–70.

Catala, R. P. (2018). La Protección del Derecho a la Intimidad del Teletrabajador. In: *Revista jurídica de los Derechos Sociales* (Vol. 8 núm, pp. 113–135). Sevilha: Lex Social.

Coca, O. G. (2016). *La Protección de Datos de Carácter Personal em los Procesos de Búsqueda de Empleo*. Ediciones Laborum.

Cordeiro, A. M. (2018). *Direito do Trabalho*. Coimbra: Almedina.

Domènech, C. H. P. (2017). *El Derecho a la Protección de Datos en el Contrato de Trabajo*. Navarra: Thomson Reuters Aranzadi.

Duarte, D. P. (2018). Registo de Tempos de Trabalho e Proteção de Dados Pessoais. In: *Tempo de Trabalho e Tempos de Não Trabalho: o regime nacional do tempo de trabalho à luz do direito europeu e internacional* (1ª edição, pp. 173–183). Lisboa: AAFDL Editora.

Fernandes, F. L. (2017). Organização do trabalho e tecnologias de informação e comunicação. In: *Revista Questões Laborais nº 50* (pp. 7–17). Coimbra: Almedina.

Gomes, J. M. V. (2007). *Direito do Trabalho* (Volume I). Coimbra: Coimbra Editora.

Hintze, M. (2018). Viewing the GDPR through a de-identification lens: a tool for

compliance, clarification, and consistency. In: *International Data Privacy Law* (Volume 8, pp. 86–101). Oxford: Oxford University Press. Disponível em: https://academic.oup.com/idpl/articleabstract/8/1/86/4763693?redirectedFrom=fulltext (consultado pela última vez a 24/09/2018 pelas 14:45)

Lopes, T. V. (2018). Responsabilidade e governação das empresas no âmbito do novo Regulamento sobre a Proteção de Dados. In: *Anuário da Proteção de Dados* (pp. 45–69). Lisboa: CEDIS.

Mañas, J. L. P., Caro, M. Á., Gayo, M. R., Varela, B. A., Martínez, C. A., Riguadias, C. Á., … Sánchez, M. C. (2016). *Reglamento General de Protección de Datos*. Madrid: Reus Editorial.

Moreira, T. C. (2017a). Algumas Implicações Laborais do Regulamento Geral de Proteção de Dados Pessoais no Trabalho 4.0. In: *Questões Laborais nº 51* (pp. 9–34). Coimbra: Almedina.

Moreira, T. C. (2017b). O direito à desconexão dos trabalhadores. In *Revista Questões Laborais nº 49* (pp. 7–28). Coimbra: Almedina.

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

Sousa, D. A. e. (2018). Registo dos Tempos de Trabalho e Proteção de Dados Pessoais. In: *Tempo de Trabalho e Tempos de Não Trabalho: o regime nacional do tempo de trabalho à luz do direito europeu e internacional* (1ª edição, pp. 117–156). Lisboa: AAFDL Editora.

Sousa, I. P. de. (2018). Do respeito pela vida (relativamente) privada no âmbito da videovigilância. In: *Fórum de Proteção de Dados Nº 5*, (pp. 60–71).

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. In: *International Data Privacy Law* (Volume 7, pp. 76–99). Oxford: Oxford University Press. Disponível em: https://academic.oup.com/idpl/article/7/2/76/3860948 (consultado pela última vez a 24/09/2018 pelas 14:49)