Quaestio Iuris

vol.14, nº.03, Rio de Janeiro, 2021. pp. 1001-1038
DOI: 10.12957/rqi.2021.58565

O CONTROLO DO TRABALHADOR EM PORTUGAL, À LUZ DO CÓDIGO DO TRABALHO PORTUGUÊS E DO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS

THE CONTROL OF WORKERS IN PORTUGAL, IN THE LIGHT OF THE PORTUGUESE LABOR CODE AND THE GENERAL DATA PROTECTION REGULATION

Patrícia Anjos Azevedo[1]
Daniela Rodrigues[2]
Susana Sousa Machado[3]

RESUMO

O presente contributo versa sobre os meios de vigilância à distância e a sua relação com o tratamento dos dados pessoais dos trabalhadores, com especial relevo na geolocalização e a legitimidade da averiguação da atividade do trabalhador, o que constitui o objetivo geral deste nosso contributo. Desde logo, temos formas de controlo, tais como a tecnologia por radiofrequência; os dados biométricos; o controlo de alcoolemia ou de substâncias psicoativas; o controlo médico no que respeita aos exames complementares e o controlo da utilização de meios eletrónicos, entre outros.

O nosso objetivo específico é, precisamente, apresentar todas estas situações, bem como os limites ao poder de controlo que o empregador possui. É também digna de destaque a matéria do tratamento posterior dos dados pessoais pelo empregador obtidos através dos sistemas de controlo ao seu dispor.

Quanto ao método, apresentamos, basicamente, uma revisão de literatura (doutrina), tentando efetuar algumas ligações à lei e a jurisprudência.

Como resultados, pretendemos demonstrar que, hoje em dia, com tantos meios ao seu dispor, será fácil que o empregador possa eventualmente colocar em causa dos direitos dos trabalhadores.

[1] CIICESI, ESTG /P. PORTO – Centro de Inovação e Investigação em Ciências Empresariais e Sistemas de Informação, Escola Superior de Tecnologia e Gestão / Politécnico do Porto, Portugal. Professora Adjunta Convidada no Departamento de Ciências Jurídicas e Sociais. Licenciada, Mestre e Doutora em Direito pela Faculdade de Direito da Universidade do Porto, Portugal. scola Superior de Tecnologia e Gestão - Politécnico do Porto. Portugal. ORCID: http://orcid.org/0000-0002-0779-9076
E-mail: patricia_anjos_azevedo86@hotmail.com

[2] CIICESI, ESTG /P. PORTO – Centro de Inovação e Investigação em Ciências Empresariais e Sistemas de Informação, Escola Superior de Tecnologia e Gestão / Politécnico do Porto, Portugal. Professora Adjunta no Departamento de Ciências Jurídicas e Sociais. Doutora em Direito pela Universidade de Santiago de Compostela, Espanha. Afiliação: CIICESI, ESTG /P. PORTO – Centro de Inovação e Investigação em Ciências Empresariais e Sistemas de Informação, Escola Superior de Tecnologia e Gestão / Politécnico do Porto. Portugal. E-mail: scm@estg.ipp.pt

[3] CIICESI, ESTG /P. PORTO – Centro de Inovação e Investigação em Ciências Empresariais e Sistemas de Informação, Escola Superior de Tecnologia e Gestão / Politécnico do Porto, Portugal. Licenciada e Mestre em Solicitadoria. Afiliação: CIICESI, ESTG /P. PORTO – Centro de Inovação e Investigação em Ciências Empresariais e Sistemas de Informação, Escola Superior de Tecnologia e Gestão / Politécnico do Porto. Portugal. E-mail:daniela.sofia.silva.rodrigues@gmail.com

vol.14, nº.03, Rio de Janeiro, 2021. pp. 1001-1038
DOI: 10.12957/rqi.2021.58565

Concluímos, assim, após o estudo de todas estas matérias, que a relação laboral levanta múltiplas questões no que respeita à aplicabilidade do Regulamento Geral da Proteção de Dados.

Palavras-chave: controlo do trabalhador; Código do Trabalho português; Regulamento Geral de Proteção de Dados; limites ao poder de controlo; tratamento dos dados pessoais.

ABSTRACT

This contribution deals with the means of remote surveillance and its relationship with the treatment of workers' personal data, with special emphasis on geolocation and the legitimacy of investigating the worker's activity, which constitutes de general objective of our contribution. From the outset, we have forms of control, such as radio frequency technology; biometric data; the control of blood alcohol or psychoactive substances; medical control with regard to complementary exams and control over the use of electronic means, among others.
Our specific objective is, precisely, to present all these situations, as well as the limits to the power of control that the employer has. Also worthy of mention is the matter of the subsequent processing of personal data by the employer obtained through the control systems at his disposal.
As for the method, we present, basically, a literature review (doctrine), trying to make some connections to the law and the jurisprudence.
As a result, we intend to demonstrate that, today, with so many means at your disposal, it will be easy for the employer to eventually call into question the rights of workers.
We conclude, therefore, after studying all these matters, that the employment relationship raises multiple issues with regard to the applicability of the General Data Protection Regulation.

Keywords: worker control; Portuguese Labor Code; General Data Protection Regulation; limits to the power of control; processing of personal data.

1. INTRODUÇÃO

É de facto notório que os avanços tecnológicos geram mudanças a todos os níveis. No âmbito da relação laboral, estes avanços permitem ao empregador o acesso a ferramentas cada vez mais sofisticadas para controlar a produtividade e o cumprimento das obrigações inerentes à relação laboral. Neste sentido, a entidade empregadora tem cada vez mais capacidade de controlo, o que poderá colocar em confronto a intimidade da vida privada de um trabalhador (PINILLA, 2017).

Um dos setores do ordenamento jurídico português mais exposto à influência de mudanças tecnológicas é o Direito do Trabalho. Estamos numa era de mudança que não se pode considerar somente estrutural, mas, também, funcional uma vez que se alterou profundamente a maneira da prestação laboral ser efetuada (MOREIRA, 2017).

vol.14, nº.03, Rio de Janeiro, 2021. pp. 1001-1038
DOI: 10.12957/rqi.2021.58565

No âmbito de uma organização, departamentos como recursos humanos, jurídicos, financeiros, entre outros são dos departamentos mais afetados pelo Regulamento Geral de Proteção de Dados (RGPD), uma vez que são os departamentos que irão recolher, tratar, processar e armazenar a maior parte dos dados pessoais da organização que é responsável pelo seu tratamento. É, de facto, claro que no contexto laboral o tratamento dos dados pessoais tem um impacto enorme na medida em que, qualquer que seja o tamanho da empresa, estão obrigados a estar em conformidade com as exigências previstas no RGPD.

Assim, e de modo a proceder sempre em conformidade com o Regulamento, colocam-se às organizações/empresas, muitos desafios de complexidade técnica sendo os mais comuns a seleção e o recrutamento dos trabalhadores; a utilização de recursos de comunicação na empresa; a utilização destes mesmos recursos fora da empresa; controlo de tempos de trabalho; utilização de sistemas de monitorização de vídeo; monitorização da atividade dos trabalhadores nas suas redes sociais; utilização de veículos automóveis; divulgação dos dados pessoais de determinado trabalhador a terceiros e a transferência internacional de dados.

Uma questão complexa é a conformidade do RGPD com a aplicação informática da gestão de recursos humanos. Mostrou-se necessário a alteração das funcionalidades, nomeadamente no caso relativo à atividades e serviços de segurança e saúde no trabalho. Obrigatoriamente, será necessária a separação lógica entre a saúde e os outros dados pessoais; a aplicação do exercício do direito ao esquecimento e o controlo da assiduidade terá que ser adaptado.

Certo é que, devido à subordinação jurídica da relação laboral, existe um maior risco de ocorrer o abuso da utilização de dados pessoais dos trabalhadores e, neste sentido, o empregador não pode exigir dos trabalhadores informações referentes à sua esfera privada. Esta situação verifica-se uma vez que não é possível tratar essa informação, pela sensibilidade dos dados pessoais em causa.

Importa a tutela dos direitos de personalidade dos trabalhadores, bem como a defesa da sua privacidade, confidencialidade de mensagens ou qualquer outro tipo de comunicações que possam existir, assim como informações recolhidas através dos vários meios que, nos dias de hoje, temos à nossa disposição.

O CT nos artigos 14.º a 22.º configura esta situação. Podemos afirmar que, mantendo esta proteção legalmente regulada no CT e acrescendo o RGPD, é garantida uma maior proteção ao trabalhador. Contudo, não nos devemos esquecer da articulação dos artigos 14.º a 22.º do CT com a matéria que se encontra regulada nos artigos 23.º e ss no que respeita à

vol.14, nº.03, Rio de Janeiro, 2021. pp. 1001-1038
DOI: 10.12957/rqi.2021.58565

igualdade e à discriminação bem como a proibição das situações de assédio. Esta subsecção do CT tem como objetivo a garantia da defesa dos direitos de personalidade dos sujeitos laborais. Contudo, a maior parte destes preceitos só fazem sentido em relação ao trabalhador. Atenda-se aos artigos 17.º a 22.º do CT. É considerada uma abordagem bastante "personalista" destas matérias laborais e, para confirmar esta afirmação, é necessário atender à matéria de liberdade de expressão e de opinião, de integridade física e moral ou da reserva da intimidade da vida privada (AMADO et. al., 2019).

Assim sendo, a principal preocupação do legislador é assegurar a posição igualitária de ambos os sujeitos contratuais uma vez que o empregador e o trabalhador não estão no mesmo patamar contratual (AMADO et. al., 2019).

Quanto à reserva da intimidade da vida privada do trabalhador, o empregador pode estabelecer regras de utilização de meios de comunicação, nomeadamente, pela imposição de limites, tempos de utilização, bem como a vedação a determinados locais, nos termos e para os efeitos do disposto no n.º 2 do artigo 22.º CT, sendo que estas regras devem revestir forma de regulamento interno e devem ainda ser adequadas e proporcionais, tendo sempre em conta as disposições do RGPD (NASCIMENTO; GAMA, 2019). O n.º 2 do artigo 22.º CT tem como objetivo repor um justo equilíbrio entre a tutela do direito à confidencialidade de que goza o trabalhador e a liberdade da gestão empresarial. Neste sentido, a reserva da intimidade da vida privada de determinado trabalhador não pode prejudicar a possibilidade de o empregador estabelecer regras de utilização dos meios de comunicação e das tecnologias manuseadas na empresa, nomeadamente através da imposição de limites, tempos de utilização, acessos ou sítios vedados aos trabalhadores. Quanto à utilização deste preceito, vigora o princípio do consensualismo, isto é, qualquer meio utilizado pelas entidades empregadoras será lícito, desde que se revele adequado para que se torne possível o seu conhecimento por parte dos trabalhadores da empresa.

Relativamente à questão do incumprimento das regras estabelecidas neste artigo, esta consubstancia uma infração disciplinar, contudo, não legitima a violação, pelo empregador, do direito à confidencialidade regulada no n.º 1 do artigo 22.º do CT. Contudo, como forma de justificar o cumprimento defeituoso do contrato ou a inobservância das regras de utilização fixadas no n.º 2 do artigo 22.º do CT pode constituir uma hipótese típica de abuso do direito, elencada no artigo 334.º do CC (MARTINEZ et. al., 2020).

vol.14, nº.03, Rio de Janeiro, 2021. pp. 1001-1038
DOI: 10.12957/rqi.2021.58565

Note-se ainda que as imagens e outros dados pessoais que possam vir a ser gravados por meios tecnológicos de vigilância à distância apenas se podem utilizar no âmbito de processo penal ou em processo disciplinar conforme iremos abordar de seguida.

2. OS MEIOS DE VIGILÂNCIA À DISTÂNCIA

2.1. A GEOLOCALIZAÇÃO

Os dados de geolocalização caracterizam-se por ser dados pessoais e, em contexto laboral, existe a necessidade de que esta utilização da tecnologia ocorra com as devidas prudências. Os sistemas de localização funcionam através de satélites, antenas e recetores que visam permitir fornecimento de estimativas precisas quanto à posição, velocidade e tempo. Um exemplo deste tipo de vigilância é o caso do GPS instalado num veículo. Este vai permitir à entidade empregadora conhecer a localização e controlar todas as deslocações do trabalhador de uma forma constante e sem diferenciar o pessoal do profissional. Estes sistemas são fórmulas bastantes eficazes para controlar as obrigações laborais dos trabalhadores durante a sua atividade profissional (MARTINEZ et. al., 2020). O empregador não pode colocar este meio de localização sem o conhecimento do trabalhador pois constitui uma violação aos direitos do mesmo.

A principal preocupação quanto à utilização destes dispositivos assenta no facto desta utilização poder violar os direitos fundamentais dos trabalhadores, nomeadamente no que respeita à reserva da intimidade da vida privada. Apesar de estes tipos de dados não estarem expressamente previstos, enquadram-se na definição de dados sensíveis na medida em que podem fragilizar o direito à privacidade dos trabalhadores (ALVES, 2020).

Como anteriormente referenciado, a geolocalização torna-se uma grande preocupação da CNPD. No fundo, a CNPD prevê que esta possa ser utilizada de forma desmedida e que acabe por violar os dados pessoais dos envolvidos.

Desta forma, e no entendimento da CNPD, a utilização do GPS nos veículos automóveis, situação mais frequente nas empresas, irá trazer às mesmas regras específicas, pois não podem ser utilizadas para controlo do desempenho do trabalhador, para prova do cumprimento do contrato, para controlo do cumprimento da legislação rodoviária e para o controlo da viatura quando esta é utilizada para fins privados do trabalhador. Dado o exposto, e se a utilização deste método for abusiva poder-se-á admitir a resolução do contrato de trabalho

vol.14, nº.03, Rio de Janeiro, 2021. pp. 1001-1038
DOI: 10.12957/rqi.2021.58565

por justa causa pelo trabalhador e o direito a uma indemnização, nos termos e para os efeitos do regulado nos artigos 394.º e 396.º do CT.

Além da situação mencionada anteriormente e quanto à geolocalização do trabalhador através de dispositivos móveis tais como, telemóveis, computadores ou tablets esta é proibida. A CNPD entende que o que está em causa neste tipo de situações é a finalidade da proteção do bem. Neste sentido, torna-se desproporcional a sua utilização até porque daria à entidade patronal muito maior amplitude para o acesso à privacidade do trabalhador e seria incoerente.

Neste contexto da geolocalização é necessário referenciar a deliberação da CNPD n.º 7680/2014 de 28 de outubro de 2014 pois já nesta deliberação eram estabelecidas orientações e condições que seriam aplicáveis no contexto do tratamento dos dados pessoais no que respeita à utilização destes sistemas de geolocalização. Com a referida deliberação foram criadas obrigações para empresas e entidades públicas que tratam dados de geolocalização. Esta contém ainda regras importantes relativas aos fabricantes de automóveis, e empresas de locação de veículos e gestão de frotas, operadores de comunicações eletrónicas bem como para fornecedores de plataformas que disponibilizam estas tecnologias de monitorização dos dispositivos de geolocalização (ALVES, 2020).

Em contexto laboral, relevante para o nosso objeto de estudo, estes dispositivos de geolocalização caracterizam-se por serem habitualmente utilizados em veículos automóveis e dispositivos móveis inteligentes, normalmente disponibilizados pela entidade empregadora ao trabalhador.

Conforme anteriormente abordado, facilmente sabemos que existem vários meios que podem permitir ao empregador aceder à localização de determinado trabalhador ou objeto. Dispositivos como o GPS, GSM e o Wi-fi são exemplos de tecnologias com as quais lidamos diariamente e que permitem que o empregador aceda a uma série de dados relativos ao utilizador destes mecanismos, identificando percursos que possam ter sido efetuados, locais, históricos de movimento e tempo de permanência em determinado local. O acesso a estes dados vem possibilitar ao empregador a elaboração de perfis comportamentais tendo em conta a informação recolhida através destes meios de geolocalização. Podem parecer simples meios inofensivos, mas permitem ao empregador localizar uma determinada viatura em mapa, percurso, tempo real, velocidade, estilo de condução, tipificação de aceleração, travagem entre outros aspetos (ALVES, 2020).

De notar que a qualificação do GPS como meio de vigilância a distância nem sempre foi pacífica na nossa jurisprudência. Veja-se, por exemplo, o entendimento vertido no Acórdão

vol.14, nº.03, Rio de Janeiro, 2021. pp. 1001-1038
DOI: 10.12957/rqi.2021.58565

do Supremo Tribunal de Justiça, referente ao Processo n.º 73/12.3TTVNF.P1.S1, datado de 13 de novembro de 2013, onde não se considera que o GPS seja um meio de vigilância à distância por entender-se que o art.º 20º, n.º 1 do Código do Trabalho se reporta apenas a equipamentos "de captação à distância de imagem, som ou som e imagem que permitam identificar pessoas e detetar o que fazem, como é o caso, entre outros, de câmaras de vídeo, equipamento audiovisual, microfones dissimulados ou mecanismos de escuta e registo telefónico". O mesmo entendimento é propugnado no Acórdão do Supremo Tribunal de Justiça, relativo ao Processo n.º 07S054, datado de 22 de maio de 2007, onde pode ler-se o seguinte: "Não se pode qualificar o dispositivo de GPS instalado no veículo automóvel atribuído a um técnico de vendas como meio de vigilância à distância no local de trabalho, já que esse sistema não permite captar as circunstâncias, a duração e os resultados das visitas efetuadas aos seus clientes, nem identificar os respetivos intervenientes."

Ora, e com base na legislação laboral o tratamento de dados, através da geolocalização, é permitido, mas com o único objetivo de proteção e segurança de pessoas e bens ou então quando alguma particularidade específica inerente à natureza da atividade desempenhada pelo trabalhador justifique tal acontecimento. A utilização destes métodos é proibida se tiver como finalidade a monitorização do trabalhador ou qualquer outro controlo no seu tempo livre. Quanto a este último tópico, é necessário salientar que é dever do empregador implementar mecanismos que possam permitir ao trabalhador evitar o controlo fora do seu horário de trabalho. Exemplo desta situação é o caso de ligar e desligar o GPS quando o trabalhador não esteja em horário laboral (ALVES, 2020).

Outro tipo de proibição de monitorização é o controlo através de dispositivos móveis, conteúdo também já abordado, pois o acesso a estes tipos de dispositivos é considerado altamente intrusivo na privacidade do trabalhador (ALVES, 2020). Em suma, a confidencialidade das mensagens e das informações que tenham caráter pessoal e que o trabalhador possa ter acesso no seu local de trabalho goza de um princípio de reserva, contudo, o empregador pode estabelecer normas de utilização dos meios de comunicação da empresa, de acordo com o artigo 22.º do CT (ALVES, 2020).

Note-se, ainda, que este tipo de conteúdos, que goza do princípio de reserva, pode ser protegido através de alguns métodos que não envolvem a geolocalização. De modo a acautelar este tipo de situações, pode-se optar por encriptação, autenticação restrita para acesso ao equipamento em questão e instalação de *Mobile Device Management.*

vol.14, nº.03, Rio de Janeiro, 2021. pp. 1001-1038
DOI: 10.12957/rqi.2021.58565

Podemos, em modo de conclusão, enunciar as finalidades em que a instalação de sistemas de geolocalização é permitida, tais como: (i) A gestão de frota em serviço externo. Torna-se relevante na distribuição do serviço, informação sobre os tempos de espera ou para melhorar a capacidade de resposta. Esta gestão de frota apenas se pode verificar em atividades como a assistência técnica externa ou ao domicílio; distribuição de bens; transporte de passageiros ou de mercadorias e segurança privada; (ii) Proteção de bens. Neste caso apenas em veículos que transportem materiais perigosos ou então materiais de elevado valor monetário.

Fora destes casos apenas será permitido o controlo desde que seja adotada uma solução que permita que estes dados de localização do trabalhador ficam selados e que só poderão ser acedidos no caso de um furto de viatura ou dos bens, para efeitos de participação criminal (ALVES, 2020).

No fundo, esta tecnologia não pode ser utilizada para o controlo de desempenho de funções do trabalhador; prova de cumprimento de contrato; controlo de cumprimento da legislação rodoviária e utilização da viatura para fins privados (ALVES, 2020).

Importante referenciar que a utilização destes mecanismos de geolocalização considera-se excessiva e desproporcional no que respeita aos dispositivos móveis, uma vez as finalidades destes serem geralmente a proteção do bem em si. Assim, sempre que as entidades empregadoras tenham ao seu dispor sistemas de geolocalização devem prontamente informar os trabalhadores, estabelecendo as condições de utilização dos mesmos, em regulamento interno e pedir o parecer prévio à Comissão de Trabalhadores no caso de existir, adaptando à deliberação da CNPD o tratamento dos dados pessoais que possam envolver dados de geolocalização (ALVES, 2020).

Em suma e quanto aos serviços de geolocalização relacionados com os dispositivos móveis podemos destacar os alarmes e relatórios; monitorização e planeamento de rotas (de modo a planear a gestão de rotas das frotas e melhoria do serviço ao cliente); localização de veículos e monitorização de sensores; identificação automática de condutores; análise do estilo de condução e gestão de tarefas (ALVES, 2020).

Assim, o RGPD vem alargar o conceito dos dados pessoais no respeita à utilização das novas tecnologias, incluindo-se com dados pessoais os "endereços IP", *"cookies"*, entre outros (ALVES, 2020).

vol.14, nº.03, Rio de Janeiro, 2021. pp. 1001-1038
DOI: 10.12957/rqi.2021.58565

2.2. OS EQUIPAMENTOS DE VIDEOVIGILÂNCIA

Nos termos do artigo 4.º n.º 1 do RGPD torna-se consensual que a videovigilância constitui e enquadra-se na definição de dados pessoais, na medida em que recolhe imagens por meio eletrónico. Assim sendo, tudo o que seja recolhido através destes equipamentos e que seja suscetível de identificar concretamente uma pessoa, ainda que seja de forma indireta, constitui a definição de dados pessoais (ALVES, 2020).

Deste modo, torna-se um tema com relevância para o nosso estudo. Imagens como uma matrícula, que permitam identificar o proprietário ou quem utiliza essa viatura constitui um dado pessoal. A vigilância à distância tem também uma regulação específica no Código do Trabalho, nomeadamente, nos seus artigos 20.º e 21.º e constitui um dos aspetos mais relevantes no âmbito do tratamento dos dados pessoais sensíveis e, nos últimos anos, tem sido objeto de vastas análises no que respeita à sua utilização.

É de conhecimento geral que a instalação de videovigilância tem como principal objeto a proteção de pessoas e bens, evitando crimes que possam vir a ocorrer. Esta videovigilância é colocada em local e de modo apropriado a não ofender, em qualquer momento, os direitos dos cidadãos. Existem algumas limitações quanto aos locais onde devem estar instalados os meios de videovigilância à distância. Esta videovigilância não pode incidir sobre a via pública, propriedades limítrofes ou quaisquer locais que não sejam do domínio exclusivo do responsável. Importante também, no momento da colocação destes meios de vigilância, é o facto de estas não permitirem captar, por exemplo, imagens de digitação de códigos de segurança em multibancos.

Na relação laboral não é diferente. Neste contexto, a videovigilância não pode ser usada como forma de controlo do desempenho de trabalhadores de determinada empresa, não podendo estes meios incidir sobre os trabalhadores de modo direto.

O CT no seu artigo 21.º n.º 1 vem permitir a utilização de meios de vigilância no local de trabalho. Esta vigilância estava sujeita a autorização da CNPD até 25 maio de 2018, contudo, este artigo, apesar de continuar a mencionar a sujeição da autorização da CNPD, apenas não permite ao empregador utilizar este meio com a finalidade de controlo do trabalhador conforme anteriormente mencionado. Certo é que se esta autorização não tivesse limites estabelecidos, o trabalhador ao ter conhecimento da existência destes meios de vigilância iria alterar a sua conduta, levando-o a fingir produtividade ou a ficar mais inibido.

vol.14, nº.03, Rio de Janeiro, 2021. pp. 1001-1038
DOI: 10.12957/rqi.2021.58565

Contudo, a realidade pode ser bem diferente do pretendido na legislação. Involuntariamente, a entidade empregadora conseguirá, em certas situações, controlar o tempo e número de vezes que um determinado trabalhador se possa deslocar a uma determinada instalação, por exemplo, numa zona de cargas e descargas onde se encontram também instalações sanitárias. Para este local, parecerá lógico a instalação de videovigilância no sentido de controlar e proteger eventuais furtos que possam ocorrer, contudo, estará também a "controlar" os trabalhadores que se deslocarem às referidas instalações.

Quanto ao tratamento de dados de videovigilância, este é objeto de regulamentação por regras gerais, aplicáveis a todos os dados pessoais e por regras específicas que se aplicam apenas ao tratamento de dados pessoais por sistemas de videovigilância.

No que respeita a regras específicas, deverão ser consideras as seguintes:

(i) As gravações de imagem obtidas pelos sistemas de videovigilância são conservadas, em registo codificado, pelo prazo de 30 dias contados desde o respetivo momento da captação. Findo este prazo as imagens devem ser destruídas. Saliente-se que em certos casos os prazos podem ser de 90 e 180 dias, salvo expressa indicação legal e nos termos da Lei 51/2006 de 29 de agosto;

(ii) Todas as pessoas que tenham acesso às gravações, em razão das suas funções, devem guardar sigilo sobre as mesmas, com exceção da legislação processual penal que pode prever a eventual possibilidade de utilização relativamente a apuramento de responsabilidade disciplinar, nos termos da Lei 51/2006 de 29 de agosto;

(iii) Nos locais de objeto de vigilância onde existem recursos às câmaras de videovigilância é obrigatória a indicação e afixação, em local visível, do sinal identificado da existência destes meios de videovigilância (ALVES, 2020).

Relativamente ao ponto 3, aqui abordado, é relevante e coerente analisar o facto da proibição desta videovigilância em interior de áreas reservadas aos trabalhadores, nomeadamente, vestiários, instalações sanitárias e zonas que são exclusivamente relacionadas com o descanso do trabalhador, nos termos do artigo 19.º n.º 2 alínea d) da Lei 58/2019.

Todos os trabalhadores devem ser informados da existência deste meio de videovigilância, aplicando-se, neste contexto, os requisitos previstos no artigo 19.º n. º 1 da Lei 58/2019. Por fim, e no que respeita à utilização destas imagens, estas só podem ser utilizadas em processo penal e de modo a ser apurada a responsabilidade disciplinar, conforme artigo 28.º n.º 4 e n.º 5 da Lei 58/2019.

vol.14, nº.03, RiodeJaneiro, 2021. pp. 1001-1038
DOI: 10.12957/rqi.2021.58565

Para além da captura de imagens e nos termos do artigo 19.º, n.º 4, Lei 58/2019, pode afirmar-se que é proibida a captação de som. Contudo, é permitida esta captação de som no período em que as instalações estejam encerradas ou com prévia autorização da Comissão Nacional da Proteção de Dados.

Face à era digital em que nos encontramos, podemos afirmar que se mostra necessária uma justa composição entre o direito à privacidade dos trabalhadores e a liberdade de gestão e organização que é conferida pela lei aos empregadores de acordo com a Deliberação n.º 1638/2013 da CNPD. No fundo, podemos considerar a utilização das câmaras de vigilância lícita desde que a sua finalidade seja a proteção e a segurança de pessoas e bens ou quando particulares exigências inerentes à natureza da atividade assim o justifiquem, nos termos e para os efeitos do disposto no artigo 20.º n.º 2 do CT. Contudo, em certos casos a utilização destas câmaras de vigilância no local de trabalho poderá colocar em confronto o direito à reserva da intimidade da vida privada e a proteção e segurança de pessoas e bens.

No Acórdão do Supremo Tribunal de Justiça, referente ao Processo n.º SJ200602080031394, datado de 8 de fevereiro de 2006, pode ler-se que "a instalação de sistemas de videovigilância nos locais de trabalho envolve a restrição do direito de reserva da vida privada e apenas poderá mostrar-se justificada quando for necessária à prossecução de interesses legítimos e dentro dos limites definidos pelo princípio da proporcionalidade."

A utilização da videovigilância à distância para controlar o desempenho profissional dos trabalhadores pode ser considerada contraproducente na relação laboral. O principal interesse do artigo 20.º n.º 1 do CT é conferir uma proteção àquela zona de privacidade a que qualquer pessoa tem direito, mesmo quando está fora do seu domicílio e da qual o trabalhador pode gozar mesmo que esteja no seu local de trabalho (AMADO et. al., 2019). O trabalhador é, na maioria dos casos, totalmente dependente da retribuição que aufere o que vai fazer com que, perante a entidade empregadora, esteja numa posição bastante mais fragilizada. Consideramos, neste sentido, indispensável uma proteção especial relativa a tudo o que poderá advir no tratamento de dados nesta relação.

Entende-se, assim, que as disposições previstas nos artigos 20.º e 21.º do CT se aplicam a qualquer meio de vigilância à distância e não somente à videovigilância e apesar da resistência inicial, os tribunais aplicam, nas suas decisões, as mesmas normas no que respeita à utilização do GPS. A doutrina tem vindo a discutir a admissibilidade da utilização destes dados recolhidos pelo método da vigilância à distância, nomeadamente, a videovigilância, quanto a efeitos

vol.14, nº.03, Rio de Janeiro, 2021. pp. 1001-1038
DOI: 10.12957/rqi.2021.58565

disciplinares e não tem sido unânime quanto a esta admissibilidade ou inadmissibilidade (LAMBELHO; DINIS, 2020).

Exemplo desta não unanimidade é o Acórdão do Tribunal da Relação de Évora datado de 11 de setembro de 2010 (Acórdão do Tribunal da Relação de Évora - Processo n.º 292/09.0TTSTB.E1. Relator: Gonçalves Rocha) que defende o facto da limitação prevista no artigo 20.º n.º 1 do CT não dever ser tratada quando um trabalhador tenha cometido algum ato que ofenda a finalidade de proteção e segurança de pessoas e bens. Afirma ainda que seria contrário a esta finalidade se não se pudesse fundamentar uma atuação contra trabalhadores que, pelas funções que desempenham, atentassem contra as finalidades que as instalações destes meios têm como objetivo defender.

Contrapondo o acórdão anteriormente referenciado, encontramos como exemplo o acórdão do Tribunal da Relação do Porto datado de 5 de setembro de 2011 (Acórdão do Tribunal da Relação do Porto – Processo n.º 379/10.6TTBCL-A. P1. Relatora: Paula Leal de Carvalho) que afirma que "o empregador não pode em processo laboral e como meio de prova recorrer à utilização das imagens que possam ser captadas por sistemas de videovigilância para fundamentar o exercício da ação disciplinar mesmo que esta infração possa constituir ilícito penal".

Por seu turno, num Acórdão, o Tribunal da Relação do Porto (processo nº 1119/13.3TTPRT.P2, Relator Nelson Fernandes, datado de 5 de março de 2018), estamos perante a situação de um funcionário bancário, que exercia a função de caixa e se apropriou "ilicitamente 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", que 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.

vol.14, nº.03, Rio de Janeiro, 2021. pp. 1001-1038
DOI: 10.12957/rqi.2021.58565

Interligada com a videovigilância encontra-se a imagem, sendo neste contexto que se encontra regulado constitucionalmente, para além da legislação da proteção de dados pessoais, o direito à imagem e à reserva da intimidade da vida privada (artigo 26.º da CRP), já abordado anteriormente. Conjugando este artigo com o artigo 79.º do CC é acautelado o direito à imagem e consequentemente a criminalização de gravações e fotografias ilícitas prevendo a punição de quem efetua, de acordo com o disposto no artigo 199.º do Código Penal (CP).

Acresce que, de acordo com um Acórdão do Supremo Tribunal de Justiça (referente ao processo n.º 03B2361, datado de 25 de setembro de 2002) "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".

Portanto, a videovigilância ao proceder à recolha de imagens de determinadas pessoas é passível de derrogação do direito à imagem e à reserva da intimidade da vida privada. Afirmando tal expressão, o Tribunal Constitucional no acórdão n.º 255/2002, declara inconstitucional alguns dos preceitos previstos no Decreto-Lei 231/98 de 22 de julho à data em vigor na medida em que "apesar de a lei impor a afixação, em local bem visível nos lugares objeto de vigilância com recurso àqueles meios, de avisos a informar do facto, prescrevendo assim uma espécie de consentimento implícito do cidadão que permanece naqueles locais, a verdade é que tal medida legal constitui também ela uma verdadeira restrição aos direitos à imagem e à reserva da intimidade da vida privada e familiar". Contudo, acrescenta ainda que "o interesse público inerente à atividade de segurança privada, expresso pelo próprio legislador, justificará as restrições em causa".

Pode assim afirmar-se a existência de um conflito de interesses no que respeita ao direito à privacidade e o interesse público. Não pode considerar-se um acaso o legislador constitucional desagregar a liberdade da segurança, nos termos e para os efeitos do artigo 27.º da CRP.

2.2.1. LEGITIMIDADE DA AVERIGUAÇÃO DA ATIVIDADE DO TRABALHADOR

Certo é que a videovigilância se encontra legalmente autorizada pela CNPD e sendo do conhecimento dos trabalhadores, é lícita a utilização deste meio para esses fins.

Tal como também já abordado, o empregador não pode utilizar os meios de vigilância à distância com a finalidade de controlar o desempenho profissional do trabalhador, contudo, a utilização destes meios de vigilância à distância torna o tratamento lícito sempre que tenha

vol.14, nº.03, Rio de Janeiro, 2021. pp. 1001-1038
DOI: 10.12957/rqi.2021.58565

como finalidade a proteção e segurança de pessoas e bens ou então se a natureza da atividade assim o exigir.

Contudo, por vezes pode ser posta em causa a questão do direito à privacidade do trabalhador e o interesse público e estes casos terão de ser devidamente analisados uma vez que, conforme supramencionado a doutrina tem vindo a discutir a utilização dos dados recolhidos pelo método da vigilância à distância, no que respeita à aplicabilidade da recolha das imagens para efeitos disciplinares, não sendo totalmente unânime.

Para reforçar o que já foi anteriormente abordado neste nosso contributo, note-se, como exemplo, da admissibilidade da utilização da videovigilância para efeitos disciplinares, o acórdão do Tribunal da Relação do Porto de 7 de dezembro de 2018 (Acórdão da Relação do Porto - Processo n.º 159/18.0T8PNF-A. P1. Relator: Domingos Morais) que retrata um posto de abastecimento de combustível, local onde se justifica a utilização de meios de videovigilância à distância. Cabe agora perceber se o tratamento destes dados para fins disciplinares o pode ser feito. É certo que a inserção de um trabalhador numa empresa vem comportar limitações à liberdade e exercício de direitos fundamentais e, por vezes, pode provocar conflitos entre a reserva da intimidade da vida privada e o direito do empregador em prosseguir os objetivos a que se propôs no pacto social de determinada empresa. No caso em apreço está em causa a prática de atos amorosos entre uma trabalhadora e o seu namorado, manifestada no seu local e horário de trabalho.

A prática destes atos pode prejudicar a atividade da empresa e, sabendo a trabalhadora que estava a ser filmada pelo sistema de videovigilância que se encontrava legalmente autorizado, a própria expôs o seu direito privado e, neste contexto estas imagens recolhidas no local de trabalho podem servir como meio de prova para o fim disciplinar que, neste caso, foi o despedimento (cfr. Acórdão da Relação do Porto - Processo n.º 159/18.0T8PNF-A. P1. Relator: Domingos Morais).

2.2.2. CESSAÇÃO DO CONTRATO DE TRABALHO NO CONTEXTO DA LEGITIMIDADE DA AVERIGUAÇÃO DA ATIVIDADE DO TRABALHADOR

De acordo com o artigo 340.º do CT, o contrato de trabalho pode cessar por caducidade, revogação, despedimento por facto imputável ao trabalhador, despedimento coletivo, despedimento por extinção do posto de trabalho, por inadaptação, resolução pelo trabalhador e ainda por denúncia pelo trabalhador.

vol.14, nº.03, Rio de Janeiro, 2021. pp. 1001-1038
DOI: 10.12957/rqi.2021.58565

Para abordagem ao nosso tema, importa analisar o despedimento por facto imputável ao trabalhador e, inicialmente é importante salientar a resolução do contrato de trabalhador por iniciativa do empregador que é a justa causa de despedimento. De acordo com a CRP, nomeadamente no seu artigo 53.º o despedimento tem de ter sempre justa causa e de acordo com o artigo 351.º n.º 1, do CT, constitui justa causa de despedimento o comportamento culposo do trabalhador que, pela sua gravidade e consequências, torne imediata e praticamente impossível a subsistência da relação laboral.

No nosso ordenamento jurídico, é certo que o poder diretivo do empregador não poderá aplicar sanções ao trabalhador fora do seu local e horário de trabalho, contudo, em determinadas situações, o empregador não conseguirá ficar indiferente a atitudes que o trabalhador possa ter e que violem os seus deveres acessórios. Se tal se verificar, ocorre o cumprimento defeituoso do contrato.

Por outro lado, também compreendemos que não caberá ao empregador censurar comportamentos do trabalhador com exceções de interesses que possam ser muito atendíveis à entidade patronal ou à prestação de trabalho. Exemplo desta situação é um trabalhador, no âmbito da sua vida pessoal, ter comportamentos que possam denegrir a imagem e o bom nome da empresa mesmo que esteja fora do seu horário de trabalho. Estes tipos de comportamento vão colocar em risco a relação de confiança entre as partes e poderão fazer com que o trabalhador seja despedido por justa causa.

O uso das redes sociais é um caso onde facilmente um determinado trabalhador poderá denegrir a imagem de um colega de trabalho ou até mesmo do empregador. Esta situação é impensável uma vez que pode afetar, obviamente, o bom ambiente de trabalho e poderá refletir-se negativamente até a um determinado ponto de denegrir completamente a boa imagem da empresa onde trabalha. Nestes casos, consideramos que constitui uma justa causa para a cessação do contrato de trabalho. Efetivamente, as redes sociais aparecem num contexto diferente dos meios de vigilância à distância, mas constituem uma forma de o empregador poder vir a recolher informações sobre os seus trabalhadores, o que pode influenciar a relação de trabalho e a imagem que o empregador tem do trabalhador.

Como exemplo desta situação, atente-se ao acórdão do Tribunal da Relação de Évora de 30 de janeiro de 2014 (Acórdão do Tribunal da Relação de Évora - Processo n.º 8/13.6TTFAR.E1. Relator: José Feteira) que vem defender a constituição grave de "violação dos deveres laborais de respeito, urbanidade e mesmo de lealdade devidos ao legal representante da sua entidade empregadora e, nessa medida, constitui justa causa de

vol.14, nº.03, Rio de Janeiro, 2021. pp. 1001-1038
DOI: 10.12957/rqi.2021.58565

despedimento, a divulgação feita pelo trabalhador, através da rede social "*Facebook*", de mensagens cujo teor sabia que feriam a honra e o bom nome do legal representante daquela e demais membros da mesa administrativa, para mais quando nada resultou demonstrado no sentido da veracidade das imputações feitas através dessas mensagens". Acrescenta ainda que "a gravidade de tal comportamento ainda se torna mais patente pela circunstância do trabalhador o haver assumido de uma forma velada, usando o subterfúgio de um nome de utilizador e fotografia nada reveladores da sua identidade, com o propósito de não ser reconhecido como trabalhador ou, sequer, como associado que também era da empregadora". Por outro lado, devemos contrapor com o acórdão do Supremo Tribunal de Justiça de 27 de novembro de 2018 (Acórdão do Supremo Tribunal de Justiça – Processo n.º 4053/15.9T8CSC.L1. S2. Relator: Júlio Gomes) no sentido em que este vem afirmar que o "trabalhador goza tanto no âmbito da empresa, como fora dele, de liberdade de expressão, ainda que tal liberdade não seja ilimitada, havendo que atender aos deveres de respeito, urbanidade e probidade". Salienta ainda, quanto à questão da aferição da gravidade de afirmações ofensivas que "para um administrador há que ponderar as circunstâncias concretas do caso, como sejam, o facto de tais afirmações serem proferidas, no *Facebook*, pelo trabalhador em momento de indignação e sem identificar o seu empregador e a ausência de danos graves para o empregador".

Face ao exposto, julgamos que para ser possível manter uma boa relação laboral, com elevado grau de confiança, não é possível se determinado trabalhador difamar nas redes sociais alguém ou algo relacionado com a empresa onde labora.

2.3. OUTROS MEIOS DE CONTROLO

2.3.1. TECNOLOGIA POR RADIOFREQUÊNCIA

A tecnologia por radiofrequência foi inventada já nos anos 40 do século passado com a utilização nos aviões militares. A sua primeira aplicação comercial surge na década de 60 do mesmo século com o objetivo de evitar eventuais furtos na área do controlo dos bens (AMADO et. al., 2019).

A tecnologia de identificação inerente à radiofrequência tem vindo a evoluir nos últimos anos, com várias finalidades e com vista a diferentes setores o que visa permitir um controlo não só de objetos como também de pessoas. Este controlo acontece em setores como o dos

vol.14, nº.03, Rio de Janeiro, 2021. pp. 1001-1038
DOI: 10.12957/rqi.2021.58565

transportes, controlo de acesso a determinados locais através de cartões e, de uma forma mais recente, o controlo nos documentos de identificação oficiais e nos passaportes bem como no setor do consumo, com especial relevo na distribuição dos bens e no seu seguimento. Não só nas vertentes enunciadas está presente este tipo de controlo por radiofrequência como, também, no setor de saúde. Exemplo da aplicabilidade desta situação é o facto da utilização destes métodos na maternidade com o objetivo de eventuais raptos de crianças ou até mesmo para avisar o médico da necessidade de se deslocarem a determinado local (AMADO et. al., 2019).

O aumento desta tecnologia está ligado com o seu baixo custo, mas também com o facto de se identificar individualmente cada objeto, uma vez que, individualmente, cada objeto tem o seu próprio identificador RFID (*radio frequency identification*) de forma exclusiva (AMADO et. al., 2019).

No contexto laboral, matéria pertinente para o nosso trabalho, os problemas que podem surgir no âmbito da utilização da radiofrequência são, por um lado, o uso de cartões RFID para identificar bens e objetos que podem originar, de forma involuntária ou não, formas de controlo dos trabalhadores cada vez mais eletrónicas e com consequências em diversos níveis, nomeadamente na saúde e, por outro lado, vem trazer várias implicações para a privacidade dos trabalhadores porque o RFID tem a oportunidade de localizar e controlar os trabalhadores durante o seu horário laboral e, por vezes, fora deste, invadindo, deste modo, a vida privada. Existem situações em que a utilização destes métodos é lícita, como é o caso do controlo de mineiros onde são incluídos na sua roupa de trabalho *chips* RFID para serem facilmente encontrados em casos de acidentes, contudo, podemos afirmar que esta utilização lícita, é uma exceção (AMADO et. al., 2019).

Exemplo de uma das formas de controlo dos trabalhadores totalmente ilícita é a inserção de *chips* RFID com tamanhos milimétricos nos uniformes dos trabalhadores de determinada empresa, ou até mesmo nas próprias fibras da roupa que funciona quase como uma antena RFID e que vem permitir aos empregadores o controlo dos trabalhadores mesmo fora do seu horário laboral bem como conhecer os seus gostos, permitindo-se criar perfis dos mesmos. Estes cartões podem ser lidos por pessoas externas à empresa o que torna a necessidade de proteção dos trabalhadores ainda maior (AMADO et. al., 2019).

Por fim, esta tecnologia permite, ainda, a implementação de *chips* na própria pele das pessoas, mas, no âmbito laboral, consideramos esta situação totalmente proibida porque por um lado viola o direito à privacidade e por outro, ainda mais importante, viola o direito à dignidade dos trabalhadores que, acima de trabalhadores são pessoas que apenas celebram um contrato de

vol.14, nº.03, Rio de Janeiro, 2021. pp. 1001-1038
DOI: 10.12957/rqi.2021.58565

trabalho e não é isto que permite ao empregador um controlo total sobre o mesmo (AMADO et. al., 2019).

2.3.2. OS DADOS BIOMÉTRICOS: CONTROLO DE ASSIDUIDADE

A LPD dispõe especificamente o tratamento dos dados biométricos dos trabalhadores que devemos, obviamente, articular com as disposições reguladas no Código do Trabalho. Os dados biométricos são os dados pessoais relativos às características físicas, fisiológicas ou comportamentais de determinada pessoa singular com o objetivo de confirmar a sua identidade única, nos termos e para os efeitos do artigo 4.º n.º 14 (ALVES, 2020). Reconhecimento por impressões digitais, geometria da mão ou da face, entre outros constituem os dados biométricos de determinado indivíduo. Certo é que com esta era digital as empresas recorrem mais frequentemente a este tipo de dados biométricos com o objetivo de controlar a atividade dos trabalhadores no que respeita à sua assiduidade, pontualidade e acessos sendo a forma mais comum e de maior aplicação, a monitorização dos trabalhadores no seu local de trabalho. Contudo, é certo que estes sistemas podem tornar-se invasivos no sentido em que o dado pessoal é utilizado e pode trazer riscos para o próprio trabalhador nomeadamente, a discriminação (SANTOS, 2019).

Como em tudo, não só estes sistemas biométricos se caraterizam pelo lado negativo pois estes apresentam vantagens em relação aos métodos tradicionais pelo facto de uma determinada informação de acesso corresponder somente a uma pessoa o que torna verdadeiramente difícil a sua perda ou apropriação por terceiros. Neste sentido, podemos caracterizar estes sistemas biométricos como um método confiável, preciso e seguro, isto porque apenas o trabalhador detém uma chave única de acesso por esta se basear nas características tão suas (SANTOS, 2019).

A finalidade do tratamento dos dados biométricos prende-se na agilização da norma prevista no artigo 18.º do CT e a integração de poderes de controlo por parte do responsável pelo tratamento no que respeita ao controlo da assiduidade, pontualidade, fixação do horário de trabalho e no controlo do trabalho suplementar caso se verifique (SANTOS, 2019).

Com o RGPD os dados biométricos passam a fazer parte das categorias especiais de dados e, de acordo com o artigo 9.º n.º 1 do RGPD apesar de o seu tratamento ser proibido, podem os dados vir a serem tratados se constituírem o cumprimento de obrigações e exercício de direitos específicos da relação laboral, conforme estipula o artigo 9.º, n.º 2 alínea b) do

vol.14, nº.03, Rio de Janeiro, 2021. pp. 1001-1038
DOI: 10.12957/rqi.2021.58565

RGPD e para a execução do contrato de acordo com o artigo 6.º, n.º 1, alínea b) do RGPD (SANTOS, 2019).

Tendo em consideração a matéria abordada e no que concerne à utilização dos dados biométricos, reforça também a Lei 58/2019, no n.º 6 do seu artigo 28.º quando rege que esta apenas é considerada legítima para o controlo da assiduidade e de acesso às instalações do empregador. Neste contexto, o consentimento do trabalhador é afastado como fundamento da legitimidade visto esta relação laboral ser uma relação de desequilíbrio, conforme fomos referindo ao longo do trabalho. Constituindo uma obrigação contratual, o titular dos dados pessoais não poderá exercer o seu direito de oposição acerca do tratamento dos seus dados (SANTOS, 2019).

2.3.3. CONTROLO DE ALCOOLEMIA OU DE SUBSTÂNCIAS PSICOATIVAS

Em momento algum deve verificar-se a discriminação de trabalhadores por determinada característica. Assim, e como medida de prevenção, a entidade empregadora deve prevenir o tratamento destas situações bem como garantir a confidencialidade de toda a informação que pode ser recolhida no âmbito destes programas, nomeadamente, nos pontos do processo de deteção, tratamento e reabilitação (ALVES, 2020).

No caso de se verificar alguma situação de consumo de bebidas alcoólicas ou substância psicoativas, devem ser garantidas ao trabalhador as mesmas oportunidades de promoção bem como o seu posto de trabalho podendo verificar-se, se for crucial para a segurança do trabalhador ou de terceiros, a transferência para funções que tenham menor risco sem nunca se perder os direitos que o trabalhador teria se esta situação não se verificasse. O empregador deve ter sempre em conta que estes testes põem em causa os direitos, liberdades e garantias do trabalhador consagrados na CRP. Assim, este controlo deve apenas ser efetuado quando a atividade dos trabalhadores possa pôr em perigo a integridade física quer dos mesmos, quer de terceiros. Deve assim ser esta situação devidamente justificada por razões de interesse público ou por situações de conflito com outros direitos que estejam constitucionalmente regulados. De notar que, em momento algum, o trabalhador deve sujeitar-se a tratamentos obrigado. Esta sujeição deve absoluta e voluntária. Assim sendo, o consumo de substâncias psicoativas deve ser considerado questão de saúde tendo assim o trabalhador direito a incapacidade temporária, subsídio de doença e outros benefícios que surgem no âmbito da medicina no trabalho (ALVES, 2020).

vol.14, nº.03, Rio de Janeiro, 2021. pp. 1001-1038
DOI: 10.12957/rqi.2021.58565

2.3.4. CONTROLO MÉDICO – EXAMES COMPLEMENTARES

No âmbito da informação inicial cabe referenciar que nem todos os dados pessoais podem ser tratados no âmbito da medicina no trabalho, isto é, apenas podem ser tratados os dados que se mostrem relevantes em relação à atividade profissional o que vem, desde logo, eliminar os dados sobre hábitos pessoais destes parâmetros (ALVES, 2020).

Também é óbvio que, por vezes, registos de dados sobre consumo de tabaco, café, drogas ou alcoolemia podem ter de ser tratados na medida em que podem estar associados a outras patologias e por isso são também objeto de tratamento (ALVES, 2020).

Acresce que, em virtude da pandemia causada pela doença de Covid-19, tem sido também polémica a monotorização da temperatura dos trabalhadores, matéria ainda em desenvolvimento legislativo e doutrinário, mas – ainda assim – achamos importante aqui aludir, ainda que a breve trecho.

Necessário ainda referenciar que pode a entidade empregadora optar pela contratação de entidade de serviços de segurança e saúde no trabalho, mas, neste caso, e de modo a que sejam em todo o momento salvaguardados os dados pessoais dos trabalhadores, é necessária a celebração de um contrato ou ato jurídico que vincule esta entidade ao responsável pelo tratamento dos dados pessoais. Saliente-se ainda que neste contrato/ato jurídico deve ser revestida a forma escrita, com valor probatório legalmente reconhecido (ALVES, 2020).

Assim, e no que respeita às informações sobre a saúde, o empregador só deverá ser informado dos resultados que se mostrem necessários à tomada de decisão, através de uma *ficha de aptidão.* Toda esta informação de saúde deve ser objeto de sigilo profissional por parte do profissional de saúde e em caso algum deve ser comunicada à entidade empregadora (ALVES, 2020).

De forma a ainda serem garantidas condições de segurança, aos servidores do sistema, deve ser garantido um acesso restrito, devendo manter um registo de auditoria de acesso a toda a informação que possa ser considerada sensível. Neste sentido, devem ser efetuadas *back-ups* da informação que apenas serão acedidas pelo administrador de sistema (ALVES, 2020).

vol.14, nº.03, Rio de Janeiro, 2021. pp. 1001-1038
DOI: 10.12957/rqi.2021.58565

2.3.5. CONTROLO DA UTILIZAÇÃO DE MEIOS ELETRÓNICOS

Certo é que o tratamento de dados pessoais na relação laboral deve consistir na harmonização do equilíbrio entre a esfera jurídica do trabalhador e o princípio da liberdade de gestão empresarial conciliando sempre com a reserva da intimidade da vida privada e a proteção de dados pessoais (ALVES, 2020).

Neste âmbito, por exemplo, o Acórdão do Tribunal da Relação de Lisboa, referente ao Processo n.º 2970/2008-4, datado de 5 de junho de 2008, afirma que o empregador ao estabelecer regras de utilização das tecnologias de informação e comunicação, nomeadamente através de um regulamento de empresa, não está a prejudicar o direito à reserva da intimidade da vida privada do trabalhador.

Quanto ao controlo de comunicações eletrónicas, é dever da entidade empregadora regular, com rigor, o grau de tolerância quanto à utilização dos telefones pois será quase inatingível que os trabalhadores possam estar impedidos de utilizar estes meios, no tempo e local de trabalho para necessidades pessoais.

Assim sendo, o acesso a este tipo de comunicações é, em geral, proibido. No caso de gravações de chamadas telefónicas, estas só serão admitidas, no caso de prova da relação contratual, situações de emergência ou monitorização de controlo/qualidade do atendimento e, nos termos do artigo 20.º do CT, nunca poderá ser para efeitos de controlo da atividade dos trabalhadores.

Relativamente ao correio eletrónico, em momento algum a entidade empregadora poderá proceder à abertura dos correios eletrónicos endereçados ao trabalhador, independentemente das regras que possam estar estabelecidas a nível da gestão empresarial.

Contudo, deve ser exigido aos trabalhadores que façam a devida distinção entre os correios eletrónicos que são de caráter pessoal e os de caráter profissional, separando em pastas diferenciadas. Existe a possibilidade de realização de controlos. Contudo, apenas devem ser efetuados quando existam suspeitas fundamentadas de determinados factos e com a finalidade de prevenção ou divulgação de segredos comerciais (ALVES, 2020).

Quando o trabalhador se encontre de férias ou licença, devem ser adotados mecanismos de resposta automática, endereçando o correio eletrónico para ser tratado por outro trabalhador. Importante ainda é quando, por exemplo, um trabalhador sai da empresa pois deve-lhe ser

vol.14, nº.03, Rio de Janeiro, 2021. pp. 1001-1038
DOI: 10.12957/rqi.2021.58565

conferido um determinado prazo para que este proceda à eliminação de correio eletrónico que possa ter cariz pessoal (ALVES, 2020).

Nesta matéria, veja-se, por exemplo, o Acórdão do Tribunal da Relação de Lisboa, referente ao Processo n.º 24163/09.0T2SNT.L1-4, datado de 7 de março de 2012, no qual podemos verificar que o Tribunal decidiu que, não havendo regulamentação prévia para a utilização profissional da *Internet* por parte dos trabalhadores, o acesso "ao conteúdo de conversas de teor estritamente pessoal da Apelada com três amigas e o marido/namorado" é ilícito.

A falta de cumprimento das ações aludidas neste ponto da nossa exposição, ações essas que visam precisamente proteger os dados pessoais dos trabalhadores, origina uma sanção penal nos termos e para os efeitos do artigo 194.º do CP que pode punir com pena de prisão até 1 ano ou com pena de multa até 240 dias. A violação do sigilo profissional também pode fazer com que o trabalhador incorra em sanção penal de acordo com o estipulado no artigo 195.º do CP que pode originar igualmente pena de prisão até 1 ano ou com pena de multa até 240 dias (ALVES, 2020).

3. LIMITES AO PODER DE CONTROLO DO EMPREGADOR

É defendida uma divisão dos poderes do empregador quadripartida: por um lado, o poder regulamentar, por outro o poder disciplinador, o poder diretivo e ainda o poder de controlo (MOREIRA, 2004). No artigo 99.º do CT encontra-se regulado o poder regulamentar do empregador, poder este que se caracteriza pela faculdade de o empregador poder elaborar o regulamento interno da empresa sobre organização e disciplina do trabalho. Tal significa que o empregador tem a liberdade para criar regulamentos gerais da empresa, ordens de serviço ou instruções que entenda por oportuno, contudo, importa ainda salientar que o limite a este poder é a audição dos representantes dos trabalhadores e a sua publicitação na empresa.

No que respeita ao poder disciplinador do empregador, este encontra-se regulado nos termos do artigo 98.º do CT e vem ceder ao empregador o poder de punir o trabalhador por violação do contrato do trabalho ou por regras que possa estar sujeito, contudo, este poder tem a duração do tempo do contrato.

Importa ainda salientar o artigo 97.º do CT relativamente ao poder diretivo do empregador, pois o trabalho deve sempre ser realizado tendo em atenção os limites expostos no contrato de trabalho. Este poder surge quando o trabalhador aceita e assina o contrato de trabalho e

vol.14, nº.03, Rio de Janeiro, 2021. pp. 1001-1038
DOI: 10.12957/rqi.2021.58565

consequentemente as diretrizes e a estrutura organizativa do empregador. Neste sentido, é da competência do empregador controlar e vigiar o trabalho que é prestado pelo trabalhador.

Certo é que, com a crescente utilização de novas tecnologias no local de trabalho, foram implementadas na maioria das empresas métodos e novos instrumentos que visam facilitar o desempenho dos trabalhadores. Por outro lado, também surgiram novas formas para o controlo da atividade destes trabalhadores por parte da entidade empregadora. Contudo, o facto da existência destas novas tecnologias tem suscitado alguns riscos que podem pôr em causa a vida privada dos trabalhadores.

Para que os trabalhadores procedam sempre em conformidade na sua atividade laboral por vezes, é exercida pressão por parte da entidade empregadora. A monitorização através destes meios pode fazer com que a privacidade dos trabalhadores fique comprometida. Neste sentido, existe um aumento de dados pessoais sujeitos a tratamento e existe também novas formas de análise dos mesmos que podem monitorizar padrões de comportamento e de desempenho dos trabalhadores. Em certos casos, os trabalhadores podem nem ter conhecimento de que determinadas ferramentas e monitorização do seu trabalho possam estar a ser aplicadas bem como os seus dados pessoais também possam estar a ser objeto de tratamento.

As técnicas de monitorização fora do local de trabalho também são importantes de abordar uma vez que estas podem colidir com a esfera privada de um determinado trabalhador isto porque, pode existir recolha de dados pessoais deste e estes dados dizerem respeito somente à sua vida privada, mas enquanto utiliza dispositivos ou veículos que são disponibilizados pela entidade empregadora.

Também já abordado, o teletrabalho pode representar um risco, pois é alargado o ambiente doméstico do trabalhador enquanto utiliza dispositivos com tecnologia que possam permitir à entidade empregadora um controlo maior e, consequentemente, violar a esfera íntima e privada do trabalhador (ALVES, 2020).

4. O TRATAMENTO POSTERIOR DOS DADOS PESSOAIS PELO EMPREGADOR OBTIDOS ATRAVÉS DESTES SISTEMAS DE CONTROLO

Tal como já referenciado anteriormente, o tratamento dos dados pessoais deve sempre ser efetuado de acordo com os princípios que estão subjacentes ao RGPD. Neste sentido, os dados só poderão ser guardados para fins lícitos e definidos e não podem ser guardados para além do período que seja necessário para cumprir a sua finalidade. É o que se rege no artigo

vol.14, nº.03, Rio de Janeiro, 2021. pp. 1001-1038
DOI: 10.12957/rqi.2021.58565

5.º, n.º 1 alínea b) do RGPD que vem estabelecer que os dados pessoais devem apenas ser recolhidos "para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades". Esta conservação dos dados pessoais deve obedecer à limitação prevista na alínea e) do n.º 1 do artigo 5.º do RGPD, isto é, deve obedecer a uma lógica de minimização. Posto isto, apenas os dados que são estritamente necessários para um determinado fim devem ser conservados (AMADO et. al., 2019).

Alguma legislação laboral específica, bem como o próprio CT, vêm já estipular prazos para a conservação dos dados pessoais dos trabalhadores e pode-se até afirmar que já estão salvaguardados os prazos e conservação de muitos dados pessoais que são objeto de tratamento no que respeita à execução do contrato de trabalho.

Assim, e de forma a que seja possível garantir o direito à autodeterminação informativa dos trabalhadores e a eventualidade de controlo da informação que é obtida sobre estes, tem de ser limitada a sua recolha e tratamento aos fins para os quais foram aceites e que são do conhecimento do trabalhador (AMADO et. al., 2019).

Sabemos que a utilização deste princípio se prende com o facto de o uso dos dados pessoais poder ser prejudicial para os trabalhadores nomeadamente, se estes forem inexatos ou incompletos, mas também se estiverem descontextualizados, existindo assim uma possibilidade de distorção da informação que pode ser bastante prejudicial para os trabalhadores. Neste contexto, apenas será possível reverter esta situação de descontextualização se se fixarem limites à elaboração de dados pessoais bem como a imposição que estes, nos termos do princípio da finalidade, sejam utilizados em estrita conformidade com o contexto inicial (AMADO et. al., 2019).

A única forma de se conseguir excluir o perigo existente de descontextualização é a inibição do uso de dados pessoais para fins diversos e incompatíveis com os originários.

Não é possível retirar, quer do RGPD, quer do CT, a existência de uma exceção do princípio da finalidade em relação a informações que podem ter sido obtidas ocasionalmente e que possam revelar incumprimentos contratuais ou ilícitos que devem ser sancionados no foro laboral (AMADO et. al., 2019).

Porém pode, em determinadas circunstâncias, ser lícita a utilização destes dados captados ocasionalmente, com fins disciplinares quando o que é descoberto são factos gravosos e constituintes ilícitos penais. Por conseguinte, devemos interpretar o artigo 20.º do CT como uma dupla proibição. Por um lado, a proibição da utilização das gravações obtidas pelos meios de vigilância com o intuito de controlar o trabalhador como também a proibição da utilização

vol.14, nº.03, Rio de Janeiro, 2021. pp. 1001-1038
DOI: 10.12957/rqi.2021.58565

para fins disciplinares destes dados pessoais quando se mostre que o trabalhador não cumpre os seus deveres laborais como, por exemplo, uma gravação por videovigilância que mostra que o trabalhador se encontra a dormir em vez de laborar (AMADO et. al., 2019).

Voltamos a referir que nestes casos onde, através de gravações obtidas ou dos dados de geolocalização ou de radiofrequência, se verifique pelo trabalhador situações de práticas de ilícitos penais com relevo bem como infrações disciplinares graves, seja possível a recolha desses dados para os utilizar para fins disciplinares e a jurisprudência tem aceitado estas situações (AMADO et. al., 2019).

Face ao exposto, acresce ainda o artigo 28.º n.º 4 e 5 da Lei 58/2019 de 8 de agosto que determina que "As imagens gravadas e outros dados pessoais registados através da utilização de sistemas de vídeo ou outros meios tecnológicos de vigilância à distância, nos termos previstos no artigo 20.º do Código do Trabalho, só podem ser utilizados no âmbito do processo penal." E ainda que "Nos casos previstos no número anterior, as imagens gravadas e outros dados pessoais podem também ser utilizados para efeitos de apuramento de responsabilidade disciplinar, na medida em que o sejam no âmbito do processo penal". Talvez a redação destes dois números não tenha sido a melhor, contudo, é bastante positiva a sua inclusão pois este artigo veio consagrar a possibilidade de utilização quando se tratem de infrações disciplinares que constituam, simultaneamente, ilícitos penais (AMADO et. al., 2019).

O artigo 127.º, n.º 1, alínea j), do CT rege que é dever do empregador manter os registos, em cada estabelecimento, organizados no que toca à vivência laboral do trabalhador no desempenho das suas funções, nomeadamente: nome, data de nascimento, data de admissão, modalidade de contrato, categoria, promoções, retribuições, datas de início e termo das férias e faltas que impliquem perda da retribuição ou diminuição de dias de férias. Estes dados devem manter-se atualizados, para numa eventualidade em que ocorra uma inspeção por parte da ACT, comprovar com os registos supramencionados a legalidade do empregador no que toca aos pressupostos legais impostos. Todavia, esta informação organizada recorrentemente não tem apenas uma finalidade preventiva, ao manter os registos devidamente atualizados o empregador zela também, pela organização do seu estabelecimento bem como, a veracidade do cumprimento das obrigações e direitos subjacentes à relação laboral.

No que respeita ao prazo de conservação dos dados, no caso de cessação do contrato de trabalho, o prazo de conservação poderá ser de um ano, de acordo o n.º 1 do artigo 337.º do CT e, o trabalhador tem precisamente um ano, para reclamar os seus créditos laborais. Um exemplo, será a conservação dos recibos de vencimento pelo prazo de um ano, sob pena de o empregador

vol.14, nº.03, Rio de Janeiro, 2021. pp. 1001-1038
DOI: 10.12957/rqi.2021.58565

não conseguir fazer prova dos pagamentos que efetuou se estes créditos forem reclamados judicialmente. No caso dos créditos laborais relacionados com a compensação por violação do direito a férias, indemnizações ou pagamento de trabalho suplementar, de acordo com o n.º 2 do artigo 337.º do CT onde os créditos se venceram há mais de cinco anos, só podem ser provados por documento idóneo. Ora, e conforme rege o princípio da minimização, o empregador deve manter durante cinco anos os registos nominativos correspondentes.

Contudo, é de quarenta anos o prazo de conservação dos registos e arquivo de documentos que sejam referentes a serviço de segurança e de saúde no trabalho quando em determinadas situações de atividade seja colocado em causa o património genético, nos termos e para os efeitos do disposto no artigo 46.º n.º 3 da Lei 102/2009 (CARNEIRO; JANSON, 2019).

De acordo com um Acórdão do TJUE (Terceira Secção), referente ao Processo C-342/12, de 30 de maio de 2013, "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 (…) características de um «tratamento de dados pessoais»".

5. CONCLUSÃO

Ao nível da proteção de dados pessoais, estes não são apenas tratados aquando a constituição do vínculo laboral, mas, ao longo de toda a relação, desde a fase de recrutamento até à fase da cessação desta relação. Mesmo após a cessação da relação laboral, colocam-se questões acerca de o empregador manter os dados pessoais de determinado trabalhador e poder proceder à transmissão destes dados para outras entidades.

Quanto à questão dos direitos de personalidade na relação laboral, temos o direito à liberdade de expressão e de opinião, o direito à reserva da intimidade da vida privada, o direito à integridade física e moral e o direito à reserva e à confidencialidade. Neste contexto, uma correta proteção daqueles direitos exige, em termos complementares, uma estrutura sólida de proteção de dados.

Realçaram-se, neste nosso contributo, os meios de vigilância à distância e a sua relação com o tratamento dos dados pessoais dos trabalhadores, com especial relevo na geolocalização e a legitimidade da averiguação da atividade do trabalhador, porque, em certas situações, podemos colocar em causa a esfera íntima e privada do trabalhador com a relação laboral; a

vol.14, nº.03, Rio de Janeiro, 2021. pp. 1001-1038
DOI: 10.12957/rqi.2021.58565

tecnologia por radiofrequência, tecnologia de identificação antiga mas com bastante evolução nos últimos anos; os dados biométricos; o controlo de alcoolemia ou de substâncias psicoativas; o controlo médico no que respeita aos exames complementares e o controlo da utilização de meios eletrónicos.

De notar, que existem limites ao poder de controlo que o empregador tem, como superior hierárquico, relativamente aos trabalhadores. Neste âmbito, defende-se uma divisão dos poderes do empregador quadripartida no sentido em que, temos o poder regulamentar, o poder disciplinador, o poder diretivo e o poder de controlo do empregador.

Face à situação pandémica atual e a sua relação com a proteção dos dados pessoais, temos a monitorização da temperatura corpórea dos trabalhadores (matéria que não foi devidamente abordada neste nosso contributo, mas apenas referenciada, pois tem sido prática habitual nos últimos tempos), bem como a realização de testes de diagnóstico e o controlo à distância em regime de teletrabalho.

Concluímos, assim, que a relação laboral tem múltiplas questões que podem colocar-se no que respeita à aplicabilidade do RGPD. Este diploma visa reforçar o direito dos trabalhadores conforme analisamos ao longo deste nosso contributo, estabelecendo algumas restrições que podem ofender os seus direitos.

REFERÊNCIAS

ALVES, Lurdes Dias, Proteção de Dados Pessoais no Contexto Laboral - O direito à privacidade do trabalhador. Coimbra: Almedina, 2020.

AMADO, João Leal [et al.], Direito do Trabalho – Relação Individual, Coimbra: Almedina, 2019.

CARNEIRO, Joana; JANSON, Joan, O RGPD no contexto laboral – O RGPD e o impacto nas organizações: 6 meses depois. Atas – X Congresso Internacional de Ciências Jurídico-Empresariais, 2019.

LAMBELHO, Ana; DINIS, Marisa, La protección de datos de los trabajadores en Portugal: el diálogo entre el Código de Trabajo, el RGPD y la nueva Ley de Protección de Datos, vigilancia e control en el Derecho del Trabajo Digital, Madrid: Thomson Reuters, Aranzadi, 2020.

MARTINEZ, Pedro Romano [et.al] – Código do Trabalho Anotado, Anotação de Guilherme Dray, 12.ª edição, Coimbra: Almedina, 2020.

vol.14, nº.03, Rio de Janeiro, 2021. pp. 1001-1038
DOI: 10.12957/rqi.2021.58565

MOREIRA, Teresa Coelho – Algumas Implicações Laborais do Regulamento Geral de Proteção de Dados Pessoais no Trabalho 4.0, Questões Laborais, Ano XXIV, julho/dezembro 2017, Coimbra: Almedina, 2017.

MOREIRA, Teresa Coelho, Da esfera privada do trabalhador e o controlo do empregador, Studia Iuridica, Coimbra: Coimbra Editora, 2004.

NASCIMENTO Ricardo; GAMA, Alexandre, RGPD em contexto laboral, 2019. [Consult. 4 set. 2020]. Disponível em http://boletim.oa.pt/project/set19-rgpd-em-contexto-laboral/.

PINILLA, Ana de la Puebla, III Encuentro Internacional sobre Transformaciones del Derecho del Trabajo Ibérico- Geolocalización y Control Biométrico - Universidad Autónoma de Madrid, Madrid, 2017. Disponível em https://docplayer.es/96623576-Iii-encuentro-internacional-sobre-transformaciones-del-derecho-del-trabajo-iberico-carolina-san-martin-mazzucconi-y-maria-regina-redinha.html .

SANTOS, Patrícia Andreia Batista, A Aplicação do Novo Regulamento Geral de Proteção de Dados no Contexto Laboral. Dissertação em Direito e Gestão na especialidade de Proteção de Dados Pessoais. Lisboa: Faculdade de Direito Universidade Nova de Lisboa, 2019.

Trabalho recebido em 21 de março de 2021
Aceito em 01 de setembro de 2021