Anabela Luna de Carvalho

A vigilância no local de trabalho

verbojurídico

A vigilância no local de trabalho

Os limites da proteção de dados na jurisprudência laboral
Os desafios do teletrabalho

ANABELA LUNA DE CARVALHO
Juíza Desembargadora

Sumário:

Introdução

A temática da videovigilância no local de trabalho, sendo muito discutida nos tribunais de trabalho, tem-no sido numa perspetiva clássica, mais focada na defesa de direitos de personalidade e da intimidade da vida privada à luz da Constituição, da legislação civil e laboral, do que numa conceção de proteção de dados pessoais de acordo com os mais recentes instrumentos legislativos da União Europeia que regulam a proteção de dados pessoais e preveem um direito à autodeterminação informacional.

Embora a jurisprudência laboral haja refletido a proteção de dados pessoais desde a Lei 67/98 de 26.10 (anterior Lei da Proteção de Dados Pessoais) que transpôs a Diretiva 95/46/CE (Diretiva de Proteção de Dados Pessoais), é apenas a partir do Regulamento (UE) 2016/679 do Parlamento e do Conselho (RGPD) aplicável a partir de 25-05-2018 e da sua Lei de execução nacional, a Lei 58/2019 de 08.08 (atual Lei da Proteção de Dados Pessoais) aplicável a partir de 09-08-2019, que se perspetiva o surgimento duma jurisprudência laboral mais impressivamente marcada pelos conceitos deste ramo do direito, onde se concebem os dados pessoais como propriedade do titular, no caso, o trabalhador, conferindo-lhe uma esfera de proteção de domínio efetivo, um poder sobre os mesmos no tratamento automatizado de dados, não apenas na fase de contratação laboral, mas no decurso de toda a vida do contrato e em certas situações para lá dele.

Esta é, pois, uma proteção que, sendo próxima não é totalmente coincidente com a dos direitos de personalidade e beneficia duma autonomia que a torna concorrente com a defesa daqueles.[1]

Uma regulação imposta pela sofisticação tecnológica da era atual, que armazena, trata, conexiona, transmite e utiliza de forma automatizada grandes quantidades de dados, sem que o titular de imediato os possa controlar ou mesmo disso se aperceber, afetando diversos modelos de relação contratual, no caso a relação laboral e, dentro desta, uma particular modalidade de prestação que a pandemia vulgarizou, o teletrabalho.

O desempenho do teletrabalho frequentemente integrado por mecanismos invasivos de controlo e de recolha de informação quanto ao exercício funcional do trabalhador, pode incorporar uma videovigilância oculta suscetível de contender com direitos de personalidade e com dados pessoais deste, o que coloca a necessidade de criar limites à recolha e ao tratamento de informação por essa via.

Por «*dados pessoais*» entende-se 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, na definição do artigo 4º nº 1 do RGPD.

Que dados pessoais são tratados e de que forma o são, como pode o titular de dados, aqui na posição de trabalhador, aceder ao seu conteúdo, à sua finalidade, retificá-los, atualizá-los, apagá-los, opor-se aos mesmos, em suma, como pode o trabalhador exercer o seu **direito à autodeterminação/identidade informacional** perante uma tecnologia deveras sofisticada, desenvolvida e processada frequentemente com recurso a empresas subcontratantes, com programas de vigilância informática à distância, são questões que advêm duma nova legislação sob um perfil

[1] Alguns autores referem a existência duma relação de interioridade constitutiva entre a proteção de dados e os direitos de personalidade (nesse sentido, Mafalda Miranda Barbosa, *in* https://www.abreuadvogados.com/media/yv0dovh3/prote%C3%A7%C3%A3o-de-dados-e-direitos-de-personalidade.pdf

vincadamente regulador e sancionatório e que abrirá caminho, num futuro próximo, a uma diferenciada discussão nos tribunais.

Nas últimas décadas a abordagem à volta dos limites da utilização da tecnologia vigilante centrou-se na utilização da videovigilância e mecanismos afins no espaço laboral exterior ao domicílio pessoal do trabalhador, ou seja, nas instalações destinadas a local de trabalho por regra da entidade patronal ou de terceiros conforme indicação desta ou, nas deslocações de trabalho, caso do GPS, tendo a jurisprudência laboral desenvolvido uma sólida fundamentação acerca dos princípios, das finalidades e das condições de licitude que haveria que se respeitar para autorizar[2] ou legitimar[3] tais mecanismos por parte das empresas[4].

Tal jurisprudência assentava na Constituição, na lei civil e laboral e acolhia como fonte interpretativa o sentido dos pareceres, orientações e recomendações da Comissão Nacional de Proteção de Dados (CNPD).

A proteção dos dados pessoais na Constituição

O artigo 35.º da CRP prevê a «Utilização da informática»:

> *"1. 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, nos termos da lei.*
>
> *(…)*
>
> *3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.*
>
> *4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei.*
>
> *5. É proibida a atribuição de um número nacional único aos cidadãos.*
>
> *(…)."*

O artigo 35.º da CRP ao conceder dignidade constitucional ao direito do indivíduo (pessoa física) de acesso aos tratamentos de dados pessoais que lhes digam respeito; ao direito de retificação e de atualização; ao direito a conhecer a finalidade dos tratamentos de dados; ao direito ao não

[2] No âmbito administrativo.

[3] Na jurisdição comum.

[4] Discussão que teve também assento na jurisdição penal, nomeadamente no âmbito de avaliação das provas (i)lícitas.

tratamento de dados cujo processamento se possa revelar especialmente sensível; ao direito ao segredo e à não divulgação (a terceiros) de dados objeto de tratamento, reúne e elege deste conjunto de direitos **um direito genérico do indivíduo à autonomia informacional**.

Importa ainda atender ao artigo 34.º da CRP que prevê a «Inviolabilidade do domicílio e da correspondência»:

> *"1. O domicílio e o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis."*

E ao artigo 26.º que prescreve «Outros direitos pessoais»:

> *"1. A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação."*

Vem a propósito referir o Acórdão n.º 241/2002 do Tribunal Constitucional[5] que analisou da conformidade constitucional da aplicação da norma do art. 519 nº 3 alª b) do Código de Processo Civil[6], numa ação de impugnação de despedimento interposta por um trabalhador, tendo o tribunal da 1ª instância, sustentando-se em tal norma, deferido o pedido da ré empregadora e ordenado a notificação de duas operadoras de telecomunicações para fornecerem aos autos, documento em seu poder, que identificava o autor de dois textos que haviam passado na Internet. O que estas cumpriram através da indicação do *username* formalmente atribuído ao autor e da faturação detalhada do número de telefone do seu domicílio.

Considerou o TC que "a faturação detalhada permite sempre quebrar o véu da intimidade da vida privada do autor, "desnudando-a", tornando-a transparente para terceiros" e ainda que "através da informação da faturação detalhada foi invadida a reserva da intimidade da vida privada do autor/recorrente, no âmbito de um processo de natureza cível, o que viola o direito fundamental à reserva da intimidade da vida privada e as garantias do sigilo (e da não-ingerência nas) das telecomunicações, consagrados na lei fundamental."

Desse modo, as informações relativas aos dados de tráfego e a faturação detalhada, enquanto **dados pessoais** não podiam, nas circunstâncias, constituir meios de prova para fundamentar o despedimento. Vindo a firmar a seguinte decisão:

> *«Julgar inconstitucional a norma ínsita no artigo 519.º, n.º 3, alínea b), do Código de Processo Civil[7] quando interpretada no sentido de que, em processo laboral, podem ser pedidas,*

[5] *In* https://dre.pt/pesquisa/

[6] Atual art. 417 CPC - dever de cooperação para a descoberta da verdade.

[7] Artigo 519.º do CPC (velho) - DL n.º 329-A/95, de 12 de dezembro

«Dever de cooperação para a descoberta da verdade

por despacho judicial, aos operadores de telecomunicações informações relativas aos dados de tráfego e à faturação detalhada de linha telefónica instalada na morada de uma parte, sem que enferme de nulidade a prova obtida com a utilização dos documentos que veiculam aquelas informações, por infração ao disposto nos artigos 26.º, n.º 1, e 34.º, n.ºs 1 e 4, da Constituição».

A videovigilância na legislação laboral

Quer o Código de Trabalho de 2003 (CT 2003) e seu Regulamento (Lei n.º 35/2004, de 29 de Julho – Regulamento CT2003), quer o Código de Trabalho de 2009 (CT 2009), nas suas sucessivas versões, moldaram-se à regulação específica da proteção de dados em vigor à data das respetivas aprovações, no caso, a Lei 67/98 de 26.10 (Lei da Proteção de Dados Pessoais que transpôs a Diretiva nº 95/46/CE).

O *Regulamento Geral sobre a Proteção de Dados*, (Regulamento (UE) 2016/679 – *doravante* RGPD) que revogou aquela e a Lei nº 58/2019 de 08.08 (*doravante* LPDP), que veio dar "execução" e "feição nacional" a este Regulamento, sucederam temporalmente ao CT 2009, importando, por isso, aferir da compatibilidade deste com tais instrumentos, direito derivado da UE[8].

A Lei n.º 67/98 de 26.10 (anterior Lei da Proteção de Dados Pessoais) dispunha no seu art. 2º como princípio geral:

"O tratamento de dados pessoais deve processar-se de forma transparente e no estrito respeito pela reserva da vida privada, bem como pelos direitos, liberdades e garantias fundamentais."

No seu artº 3 b) definia como «Tratamento de dados pessoais»:

"Qualquer operação ou conjunto de operações sobre dados pessoais, efetuadas com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição."

E no art. 6º) enunciava as *condições de legitimidade* no tratamento de dados: o *consentimento* do titular *ou* a verificação da *necessidade do tratamento* para a prossecução de interesses legítimos

1 - Todas as pessoas, sejam ou não partes na causa, têm o dever de prestar a sua colaboração para a descoberta da verdade, respondendo ao que lhes for perguntado, submetendo-se às inspeções necessárias, facultando o que for requisitado e praticando os atos que forem determinados.

(…)

3 - A recusa é, porém, legítima se a obediência importar:

(…)

b) Intromissão na vida privada ou familiar, no domicílio, na correspondência ou nas telecomunicações;»

[8] Artigo 8º da CRP.

numa ponderação de razoabilidade perante o sacrifício dos interesses ou dos direitos, liberdades e garantias do titular dos dados.

O Código de Trabalho de 2003

O Código de Trabalho de 2003 (CT 2003) aprovado pela Lei n.º 99/2003, de 27.08 veio, inovadoramente, regular *a proteção dos dados pessoais do trabalhador*. Em consonância com a perspetiva personalista que o inspirou.

Colhe-se da proposta de lei n.º 29/IX (decreto preambular) que aprovou o Código do Trabalho de 2003[9]:

> "O Código do Trabalho situa-se, pois, numa perspetiva personalista: as pessoas, em particular os trabalhadores, constituem o fundamento de todas as ponderações. Com efeito, o Código revela, independentemente da expressa consagração dos direitos da personalidade, uma preocupação em manter um equilíbrio entre as necessidades dos trabalhadores e dos empregadores, tendo presente que sem aqueles não é possível a existência destes, e sem estes aqueles não existiriam. É esta comunhão de interesses que está presente em todo o texto."

Daí o surgimento duma regulação específica dos *direitos de personalidade* na relação trabalhador/empregador e, neste âmbito, duma regulação particular da *proteção de dados pessoais* e da *instalação de meios de vigilância nos locais de trabalho*.

Estatuindo a propósito:

"Artigo 16.º - Reserva da intimidade da vida privada

> *1 - O empregador e o trabalhador devem respeitar os direitos de personalidade da contraparte, cabendo-lhes, designadamente, guardar reserva quanto à intimidade da vida privada.*
>
> *2 - O direito à reserva da intimidade da vida privada abrange quer o acesso, quer a divulgação de aspetos atinentes à esfera íntima e pessoal das partes, nomeadamente relacionados com a vida familiar, afetiva e sexual, com o estado de saúde e com as convicções políticas e religiosas."*

[9] https://app.parlamento.pt/

"Artigo 17.º - Proteção de dados pessoais

1 - O empregador não pode exigir ao candidato a emprego ou ao trabalhador que preste informações relativas 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.

2 - O empregador não pode exigir ao candidato a emprego ou ao trabalhador que preste informações relativas 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.

3 - As informações previstas no número anterior são prestadas a médico, que só pode comunicar ao empregador se o trabalhador está ou não apto a desempenhar a atividade, salvo autorização escrita deste.

4 - 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.

5 - Os ficheiros e acessos informáticos utilizados pelo empregador para tratamento de dados pessoais do candidato a emprego ou trabalhador ficam sujeitos à legislação em vigor relativa à proteção de dados pessoais."

"Artigo 20.º - Meios de vigilância à distância

1 - O empregador não pode utilizar meios de vigilância à distância no local de trabalho, mediante o emprego de equipamento tecnológico, com a finalidade de controlar o desempenho profissional do trabalhador.

2 - A utilização do equipamento identificado no número anterior é lícita sempre que tenha por finalidade a proteção e segurança de pessoas e bens ou quando particulares exigências inerentes à natureza da atividade o justifiquem.

3 - Nos casos previstos no número anterior o empregador deve informar o trabalhador sobre a existência e finalidade dos meios de vigilância utilizados."

Desta regulação do CT 2003 decorria que, sendo a utilização dos meios de vigilância à distância, potencialmente violadora dos direitos de personalidade do trabalhador, a justificação para a mesma haveria de ser aferida da finalidade subjacente: se visasse controlar o desempenho profissional do trabalhador, não seria permitida; se visasse proteger a segurança de pessoas e bens ou se particulares exigências inerentes à natureza da atividade o reclamassem, seria permitida.

O que, como a jurisprudência expôs, no juízo casuístico e concreto, nem sempre as duas finalidades se excluem, os campos de incidência não são estanques nem individualizáveis, comportando antes zonas de sobreposição ou confluência, obrigando o julgador a uma ponderação de proporcionalidade quanto ao peso relativo de cada uma, hierarquizando as finalidades em potencial conflito.

Embora o CT 2003 não previsse expressamente a necessidade de autorização prévia da Comissão Nacional de Proteção de Dados (CNPD), essa necessidade surgia diretamente do seu Regulamento (Lei n.º 35/2004, de 29 de Julho)[10], que dispunha:

"Artigo 28.º - Utilização de meios de vigilância a distância

1 - Para efeitos do n.º 2 do artigo 20.º do Código do Trabalho, a utilização de meios de vigilância a distância no local de trabalho está sujeita a autorização da Comissão Nacional de Proteção de Dados.

2 - A autorização referida no número anterior só pode ser concedida se a utilização dos meios for necessária, adequada e proporcional aos objetivos a atingir."

Prevendo ainda o *Regulamento ao CT 2003* no seu artigo 29º, a obrigação para o empregador de publicitar essa vigilância no local de trabalho.

Ainda que o CT 2003 assentasse apenas na finalidade geral «não visar o controlo o trabalhador/proteger pessoas e bens» o critério definidor da licitude quanto à recolha e tratamento de imagens, o seu Regulamento sobrepunha uma tripla conformação da atuação aos *princípios da necessidade, adequação e proporcionalidade*, em sintonia com a Lei 67/98 de 26/10, que determinava a observância de *juízos de adequação, de pertinência e de proporção* (art. 5º, n.º 1, alª c)).

A Comissão Nacional de Proteção de Dados procurando dar resposta aos diversos pedidos de autorização de tratamentos de videovigilância que neste contexto lhe foram dirigidos, estabeleceu na sua Deliberação n.º 61/2004 (*www.cnpd.pt*) os **"Princípios sobre o Tratamento de Dados por Videovigilância"**, assim se exprimindo:

"O tratamento a realizar e os meios utilizados devem ser considerados os necessários, adequados e proporcionados com as finalidades estabelecidas: a proteção de pessoas e bens. Ou seja, para se poder verificar se uma medida restritiva de um direito fundamental supera o juízo de proporcionalidade imporá verificar se foram cumpridas três condições: se a medida adotada é idónea para conseguir o objetivo proposto (princípio da idoneidade que é mais do que adequação); se é necessária, no sentido de que não existia outra medida capaz de assegurar o objetivo com igual grau de eficácia (princípio da necessidade); se a medida adotada foi

[10] Em consonância com a Lei 67/98 de 26/10, aplicável à videovigilância através do seu art. 4º nº 4.

ponderada e é equilibrada ao ponto de através dela, serem atingidos substanciais e superiores benefícios ou vantagens para o interesse geral quando confrontados com outros bens ou valores em conflito (juízo de proporcionalidade em sentido restrito).”

Esta deliberação, remetendo para uma apreciação casuística, veio definir os princípios gerais no âmbito da Lei 67/98, a que deveriam obedecer os atos de autorização ou de recusa de utilização de sistemas de videovigilância, pela CNPD.

A jurisprudência no âmbito do CT 2003

Vejamos como se afirmou a jurisprudência laboral no âmbito da Lei 67/98 (proteção de dados) e do CT 2003 relativamente à videovigilância no local de trabalho.

Respeitando os Princípios sobre o Tratamento de Dados por Videovigilância definidos na referida Deliberação n.º 61/2004 da CNPD (como fonte interpretativa).

Nesse sentido se pronunciou o Supremo Tribunal de Justiça (Ac. de 08/02/2006) numa ação em que foi chamado a apreciar o conflito entre os trabalhadores da indústria farmacêutica e a empresa empregadora[11].

A Ré colocara câmaras de filmar/vídeo em todo o armazém, as quais se mostravam colocadas em ângulo de forma a abranger todo o espaço onde os trabalhadores exerciam as suas funções, incidindo sobre estes, de tal modo que as tarefas que exerciam estavam a ser permanentemente filmadas e gravadas. Existiam monitores que visualizavam todos os locais de trabalho e os trabalhadores estavam permanentemente sob observação do operador das câmaras. A Ré defendera-se alegando que, antes da implementação do sistema de videovigilância, vira-se confrontada com furtos de medicamentos e outros produtos que comercializava, e que muitas dessas situações eram perpetradas por pessoas que se encontravam devidamente autorizadas pela Ré a penetrar no interior das instalações.

Embora o Tribunal da Relação de Lisboa (Ac.18/05/2005)[12] tivesse considerado legítima a atuação da Ré, considerando-a a coberto da finalidade de proteção e segurança de pessoas e bens ou da justificação das particulares exigências inerentes à natureza da atividade profissional (nº 2 do art. 20º do CT 2003), o Supremo Tribunal de Justiça, num reforço de tutela privada, assim não o entendeu, pronunciando-se desfavoravelmente, como reporta o sumário do referido acórdão:

«I – 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.

[11] Cfr. Ac. STJ de 08-02-2006 (Fernandes Cadilha), www.dgsi.pt

[12] Cfr. Ac. TRL de 18-05-2005 (Seara Paixão) - P. 10740/2004-4, www.dgsi.pt

II – O empregador pode utilizar meios de vigilância à distância sempre que tenha por finalidade a proteção e segurança de pessoas e bens, devendo entender-se, contudo, que essa possibilidade se circunscreve a locais abertos ao público ou a espaços de acesso a pessoas estranhas à empresa, em que exista um razoável risco de ocorrência de delitos contra as pessoas ou contra o património.

III – Por outro lado, essa utilização deverá traduzir-se numa forma de vigilância genérica, destinada a detetar factos, situações ou acontecimentos incidentais, e não numa vigilância diretamente dirigida aos postos de trabalho ou ao campo de ação dos trabalhadores; (…)

V- Nos termos das precedentes proposições, ***é ilícita,*** *por violação do direito de reserva da vida privada,* ***a captação de imagem através de câmaras de vídeo instaladas no local de trabalho e direcionadas para os trabalhadores,*** *de tal modo que a atividade laboral se encontre sujeita a uma contínua e permanente observação."*

O Supremo considerou assim que, a captação de imagem através de câmaras de vídeo instaladas no local de trabalho e direcionadas para os trabalhadores, de tal modo que a atividade laboral se encontrava sujeita a uma contínua e permanente observação, violava o direito de reserva da vida privada, sendo, por isso, ilícita.

Rapidamente a discussão sobre a possibilidade ou não da captação de imagem derivou para a discussão sobre a possibilidade ou não do uso das imagens no processo disciplinar, ou seja, como *meio de prova* para o reconhecimento de uma infração disciplinar.

Numa posição restrita quanto à possibilidade de uso das imagens no procedimento disciplinar, o Tribunal da Relação de Lisboa (Ac.03/05/2006)[13] veio afirmar:

"*III – A videovigilância não só não pode ser utilizada como forma de controlar o exercício da atividade profissional do trabalhador, como não pode, por maioria de razão, ser utilizado como meio de prova em sede de procedimento disciplinar pois, nestas circunstâncias, a divulgação da cassete constitui, uma abusiva intromissão na vida privada e a violação do direito à imagem do trabalhador, - arts. 79º do Cód. Civil e 26º da Constituição da República Portuguesa – criminalmente punível – art. 199º, nº 1, alínea b) do Cód. Penal."*

Ou seja, afirmava-se que a videovigilância não podendo ser utilizada como forma de controlar o exercício da atividade profissional do trabalhador, não poderia, por maioria de razão, ser utilizada como meio de prova em sede de procedimento disciplinar, sob pena de a divulgação da "cassete" vir a constituir, uma abusiva intromissão na vida privada e violar o direito à imagem do trabalhador.[14]

[13] Cfr. Ac. TRL de 03-05-2006 (Isabel Tapadinhas) - P. 872/2006-4, www.dgsi.pt

[14] Escudando-se ainda o referido acórdão na afirmação de que não sendo o direito de prova um direito absoluto, em consonância com o Acórdão do Tribunal Constitucional nº 209/95 de 20 de Abril, publicado no DR, II Série, nº 295 de 23.12.95, o direito subjetivo à produção de prova não obriga à admissão de todos os meios de prova permitidos em direito.

Neste sentido, também, o Tribunal da Relação de Lisboa (Ac. 19/11/2008)[15]:

> *"Não é admissível, no processo laboral e como meio de prova, a captação de imagens por sistema de videovigilância, envolvendo o desempenho profissional do trabalhador, incluindo os atos disciplinarmente ilícitos por ele praticados."*

Para certa jurisprudência essa nulidade de prova por videovigilância – em local de trabalho, não consentida pelo trabalhador ou do seu desconhecimento - não inquinava só a prova disciplinar como poderia mesmo inquinar a prova criminal, desde que o ilícito criminal fosse praticado em local de trabalho.

Foi o caso do Tribunal da Relação de Lisboa (Ac.03/05/2006)[16] que, com voto de vencido[17], considerou:

> *"I - São provas nulas as imagens de vídeo obtidas sem o consentimento ou conhecimento do arguido, através de câmara oculta colocada pelo assistente no seu estabelecimento de gelataria e que é o local de trabalho do arguido, sem que estivesse afixada informação sobre a existência de meios de videovigilância e qual a sua finalidade (…).*
>
> *II – Arrolados tais meios de prova na acusação pública por crime de furto e valorados em audiência, onde foram visionadas as imagens de vídeo, é nulo todo o processado desde a acusação, inclusive, e ulteriores termos do processo – artº 122º nº1 do C.P.P."*

O que resultava pacífico era a exclusão da videovigilância com a finalidade de controlar o desempenho do trabalhador e como meio de prova disciplinar quando aquela tivesse por finalidade vigiar o desempenho profissional do trabalhador.

Seguindo as linhas orientadoras da CNPD (Deliberação n.º 61/2004) os tribunais sobrepunham ainda um juízo de *necessidade, adequação e proporcionalidade* e um juízo de *intervenção mínima* na colocação das câmaras de videovigilância.

Num litígio que opôs uma estação de televisão e a CNPD e que correu termos no foro administrativo, discutiu-se, entre o mais, a decisão desta entidade de controlo de não autorização do tratamento de imagens através de três concretas câmaras colocadas na sala de redação da Direção de Informação, alegadamente pela necessidade de salvaguarda do direito à privacidade dos trabalhadores, tendo o Tribunal Central Administrativo Sul (Ac.14/05/2009)[18] considerado:

---

[15] Cfr. Ac.TRL de 19-11-2008 (Ramalho Pinto) - P.7125/2008-4, www.dgsi.pt

[16] Cfr. Ac.TRL de 03-05-2006 (Carlos Sousa) - P. 83/2006-3, www.dgsi.pt

[17] - Há declaração de voto do Exmº Desembargador Mário Morgado neste sentido: "A prova obtida é válida nos termos do artº 167º nº1 do C.P.P., já que a captação de imagens realizada não ofende a integridade física ou moral do arguido nem a sua dignidade e intimidade, como não é ilícita e nem integra o crime p. e p. pelo artº 199º nº 2 a) do C.P.."

[18] Cfr. Ac. TCA Sul de 14-05-2009 (Coelho da Cunha) – P.01614/06, www.dgsi.pt

> *"O tratamento a realizar e os meios utilizados devem ser os necessários, adequados e proporcionais, o que implica uma ponderação dos interesses fundamentais em conflito, designadamente da segurança, versus, respeito pela privacidade ou direito à imagem.*
>
> *Deverá, por isso, analisar-se as circunstâncias de cada caso concreto e adotar-se como princípio geral que a gravação de imagens se deve limitar, sempre que possível, a uma intervenção preventiva ou dissuasora (princípio da intervenção mínima)."*

A fronteira entre licitude e ilicitude da videovigilância no local de trabalho assentava assim não apenas na finalidade, mas igualmente na razoabilidade dos meios, de acordo com um *juízo de proporcionalidade* e de *intervenção mínima*, cabendo à entidade patronal o ónus de provar essa finalidade e essa razoabilidade.

O dever de informar o trabalhador da utilização de meios de vigilância no local de trabalho configurava igualmente uma condição de licitude.

Assim se pronunciou o Supremo Tribunal de Justiça (27/05/2010)[19] sob a alçada do CT 2003:

> *"De acordo com o disposto no art. 20.º do Código do Trabalho, a utilização de meios de vigilância será sempre ilícita (ainda que com aviso prévio da sua instalação feito ao trabalhador), desde que tenha a finalidade de controlar o desempenho profissional do ou dos trabalhadores, só sendo, pois, lícita a sua utilização quando a tal finalidade se não destine e, outrossim, se destine à proteção e segurança de pessoas e bens ou quando as exigências inerentes à natureza da atividade o justifiquem, caso em que se torna imprescindível o cumprimento pela empregadora do dever de informar o trabalhador."*

Em suma, no âmbito da Lei 67/98 de 26/10 (anterior LPDP) e do CT 2003 e seu Regulamento, a jurisprudência definiu-se relativamente à videovigilância do seguinte modo: concebendo-a como uma restrição do direito de reserva da vida privada, direito com tutela constitucional, considerando-a justificada quando necessária à finalidade de proteção e segurança de pessoas e bens, dentro de limites de proporcionalidade e de intervenção mínima e, de forma genérica, ou seja, a sua utilização não poderia constituir uma vigilância direta dirigida aos postos de trabalho ou ao campo de ação dos trabalhadores, que da sua existência deveriam ser informados.

A jurisprudência laboral a partir do CT 2003 reforçou, assim, o direito à privacidade do trabalhador como uma exigência dos direitos fundamentais.

[19] Cfr. Ac. STJ de 27-05-2010 (Sousa Grandão) – P.467/06.3TTCBR.C1.S1, www.dgsi.pt

A videovigilância enquanto direito do trabalhador *versus* obrigação da entidade patronal

E se, por norma, a videovigilância vem sendo configurada como uma limitação do direito de personalidade do trabalhador, decisões judiciais houve em que, pelo contexto, a vigilância à distância foi considerada não como uma restrição de um direito fundamental, mas sim como um meio de salvaguarda de direitos fundamentais.

Ou seja, como um direito do trabalhador à salvaguarda da sua integridade física, se não mesmo da vida e, enquanto tal, uma obrigação da entidade patronal em criar condições de segurança na prestação do trabalho, cuja violação confere ao trabalhador, justa causa na resolução do contrato.

Nesse sentido o Acórdão do Tribunal da Relação do Porto (07/06/2010)[20]

> *"I- Nos termos do art.° 59º, n.° 1, alínea c) da Constituição da República Portuguesa, ao trabalhador assiste o direito fundamental de só "prestar trabalho quando se encontrem observadas as regras de higiene, de segurança e saúde" no trabalho.*
>
> *II- Assumindo o trabalhador a posição de contraente débil, encontrando-se limitado na sua liberdade individual, sujeito ao poder de direção do empregador, que é quem retira benefício da sua atividade, cabe a este organizar e dirigir o trabalho por forma a proporcionar as necessárias condições de segurança na prestação do trabalho, sendo o responsável por essa segurança.*
>
> *III. Deve concluir-se pela verificação de justa na resolução do contrato por parte de trabalhadora que, enquanto caixa num supermercado, ao longo de vários anos foi vítima de assaltos, ofensas à sua integridade física e psíquica e de roubo, sem que a entidade patronal tenha tomado as medidas adequadas para evitar ou minorar os riscos de ocorrência dessas situações."*

Reclamava a trabalhadora a colocação de um dispositivo de videovigilância como recurso dissuasor dos assaltos de que repetidamente fora alvo, enquanto caixa num supermercado. O Tribunal deu-lhe razão.

O Código de Trabalho de 2009

Nascido da proposta de lei n.º 216/X (decreto preambular)[21], teve em vista, entre o mais, estabelecer "*um quadro normativo mais eficaz, que unifica os dois principais instrumentos legislativos que disciplinam as relações de trabalho - o Código do Trabalho e o seu Regulamento –, tornando-os mais inteligíveis, mais acessíveis, sendo previsíveis os ganhos ao nível da divulgação efetiva do seu conteúdo normativo pelos destinatários e, assim, também no que respeita ao seu cumprimento."*

[20] Cfr. TRP de 07-06-2010 (Albertina Pereira) – P.807/08.0TTVNG.P1, www.dgsi.pt

[21] https://app.parlamento.pt/

O CT 2009[22], atualmente em vigor, manteve sensivelmente idênticos os artigos 16º (reserva da intimidade da vida privada) e 17º (proteção de dados pessoais) do CT 2003, acrescentando quanto a este último uma previsão contraordenacional (nº 5).

Preservou o art. 20º do CT 2003 alusivo aos meios de vigilância à distância, nos seus nºs 1 e 2, deu uma nova redação ao nº 3, *acentuando a obrigatoriedade* para o empregador de *informar e publicitar a utilização da videovigilância* em consonância com o Regulamento do CT 2003 e, acrescentou um nº 4 com previsão contraordenacional.

> *"3 - Nos casos previstos no número anterior, o empregador informa o trabalhador sobre 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.*
>
> *4 - Constitui contraordenação muito grave a violação do disposto no n.º 1 e constitui contraordenação leve a violação do disposto no n.º 3."*

E, estatuiu uma previsão – o art. 21º - acolhida do Regulamento do CT 2003, reforçando a componente sancionatória:

> *"Artigo 21.º [23] - Utilização de meios de vigilância a distância*
>
> *1 - A utilização de meios de vigilância a distância no local de trabalho está sujeita a autorização da Comissão Nacional de Proteção de Dados.*
>
> *2 - A autorização só pode ser concedida se a utilização dos meios for necessária, adequada e proporcional aos objetivos a atingir.*
>
> *3 - 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.*
>
> *4 - O pedido de autorização a que se refere o n.º 1 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.*
>
> *5 - Constitui contraordenação grave a violação do disposto no n.º 3."*

[22] Lei n.º 7/2009 de 12 de Fevereiro - Aprovou a revisão do Código do Trabalho.

[23] O artigo 21.º do CT 2003: "Confidencialidade de mensagens e de acesso a informação" passou a integrar o art. 22 do CT de 2009.

A jurisprudência no âmbito do CT 2009

No âmbito do CT 2009 e na vigência da Lei 67/98 de 26/10, a jurisprudência acentuou a dependência da *licitude* da videovigilância e da prova nela assente, da existência de *autorização prévia da CNPD*.

Ou seja, afirmava não ser admissível o tratamento ou a visualização das imagens, nomeadamente para efeitos disciplinares, ainda que obedecesse ao escopo da proteção e segurança de pessoas (nº 2 do art. 20º), se o empregador não fizesse *prova da autorização prévia concedida pela CNPD* e dos demais requisitos objetivos (audição da comissão de trabalhadores (existindo) / junção do parecer ao pedido de autorização à Comissão Nacional de Proteção de Dados / instalação dos meios de vigilância nos termos da autorização concedida / informação aos trabalhadores e publicidade sobre a existência e finalidade dos meios de vigilância utilizados (n.º 3 do art. 20.º).

Ressalvando a possibilidade da sua utilização para efeitos criminais.

Nesse sentido, o Tribunal da Relação do Porto (Ac. 04/02/2013)[24]

> *"IV - A licitude da utilização de meios de vigilância à distância não depende apenas dessa concreta ponderação material de interesses divergentes, mas igualmente da verificação das condições e procedimentos objetivos previstos no artº 20º nº3 e 21º do Código do Trabalho.*
>
> *V - Sendo imputado pelo empregador ao trabalhador a prática de um ilícito disciplinar por violação do dever de lealdade, passível de integrar igualmente um crime de furto, é de admitir a exibição em audiência de julgamento das gravações de imagens num caso em que está alegado, sem impugnação, que o estabelecimento onde ocorreu aquele ilícito está a videovigilância autorizada pela CNPD, a existência e funcionamento desse sistema foi participado ao trabalhador, está devidamente publicitado por dois dísticos afixados nesse estabelecimento e o dito sistema foi implementado com vista a salvaguardar os bens e produtos à venda."*

Ou, o Tribunal da Relação de Coimbra, num litígio reportado a um salão de jogos/casino (Ac. 06/02/2015)[25]:

> *"I – O artº 20º, nº 1 do Código do Trabalho proíbe a utilização de meios de vigilância à distância para controlar de forma dedicada e permanente o desempenho profissional do trabalhador.*

[24] Cfr. TRP de 04-02-2013 (João Diogo Rodrigues) – P.229/11.6TTLMG.P1, www.dgsi.pt

[25] Cfr. TRC de 06-02-2015 (Luís Azevedo Mendes) – P. 359/13.0TTFIG, www.dgsi.pt

II – A utilização desses meios de vigilância no local de trabalho é, no entanto, lícita se cumprir os requisitos de fim e publicidade previstos nos nºs 2 e 3 do mesmo artº 20º e for obtida a autorização da Comissão Nacional de Proteção de Dados."

No âmbito desta legislação, alguma jurisprudência bastava-se com a autorização dada pela CNPD. Existindo esta, o respeito pelas diversas finalidades estaria implícito e a licitude formal e material assegurada.

Outra, exigia a prova da conformidade prática da colocação de sistema de videovigilância, com a autorização concedida.

A inobservância dos requisitos objetivos, como fundamento de resolução por parte do trabalhador:

A inobservância de algum dos requisitos legais, nomeadamente, a informação prévia dos trabalhadores e a autorização prévia da CNPD, poderia constituir fundamento de resolução do contrato por parte do trabalhador.

Assim afirmou o Tribunal da Relação do Porto (Ac.04/03/2013)[26]:

"I – Constitui justa causa de resolução do contrato, pelo trabalhador, a implementação de um sistema de videovigilância, por parte da R., sem observância de qualquer dos requisitos legais, nomeadamente, informação prévia dos trabalhadores, na forma legal e autorização da CNPD.

II – Apesar de as provas obtidas pelo sistema de videovigilância não poderem ser consideradas em sede disciplinar, por ilícitas, tal não impede que a trabalhadora invoque tal matéria se decidir resolver o contrato, com invocação de justa causa pois, em qualquer dos casos, estamos sempre perante o mesmo comportamento ilícito da R., não tendo a A. produzido qualquer prova."

A interpretação da finalidade

A interpretação da finalidade "proteção de pessoas e bens/particulares exigências inerentes à natureza da atividade" prevista no art. 20º nº 2 do CT 2009[27] teve num caso judicial, *sui generis,* um alcance demonstrativo do quão ampla pode ser a sua valoração na atividade empresarial produtiva. Acolhendo interesses não apenas privados, mas igualmente públicos e de caráter moral/social.

[26] Cfr. TRP de 04-03-2013 (Ferreira da Costa) – P. 787/10.2TTVCT.P1, www.dgsi.pt

[27] À semelhança do art. 20 nº 2 do CT 2003.

Interpretação dada pelo Tribunal da Relação do Porto (Ac. 07/12/2018)[28] :

> *"I - A inserção do trabalhador numa organização empresarial comporta limitações à liberdade e exercício de direitos fundamentais, que pode provocar conflito entre o direito fundamental do trabalhador à reserva sobre a intimidade da sua vida privada e o direito do empregador a prosseguir os objetivos que se propôs no pacto social da empresa.*
>
> *III – A prática de atos amorosos entre uma trabalhadora e o namorado não pode ser manifestada no local e durante o horário de trabalho - bar/café de "bomba de gasolina" -, sendo um espaço privado, é de acesso público.*
>
> *VII – Neste contexto, é de admitir a visualização, em sede de audiência de discussão e julgamento, das imagens de videovigilância recolhidas no local de trabalho, como meio de prova para o fim disciplinar específico dos autos."*

O enquadramento normativo recente

O RGPD e a atual LPDP

Em 25 de maio de 2018 passou a ser aplicável o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016[29] relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (RGPD).

Embora nos termos do artigo 288.º do Tratado de Funcionamento da União Europeia (TFUE), o regulamento seja um ato legislativo desta que não carece de transposição, tendo aplicabilidade direta e efeito direto no ordenamento jurídico de cada Estado-Membro da União Europeia, o RGPD contém inúmeras cláusulas de abertura implicando os Estados-Membros na definição de um conteúdo concretizador ou complementar. E, ainda que aprovado em 2016 estabeleceu no seu artigo 99.º que apenas passaria a ser aplicável em todos os Estados-Membros a 25 de maio de 2018, de modo a permitir que os Estados-Membros adotassem medidas necessárias à correta vigência do RGPD.

A. Barreto Menezes Cordeiro *in* "Direito da Proteção de Dados à luz do RGPD e da Lei 58/2019", p. 30, resume assim alguns dos seus aspetos inovadores:

> *"Apesar de o Direito da proteção de Dados não ser um ramo jurídico novo, é certo que apenas com o RGPD assumiu uma importância indiscutível no panorama jurídico nacional. As razões para esta descoberta (…) são um reflexo da revolução imprimida pelo RGPD: a densificação dos direitos dos titulares de dados pessoais, o agravamento dos deveres dos responsáveis pelo tratamento de dados e dos subcontratantes, o reforço das competências das*

[28] Cfr. TRP de 07-12-2018 (Domingos Morais) – P.159/18.0T8PNF-A.P1, www.dgsi.pt

[29] Tendo revogado a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24-10-1995.

autoridades de controlo ou a obrigatoriedade de designação de encarregados de proteção de dados."

O Parecer n.º 20/2018 da Comissão Nacional de Proteção de Dados (CNPD) sobre a Proposta de Lei n.º 120/XIII/3.ª (Gov), *in* https://app.parlamento.pt/, que antecedeu a Lei de execução do RGPD reforça a sua justificação, criada pela necessidade de garantir ao titular dos dados uma maior segurança dos seus dados pessoais face à tecnologia hoje disponível:

"Na verdade, o que o RGPD toma como paradigma é a tecnologia hoje disponível para a realização de tratamentos de dados pessoais e, portanto, visa conciliar a utilização de soluções tecnológicas no seu estado atual e futuro de desenvolvimento, e os riscos que comportam, com a defesa dos direitos e liberdades das pessoas cujos dados são objeto de tratamento."

E fá-lo sob uma perspetiva de pessoa singular/titular de dados na União Europeia e fora dela.

"O Regulamento fortalece e expande o regime de proteção de dados europeus, na medida que protege os dados pessoais de todos os residentes da União Europeia, independentemente da localização do tratamento, aumentando amplamente o alcance do novo quadro legal europeu, abrangendo toda a informação que, diretamente ou indiretamente, possam identificar um indivíduo, incluindo identificadores online como endereços de IP, cookies, dados de localização, estatuindo um conceito de dados muito mais amplo do que a anterior Diretiva" - conclui Daniela Medeiros Teves *in* " A proteção de dados pessoais – o novo paradigma jurídico". [30]

Mantendo válidos os princípios gerais outrora aplicáveis aos tratamentos de dados, agora sob melhor concetualização.

Assim o artigo **5º do RGPD** ao enunciar os - **Princípios gerais a respeitar em qualquer tratamento:**

"1. Os dados pessoais são:

*a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados («**licitude, lealdade e transparência**»);*

*b) 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 89.º, n.º 1 («**limitação das finalidades**»);*

[30] - Dissertação de Mestrado *in* https://repositorio.uac.pt/.

*c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («**minimização dos dados**»);*

*d) Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora («**exatidão**»);*

*e) Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.º, n.º 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados («**limitação da conservação**»);*

*f) Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas («**integridade e confidencialidade**»);*

*2. O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 e tem de poder comprová-lo («**responsabilidade**»).”*

O regime da videovigilância no âmbito laboral a partir do RGPD e da LPDP

Os artigos 20º e 21º do Código do Trabalho mantêm formalmente a sua redação originária, nomeadamente, no que respeita à necessidade de autorização prévia da Comissão Nacional de Proteção de Dados quanto à utilização de meios de vigilância a distância no local de trabalho (n.º 1 do artigo 21º).

Sucede que com a entrada em vigor do RGPD e da LPDP, esta exigência – autorização prévia da autoridade de controlo - perdeu a sua razão de ser.

O RGPD veio alterar o paradigma de intervenção da autoridade de controlo, passando de um regime de autorização prévia para uma solução – regra de **autorresponsabilização e de autodisciplina no tratamento**, podendo conduzir, em situações excecionais, a um pedido de consulta prévia daquela.

Cabe aos responsáveis pelo tratamento e aos subcontratantes o *dever prévio de verificação do cumprimento do RGPD*, dever este impulsionado pela obrigação, em determinados casos, de registo das atividades de tratamento (artigo 30.º do RGPD), o qual deve ser disponibilizado à autoridade de controlo quando pedido (art. 30 nº 4 do RGPD)

O artigo 35º do RGPD alusivo à “Avaliação de impacto sobre a proteção de dados” veio estabelecer no seu nº 1 que: *“ Quando um certo tipo de tratamento, em particular que utilize novas*

tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação."

O artigo 36º do RGPD admite situações de controlo prévio para situações específicas, sendo a mais evidente a que deriva da aplicação do artigo 35º, bem como, confere aos Estados-Membros o poder de exigir esse controlo *prévio em razão do interesse público*.

Assim, a partir de 25-05-2018, pela aplicabilidade do RGPD ou, mais rigorosamente, a partir de 09-08-2019, data em que entrou em vigor a LPDP, as normas nacionais que previam autorizações da autoridade de controlo, mostram-se tacitamente revogadas por incompatibilidade de regime.

O que resulta claro do artigo 62.º nº 2 da LPDP, que dispõe *"Todas as normas que prevejam autorizações ou notificações de tratamento de dados pessoais à CNPD, fora dos casos previstos no RGPD e na presente lei, deixam de vigorar à data de entrada em vigor do RGPD."*

Estão desse modo revogadas as normas do CT 2009 na parte em que exigiam uma autorização prévia da autoridade de controlo, contidas nos artigos 18.º n.º 1 *"O empregador só pode tratar dados biométricos do trabalhador após notificação à Comissão Nacional de Proteção de Dados"* e 21.º n.º 1 *"A utilização de meios de vigilância a distância no local de trabalho está sujeita a autorização da Comissão Nacional de Proteção de Dados."*

No que respeita à *videovigilância* a Lei de execução prevê apenas uma situação em que se exige o controlo prévio da CNPD: a videovigilância que inclua captação de som quando as instalações vigiadas não se encontrem encerradas, conforme o n.º 4 do artigo 19.º. O que se aplica ao contexto laboral.

Fora desta situação particular a videovigilância no local de trabalho deixou de estar sujeita a autorização prévia por parte da CNPD.[31]

[31] Interpretação que não é consensual. A concluir que "a videovigilância em contexto laboral continua a carecer de autorização prévia da CNPD, independentemente da captação de som, mantendo-se em vigor o regime anterior ao RGPD, com exceção do valor das coimas a aplicar" ver Alexandre Sousa Pinheiro e Tatiana Duarte (cf. o artigo de opinião "A Videovigilância no Código do Trabalho à luz do RGPD e da Lei nacional de Execução", disponível em https://www.publico.pt/2019/10/30/sociedade/ opiniao/videovigilancia-codigo-trabalho-luz-rgpd- -lei-nacional-execucao-1891769.

A videovigilância na LPDP

O artigo 19.º da Lei nº 58/2019 de 08.08 (LPDP) versa sobre as condições e critérios para a delimitação do âmbito dos tratamentos de dados pessoais decorrentes dos sistemas de **videovigilância.**

Assim dispondo:

> *«1 - Sem prejuízo das disposições legais específicas que imponham a sua utilização, nomeadamente por razões de segurança pública, os sistemas de videovigilância cuja* ***finalidade seja a proteção de pessoas e bens*** *asseguram os requisitos previstos no artigo 31.º da Lei n.º 34/2013, de 16 de maio, com os limites definidos no número seguinte.*
>
> *2 - As câmaras não podem incidir sobre:*
>
> *(…)*
>
> *d) O interior de áreas reservadas aos trabalhadores, designadamente zonas de refeição, vestiários, ginásios, instalações sanitárias e zonas exclusivamente afetas ao seu descanso.*
>
> *(…)*
>
> *4 - Nos casos em que é admitida a videovigilância, é proibida a captação de som, exceto no período em que as instalações vigiadas estejam encerradas ou mediante autorização prévia da CNPD."*

Assim, para além de remeter para os requisitos previstos no artigo 31.º da Lei n.º 34/2013, de 16 de maio, lei que estabelece o regime do exercício da *atividade de segurança privada*, a LPDP cria limitações ao referido tratamento, por exemplo, e no que ao âmbito laboral importa, *impedindo que as câmaras incidam sobre o interior de áreas reservadas aos trabalhadores.*

O artigo 21.º nº 2 do CT 2009 respeitante à utilização de meios de vigilância a distância, mantém-se válido quanto aos critérios de *necessidade, adequação e proporcionalidade* dos meios aos objetivos a atingir, numa compatibilidade de conteúdo com um dos princípios atuais, o **princípio da minimização de dados** (art. 5º nº 1 alª c) do RGPD).

E, o nº 3 do art. 21 do CT 2009 referente às finalidades e conservação, mantém compatibilidade com os princípios da **limitação das finalidades** e **limitação da conservação** do regime atual (art. 5º nº 1 alªs b) e e) do RGPD).

O art. 28 da LPDP aludindo às «*Relações laborais*» dispõe:

"*1 - O empregador pode tratar os dados pessoais dos seus trabalhadores para as finalidades e com os limites definidos no Código do Trabalho e respetiva legislação complementar ou noutros regimes setoriais, com as especificidades estabelecidas no presente artigo. (…)*

3 - Salvo norma legal em contrário, o consentimento do trabalhador não constitui requisito de legitimidade do tratamento dos seus dados pessoais:

a) Se do tratamento resultar uma vantagem jurídica ou económica para o trabalhador; ou

b) Se esse tratamento estiver abrangido pelo disposto na alínea b) do n.º 1 do artigo 6.º do RGPD.[32]

4 - 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.

5 - 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. (…)."

Resulta dos n.ºs 4 e 5 que *as imagens gravadas só podem ser utilizadas no âmbito de processo penal*, embora sequencialmente e em idêntica medida possam também ser utilizadas para efeitos de *apuramento de responsabilidade disciplinar*.

O controlo à distância no regime de teletrabalho

Com o incremento do teletrabalho[33] na sequência da pandemia decorrente do novo coronavírus SARS-CoV-2 e da doença Covid-19, tem-se vindo a discutir até onde pode ir o controlo por parte das entidades patronais, da atividade laboral à distância.

Algumas empresas recorrem a *software* que permite controlar a atividade dos trabalhadores, rastreando os tempos de trabalho *versus* os tempos de inatividade, registando as páginas por estes consultadas, os *chats* por estes realizados ou mesmo a sua localização em tempo real. Por sua vez a captação de som ou imagens de parte do desempenho laboral são complementos que têm vindo a ser denunciados na comunicação social.

Mecanismos que possibilitam o controlo à distância do desempenho profissional do trabalhador, proibido pelo art. 20 nº 1 do CT e, suscetíveis de atingir os direitos de personalidade

[32] Art. 6º nº 1 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"

[33] Considera-se teletrabalho a prestação laboral realizada com subordinação jurídica, habitualmente fora da empresa e através do recurso a tecnologias de informação e de comunicação (cf. artigo 165.º do Código do Trabalho).

do trabalhador e até mesmo do seu agregado familiar, afetando **dados pessoais sensíveis** deste e do agregado, uma vez que as *questões da vida privada* se inserem no campo dos dados sensíveis a proteger (art. 7º n.º 1 do LPDP).

A Comissão Nacional de Proteção de Dados (CNPD) divulgou *«orientações sobre o controlo à distância em regime de teletrabalho»* (17-04-2020)[34], relacionadas com a utilização de diversos *softwares* para o controlo da atividade laboral, de modo a garantir a conformidade dos tratamentos de dados pessoais dos trabalhadores com o regime jurídico de proteção de dados e minimizar o impacto sobre a privacidade em regime de teletrabalho. Assim:

> *"1. Em circunstâncias normais, os instrumentos de trabalho respeitantes a tecnologias de informação e de comunicação utilizados pelo trabalhador em teletrabalho pertencem ao empregador*[35]*.*
>
> *Quando seja este o caso, os trabalhadores devem observar as regras de utilização e funcionamento dos instrumentos de trabalho que lhe forem disponibilizados, só podendo, salvo acordo em contrário, utilizá-los para a prestação de trabalho. (…)*
>
> *Naturalmente que, independentemente da propriedade dos instrumentos de trabalho, no regime de teletrabalho o empregador mantém os poderes de direção e de controlo da execução da prestação laboral. No entanto, neste regime não existe qualquer disposição legal que regule o controlo à distância*[36]*, pelo que a regra geral de proibição de utilização de meios de vigilância à distância, com a finalidade de controlar o desempenho profissional do trabalhador*[37]*, é plenamente aplicável à realidade de teletrabalho. Aliás, à mesma conclusão sempre se chegaria pela aplicação dos princípios da proporcionalidade e da minimização dos dados pessoais*[38]*, uma vez que a utilização de tais meios implica uma restrição desnecessária e seguramente excessiva da vida privada do trabalhador.*
>
> *Por esta razão, soluções tecnológicas para controlo à distância do desempenho do trabalhador não são admitidas. São disso exemplo os softwares que, para além do rastreamento do tempo de trabalho e de inatividade, registam as páginas de Internet visitadas, a localização do terminal em tempo real, as utilizações dos dispositivos periféricos (ratos e teclados), fazem captura de imagem do ambiente de trabalho, observam e registam quando se inicia o acesso a uma aplicação, controlam o documento em que se está a trabalhar e registam o respetivo tempo gasto em cada tarefa (v.g., TimeDoctor, Hubstaff, Timing, ManicTime, TimeCamp, Toggl, Harvest).*

---

[34] https://www.cnpd.pt/media/zkhkxlpx/orientacoes_controlo_a_distancia_em_regime_de_teletrabalho.pdf

[35] Cf. alínea e) do n.º 5 do artigo 166.º e artigo 168.º do Código de Trabalho.

[36] Na verdade, em matéria de teletrabalho, está expressamente regulada a possibilidade de o empregador efetuar esse controlo através do acesso à residência do trabalhador, entre as 9h00 e as 19h00.

[37] Cf. n.º 1 do artigo 20.º do Código de Trabalho.

[38] Cf. alínea c) do n.º 1 do artigo 5.º do RGPD.

Ferramentas deste tipo recolhem manifestamente em excesso dados pessoais dos trabalhadores, promovendo o controlo do trabalho num grau muito mais detalhado do que aquele que pode ser legitimamente realizado no contexto da sua prestação nas instalações da entidade empregadora. E a circunstância de o trabalho estar a ser prestado a partir do domicílio não justifica uma maior restrição da esfera jurídica dos trabalhadores. Nessa medida, a recolha e o subsequente tratamento daqueles dados violam o princípio da minimização dos dados pessoais.

Do mesmo modo, não é admissível impor ao trabalhador que mantenha a câmara de vídeo permanentemente ligada, nem, em princípio, será de admitir a possibilidade de gravação de teleconferências entre o empregador (ou dirigentes) e os trabalhadores.

Apesar da inadmissibilidade da utilização de tais ferramentas, reafirma-se que o empregador mantém o poder de controlar a atividade do trabalhador, o que poderá fazer, designadamente, fixando objetivos, criando obrigações de reporte com a periodicidade que entenda, marcando reuniões em teleconferência.

2. Situação diversa é a necessidade de registo de tempos de trabalho, que pode ser efetuado por recurso a soluções tecnológicas específicas neste regime de teletrabalho.

Tais soluções devem limitar-se a reproduzir o registo efetuado quando o trabalho é prestado nas instalações da entidade empregadora (i.e., registar o início e fim da atividade laboral e pausa para almoço). Portanto, estas ferramentas devem estar desenhadas de acordo com os princípios da privacidade desde a conceção e por defeito, não recolhendo mais informação do que a necessária para a prossecução daquela finalidade[39](…).”

Software, como o que ora damos como exemplo, publicitado na internet[40], comporta os referidos riscos.

«Como funciona o MyAnalytics

O MyAnalytics fornece informações com os seguintes tipos de dados.

*1. **Dados da caixa de correio:** atividades do email, calendário, chat e chamada que você gera usando o Office 365, como o tempo gasto em reuniões ou emails enviados para uma pessoa específica ou grupo.*

*2. **Dados do histórico de atividades do Windows 10:** dados sobre o uso de aplicativos e serviços no seu dispositivo: se você trabalhou em um documento e se você navegou na Web.*

[39] Cf. artigo 25.º do RGPD.

[40] https://docs.microsoft.com/pt-br/workplace-analytics/myanalytics/overview/privacy-guide-users

Dados de caixa de correio

Por exemplo, o MyAnalytics fornece modos de exibição que permitem que você entenda rapidamente o tempo gasto em reuniões e emails todos os dias, com quem você colabora com mais frequência, com quem você está perdendo contato e com que você tem compromissos e solicitações.

***Dados do histórico de atividades do Windows 10** - O MyAnalytics usa os dados do histórico de atividades do Windows 10 para calcular informações (por exemplo, o tempo gasto em aplicativos, várias tarefas em reuniões) sobre seus hábitos de trabalho. Essas informações são privadas e armazenadas na sua caixa de correio do Exchange Online.*

***Taxas de leitura de email** - O MyAnalytics controla a porcentagem de destinatários que abriram uma mensagem de email (no suplemento do Outlook) para os emails que você enviou para cinco ou mais pessoas.»*

Sendo um *software* controlador de eficiência no trabalho alegadamente para proveito do trabalhador que poderá, com as informações por ele produzidas, auto melhorar o seu desempenho, será legítimo questionar: sendo um programa disponibilizado por iniciativa da entidade patronal, que contratou com terceiros fornecedores do programa, como pode o trabalhador assegurar-se que o tratamento de dados dele resultante não será igualmente, ainda que em parte, disponibilizado àquela para aferir do seu desempenho?

Resposta que não é simples.

A responsabilidade civil

O RGPD prevê no artigo 82.º nº 1 que qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do referido regulamento tem direito a receber *uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofridos*. Acrescentando o nº 2 que qualquer responsável pelo tratamento que esteja envolvido no tratamento é responsável pelos danos causados por um tratamento que viole o regulamento, sendo o subcontratante responsável pelos danos causados pelo tratamento, apenas se não tiver cumprido as obrigações decorrentes do regulamento dirigidas especificamente aos subcontratantes ou se não tiver seguido as instruções lícitas do responsável pelo tratamento.

Esta responsabilidade pode ser afastada se o responsável pelo tratamento ou o subcontratante provar que não é de modo algum responsável pelo evento que deu origem aos danos. Uma regra de *inversão do ónus da prova*.

Responsabilidade criminal

O artigo 46.º da Lei n.º 58/2019 prevê ainda que *"Quem utilizar dados pessoais de forma incompatível com a finalidade determinante da recolha é punido com pena de prisão até um ano ou com pena de multa até 120 dias"*.

A expressão coerciva à evidência.

O agravamento dos deveres dos responsáveis pelo tratamento de dados e dos subcontratantes, se fizerem uma utilização dos dados de forma incompatível com a finalidade determinante.

A revolução que o RGPD e a lei nacional pretendem imprimir.

Caberá à sociedade e a cada um de nós a assunção desse compromisso.

ANABELA LUNA DE CARVALHO
Juíza Desembargadora
maio de 2021