UNIVERSIDADE DE LISBOA
FACULDADE DE DIREITO

O RGPD e a videovigilância no âmbito laboral

Arthur de Moura Cebolão

Orientadora
Professora Doutora
Cláudia Alexandra dos Santos Madaleno

Lisboa
2025

UNIVERSIDADE DE LISBOA
FACULDADE DE DIREITO

O RGPD e a videovigilância no âmbito laboral

Trabalho apresentado ao Mestrado de Direito e Ciência Jurídica, submetido à avaliação da banca examinadora, sob orientação da professora Cláudia Alexandra dos Santos Madaleno pelo aluno Arthur Moura Cebolão.

Lisboa

2025

AGRADECIMENTOS

Ao concluir este trabalho, gostaria de expressar minha sincera gratidão a todas as pessoas que, de alguma forma, contribuíram para o desenvolvimento e a realização deste projeto.

Em primeiro lugar, agradeço aos meus pais, Fernando e Lilian, pelo apoio incondicional, amor e dedicação ao longo de toda minha trajetória académica e pessoal. Seu exemplo de perseverança, ética e compromisso com a educação foi a maior fonte de inspiração para que eu pudesse chegar até aqui. Agradeço profundamente pela confiança, paciência e, sobretudo, pela fé que sempre depositaram em mim, mesmo nos momentos de maior desafio.

Aos meus orientadores e professores da Faculdade de Direito da Universidade de Lisboa, agradeço por sua orientação e pelos ensinamentos preciosos que me permitiram compreender melhor o tema do RGPD e da videovigilância no âmbito laboral. Suas valiosas contribuições acadêmicas e sua dedicação fizeram toda a diferença na construção deste trabalho.

A todos os colegas, amigos e familiares que, de alguma forma, participaram deste percurso, meu agradecimento sincero. Cada palavra de incentivo, cada gesto de amizade e cada contribuição foi fundamental para que eu pudesse completar esta jornada.

Por fim, agradeço a todos aqueles que, de maneira direta ou indireta, ajudaram a enriquecer este estudo e tornaram este momento possível.

RESUMO

Atualmente, surgem novos desafios éticos no local de trabalho, onde questões centram-se na utilização das tecnologias da comunicação e informação para melhorias de produtividade versus a privacidade do trabalhador. Desse modo, a questão centra-se no fato de que as novas tecnologias e a própria utilização da IA podem conduzir a uma vigilância excessiva, recolhendo dados sobre as atividades, emoções e produtividade dos trabalhadores, muitas vezes sem o seu conhecimento ou consentimento, o que suscita preocupações em matéria de privacidade. Além disso, a crescente dependência das novas tecnologias de videovigilância pode reduzir o controlo dos trabalhadores sobre o seu ambiente de trabalho, comprometendo potencialmente a sua autonomia e satisfação profissional. A resposta a estes desafios exige uma governação transparente da videovigilância nos locais do trabalho, bem como orientações éticas e o envolvimento ativo dos trabalhadores na implementação de tecnologias de vídeo para garantir que estes sistemas apoiam o trabalho humano ao invés de o explorarem. A videovigilância envolve a gravação e o processamento de imagens através de sistemas de câmaras integrados em espaços públicos ou em ambientes de trabalho. Estes sistemas são frequentemente implementados com o objetivo de aumentar a segurança, a produtividade e a conformidade em vários setores, desde a indústria transformadora aos escritórios das empresas. No entanto, a implantação generalizada da vigilância por vídeo gera preocupações significativas sobre privacidade, ética e o impacto nos direitos trabalhistas. A investigação tem como objetivo analisar a regulamentação da videovigilância no local de trabalho, avaliando o seu impacto na privacidade e na dignidade dos trabalhadores. Procura identificar as finalidades da vigilância, como a segurança e o controlo da produtividade, e explorar o equilíbrio entre estas práticas e os direitos fundamentais. O estudo propõe recomendações para políticas que respeitem a privacidade dos trabalhadores, sugestões de melhorias legislativas e sensibilização para o direito à privacidade. Pretende contribuir para melhores práticas empresariais e debates éticos sobre a utilização da vigilância, garantindo que as tecnologias de monitorização são utilizadas de forma proporcional, transparente e ética no local de trabalho.

Palavras-chave: videovigilância; RGPD; Direito do Trabalho; Trabalhador; Empregador.

ABSTRACT

Today, new ethical challenges are emerging in the workplace, where questions center on the use of communication and information technologies to improve productivity versus worker privacy. Thus, the issue centers on the fact that new technologies and the use of AI itself can lead to excessive surveillance, collecting data on workers' activities, emotions and productivity, often without their knowledge or consent, which raises privacy concerns. In addition, the growing reliance on new video surveillance technologies can reduce workers' control over their working environment, potentially compromising their autonomy and job satisfaction. Addressing these challenges requires transparent governance of video surveillance in the workplace, as well as ethical guidelines and the active involvement of workers in the implementation of video technologies to ensure that these systems support human work rather than exploit it. Meeting these challenges requires transparent governance of video surveillance in the workplace, as well as ethical guidelines and the active involvement of workers in the implementation of video technologies to ensure that these systems support human work rather than exploit it. Video surveillance involves recording and processing images through integrated camera systems in public spaces or work environments. These systems are often implemented with the aim of increasing security, productivity and compliance in various sectors, from manufacturing to corporate offices. n addition, the growing reliance on new video surveillance technologies can reduce workers' control over their working environment, potentially compromising their autonomy and job satisfaction. Addressing these challenges requires transparent governance of video surveillance in the workplace, as well as ethical guidelines and the active involvement of workers in the implementation of video technologies to ensure that these systems support human work rather than exploit it. Video surveillance involves recording and processing images through integrated camera systems in public spaces or work environments. These systems are often implemented with the aim of increasing security, productivity and compliance in various sectors, from manufacturing to corporate offices. However, the widespread deployment of video surveillance raises significant concerns about privacy, ethics and the impact on labor rights. The research aims to analyze the regulation of video surveillance in the workplace, assessing its impact on workers' privacy and dignity. It seeks to identify the purposes of surveillance, such as security and productivity control, and to explore the balance between these practices and fundamental rights. The study proposes recommendations for policies that respect workers' privacy, suggestions for legislative improvements and raising awareness of the right to privacy. It aims to contribute to better business practices and ethical debates on the use of surveillance, ensuring that monitoring technologies are used proportionately, transparently and ethically in the workplace.

Keywords: video surveillance; GDPR; employment law; worker; employer.

LISTA DE ABREVIATURAS

AEPD – Autoridade Europeia para a Proteção de Dados

CE – Comissão Europeia

CLT – Consolidação da Leis do Trabalho

CRFB – Constituição da República Federativa do Brasil

CRP – Constituição da República Portuguesa

CEDH – Convenção Europeia dos Direitos Humanos e das Liberdades Fundamentais

CNPD – Comissão Nacional de Proteção de Dados

ECHR – Corte Europeia de Direitos Humanos

IRCT – Instrumentos de Regulamentação Coletiva de Trabalho

LGPD – Lei Geral de Proteção de Dados

OCDE – Organização para a Cooperação e Desenvolvimento Econômico

RGPD – Regime Geral de Proteção de Dados

TEDH – Tribunal Europeu de Direitos Humanos

UE – União Europeia

Índice

INTRODUÇÃO

O uso cada vez maior da tecnologia, incluindo a vigilância por vídeo, no local de trabalho tem levantado desafios éticos e jurídicos significativos, principalmente com relação à privacidade e à proteção de dados. Os empregadores dos setores público e privado estão implantando cada vez mais tecnologias de informação e comunicação, inclusive vigilância por vídeo, para monitorar o desempenho dos funcionários. Essa prática geralmente ocorre sem o pleno conhecimento ou consentimento dos funcionários, levantando preocupações sobre privacidade, autonomia e a possibilidade de vigilância excessiva[1].

A escolha de focar apenas a videovigilância neste estudo justifica-se pela sua relevância prática e impacto direto nos direitos fundamentais no local de trabalho, particularmente no que diz respeito à privacidade, dignidade e proteção de dados[2]. A videovigilância emergiu como uma das ferramentas mais utilizadas para monitorizar os ambientes de trabalho, impulsionada pela crescente acessibilidade da tecnologia e por preocupações acrescidas com a segurança e a produtividade[3]. Por conseguinte, a compreensão dos aspectos legais e éticos da videovigilância é fundamental para um debate estruturado sobre os seus limites e potenciais aplicações em contextos profissionais.

A restrição do âmbito de aplicação exclusivamente à videovigilância baseia-se também na sua especificidade no contexto das relações laborais. Embora outras formas de vigilância, como a monitorização digital de e-mails e da utilização da Internet, o rastreio da geolocalização e o controlo biométrico, sejam inegavelmente relevantes, cada uma destas práticas apresenta desafios jurídicos e técnicos distintos[4]. Por exemplo, a monitorização digital pode envolver debates sobre a liberdade de expressão e a confidencialidade, enquanto o controlo biométrico suscita preocupações quanto ao tratamento de dados sensíveis como as caraterísticas faciais ou as impressões digitais. Um tratamento exaustivo de todas estas modalidades poderia comprometer a profundidade da análise efetuada neste estudo.

---

[1] KOBRON GASIOROWSKA, Lucja. (2023). The Involvement of Artificial Intelligence in Labour Rights Violations: European Union Perspective. Kwartalnik Prawa Międzynarodowego. III. 58-73. 10.5604/01.3001.0053.8986.

[2] PINTO FURTADO. A. *Videovigilância e Direitos dos Trabalhadores:* Perspetivas Éticas e Jurídicas. Lisboa: Livraria Jurídica, 2022.

[3] BARRETO, A. M. *A Proteção de Dados no Ambiente de Trabalho: Videovigilância e Privacidade.* Coimbra: Almedina, 2019, p. 15.

[4] OLIVEIRA, A. S. P. *Direitos Fundamentais e o RGPD: Proteção de Dados na Era Digital*. Coimbra: Almedina, 2020.

Para a presente pesquisa, vale mencionar que a escolha da videovigilância deve-se ao fato de permitir uma investigação aprofundada de uma forma específica de controle que se cruza com vários direitos fundamentais, como o direito à privacidade e a proteção contra a discriminação. A utilização de câmaras no local de trabalho tem implicações claras no âmbito da regulamentação nacional, como a Lei n.º 58/2019, que implementa o Regulamento Geral de Proteção de Dados (RGPD) em Portugal, e outros quadros legislativos relevantes. Este trabalho aborda os dilemas entre o direito do empregador à segurança e os direitos do trabalhador à privacidade e à dignidade, com o objetivo de fornecer uma perspectiva equilibrada sobre este debate[5].

Este estudo reconhece que práticas como a monitorização das comunicações digitais, a gravação áudio ambiental e os dispositivos de localização podem ser exploradas em investigações futuras. Cada um destes métodos de vigilância requer uma análise específica, considerando as suas nuances tecnológicas, éticas e legais[6]. Ao centrar-se na videovigilância, esta investigação procura contribuir para o debate sobre práticas de monitorização proporcionais e éticas no local de trabalho, estabelecendo um equilíbrio entre as necessidades das empresas e a proteção dos direitos fundamentais.

A vigilância por vídeo envolve a gravação e o processamento de imagens por meio de sistemas integrados de câmeras em espaços públicos ou em ambientes de trabalho[7]. Esses sistemas são empregados principalmente para garantir a segurança de pessoas e propriedades. Entretanto, os dados coletados por meio da vigilância podem afetar os direitos fundamentais, como o direito à privacidade e à dignidade dos funcionários, criando uma tensão entre as necessidades de segurança e os direitos individuais[8].

As atuais legislações sobre o tema estabelecem diretrizes sobre o uso legal de tecnologias de vigilância, enfatizando a importância da transparência, do consentimento e da minimização de dados. No entanto, a aplicação da videovigilância nas relações laborais

[5] OLIVEIRA, A. S. P. *Direitos Fundamentais e o RGPD: Proteção de Dados na Era Digital.* Coimbra: Almedina, 2020.

[6] A crescente integração da inteligência artificial nos sistemas de vigilância por vídeo acrescenta uma nova camada de complexidade à discussão. Essas tecnologias avançadas, capazes de reconhecer emoções e analisar comportamentos, exigem um escrutínio ético e legal ainda mais rigoroso. Isto reforça a importância de abordar a videovigilância como um ponto focal, ao mesmo tempo que prepara o terreno para explorações mais alargadas das tecnologias de vigilância em estudos subsequentes.

[7] BALL, K. (2010). Workplace surveillance: An overview. *Labor History, 51*(1), 87–106. https://doi.org/10.1080/00236561003654776

[8] BALL, K. (2021). Electronic Monitoring and Surveillance in the Workplace. Publications Office of the European Union. https://doi.org/10.2760/5137

continua a ser controversa, uma vez que entra frequentemente em conflito com o direito fundamental à privacidade, reconhecido como um direito constitucional em muitas jurisdições, incluindo Portugal.

O quadro legal que envolve a videovigilância procura equilibrar o direito dos empregadores a proteger os seus interesses comerciais com o direito dos trabalhadores à privacidade e a um tratamento justo. Isto exige que a videovigilância seja utilizada de forma transparente, com objetivos específicos e legítimos, e apenas como último recurso quando outros meios menos intrusivos de monitorização são inadequados.

Globalmente, a regulamentação da videovigilância no local de trabalho é crucial para garantir que, embora os empregadores possam proteger os seus interesses comerciais, os direitos fundamentais dos trabalhadores não sejam indevidamente comprometidos[9]. O debate em curso sublinha a necessidade de orientações éticas e de um envolvimento ativo dos trabalhadores na implementação de tecnologias de vigilância para apoiar abordagens centradas no ser humano no local de trabalho.

Para uma análise mais detalhada da temática, a presente pesquisa inicia com uma abordagem estruturada para tratar dos aspectos legais, éticos e regulatórios, com foco no Regulamento Geral de Proteção de Dados (RGPD). Essa etapa teve como objetivo entender os limites legais dentro dos quais a vigilância por vídeo opera, destacando princípios críticos como a transparência, o consentimento e a proteção de dados.

Num segundo momento, o estudo busca analisar em leis nacionais específicas em Portugal, incluindo a evolução de normas legais como a Lei de Proteção de Dados de 1998 e as suas alterações posteriores até os dias de hoje. Essa análise explorou como essas regulamentações influenciam a vigilância no local de trabalho e como elas se alinham aos padrões europeus. O foco principal foi nas implicações éticas da vigilância por vídeo na privacidade e na dignidade dos funcionários, avaliando como a vigilância afeta os direitos fundamentais garantidos em Portugal e os possíveis conflitos entre as necessidades de segurança e a privacidade individual.

A pesquisa também examinou a governança e o uso de sistemas de vigilância, investigando as finalidades da vigilância por vídeo, como segurança e monitoramento de

[9] SIEGEL, R., König, C. J., & Lazar, V. (2022). The impact of electronic monitoring on employees' job satisfaction, stress, performance, and counterproductive work behavior: A meta-analysis. Computers in Human Behavior Reports, 8, 100227. https://doi.org/10.1016/j.chbr.2022.100227

produtividade. Ela avaliou se esses usos estão alinhados com os padrões éticos e legais e considerou o papel dos órgãos reguladores, como a Comissão Nacional de Proteção de Dados. (CNPD), na supervisão dessas práticas. Foi realizada uma análise legal comparativa, explorando as regulamentações de vigilância por vídeo em diferentes jurisdições, incluindo a União Europeia e o Brasil, para identificar as melhores práticas e as áreas que precisam de aprimoramento regulatório.

Por fim, a pesquisa buscou analisar recomendações para aprimoramentos de políticas e diretrizes éticas que promovam práticas de vigilância transparentes e equilibradas no local de trabalho, garantindo que tanto os interesses de segurança do empregador quanto os direitos dos funcionários sejam respeitados.

1. PRELIMINARMENTE: DELINEAMENTO CONSTITUCIONAL E INTERNACIONAL DE DIREITOS FUNDAMENTAIS ATINENTES À VIDEOVIGILÂNCIA

A utilização de sistemas de videovigilância no local de trabalho levanta importantes questões sobre os direitos fundamentais dos trabalhadores, nomeadamente no que respeita à proteção da privacidade e da dignidade da pessoa humana. A Constituição da República Portuguesa, ao estabelecer princípios como o direito à identidade pessoal, à imagem e à privacidade (artigo 26.º), impõe limites claros à atuação do empregador na implementação destas tecnologias. Estes direitos devem ser respeitados para que a vigilância não resulte em abuso ou violação das garantias individuais[10].

No local de trabalho, o artigo 59.º da Constituição reforça a necessidade de proporcionar condições de trabalho dignas, seguras e higiénicas, bem como de garantir o respeito pela personalidade dos trabalhadores. A videovigilância não deve comprometer estes princípios, devendo a sua utilização ser proporcional e justificada, restringindo-se às situações em que seja absolutamente necessária para a proteção da propriedade e da segurança. A adoção destas medidas deve também ser transparente, informando os trabalhadores dos objectivos e limites da vigilância[11].

Entre as garantias constitucionais aplicáveis está o direito à privacidade, consagrado no artigo 26.º da Constituição, que protege os trabalhadores de intromissões indevidas na sua esfera pessoal e familiar. Esta disposição impõe limites à recolha e utilização de imagens e informações pessoais, assegurando que tais práticas sejam sempre justificadas e proporcionais[12].

Outro aspeto fundamental é o princípio da dignidade humana, consagrado no artigo 1.º da Constituição, que deve nortear a aplicação de qualquer medida no local de trabalho. Isto significa que os sistemas de videovigilância não podem ser utilizados para constranger,

[10] CANOTILHO, J. J. GOMES; MOREIRA, VITAL. *Constituição da República Portuguesa anotada*. Coimbra: Coimbra Editora, 2010.
[11] MIRANDA, JORGE; MEDEIROS, RUI. *Constituição da República Portuguesa anotada*. Lisboa: Wolters Kluwer, 2017.
[12] VIEIRA DE ANDRADE, J. C. *Os Direitos Fundamentais na Constituição Portuguesa de 1976.* Coimbra: Coimbra Editora, 2017.

humilhar ou desvalorizar os trabalhadores, sendo essencial garantir um tratamento respeitoso e ético[13].

Além disso, o direito à proteção contra a discriminação, previsto no artigo 13.º, reforça a necessidade de igualdade de tratamento na aplicação destas tecnologias. A utilização da videovigilância não deve ser direcionada seletivamente contra determinados trabalhadores, evitando práticas discriminatórias que violem a igualdade de direitos[14].

A Lei 58/2019, que assegura a implementação do Regulamento Geral de Proteção de Dados (RGPD) em Portugal, desempenha também um papel crucial na regulação da videovigilância no local de trabalho. Esta legislação estabelece normas rigorosas para o tratamento de dados pessoais, incluindo imagens captadas por sistemas de vigilância, exigindo transparência, minimização de dados e motivos legítimos para a sua utilização. Reforça ainda os direitos dos trabalhadores ao acesso, retificação e eliminação de dados, impondo obrigações claras aos empregadores para evitar abusos e garantir a proteção de direitos fundamentais, como o direito à privacidade, a autodeterminação informativa e a proteção contra o tratamento abusivo de dados pessoais[15].

Diante do exposto, frise-se o seguinte:

A questão da videovigilância no local de trabalho envolve o confronto entre dois grupos de direitos fundamentais. Por um lado, os direitos dos trabalhadores à privacidade (artigo 26.º), à dignidade (artigo 1.º) e à proteção contra a discriminação (artigo 13.º) são essenciais para garantir um ambiente de trabalho respeitoso e justo. Estes direitos garantem que os trabalhadores não estão sujeitos a vigilância abusiva, constrangimento ou exposição indevida, preservando a sua esfera íntima e a igualdade de tratamento[16].

Por outro lado, os empregadores têm o legítimo direito à propriedade (artigo 62.º) e à liberdade de iniciativa económica (artigo 61.º), que incluem a proteção do património e o cumprimento das obrigações contratuais no local de trabalho. Estes direitos permitem a adoção de medidas de segurança e controlo, como a videovigilância, para evitar fraudes, roubos e outros comportamentos ilícitos. No entanto, o exercício destes direitos deve ser cuidadosamente

[13] *Idem.*
[14] BARRETO, A. M. *A Proteção de Dados no Ambiente de Trabalho:* Videovigilância e Privacidade. Coimbra: Almedina, 2019.
[15] OLIVEIRA, A. S. P. *Direitos Fundamentais e o RGPD:* Proteção de Dados na Era Digital. Coimbra: Almedina, 2020.
[16] BARRETO, A. M. *A Proteção de Dados no Ambiente de Trabalho:* Videovigilância e Privacidade. Coimbra: Almedina, 2019.

ponderado para evitar violações dos direitos fundamentais dos trabalhadores, observando sempre os princípios da proporcionalidade e da necessidade[17].

Ainda, a implementação da videovigilância no local de trabalho é uma questão complexa que se cruza com vários tratados internacionais de que Portugal é parte. Estes instrumentos também auxiliam na consecução do equilíbrio entre o interesse do empregador na segurança e na proteção da propriedade com os direitos fundamentais dos trabalhadores à privacidade e à proteção de dados. Os tratados internacionais mencionados a diante abrangem disposições específicas de pertinência relevante para a regulamentação da videovigilância no local de trabalho.

Adotada pela Assembleia Geral das Nações Unidas em 1948, a Declaração Universal dos Direitos Humanos (DUDH) descreve os direitos fundamentais do homem que devem ser protegidos universalmente. O artigo 12.º da DUDH refere que ninguém será sujeito a interferências arbitrárias na sua privacidade, família, lar ou correspondência, nem a ataques à sua honra e reputação, e todos têm direito a protecção legal contra tais interferências ou ataques[18].

Esta disposição sublinha a importância da privacidade como um direito humano fundamental. No local de trabalho, isto traduz-se na expetativa de que o espaço pessoal e as comunicações dos funcionários sejam respeitados. A utilização da videovigilância deve, por conseguinte, ser cuidadosamente ponderada para evitar interferências arbitrárias na privacidade dos trabalhadores[19].

A Organização Internacional do Trabalho (OIT) desenvolveu convenções com o objetivo de promover condições de trabalho justas e decentes. Embora nenhuma convenção específica trate da vigilância por vídeo, várias são pertinentes à privacidade e à proteção dos trabalhadores.

Nestes termos, listam-se algumas, como a Convenção nº 87 sobre Liberdade de Associação e Proteção do Direito de Organização (1948) garante aos trabalhadores e empregadores o direito de formar e aderir a organizações da sua escolha, sem autorização prévia e sem distinções. Estas organizações têm autonomia para redigir os seus estatutos, eleger representantes, gerir as suas actividades e formular programas de ação sem interferência ou

[17] *Idem.*
[18] RAUHOFER, Judith; CLARKE, Roger. *Privacidade e Direitos Humanos na Era Digital*. Porto Alegre: Editora Juruá, 2019.
[19] *Idem.*

restrições impostas pelo Estado. Além disso, a convenção proíbe a dissolução ou suspensão administrativa dessas organizações e assegura seu direito de formar federações e confederações, bem como de se filiar a organizações internacionais. Estabelece ainda que a legislação nacional não pode restringir ou prejudicar as garantias previstas, assegurando assim uma proteção eficaz da liberdade de associação e do direito de organização[20].

A Convenção n.º 98 sobre o Direito de Organização e de Negociação Colectiva (1949): A convenção proíbe a discriminação de trabalhadores por serem membros de sindicatos ou participarem em actividades sindicais. Garante que o emprego não pode ser condicionado à ausência de filiação sindical ou à renúncia à mesma, nem os trabalhadores podem ser despedidos ou prejudicados pelo seu envolvimento sindical. Também protege as organizações de trabalhadores e de empregadores de interferências mútuas, proibindo acções destinadas a controlar ou dominar essas organizações. Além disso, a convenção exige o estabelecimento de mecanismos para encorajar e promover negociações voluntárias entre empregadores e organizações de trabalhadores para regular as condições de emprego através de acordos coletivos[21].

A Convenção n.º 155 sobre Segurança e Saúde no Trabalho (1981) exige que os Estados-Membros estabeleçam, implementem e revejam políticas nacionais para prevenir acidentes de trabalho e perigos para a saúde, abordando os riscos na sua origem. A convenção dá ênfase à adaptação dos processos de trabalho, à garantia de equipamento adequado e à formação para proteger a segurança e a saúde dos trabalhadores[22].

Enquanto Estado-Membro da UE, Portugal está sujeito ao Regulamento Geral de Proteção de Dados (RGPD), que estabelece requisitos rigorosos para o tratamento de dados pessoais, incluindo os recolhidos através da videovigilância no local de trabalho. Os princípios-chave incluem a legalidade, a justiça e a transparência, exigindo que os dados sejam processados de forma legal, ética e aberta, com os empregadores a informar os funcionários sobre a existência e a finalidade dos sistemas de vigilância. A limitação da finalidade exige que os dados sejam recolhidos para fins específicos, explícitos e legítimos, proibindo o

[20] ORGANIZAÇÃO INTERNACIONAL DO TRABALHO (OIT). *Convenção nº 87, sobre Liberdade de Associação e Proteção do Direito de Organização, 1948*. Disponível em: https://www.ilo.org. Acesso em: 8 de dezembro de 2024.
[21] ORGANIZAÇÃO INTERNACIONAL DO TRABALHO (OIT). *Convenção nº 98, sobre o Direito de Organização e de Negociação Coletiva, 1949*. Disponível em: https://www.ilo.org. Acesso em: 8 de dezembro de 2024.
[22] ORGANIZAÇÃO INTERNACIONAL DO TRABALHO (OIT). *Convenção nº 155, sobre Segurança e Saúde no Trabalho*. Disponível em: https://www.ilo.org. Acesso em: 8 de dezembro de 2024.

processamento posterior incompatível com esses fins. A minimização dos dados exige que apenas sejam recolhidos dados adequados, relevantes e limitados ao necessário. A limitação do armazenamento determina que os dados pessoais sejam mantidos numa forma que permita a identificação dos titulares dos dados apenas durante o tempo necessário para os fins para os quais os dados são processados[23].

Estas convenções sublinham a necessidade de equilibrar a segurança no local de trabalho com a proteção dos direitos dos trabalhadores à privacidade e à liberdade de vigilância indevida.

Dessa forma, o uso de videovigilância no ambiente de trabalho exige a observação rigorosa das disposições constitucionais e legais aplicáveis. O respeito pela privacidade e dignidade dos trabalhadores deve estar no centro das decisões relacionadas a essa prática, equilibrando os interesses empresariais com os direitos fundamentais assegurados pela Constituição.

[23] WRIGHT, David; DE HERT, Paul. *Understanding the General Data Protection Regulation (GDPR).* Cham: Springer, 2019.

2. REGULAMENTAÇÃO GERAL DA PROTEÇÃO DE DADOS E A VIDEOVIGILÂNCIA NO AMBIENTE DE TRABALHO

A proteção de dados pessoais aplica-se a todas as nossas interações com organizações do setor público e privado e, portanto, aplica-se a aplicações, compras e transações em serviços do Estado, assuntos comerciais e econômicos, nas áreas social e médica, no local de trabalho e na arena tecnológica globalizada[24]. Um Regulamento Geral de Proteção de Dados Pessoais (RGPD) consolida regras firmes de proteção de dados, criando um cenário de segurança jurídica que beneficia setores econômicos e sociais e modernizando aspectos legislativos para que os direitos fundamentais continuem protegidos diante dos avanços técnico científicos.

Neste ponto, serão consignados alguns marcos legislativos importantes acerca da proteção de dados no âmbito da União Europeia.

No que concerne à proteção de dados a pessoas singulares, especificamente com relação ao tratamento e circulação de dados pessoais, instituiu-se no âmbito da União Europeia o Regulamento do Parlamento Europeu e do Conselho (UE) n. 2016/679, de 27 de abril de 2016, popularmente conhecido como RGPD.

O RGPD é resultado de incursões normativas importantes verificadas desde a segunda metade do século XX, mesmo que, de início, a ênfase estivesse na concepção mais genérica de proteção, qual seja a proteção à vida privada.

Nesse caminhar, a Convenção Europeia dos Direitos Humanos e das Liberdades Fundamentais (CEDH), de 4 de novembro de 1950, estabelece, no art. 8º, o direito de qualquer pessoa ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.

Na década de 80, segundo A. Barreto Menezes Cordeiro[25], a Europa começou a materializar de forma mais precisa a questão relativa à proteção de dados. O autor cita como exemplos mais marcantes desse fato o *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, elaborado pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE) e a Convenção 108 do Conselho Europeu para a Proteção das Pessoas Singulares.

[24] MARTINEZ, Pedro Romano. *Direito do Trabalho.* 11.ª ed. Coimbra: Almedina, 2023.
[25] CORDEIRO, A. Barreto Menezes. *Direito da Proteção de Dados – À luz do RGPD e da Lei n.º 58/2019*. Coimbra: Almedina, 2020, p. 66 e ss.

Por conseguinte, há que se falar que a Convenção 108 do Conselho Europeu para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, de 28 de janeiro de 1981, foi o primeiro documento internacional de cunho normativo a ser instituído para regular a proteção de dados.

Em continuidade, a Carta dos Direitos Fundamentais da União Europeia consagrou, nos arts. 7º e 8º, o direito à privacidade e a proteção dos dados pessoais[26].

Em 24 de outubro de 1995, entrou em vigor a Diretiva nº 95/46/CE, que foi resultado da compilação das propostas de duas diretivas, regulando a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Foi esta diretiva que foi aplicada até a entrada em vigor do Regulamento nº 2016/679, de 27 de abril de 2016.

A partir do atual regulamento (2016/679), surgiram outros que visavam reforçar a proteção de dados sob alguns outros aspectos. Exemplo disso é a Diretiva (EU) 2016/680, de 27 de abril, que regula a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados[27].

Além de medidas legislativas, observa-se a adoção de medidas organizacionais, como a criação da Autoridade Europeia para a Proteção de Dados (AEPD) e do Comitê Europeu para a Proteção de Dados.

A AEPD é entidade autônoma que possui uma função essencialmente fiscalizatória e que busca promover a efetividade das medidas relativas à proteção de dados no âmbito das instituições e órgãos da União Europeia.

Já o Comitê Europeu para a Proteção de Dados é um órgão consultivo e deliberativo, de forma que atua como órgão competente para decidir nos conflitos entre as autoridades de

[26]Artigo 7º. Respeito pela vida privada e familiar. Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações. Acerca da proteção dos dados pessoais, o art. 8º dispõe: Artigo 8º. Proteção de dados pessoais 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

[27] TIKKINEN-PIRI, C.; ROHUNEN, A.; MARKKULA, J. *EU general data protection regulation: Changes and implications for personal data collecting companies*. *Computer Law & Security Review*, v. 34, p. 134-153, fev. 2018.

controle nacionais e define diretrizes para a adequada aplicação do RGPD. É composto pelo diretor de uma autoridade de controle de cada Estado-Membro e da Autoridade Europeia para a Proteção de Dados, ou pelos respetivos representantes.

Infere-se que o RGPD é fruto dos avanços técnico-científicos observados da segunda metade do século XX em diante, especialmente na área da tecnologia da informação, onde os dados circulam de uma forma rápida e, por vezes, massificada. A harmonização resultante na lei torna mais fácil para os cidadãos da UE entenderem como seus dados estão sendo usados e como eles podem fazer reclamações, mesmo que não estejam localizados em um país membro da UE. O RGPD não se aplica somente a dados relacionados à tecnologia de informação; ele tem implicações abrangentes para toda a empresa, como o manuseio de dados de vendas, marketing e recursos humanos. O RGPD é, na verdade, um instrumento de garantia do direito à privacidade e à liberdade no contexto descrito.

Tal argumento pode ser corroborado por meio da leitura dos arts. 1° e 2° do RGPD, que dispõem acerca do objetivo e do âmbito de aplicação, respectivamente.

O artigo 1.º do RGPD estabelece o objeto e os objetivos principais do regulamento. O artigo visa proteger os direitos e liberdades fundamentais das pessoas singulares, em particular o seu direito à proteção dos dados pessoais. Salienta a necessidade de regulamentar o tratamento de dados pessoais para garantir um elevado nível de proteção na UE. O âmbito de aplicação do artigo 1.º vai além da mera proteção de dados; incorpora o compromisso da UE de defender a privacidade como um direito humano fundamental, alinhando-se assim com os valores mais amplos articulados na Carta dos Direitos Fundamentais da UE[28].

Os objetivos delineados no artigo 1.º refletem a posição proativa da UE em matéria de proteção de dados, contrastando com abordagens mais reativas ou fragmentadas observadas noutras jurisdições. Ao estabelecer uma estrutura legal harmonizada, o GDPR busca resolver as discrepâncias nas leis de proteção de dados entre os estados membros, promovendo assim uma abordagem de mercado único. Essa harmonização é fundamental não apenas para proteger os dados pessoais, mas também para garantir a segurança jurídica das empresas e aumentar a confiança nos serviços digitais, que são cruciais para o crescimento econômico na UE.

[28] Artigo 1.° Objeto e objetivos 1. O presente regulamento estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. 2. O presente regulamento defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais. 3. A livre circulação de dados pessoais no interior da União não é restringida nem proibida por motivos relacionados com a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais.

O artigo 2.º define o âmbito de aplicação material do RGPD, especificando os tipos de atividades de tratamento de dados que se enquadram no âmbito das suas competências. Aplica-se ao tratamento de dados pessoais, total ou parcialmente, por meios automatizados, e ao tratamento de dados pessoais que façam parte de um ficheiro ou se destinem a fazer parte de um ficheiro. Essa definição ampla garante que praticamente todas as formas de tratamento de dados, sejam digitais ou manuais, estejam sujeitas às disposições do RGPD, desde que envolvam dados pessoais[29].

No art. 3°, observa-se uma aplicação baseada na extraterritorialidade. Isso porque abre a possibilidade de o RGPD ser aplicado independentemente de o tratamento ocorrer dentro ou fora da União.

Dessa forma, permite que o tratamento de dados pessoais de titulares residentes no território da União seja efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União – desde que se trate de oferta de bens ou serviços aos titulares de dados da União ou do controle comportamental no âmbito da UE.

Ainda, é aplicável em regiões submetidas ao ordenamento jurídico de um Estado-membro em decorrência da vinculação a normas de Direito Internacional Público.

Mais relacionado com o tema desta pesquisa, os limites do controle de um funcionário por meio do monitoramento por vídeo são determinados principalmente pelos princípios mencionados no Artigo 5(1) do RGPD.

Inicialmente, é importante determinar a finalidade da introdução da vigilância por vídeo e o período de retenção de dados. O Artigo 5(1) do RGPD indica que os dados pessoais podem

[29] Artigo 2. ° Âmbito de aplicação material 1. O presente regulamento aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados. 2. O presente regulamento não se aplica ao tratamento de dados pessoais: a) Efetuado no exercício de atividades não sujeitas à aplicação do direito da União: b) Efetuado pelos Estados-Membros no exercício de atividades abrangidas pelo âmbito de aplicação do título V, capítulo 2, do TUE; c) Efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas; d) Efetuado pelas autoridades competentes para efeitos de prevenção, investigação, detecção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública. 3. O Regulamento (CE) n.º 45/2001 aplica-se ao tratamento de dados pessoais pelas instituições, órgãos, organismos ou agências da União. O Regulamento (CE) n.º 45/2001, bem como outros atos jurídicos da União aplicáveis ao tratamento de dados pessoais, são adaptados aos princípios e regras do presente regulamento nos termos previstos no artigo 98.°. 4. O presente regulamento não prejudica a aplicação da Diretiva 2000/31/CE, nomeadamente as normas em matéria de responsabilidade dos prestadores intermediários de serviços previstas nos seus artigos 12.° a 15.°.

ser coletados para fins específicos, explícitos e legítimos[30]. Em princípio, os dados não podem ser processados se isso for incompatível com essas finalidades.

Além disso, os dados de identificação pessoal não podem ser mantidos por mais tempo do que o necessário para as finalidades para as quais os dados são processados. Os dados pessoais também devem ser corretos e atualizados conforme necessário, enquanto aqueles que estiverem incorretos em relação às finalidades para as quais são processados devem ser excluídos ou retificados sem demora.

Um dos limites é a necessidade de definir as bases para a permissibilidade do processamento de dados pessoais em conexão com a vigilância por vídeo. As bases legais para o processamento dos chamados dados pessoais "comuns" estão listadas no Artigo 6º do RGPD. O controlador deve fazer sua própria avaliação do que é uma base apropriada e legal para o processamento planejado em uma determinada situação.

Assim, importa mencionar os fundamentos sobre os quais o tratamento de dados deve ser estabelecido para que seja considerado lícito, sendo eles, o consentimento do titular dos dados; a imprescindibilidade do tratamento para: a execução de um contrato; para o cumprimento de obrigações jurídicas; na defesa de interesses substanciais do titular dos dados ou de terceiros; para garantir o exercício das funções de interesse público ou da autoridade pública; e para assegurar os efeitos dos interesses perseguidos pelo responsável pelo tratamento ou por terceiro (art. 6°)[31].

---

[30] [---] Os dados pessoais são: 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»);

[31] Art. 6º. 1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações: a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas; b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados; c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular; e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento; f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança. O primeiro parágrafo, alínea f), não se aplica ao tratamento de dados efetuado por autoridades públicas na prossecução das suas atribuições por via eletrónica. 2. Os Estados-Membros podem manter ou aprovar disposições mais específicas com o objetivo de adaptar a aplicação das regras do presente regulamento no que diz respeito ao tratamento de dados para o cumprimento do n.º 1, alíneas c) e e), determinando, de forma mais precisa, requisitos específicos para o tratamento e outras medidas destinadas a garantir a licitude e lealdade do tratamento, inclusive para outras situações específicas de tratamento em conformidade com o capítulo IX. 3. O fundamento jurídico para o tratamento referido no n.º 1, alíneas c) e e), é definido: a) Pelo direito da União; ou b) Pelo direito do Estado-

No caso da vigilância por vídeo, dois pré-requisitos para o processamento legal de dados são mais comumente usados. Primeiro, de acordo com o Artigo 6(1) do GDPR, o processamento deve ser necessário para cumprir uma obrigação legal do controlador. Geralmente, esse é o caso quando uma disposição legal impõe explicitamente a uma entidade a obrigação de usar o monitoramento por vídeo, ou quando uma disposição legal impõe uma obrigação para cujo cumprimento o uso do monitoramento é necessário. Em segundo lugar, a lógica também pode ser a chamada cláusula de interesse legítimo. De acordo com essa disposição, o processamento de dados pessoais é permitido se for necessário para fins de interesses legítimos do controlador (ou de um terceiro), exceto quando esses interesses forem sobrepostos pelos direitos e liberdades fundamentais do titular dos dados, que exigem a proteção dos dados pessoais.

Potencialmente, em algumas situações, o Artigo 9 do RGPD, que proíbe o processamento de categorias especiais de dados (os chamados dados sensíveis), também pode desempenhar um papel importante na aquisição de dados relacionados à vigilância por vídeo de funcionários. Entre os dados especiais, essa disposição lista os dados biométricos processados para identificar um indivíduo de forma exclusiva[32].

Conforme definido no Artigo 4(14) do RGPD, dados biométricos significam: "dados pessoais que resultam de processamento técnico especial, dizem respeito a características

Membro ao qual o responsável pelo tratamento está sujeito. A finalidade do tratamento é determinada com esse fundamento jurídico ou, no que respeita ao tratamento referido no n.º 1, alínea e), deve ser necessária ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento. Esse fundamento jurídico pode prever disposições específicas para adaptar a aplicação das regras do presente regulamento, nomeadamente: as condições gerais de licitude do tratamento pelo responsável pelo seu tratamento; os tipos de dados objeto de tratamento; os titulares dos dados em questão; as entidades a que os dados pessoais poderão ser comunicados e para que efeitos; os limites a que as finalidades do tratamento devem obedecer; os prazos de conservação; e as operações e procedimentos de tratamento, incluindo as medidas destinadas a garantir a legalidade e lealdade do tratamento, como as medidas relativas a outras situações específicas de tratamento em conformidade com o capítulo IX. O direito da União ou do Estado-Membro deve responder a um objetivo de interesse público e ser proporcional ao objetivo legítimo prosseguido. 4. Quando o tratamento para fins que não sejam aqueles para os quais os dados pessoais foram recolhidos não for realizado com base no consentimento do titular dos dados ou em disposições do direito da União ou dos Estados-Membros que constituam uma medida necessária e proporcionada numa sociedade democrática para salvaguardar os objetivos referidos no artigo 23.º, n.º 1, o responsável pelo tratamento, a fim de verificar se o tratamento para outros fins é compatível com a finalidade para a qual os dados pessoais foram inicialmente recolhidos, tem nomeadamente em conta: a) Qualquer ligação entre a finalidade para a qual os dados pessoais foram recolhidos e a finalidade do tratamento posterior; b) O contexto em que os dados pessoais foram recolhidos, em particular no que respeita à relação entre os titulares dos dados e o responsável pelo seu tratamento; c) A natureza dos dados pessoais, em especial se as categorias especiais de dados pessoais forem tratadas nos termos do artigo 9.º, ou se os dados pessoais relacionados com condenações penais e infrações forem tratados nos termos do artigo 10.º; d) As eventuais consequências do tratamento posterior pretendido para os titulares dos dados; e) A existência de salvaguardas adequadas, que podem ser a cifragem ou a pseudonimização.

[32] Art. 9. 1. É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.

físicas, fisiológicas ou comportamentais de uma pessoa física e permitem ou confirmam a identificação inequívoca dessa pessoa, como imagem facial ou dados dactiloscópicos".

De acordo com o Considerando 51 do preâmbulo, o tratamento de fotografias nem sempre constitui o tratamento de categorias especiais de dados pessoais. As fotografias são consideradas dados biométricos apenas quando são processadas através de métodos técnicos específicos que permitem a identificação ou confirmação inequívoca da identidade de um indivíduo[33].

Tal situação ocorre quando o administrador utiliza tecnologias especiais na forma de vários tipos de algoritmos e mecanismos de análise automática de imagens para atribuir imagens faciais a indivíduos específicos (independentemente das finalidades para as quais essa identificação é realizada). Em contrapartida, o caso acima não ocorre quando as gravações são utilizadas quando ocorrem eventos específicos e são analisadas somente na situação de sua ocorrência e na extensão apropriada.

Deve-se presumir que, como regra, o empregador não pode instalar sistemas de monitoramento que utilizem tecnologias que permitam a identificação das pessoas observadas. Somente em situações completamente excepcionais o processamento de dados biométricos poderia encontrar justificativa no Artigo 9(2) do RGPD, que lista os fundamentos para a permissibilidade da coleta dos dados mencionados acima.

O empregador também tem obrigações de informação relacionadas à introdução do monitoramento. O artigo 13 do RGPD impõe obrigações de informação relacionadas à coleta de dados pessoais diretamente do titular dos dados. Isso é feito, por exemplo, pela própria presença da pessoa na área de monitoramento. As informações relevantes devem ser fornecidas não apenas aos funcionários, mas também a quaisquer terceiros que possam estar dentro da área de monitoramento. Tanto para os funcionários contratados na época da introdução do monitoramento quanto para os contratados após essa data, as informações devem ser de natureza anterior. Isso é importante em termos de avaliação da expectativa legítima de privacidade de um funcionário.

[33] Considerando 51: "o processamento de fotografias nem sempre deve constituir o processamento de categorias especiais de dados pessoais, uma vez que as fotografias se enquadram na definição de dados biométricos somente nos casos em que são processadas por métodos técnicos especiais que permitem a identificação inequívoca de um indivíduo ou confirmam sua identidade."

Não é equivocado dizer que o consentimento é um dos principais pilares do RGPD, ainda mais se for levado em conta que o considerando 32 explana que o consentimento do titular dos dados deve ser consubstanciado por um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito.

3. DIREITO INTERNO PORTUGUÊS

3.1. A Lei nº 67/98 de 26 de outubro

A Constituição da República Portuguesa foi revisada diante da Diretiva nº 95/46/CE, mais especificamente no tocante ao art. 35°, que passou a ter a seguinte redação:

> **Artigo 35.º**
> **(Utilização da informática)**
>
> 1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.

Na antiga redação, o referido dispositivo dispunha o seguinte:

> **Artigo 35.º**
> **(Utilização da informática)**
>
> 1. Todos os cidadãos têm o direito de tomar conhecimento de dados constantes de ficheiros ou registros informáticos a seu respeito e do fim a que se destinam, podendo exigir sua retificação e atualização, sem prejuízo do disposto na lei sobre segredo do Estado e segredo de justiça.

A alteração em comento se deu em virtude da necessidade de conformar a legislação portuguesa com os parâmetros definidos pela União Europeia em matéria de proteção de dados, mais precisamente quanto ao alinhamento do direito interno com o estabelecido na Diretiva nº 95/46/CE, haja vista que a privacidade e a proteção de dados dos cidadãos deveriam estar balizadas não somente nas diretrizes internas, mas também naquilo que dispõe o Direito Comunitário.

Por conseguinte, ainda nesse movimento de adaptar o Direito Interno Português ao asseverado pelas normas do Direito Comunitário, especialmente pela Diretiva nº 95/46/CE, promulgou-se a Lei nº 67, de 26 de outubro de 1998, reconhecida como a Lei Geral de Proteção de Dados. Por meio dela, passaram a ser acobertados tanto os dados pessoais automatizados, quanto os não automatizados.

No que respeita à aplicação da Lei n.º 67/98, foram levantadas preocupações sobre uma disposição específica, nomeadamente o artigo 4.º, que estabelece o âmbito de aplicação. De acordo com o n.º 2, a lei não se aplica ao tratamento de dados pessoais realizado por um indivíduo no âmbito de atividades exclusivamente pessoais ou domésticas[34].

[34] Lei nº 67/98:
"Art. 4.º
Âmbito de aplicação
[...]
2 - A presente lei não se aplica ao tratamento de dados pessoais efectuado por pessoa singular no exercício de actividades exclusivamente pessoais ou domésticas."

Acerca da aplicação da Lei nº 67/98, exsurgiu preocupação quanto ao seguinte dispositivo:

A expressão 'exclusivamente' soou inconclusiva para alguns juristas, especialmente quando se desejava definir com exatidão as restrições impostas pela lei. Havia, no entendimento de Alexandre Sousa Pinheiro[35], uma espécie de ambiguidade que colocou em risco a aplicação adequada e consistente da legislação.

Tal risco era observado quando da possível ausência de proteção em decorrência de lacuna legislativa em situações nas quais o tratamento de dados deveria ocorrer, mas não ocorria, porque havia de se cumprir estritamente o disposto na norma retromencionada. Tais situações podem ser de cunho comercial, profissional ou governamental.

Em outras palavras, a adoção do termo "exclusivamente" poderia ensejar dúvidas quanto a aplicação da lei em conjunturas nas quais as atividades não eram exclusivamente pessoais ou domésticas, mas ocorriam em um contexto pessoal ou doméstico.

O importante é deixar claro que mesmo nas conjunturas onde as atividades não são exclusivamente pessoais ou domésticas, mas realizadas em um contexto pessoal ou doméstico, existe o dever de observar os princípios e regras que norteiam a proteção de dados.

Ainda, há que se conferir a devida atenção para dados que são tratados para finalidades distintas daquelas incialmente previstas, situações nas quais o consentimento do titular dos dados é imprescindível, urgindo-se a atribuição de garantias adicionais de proteção e segurança no processamento e possível transmissão.

Não é equivocada a ideia de que o ponto de partida da análise acerca do âmbito de aplicação do RGPD é a finalidade para a qual os dados foram coletados. Ora, a partir do momento que a finalidade da coleta de dados extrapola os limites legalmente fixados (na ocasião da Lei nº 67/98, atividades exclusivamente domésticas ou pessoais), há que se ter em mente que a proteção será necessária. A privacidade no local de trabalho tornou-se uma questão no radar das autoridades nacionais de proteção de dados. Várias delas emitiram recomendações aos empregadores sobre a coleta de dados sobre forças de trabalho remotas.

É nesse ponto que convém destacar a necessidade de adaptação da legislação a realidade social que emerge a partir dos avanços tecnológicos, em um movimento de busca por

[35] PINHEIRO, Alexandre de Sousa. *Privacy e Proteção de dados pessoais:* a construção dogmática do Direito à identidade informacional. Lisboa: Associação Académica da Faculdade de Direito de Lisboa, 2015.

modernização da lei e, em consequência, pelo estabelecimento de diretrizes mais coerentes com as demandas factuais.

3.2. A Nova Lei de Execução Nacional – Lei nº 58/2019, de 8 de agosto

A partir da Lei nº 58, de 9 de agosto de 2019, implementaram-se algumas alterações, dentre as quais destaco as que discorro neste tópico.

Consolidou-se de forma mais robusta o estatuto jurídico da Comissão Nacional de Proteção de Dados (CNPD), de maneira que houve o reconhecimento do referido órgão como autoridade nacional de controle dos efeitos da RGPD, com a ampliação de suas funções, outrora limitadas ao que previa o art. 57.º da Diretiva 679/2016. É inegável que providências como essa demonstram a preocupação com a eficácia e o âmbito de aplicação da proteção de dados.

Um ponto importante acerca da Lei nº 58/2019 foi a atribuição de uma postura proativa para a CNPD, na medida em que sua atuação gere resultados mais eficientes no que tange a defesa da privacidade e dos direitos dos cidadãos em relação aos seus dados pessoais. Tal mudança de postura visa conformar os órgãos de controle aos avanços tecnológicos e, consequentemente, às novas questões que surgem na seara do tratamento de dados.

Há que se destacar a relevância que foi conferida aos Tribunais Administrativos, que passam a ser encarregados de deliberar acerca de todas as ações legais propostas contra a CNPD, de modo que as resoluções acerca dos conflitos existentes em torno da autoridade de controle sejam proferidas de modo mais uniforme e especializado (*vide* art. 34.º da Lei nº 58/2019), o que é extremamente favorável à promoção da segurança jurídica em matéria de proteção de dados[36].

O foco na definição das funções do chamado Encarregado de Proteção de Dados foi imprescindível para a atuação das entidades privadas e públicas.

Acerca das entidades privadas, o Encarregado de Proteção de Dados deve atuar quando a atividade principal da entidade privada abranger operações de tratamento de dados que demandam controle regular e sistemático dos dados em grande escala; operações de tratamento de dados em grande escala tidos como de categorias especiais; e operações de tratamento de dados relacionados com condenações penais e contraordenacionais (*vide* art. 13.º da Lei nº 58/2019).

[36] MARTINEZ, Pedro Romano. *Direito do Trabalho.* 11.ª ed. Coimbra: Almedina, 2023.

No âmbito de organizações públicas, o tratamento de dados pessoais é realizado com base na demonstração de que o mesmo é imprescindível para a prossecução do interesse público, com a formalização de um protocolo que defina claramente as responsabilidades de cada entidade envolvida, tanto no momento da transferência dos dados, quanto em outros tratamentos que, porventura, venham a ser necessários. Referido protocolo é de suma relevância quando se está diante da transferência de dados pessoais entre entidades públicas, o que garante transparência, responsabilização e devido cumprimento das normas de proteção de dados em todas as fases do processo (*vide* art. 23.º da Lei nº 58/2019).

Outro aspecto a se registrar é quanto ao prazo de conservação dos dados pessoais. Referido prazo está sujeito às disposições estabelecidas por normas legais ou regulamentares. Caso não haja normatização ou regulamentação nesse sentido, o prazo de conservação deve ser determinado de acordo com a necessidade para a continuidade das atividades das quais os dados são provenientes (*vide* art. 21.º da Lei nº 58/2019). O cumprimento do prazo é indispensável por parte do responsável pelo tratamento dos dados, de forma que, findo o prazo, os dados sejam destruídos ou anonimizados.

O prazo em causa tem por base o artigo 8.º(2) da Convenção Europeia dos Direitos do Homem (CEDH), que estabelece que as autoridades públicas só podem interferir no exercício do direito ao respeito pela vida privada e familiar quando tal interferência seja prescrita por lei e constitui uma medida necessária numa sociedade democrática por razões como a segurança nacional, a segurança pública, o bem-estar económico do país, a prevenção da desordem ou do crime, a protecção da saúde ou da moral, ou a protecção dos direitos e liberdades dos outros[37].

Tanto é assim que no caso Gaughran contra Reino Unido, onde se discutiu o limite da conservação de dados referentes a um cidadão inglês que foi flagrado dirigindo sob efeito de álcool na Irlanda diante da determinação de prazo indefinido para a conservação das evidências coletadas, suscitou-se violação direta ao art. 8º, 2, da CEDH.

[37] CEDH:
Art. 8.º
(Direito ao respeito pela vida privada e familiar)
[...]
2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros.

O prazo de conservação de dados tem natureza de cláusula aberta no ordenamento jurídico interno de cada Estado-Membro. Assim, as autoridades competentes encarregadas de decidir sobre o tratamento de dados pessoais têm a liberdade de estabelecer prazos de conservação adequados e devem garantir o cumprimento rigoroso da destruição dos dados quando o tratamento encerrar.

Essa abordagem flexível permite que cada Estado adapte suas políticas de conservação de dados a necessidades específicas, considerando fatores como segurança nacional, proteção da ordem pública, prevenção de crimes e proteção dos direitos individuais. Ao manter a cláusula aberta, as autoridades podem ajustar os prazos de conservação conforme necessário, em resposta a mudanças na conjuntura tecnológica.

Além disso, por meio da flexibilidade quanto a definição dos prazos de conservação dos dados, de acordo com cada situação, pelos Estados-Membros, é possível a criação de um cenário propício à atualização periódica das políticas de conservação de dados, o que é imprescindível diante das mudanças constantes do cenário digital, que, caso não consideradas devidamente, podem representar ameaças à privacidade e à segurança de dados.

Uma exceção ao estabelecimento de um prazo de conservação de dados é a que consta no art. 21.º, nº 6, da Lei nº 58/2019. O disposto trata da hipótese de processos de aposentadoria ou reforma, especificamente relacionados à declaração contributiva pra a segurança social. A exceção em tela tem a finalidade de facilitar a reconstituição das carreiras contributivas dos titulares dos dados, sob a condição de que sejam implementadas medidas técnicas e organizacionais apropriadas para garantir a segurança e a integridade desses dados.

O art. 28.º da Lei nº 58/2019 trata de disposições acerca de proteção de dados pessoais nas relações laborais. Do dispositivo em comento, importa destacar a regulamentação relativa ao consentimento do trabalhador. Referido consentimento não é necessário se o tratamento dos dados resultar em vantagem jurídica ou econômica para o próprio trabalhador, o que visa afastar a concessão ou não concessão de consentimento baseadas em qualquer tipo de coerção[38].

No tocante aos sistemas de videovigilância, a utilização de imagens captadas à distância em processos disciplinares é possível desde que tenham sido previamente utilizadas em processos penais. A captação de som por parte de câmeras de videovigilância é proibida, com exceção do período em que as instalações vigiadas estão encerradas ou mediante autorização

[38] MARTINEZ, Pedro Romano. *Direito do Trabalho.* 11.ª ed. Coimbra: Almedina, 2023.

prévia da CNPD. O que resta claro é que a tendência é que o uso de tecnologias de vigilância, dentre elas a videovigilância, seja rigorosamente controlado e justificado.

Em continuidade, o tratamento de dados biométricos só é permitido para controlar a assiduidade do empregado e o acesso às instalações, ainda sendo necessária a implementação de medidas adequadas de segurança e proteção de dados para esse caso.

As mudanças aqui elencadas reforçam o cumprimento do dever de observar os princípios fundamentais do Direito de Proteção de Dados, que detalharei mais adiante e que são, em breve síntese, as bases éticas do processamento de informações pessoais.

Tais alterações podem ser vistas como uma demonstração do compromisso do Estado Português de proteger veementemente a privacidade e os direitos individuais dos cidadãos em um contexto onde a digitalização e a conectividade informacional comandam as relações interpessoais.

No entanto, a Lei nº 58/2019 não foi bem recepcionada de forma unânime. E um dos pontos de maior discordância reside no tratamento de dados no âmbito das relações laborais, especificamente quanto a questão da videovigilância.

3.3. Críticas à Nova Lei de Execução – Deliberações da CNPD

A CNPD atuou de modo bastante relevante por meio da emissão de comentários inscritos no Parecer nº 20/201849, de 2 de maio de 2018, à Proposta de Lei de Execução 120/XIII.

No referido parecer, a CNPD fez críticas ao projeto baseada em uma análise minuciosa do mesmo e forneceu ideias significativas a respeito da melhoria da conformidade da lei com os princípios e normas de proteção de dados em prol da máxima eficácia possível, de forma que identificou algumas searas normativas que necessitavam de aprimoramento para proteger adequadamente os direitos de privacidade relativos aos dados pessoais dos cidadãos.

Os apontamentos da CNPD contribuíram para o aperfeiçoamento do texto da proposta de lei, com vistas à consolidação de um arcabouço normativo confluente com os princípios da transparência, da segurança e da responsabilização.

O primeiro destaque ao parecer em questão foi o apontamento suscitado pela CNPD ao art. 2° da lei, que dispõe acerca do âmbito de aplicação. A preocupação do órgão residia no fato de que o preceito inscrito no dispositivo mencionado pudesse estar em conflito com o

RGPD, mais especificamente no que diz respeito à inobservância do princípio do "balcão único".

Em síntese, o princípio do "balcão único" visa simplificar e facilitar o processo de conformidade com as leis de proteção de dados para empresas que operam em diferentes países da União Europeia.

Há quem discorde da crítica ora em comento, como é o caso de António Barreto Menezes Cordeiro[39], que argumenta que o princípio do "balcão único" é direcionado somente às autoridades de controle, conforme preconiza o art. 56.º da Diretiva 2016/679. Ainda, sugere que não há na diretiva de proteção de dados uma norma que determine qual será a lei aplicável nos casos em que há mais de um estabelecimento dentro da União Europeia, o que acaba configurando uma lacuna normativa.

Desta feita, o ponto de crítica da CNPD é a violação ao princípio do "balcão único", na medida em que António Barreto Menezes Cordeiro[40] rebate tal crítica com base no argumento de que a Diretiva 2016/679 não delineou de forma precisa como que a legislação acerca da proteção de dados será aplicada nos casos de múltiplos estabelecimentos, deixando indefinido o princípio do balcão único.

Após a Lei nº 58/2019 ter entrado em vigor, a CNPD decidiu, por meio da Deliberação 2019/494, de 3 de setembro, que tanto os tribunais, quanto os órgãos da Administração Pública tinham a incumbência de aplicar o direito comunitário, de modo que, em um possível conflito entre normas nacionais e o direito comum europeu, deve-se dar preferência a este último.

Referida deliberação tinha o objetivo de assegura que o direito da União Europeia mantivesse sua primazia, favorecendo a plena eficácia do Regime Geral de Proteção de Dados (RGPD) estatuído por meio da Diretiva 2016/679. Sendo assim, o CNPD adotou a seguinte medida:

> Com os fundamentos acima expostos, de forma a assegurar o primado do direito da União Europeia e a plena efetividade do RGPD, a CNPD delibera desaplicar, nas situações de tratamento de dados pessoais que venha a apreciar, as seguintes normas da Lei n.º 58/2019, de 8 de agosto:
> i. Artigo 2.º, n.ºs 1 e 2
> [...]

[39] CORDEIRO, A. Barreto Menezes. *Direito da Proteção de Dados – À luz do RGPD e da Lei n.º 58/2019*. Coimbra: Almedina, 2020.
[40] *Idem*.

A CNPD defende enfaticamente que as leis nacionais devem ter estrita conformidade com as normas comuns europeias, inclusive se isso demandar que os Estados desconsiderem certas normas nacionais que possam entrar em conflito com o direito da União Europeia e prejudicar a eficácia do RGPD. Essa postura reforça o grau de importância de garantir a conformação e a aplicação das normas de proteção de dados em toda a União Europeia.

O artigo 20º, nº 1, intitulado "Dever de Segredo", estabelece que o direito de informação e acesso a dados pessoais, conforme delineado nos artigos 13º a 15º do RGPD, não pode ser exercido caso exista um deve de segredo imposto pela lei ao responsável pelo tratamento ou ao subcontratante, quando aplicável, e esse dever seja oponível ao próprio titular dos dados.

A CNPD defende que esse artigo não deve ser aplicado com base no fato de que ele é um tanto irrelevante do ponto de vista jurídico quando se leva em consideração o art. 14º do RGPD, que trata da recolha indireta de dados pessoais e estabelece as circunstâncias em que essa recolha pode ser restrita. O artigo 20º, nº 5, alínea d, do RGPD específica o dever legal de segredo.

Sendo assim, devido a contrariedade com as normas constantes nos artigos 13º, 15º e 23º do RGPD e com o nº 2 do artigo 8º da CEDH, a CNPD deliberou pela não aplicação do dispositivo em comento em situações futuras que possam ser objeto de análise.

O art. 23º, nº 1, abre a possibilidade de entidades públicas processarem dados pessoais para fins distintos, sob a condição de apresentação de justificativas pautadas no interesse público para a utilização excepcional dos dados. A CNPD defende que o termo "interesse público" está empregado genericamente, de maneira que o art. 23º não específica quais fins de interesse público podem respaldar o processamento de dados para fins distintos, diferente do que ocorre na Diretiva 2016/679, mais especificamente no art. 6º, nº 4.

A crítica é uma preocupação da CNPD de que o processamento de dados para fins distintos ocorra para prosseguir qualquer interesse público, indo de encontro ao que dispõe o RGPD da União Europeia. Para a CNPD, viola-se, deste modo, o princípio da finalidade ou das limitações das finalidades.

O art. 28º, nº 3, alínea a, estabelece a desnecessidade do consentimento do trabalhador como condição para legitimar o tratamento dos seus dados se o tratamento resultar em uma vantagem jurídica ou econômica para o trabalhador. A CNPD defende que a regra mencionada viola dois dispositivos da Diretiva 2016/679:

O art. 9º, nº 1, que dispõe que os tratamentos de dados pessoas só devem ocorrer caso seja necessário para o cumprimento de obrigações ou o exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados no contexto da legislação trabalhista.

O art. 88º, nº 2, que dispõe que todas as normas devem proteger a dignidade, interesses legítimos e direitos fundamentais do titular de dados, com ênfase na transparência do tratamento, transferência de dados dentro de um grupo empresarial ou de empresas envolvidas em atividade econômica conjunta e sistemas de controle no local de trabalho.

A CNPD também teceu críticas aos arts. 37º, 38º e 39º, que tratam das contraordenações, mais especificamente as muito graves, as graves e as penas cabíveis, respectivamente.

Quanto ao art. 37º, a CNPD dispôs que o nº 1, alínea a, que classifica como contraordenação muito grave o tratamento de dados pessoais com violação intencional dos princípios dispostos no art. 5ª da Diretiva 2016/679, está em dissonância com o que dispõe o art. 83º, nº 5, da Diretiva 2016/679, que não apresenta uma distinção entre condutas negligentes e intencionais, de forma que não há uma abertura para que os legisladores nacionais disponham acerca da redução do alcance das infrações passíveis de sanção.

Ainda, a CNPD deliberou que a alínea h do mesmo artigo, que trata da não prestação de informações relevantes nos termos dos artigos 13º e 14º, consubstanciada na omissão de informações (considerando também o disposto no art. 38º, nº 1, alínea b), está em desconformidade com o art. 83º da Diretiva 2016/679, que abrange todas as facetas do direito à informação, sem reduzir suas áreas de aplicação.

Por fim, o art. 37º, nº 1, alínea k, estipula como contraordenação muito grave a recusa de colaboração exigida pela CNPD, no exercício dos seus poderes. Consoante a CNPD, a referida previsão vai de encontro ao previsto no art. 83º, nº 4 e nº 5, da Diretiva nº 2016/679, cujo rol é taxativo.

Diante do exposto, a CNPD deliberou pela não aplicação do art. 37º, nº 1, alíneas a, h e k, e do art. 38, nº 1, alínea b, todos da Lei nº 58/2019.

A CNPD optou por não aplicar os arts. 37, nº 2, e 38º, nº 2, estabelecem as escalas das penas para as contraordenações q, com o objetivo de garantir a plena eficácia do sistema sancionatório estabelecido na Diretiva 2016/679 (art. 83º, nº 4 e nº 5).

A CNPD decidiu aplicar apenas o art. 37º, nº 1, alíneas ‘e’ e l, e o art. 38º, alíneas q e r, da Lei nº 58/2019.

O art. 39º traz as últimas disposições em torno do regime de contraordenações da Lei nº 58/2019. Nele, definem-se três critérios de determinação de pena (art. 39º, nº 1, alíneas a, b e c). Os argumentos para afastar esses critérios centram-se na figura habilitante para a aplicação da norma, que não é o legislador nacional de cada Estado-Membro, mas sim a entidade administrativa ou judicial responsável pela sua aplicação em cada caso específico. As autoridades mencionadas só poderão aplicar esses critérios no âmbito das infrações previstas anteriormente.

O art. 39º, nº 3, estabelece uma exigência a CNPD, que consiste em um passo prévio à decisão de iniciar um procedimento sancionatório: advertência para corrigir a ilegalidade dentro de um prazo razoável. Fixa-se, ainda, um regime especial para as condutas ilícitas praticadas com negligência pelos responsáveis pelos tratamentos, o qual não está em conformidade com a Diretiva 2016/679. Isso porque o art. 58º, nº 2, alínea a, da Diretiva 2016/679 atribui às autoridades nacionais o poder de emitir advertências ao responsável pelo tratamento ou subcontratante, alertando que as operações de tratamento planejadas podem violar disposições do regulamento. A disposição da lei nacional, prevê, em termos abstratos, a adoção de uma medida corretiva específica, sem avaliação caso a caso.

O art. 61º trata da renovação do consentimento. O art. 61º, nº 2, estipula os casos em que o consentimento caduca, particularmente quando o contrato no qual o titular dos dados é parte chega ao fim, determinando que o tratamento de dados é legal até esse momento. A razão para a não aplicação desta norma é o fato de o contrato não ser instrumento com força para legitimar o tratamento de dados sensíveis. Por essa via, todas as atividades podem carecer de um fundamento de legalidade para o tratamento de dados pessoais necessários para a execução contratual quando o fundamento for tão somente o contrato.

A Diretiva 2016/679, no art. 4º, nº 11, define o consentimento como uma manifestação de vontade livre, específica, informada e explícita e no considerando 42, ressalta que o consentimento não pode ser considerado livre se o titular dos dados não tiver uma verdadeira escolha ou liberdade, ou se não puder recusar ou retirar o consentimento sem sofrer prejuízos.

4. OS MEIOS DE VIGILÂNCIA NO CONTEXTO LABORAL

Em Portugal, os meios de vigilância são abrangentes do ponto de vista jurídico e não possuem uma operacionalização isolada. Abrangem uma gama diversificada de dispositivos, incluindo equipamentos audiovisuais, câmeras de vídeo, microfones escondidos e sistemas de escuta e gravação telefônica. O monitoramento recai tanto sobre pessoas, quanto sobre objetos[41].

É importante mencionar que os meios de vigilância podem ser utilizados para respaldar fatos em diferentes áreas do direito, tais como o Direito Processual Penal e o Direito do Trabalho. Frise-se que em alguns ramos do direito, como é o caso do Direito do Trabalho, a utilização de meios de videovigilância ainda gera controvérsias relevantes, que envolvem questões éticas, legais e práticas, haja vista que tende a atingir direitos fundamentais dos trabalhadores, tais como a privacidade e a dignidade no trabalho.

Na medida em que a tecnologia avança, prolifera-se a existência de dispositivos de vigilância. Com isso, alguns dilemas de cunho jurídico surgem, de modo que não podem ser discutidos tendo como parâmetro abordagens jurídicas tradicionais. Sendo assim, eleva-se a urgência de consolidar normas e diretrizes que fomenta a transparência na utilização dos meios de vigilância, o consentimento informado dos indivíduos e a supervisão adequada das autoridades competentes.

4.1. O caso específico da videovigilância

Videovigilância é o processo de gravação de imagens e o respectivo tratamento por meio de sistemas integrados de câmeras que podem ser acopladas em espaços públicos e no interior de instalações. O processo consiste em captar vídeo em tempo real durante um período significativo para posterior tratamento e armazenamento das imagens captadas.

É possível compreender que a videovigilância é uma prática precipuamente ubíqua, já que é empregada em espaços diversos e, na grande maioria das vezes, com o mesmo objetivo, qual seja a promoção de segurança para pessoas e objetos. A principal e mais relevante distinção no uso da videovigilância nos diferentes espaços é a forma como o produto desse mecanismo será tratado.

[41] DRAY, Guilherme. *Código do Trabalho Anotado*. 6.ª ed. Coimbra: Almedina, 2008. Anotação ao art.º 20.º, p. 130. No mesmo sentido: MARTINEZ, Pedro Romano. *Direito do Trabalho.* 11.ª ed. Coimbra: Almedina, 2023.

A respeito da utilização de sistema de videovigilância para a garantia de segurança às pessoas e bens, o Tribunal de Justiça Europeu proferiu a seguinte conclusão no Acórdão de 11 de dezembro de 2019:

> Em face do exposto, há que responder às questões submetidas que o artigo 6.º, n.º 1, alínea c), e o artigo 7.º, alínea f), da Diretiva 95/46, lidos à luz dos artigos 7.º e 8.º da Carta, devem ser interpretados no sentido de que não se opõem a disposições nacionais que autorizam a instalação de um sistema de videovigilância, como o sistema em causa no processo principal, instalado nas partes comuns de um imóvel para habitação, para prosseguir interesses legítimos de garantia da segurança e da proteção das pessoas e dos bens, sem o consentimento das pessoas em causa, se o tratamento dos dados pessoais recolhidos através desse sistema de videovigilância cumprir os requisitos previstos no mencionado artigo 7.º, alínea f), o que incumbe ao órgão jurisdicional de reenvio verificar.

No contexto apresentado, o emprego de videovigilância tem o potencial de afetar direitos e deveres fundamentais consagrados na Constituição da República Portuguesa. Pode-se citar como exemplo o previsto no art. 27.º, que tutela a liberdade e a segurança. O dispositivo em comento estabelece que ninguém pode ser total ou parcialmente privado da liberdade, salvo sentença judicial condenatória cuja pena seja a prisão ou aplicação de medida de segurança.

A garantia da segurança pode conflitar com o direito à privacidade e à liberdade individual, o que demanda a harmonia entre proteção da segurança pública e salvaguarda dos direitos individuais.

Alguns defendem que garantir a segurança pública por meio de sistemas de videovigilância policial demanda respaldo legal específico, já que o que está ocorrendo é uma verdadeira restrição de um ou mais direitos fundamentais. Outros defendem que a videovigilância policial é um dos instrumentos pelos quais a segurança pública resta concretizada, não havendo óbices para sua utilização mesmo diante da ausência de uma legislação específica, sendo totalmente suficiente os princípios jurídicos existentes relacionados ao tema.

4.1.1. A videovigilância em Portugal – A admissibilidade do controlo de videovigilância

A norma editada para regular o exercício da atividade de segurança privada foi o Decreto-Lei 231/98, de 22 de julho de 1998. A norma em questão foi anterior a legislação relativa à proteção de dados e tinha como objetivo regular a segurança privada de modo que fossem tutelados pessoas e bens e prevenidos e reprimidos o cometimento de ilícitos penais. À época da promulgação do decreto em tela, o legislador buscou preencher lacunas jurídicas que ainda subsistiam sobre a matéria.

O Tribunal Constitucional, por meio do Acórdão de 12 de junho de 2002, com base no art. 12.º, n.º 1, do Decreto-Lei n.º 231/98, declarou a inconstitucionalidade orgânica da utilização de sistemas de videovigilância por parte das entidades que prestavam serviços de segurança privada.

Por meio da Lei n.º 67/98, revogada pela Lei n.º 58/2019, buscou-se regular de maneira mais precisa a questão da videovigilância. O art. 4º, nº 4, da lei revogada, dispunha que a mesma se aplicava à videovigilância e outras formas de captação, tratamento e difusão de sons e imagens que permitam identificar pessoas quando o responsável pelo tratamento esteja domiciliado ou sediado em Portugal ou cujo fornecedor de rede esteja estabelecido em Portugal.

Após uma lacuna de sete anos, publicou-se a Lei n.º 1, de 10 de janeiro de 2005, que regulamentou o mecanismo da videovigilância em locais públicos de uso comum pelas forças e serviços de segurança. Posteriormente, referida norma foi alterada pela Lei n.º 9, de 23 de fevereiro de 2012.

Para a instalação de um sistema de videovigilância com câmeras fixas, deve-se observar as seguintes condições: autorização do agente público responsável pelo serviço de segurança requerido; e parecer favorável da CNPD. A lei estabelece alguns outros critérios a serem preenchidos, como condições de instalação, formato do pedido de autorização, além de alguns princípios orientadores[42].

O art. 10.º da Lei n.º 1/2005 dispõe acerca dos direitos dos interessados e assegura a todas as pessoas que figurem em gravações o direito de acesso e eliminação, salvo quando o conteúdo das gravações constituir perigo para a defesa do Estado ou para a segurança pública; constituir ameaça ao exercício dos direitos e liberdades de terceiros ou quando referido direito prejudicar investigação criminal em curso.

Quanto aos sistemas de videovigilância rodoviária, o governo português formulou medidas de prevenção e segurança rodoviárias, abrangendo a detecção de infrações. O governo ficou autorizado a elaborar decretos-lei especificamente voltados para a questão em estudo, por meio de modificação perpetrada pela Lei n.º 39-A/2005 ao art. 23.º da Lei n.º 1/2005. Nesse caminhar, foi editado o Decreto-Lei n.º 207, de 29 de novembro de 2005, pelo qual fixou-se um regime especial para sistemas de vigilância rodoviária.

[42] RAMALHO, Maria do Rosário Palma. *Tratado de Direito do Trabalho.* Parte I: *Dogmática Geral.* 6.ª ed. Coimbra: Almedina, 2021.

Houve uma ampliação dos procedimentos atinentes à instalação dos sistemas de videovigilância pelos órgãos de segurança, colocando ainda mais em evidência a relevância do tratamento de dados, as finalidades e os objetos do tratamento, conformando com as diretrizes da Lei de Proteção de Dados então vigente. Consignou-se a possibilidade de a CNPD acessar os dados, incluindo informações como data, hora e local das ocorrências, número de registros, normas violadas, entre outros.

Acerca da captação e registro de imagens e sons, o artigo 12.º estabelece que a captação deve estar limitada ao tipo de ação desenvolvida e a sua finalidade, obedecendo as restrições legais.

Por meio de medidas como esta resta evidente que o governo português depositou uma atenção especial à videovigilância, ainda mais se considerarmos o movimento de conformação das medidas com a Lei de Proteção de Dados.

Além dos diplomas mencionados, que regulam os sistemas de videovigilância, é relevante abordar a Lei n.º 51, de 29 de agosto de 2006, que dispõe especificidades relativas à vigilância rodoviária realizada pelas Estradas de Portugal e pelas concessionárias rodoviárias.

Esta lei define o regime aplicável à criação e utilização de sistemas de gestão de eventos pelas Estradas de Portugal e de sistema de informação pelas concessionárias para registrar acidentes e incidentes ocorridos nas zonas concessionadas.

A Lei n.º 51/2006 atribuiu claramente a responsabilidade pelo tratamento de dados pessoais às Estradas de Portugal e a concessionárias que criam e utilizam tais sistemas de informação de acidentes e incidentes (*vide* art. 6.º). O artigo 10.º estabelece a possibilidade contratual de delegar o tratamento de dados a subcontratantes, bem como as obrigações legais que estes devem cumprir.

No Acórdão n.º 376, de 25 de maio de 2016, do Tribunal da Relação do Porto, discutiu-se a respeito de uma questão de suma relevância para o Direito Penal, cujo objeto era a investigação de um crime de furto qualificado de um veículo. O cerne da discussão residiu na recusa de uma concessionária em fornecer informações sobre a passagem de um veículo por um de seus pátios, sob o fundamento do disposto no art. 20.º da Lei n.º 51/2006, que dispõe que é proibida a transmissão a terceiros ou a cópia dos dados pessoais obtidos e tratados nos termos da lei em tela, exceto em circunstâncias específicas delineadas nos artigos 15.º e 16.º.

A recusa da concessionária foi inicialmente considerada legítima, desencadeando um incidente para afastar o sigilo profissional. No entanto, este incidente foi rejeitado com base na legitimidade da recusa e na constatação de que os elementos solicitados não eram relevantes para a descoberta da verdade material. O recurso interposto contestou esta decisão, invocando o artigo 16.º da mesma lei, que autoriza a comunicação de dados a entidades, nomeadamente às autoridades judiciárias, para efeitos de instauração ou condução de processos.

O Acórdão em análise proferiu interpretação extensiva ao art. 16.º, de forma que não restringiu o dever de informação a casos de investigação criminal, mesmo diante de possíveis conflitos com direitos de privacidade dos indivíduos. Consequentemente, explanou-se o entendimento de que a competência de avaliar a relevância dos dados e ponderar os interesses em jogo não era do juiz do tribunal de primeira instância, mas uma prerrogativa do tribunal superior.

O tribunal deliberou, fundamentado no art. 16.º, alínea b, da Lei n.º 51/2006, pela ilegitimidade da recusa da concessionária, ordenando a notificação da mesma para, dentro de um prazo determinado, fornecer os dados de identificação solicitados no âmbito do inquérito. Esta decisão foi de encontro à proferida pelo tribunal de primeira instância.

O caso apresentado exemplifica a aplicação direta das exceções previstas no art. 20.º da Lei n.º 51/2006. Esta lei traz uma seção especificamente voltada aos direitos dos titulares dos dados, a Seção V, garantindo o direito à informação (art. 18.º) e o direito de acesso e eliminação (art. 19.º). O ponto de confluência com a interpretação legislativa outrora adotada é a exigência de cumprimento do requisito previsto no art. 12.º, que consiste na notificação obrigatória à CNPD.

É relevante registrar que a competência para fiscalizar o cumprimento da Lei n.º 51/2006 é da CNPD, que busca garantir que os sistemas de videovigilância eletrônica sejam confiáveis, de modo que sejam utilizados estritamente para o objetivo proposto e sejam tutelados os direitos, liberdades e garantias do cidadão, conforme prever o art. 3.º.

Ademais, é por meio do dispositivo retromencionado que a lei ora em estudo firma um compromisso com a proteção dos direitos dos titulares dos dados, deixando expresso de forma clara e precisa os mecanismos pelos quais deve se garantir transparência das informações pessoais, bem como o modo de acesso e eliminação. Pode-se, então, dizer que a notificação obrigatória à CNPD é um exemplo desses mecanismos.

Em 2007, entrou em vigor a Lei n.º 33, de 13 de agosto de 2007, que regula a instalação e utilização de sistemas de videovigilância em táxis. Consoante a lei mencionada, referidos sistemas tem o objetivo de registrar imagens para proteger pessoas e bens nos casos de emergência, ameaça ou ofensa à integridade física de motoristas de táxis ou de usuários do serviço, de modo que as autoridades de segurança possam identificar e responsabilizar os agentes criminosos mais fácil e adequadamente.

Em conformidade com legislações anteriores sobre videovigilância e proteção de dados, a Lei n.º 33/2007 atribuiu à CNPD a responsabilidade de fiscalizar a aplicação da lei e regular as comunicações relacionadas com esses sistemas.

O art. 9.º da Lei n.º 33/2007 estabelece que os sistemas de videovigilância instalados nos táxis só poderão ser ativados caso se observe risco ou perigo potencial ou iminente. Na hipótese de a situação de risco ou perigo potencial ou iminente não se concretizar, as imagens gravadas deverão ser imediatamente eliminadas. Há, ainda, a obrigação de cientificar os usuários acerca da existência do sistema de videovigilância móvel, deixando claro que ocorre a captação e gravação de imagens por razões de segurança e identificando o responsável pelo tratamento de dados, inclusive com a disponibilização do contato do mesmo.

A Portaria n.º 1164-A/2007 regulamentou a cientificação descrita no parágrafo anterior. Dentre outras especificações, há a previsão de o titular dos dados acessar e eliminar os registros, tanto por meio do responsável pelo tratamento, quanto por meio da CNPD.

Observa-se uma preocupação de harmonizar a necessidade de segurança com o respeito pelos direitos individuais dos cidadãos, assegurando-se uma utilização adequada e transparente dos sistemas de videovigilância em táxis.

Em 2013, foi publicada a Lei n.º 34, de 16 de maio de 2013, que estabeleceu o regime do exercício da atividade de segurança privada. Por meio do diploma normativo em questão restou delimitada o âmbito da atividade de segurança privada, estabelecendo-se a distinção entre atividade de segurança privada, prestação de serviços a terceiros e organização interna de serviços de segurança privada.

A Lei n.º 34/2013 alterou o Decreto-Lei n.º 35, de 21 de fevereiro de 2004. Este último já possuía um caráter avançado para a época em que foi promulgado por trazer especificações relativas as funções a serem exercidas pelo pessoal de vigilância, dentre elas a possibilidade de os vigilantes de segurança privada realizarem revistas de prevenção e segurança no controle de acessos a determinados locais.

A Lei n.º 34/2013 trouxe requisitos mais rigorosos para a formação e certificação dos profissionais de segurança privada, objetivando redimensionar o padrão de qualidade e o nível de profissionalismo do setor. Além disso, fomentou os mecanismos de fiscalização e supervisão, conferindo competências específicas às entidades responsáveis pela regulamentação da atividade de segurança privada.

A lei em estudo dispôs que sistemas de vigilância eletrônica são um meio de segurança apto a serem utilizados no exercício da segurança privada, de acordo com o previsto no art. 13.º. Para os fins da segurança privada, os sistemas devem permitir a captação de imagens e som com conservação de 30 dias. Transcorrido esse prazo, os registros devem ser destruídos, a não ser que ainda possam ser utilizados no âmbito do processo penal.

É importante registrar que a Lei n.º 34/2013 abrangeu questões relativas à proteção de dados, com vistas a tutelar os direitos dos titulares, especialmente o de acesso, informação e oposição, alinhado com o previsto na Lei de Proteção de Dados então vigente.

Diante do exposto, é inegável que o diploma normativo em comento representou um avanço relevante na garantia de segurança e proteção adequadas, tanto sob o ponto de vista dos profissionais que atuam neste setor, quanto para o público em geral.

A compreensão dos diplomas legais que dispõem delineamentos acerca de sistemas de videovigilância é crucial para dimensionar o nível de inserção desse mecanismo na sociedade em suas mais diversas atividades. As leis em estudo abrangem regramentos acerca do tratamento de dados pessoais, especialmente no que tange a tutela dos direitos à privacidade dos indivíduos, sempre deixando claro que os sistemas de videovigilância devem funcionar estritamente para garantir a segurança de pessoas e bens.

Pode-se dizer que abordagem pelas legislações relativas à videovigilância de questões relativas a proteção de dados e da necessidade de garantir que o uso desses sistemas seja proporcional e transparente representa, em verdade, uma evolução.

Mais uma vez importa ressaltar a necessidade de garantir que os direitos individuais sejam devidamente observados diante dos mecanismos utilizados para a consecução da segurança pública, esclarecendo-se os limites para o uso da videovigilância, de forma que o mesmo ocorra de maneira ética e responsável com mecanismos de supervisão e controle fortalecidos e operantes.

4.1.2. Princípios norteadores da utilização deste meio

O acórdão de 12 de junho de 2002 analisou ainda o artigo 18.º, n.º 2, da Constituição da República Portuguesa, que estabelece que a lei só pode restringir direitos, liberdades e garantias nos casos expressamente previstos na Constituição, devendo tais restrições limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos[43].

A CRP impõe um limite a restrição de direitos, de modo que só ocorra para salvaguardar outros direitos ou interesses constitucionalmente protegidos. Referida restrição deve advir de determinações legais, como é o caso da utilização de mecanismos de videovigilância.

No tópico anterior, foram apresentadas algumas legislações que permitem a utilização de sistemas de videovigilância diante do cumprimento de algumas condições específicas que visam assegurar que nenhum direito seja abusadamente restringido em prol da garantia de segurança para pessoas e bens.

Diante do crescente número de instalação de sistemas de videovigilância, alguns pontos de debate foram surgindo no âmbito da União Europeia, motivo pelo qual se formou o Grupo de Trabalho do Artigo 29. ° da Diretiva nº 95/46/CE, cuja atuação deu origem ao Parecer 4/2004[44], que tinha como objeto a análise do tratamento de dados pessoais por meio de videovigilância para a fixação de limites claros entre o emprego de sistemas de videovigilância e a preservação do direito à privacidade.

Para a realização dos estudos, o Parecer 4/2004 levou em conta o arcabouço normativo de todos os Estados-Membros para que fosse possível definir orientações que estivessem em conformidade com o ordenamento jurídico de todos os membros da União Europeia. À época, alguns países da União Europeia ainda não possuíam legislações específicas voltadas para o tema, como é o caso da Finlândia. Em outros, não só havia legislação, como era possível identificar mais de uma, como é o caso da França, de Portugal e da Suécia.

---

[43] Constituição da República Portuguesa:
Art. 18.°
(Força jurídica)
[...]
2. A lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na Constituição, devendo as restrições limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos.

[44]GRUPO DE TRABALHO DO ARTIGO 29 "Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679", adotadas em 28 de novembro de 2017, sendo a última redação revista e adotada em 13 de abril de 2018. Disponível em: <https://www.cnpd.pt/bin/rgpd/docs/wp259rev0.1_PT.pdf>. Acesso em: 24 abr. 2024.

O parecer suscitou questões bastante relevantes, como a necessidade de conformar as legislações nacionais em vigor com a legislação de proteção de dados.

Ainda, restou sedimentado que o tratamento de dados pessoais não só pode, como deve considerar dados em forma de imagem e som, precipuamente quando se estiver sob o uso de sistemas de videovigilância.

Diante disso, a função do Responsável pelo Tratamento de Dados ganhou contornos mais precisos, dentre as quais a averiguação da necessidade de tratamento dos dados provenientes da captação de imagem e som por sistemas de videovigilância, nos seguintes termos:

> [...] uma das primeiras precauções que o responsável pelo tratamento deve tomar é verificar se a videovigilância implica o tratamento de dados pessoais, na medida em que diga respeito a pessoas identificáveis. Nesse caso, a Directiva aplica-se independentemente das disposições nacionais que exijam, além disso, autorização para fins de segurança pública[45].

Depois de averiguada a necessidade de tratamento dos dados, o parecer elencou obrigações e precauções aplicáveis ao responsável pelo tratamento de dados, sendo elas: legitimidade do tratamento; especificidade, especificação e legitimidade dos fins; critérios relativos à legitimidade do tratamento; proporcionalidade do recurso à videovigilância; e proporcionalidade das atividades de videovigilância.

Aqui, destaco a ênfase no princípio da proporcionalidade. A videovigilância deve ser empregada para atingir exatamente as finalidades para a qual se propôs, dentro de um limite imposto pelas diretrizes advindas de direitos individuais indispensáveis. Sendo assim, é de fundamental importância que os sistemas de videovigilância sejam utilizados com a devida adequação quanto aos objetivos estabelecidos, quanto a pertinência da funcionalidade dos dados e quanto ao uso moderado dos mesmos.

Do disposto no parágrafo anterior, inferem-se os seguintes princípios: limitação dos tratamentos às finalidades; minimização dos dados; exatidão; limitação da conservação; integridade e confidencialidade; e responsabilidade.

Além disso, deve-se atentar para as diretrizes impostas pelos seguintes princípios: licitude, lealdade e transparência.

[45] Idem, p. 15.

O princípio da limitação da finalidade é apoiado pelo artigo 5.º, n.º 1, alínea b), da Regulamento n.º 679/2016 (RGPD), que estabelece que os dados pessoais devem ser recolhidos para finalidades específicas, explícitas e legítimas e não devem ser posteriormente tratados de forma incompatível com esses fins. No entanto, o tratamento posterior para efeitos de arquivo de interesse público, investigação científica ou histórica, ou fins estatísticos não é considerado incompatível com os fins iniciais, em conformidade com o artigo 89.º[46].

Alexandre Sousa Pinheiro dispõe que o princípio da finalidade é, em essência, a justificativa para o tratamento de dados pessoais e é prévio ao consentimento. É a determinação de que a coleta de informações pessoais e o respectivo tratamento não sejam realizados de forma desarrazoada, o que implica na necessidade de que referidos procedimentos estejam respaldados por uma razão específica. A razão traça os limites do tratamento de dados, fazendo com que os mesmos não sejam utilizados com excessos, isto é, com desvio de finalidade[47].

É importante consignar que é possível que o tratamento de dados seja empregado por razões outras que não aquelas que fundamentaram o tratamento de início. O que se compreende como uma proibição é armazenar os dados para finalidades ainda não existentes, imprevisíveis e futuras.

O permissivo do art. 5.°, n.° 1, alínea b, com relação ao tratamento posterior, é a utilização dos dados para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos.

O artigo 6.º(4) da Regulamento n.º 679/2016 (RGPD) descreve os requisitos para avaliar a compatibilidade do tratamento para finalidades diferentes daquelas para as quais os dados pessoais foram inicialmente recolhidos. Esta avaliação, quando não se baseia no consentimento do titular dos dados ou no direito da União ou dos Estados-Membros que constitui uma medida

[46] Regulamento nº 679/2016 (RGPD):
"Artigo 5.°
Princípios relativos ao tratamento de dados pessoais
1. Os dados pessoais são:
[...]
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."

[47]PINHEIRO, Alexandre de Sousa. Privacy e Proteção de dados pessoais: a construção dogmática do Direito à identidade informacional. Lisboa: Associação Académica da Faculdade de Direito de Lisboa, 2015. p. 207.

necessária e proporcionada numa sociedade democrática para salvaguardar os objetivos referidos no artigo 23.º, n.º 1, considera fatores como:

(a) qualquer ligação entre a finalidade original para a qual os dados pessoais foram recolhidos e a nova finalidade do tratamento posterior;

(b) o contexto em que os dados pessoais foram recolhidos, nomeadamente no que diz respeito à relação entre os titulares dos dados e o responsável pelo tratamento;

(c) a natureza dos dados pessoais, especialmente se forem tratadas categorias especiais de dados pessoais ao abrigo do artigo 9.º ou se os dados pessoais relacionados com condenações penais e infrações forem tratados ao abrigo do artigo 10.º;

(d) as potenciais consequências do tratamento posterior pretendido para os titulares dos dados; e

(e) a presença de salvaguardas adequadas, como a encriptação ou a pseudonimização.

Diante do exposto, não é equivocado dizer que o princípio da finalidade incide na necessidade de delinear os objetivos do tratamento de dados. Uma vez estabelecidos os objetivos de maneira clara, aos titulares dos dados são devidas informações relativas ao tratamento de dados para que se concretize a fase de consentimento.

Após o consentimento, ou restando verificado que o tratamento decorre de diretrizes cogentes avindas do âmbito externo (União Europeia) ou interno (Estado-Membro), o responsável pelo tratamento de dados poderá, dentro dos limites mencionados anteriormente, proceder com o tratamento posterior dos dados pessoais.

O princípio da minimização dos dados é apoiado pelo artigo 5.º, n.º 1, alínea c), da Regulamento n.º 679/2016 (RGPD), que estabelece que os dados pessoais devem ser adequados, relevantes e limitados ao que é necessário em relação às finalidades para as quais são tratados[48].

Alexandre Sousa Pinheiro dispõe que o princípio da minimização de dados está consubstanciado no ato de assegurar que a coleta e o tratamento de dados sejam veementemente

[48] Regulamento nº 679/2016 (RGPD):
"Artigo 5.°
Princípios relativos ao tratamento de dados pessoais
1. Os dados pessoais são:
[...]
c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados."

necessários para determinada finalidade, sem que subsista qualquer outro meio razoável para atingir a finalidade incialmente determinada. É, pode-se dizer, um princípio decorrente do princípio da proporcionalidade[49].

A respeito do princípio da minimização de dados, o Tribunal de Justiça da União Europeia, por meio do Acórdão datado de 20 de maio de 2003[50], proferiu o seguinte entendimento:

> Ora, nos termos da Directiva 95/46, sem prejuízo das derrogações admitidas ao abrigo do seu artigo 13.°, qualquer tratamento de dados pessoais deve ser conforme, por um lado, aos «princípios relativos à qualidade dos dados», enunciados no artigo 6.° da directiva e, por outro, a um dos «princípios relativos à legitimidade do tratamento de dados», enumerados no artigo 7.° da mesma.

O princípio da exatidão dos dados é apoiado pelo artigo 5.º, n.º 1, alínea d), da Regulamento n.º 679/2016 (RGPD), que estabelece que os dados pessoais devem ser exatos e, sempre que necessário, mantidos atualizados. Exige ainda que sejam tomadas todas as medidas razoáveis para garantir que os dados imprecisos, considerando as finalidades para as quais são processados, são apagados ou retificados sem demora[51].

O princípio da exatidão demanda a clareza e a atualização dos dados coletados, o que contribui para que os mesmos permaneçam íntegros durante o período de conservação. As incorreções ou desatualizações dos dados devem ser imediatamente sanadas, com vistas a prevenir potenciais danos aos titulares dos dados. O pressuposto para a consecução do princípio da exatidão é o direito de acesso, retificação e eliminação de dados, regulamento pelos artigos 15.°, 16.° e 17.° da Diretiva n.° 679/2016.

A respeito do princípio da minimização de dados, o Tribunal de Justiça da União Europeia, por meio do Acórdão datado de 7 de maio de 2009[52], proferiu o seguinte entendimento:

---

[49]PINHEIRO, Alexandre de Sousa. *Privacy e Proteção de dados pessoais:* a construção dogmática do Direito à identidade informacional. Lisboa: Associação Académica da Faculdade de Direito de Lisboa, 2015, p. 209.

[50] Acórdão do Tribunal de Justiça de 20 de maio de 2003, processo C-465/00 – Österreichischer Rundfunk e outros, ECLI:EU:C:2003:294. Disponível em <http://curia.europa.eu/juris/showPdf.jsf?text=&docid=48330&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=9063485>. Acesso em 24 abr. 2024.

[51] Regulamento nº 679/2016 (RGPD):

"Artigo 5.°

Princípios relativos ao tratamento de dados pessoais

1. Os dados pessoais são:

[...]

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."

[52]Acórdão do Tribunal de Justiça de 7 de maio de 2009, processo C-553/07 – Rijkeboer, ECLI:EU:C:2009:293. Disponível em:

> Este direito ao respeito da vida privada implica que a pessoa em causa possa assegurar-se de que esses dados pessoais são tratados com exactidão e de forma lícita, ou seja, em especial, que os dados de base que lhe dizem respeito são exactos e são enviados a destinatários autorizados. Como referido no quadragésimo primeiro considerando da directiva, para poder efectuar as verificações necessárias, a pessoa em causa deve dispor de um direito de acesso aos dados que lhe dizem respeito e que estão em fase de tratamento.

O princípio da limitação da conservação é apoiado pelo artigo 5.º, n.º 1, alínea e), da Regulamento n.º 679/2016 (RGPD), que prevê que os dados pessoais devem ser conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessários para os fins para os quais são tratados. Os dados podem ser conservados por períodos mais longos exclusivamente para fins de arquivo de interesse público, investigação científica ou histórica, ou fins estatísticos, em conformidade com o artigo 89.º(1), desde que sejam implementadas medidas técnicas e organizacionais adequadas para salvaguardar os direitos e liberdades dos titulares dos dados[53].

O princípio da limitação da conservação encontra respaldo no art. 5°, n° 1, alínea e, da Diretiva n.° 679/2016 (RGPD), que dispõe o seguinte:

Os dados pessoais não podem ser armazenados *ad aeternum*, por isso, serão conservados apenas pelo prazo estritamente necessário para a concretização das finalidades incialmente determinadas. Com o alcance da finalidade, finda a necessidade de conservação, o que impõe ao responsável pelo tratamento de dados o dever inescusável de eliminar ou tornar anônimo os dados de forma permanente. Importa consignar que o prazo de conservação é fixado pelo responsável pelo tratamento.

O princípio da integridade e da confidencialidade é apoiado pelo artigo 5.º, n.º 1, alínea f), da Regulamento n.º 679/2016 (RGPD), que estabelece que os dados pessoais devem ser

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=74028&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=9063485>. Acesso em 24 abr. 2024.

[53] Regulamento nº 679/2016 (RGPD):
"Artigo 5.°
Princípios relativos ao tratamento de dados pessoais
1. Os dados pessoais são:
[...]
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."

tratados de forma a garantir a sua segurança, incluindo a proteção contra o acesso não autorizado ou ilícito[54].

O princípio da integridade e da confidencialidade implica em implementação de medidas de segurança adequadas, de forma que os dados dos titulares sejam utilizados somente para a finalidade para a qual foram coletados, sem que possíveis impactos negativos advenham de acessos, usos, alterações, publicações e qualquer outro tipo de atos ilegais.

É importante que as medidas de segurança sejam postuladas de maneira contextualizada, o que significa dizer que cada situação demanda um procedimento de segurança específico, com a utilização de técnicas diversas, de forma que se promova a confiabilidade e a segurança dos mecanismos de armazenamento de dados. É nesse momento que o direito de acesso é delineado, posto que por meio do princípio da integridade e da confidencialidade é que o acesso passa por uma deliberação acerca de limites e de autorizações.

O princípio da responsabilização é apoiado pelo artigo 5.º, n.º 2, da Regulamento n.º 679/2016 (RGPD), que estabelece que o responsável pelo tratamento é responsável por garantir o cumprimento das disposições do artigo 5.º, n.º 1, devendo ser capaz de demonstrar esse cumprimento[55].

O responsável pelo tratamento tem a obrigação de analisar se os procedimentos relativos ao tratamento de dados ocorreram de acordo com os preceitos legais. Não há que se falar, tomando por base a Diretiva n.° 679/2016, em controle administrativo prévio. O que ocorre é o completo embasamento das operações na transparência daqueles que tratam os dados, restando nítida a preferência por um método de autocontrole.

A análise de legalidade dos procedimentos de tratamento de dados realizada pelos responsáveis deve resultar na demonstração de conformidade com o arcabouço jurídico a

[54] Regulamento nº 679/2016 (RGPD):
"Artigo 5.°
Princípios relativos ao tratamento de dados pessoais
1. Os dados pessoais são:
[...]
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."

[55]Diretiva nº 679/2016 (RGPD):
"Artigo 5.°
Princípios relativos ao tratamento de dados pessoais
[...]
2. O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 e tem de poder comprová-lo."

respeito da proteção de dados. Como dito, privilegia-se o autocontrole. Tal fato também abrange os subcontratantes, que possuem uma relação estreita com o responsável pelo tratamento de dados, bem como diversas atribuições.

Os princípios da legalidade, equidade e transparência são apoiados pelo artigo 5.º (1) (a) da Regulamento n.º 679/2016 (RGPD), que estabelece que os dados pessoais devem ser tratados de forma lícita, leal e transparente em relação aos dados assunto[56].

A transparência está relacionada a acessibilidade e compreensão do tratamento de dados pessoais. Os atributos de acessibilidade e de compressão devem ser concretizados por meio de medidas como o fornecimento de informações sobre a identidade do responsável pelo tratamento aos titulares dos dados, as finalidades do tratamento e consentimento e comunicação dos dados pessoais das pessoas afeta. A transparência pode ser atrelada, também, ao dever de isonomia em relação àqueles que terão seus dados tratados.

A licitude depende de dois pressupostos: obediência as leis nos procedimentos de tratamento de dados e observância do art. 52 da Carta dos Direitos Fundamentais da União Europeia. O art. 6. ° da Regulamento n.º 679/2016 estabelece os requisitos a serem contemplados para que o tratamento de dados seja essencialmente lícito, a saber:

> Artigo 6.°
>
> **Licitude do tratamento**
>
> 1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:
>
> a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;
>
> b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;
>
> c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;
>
> d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;
>
> e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;
>
> f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou

[56] Regulamento nº 679/2016 (RGPD):
"Artigo 5.°
Princípios relativos ao tratamento de dados pessoais
1. Os dados pessoais são:
a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados."

> direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

A lealdade pode ser descrita como o equilíbrio relacional. É a harmonia da relação entre responsáveis pelo tratamento, subcontratantes e titulares dos dados, especialmente quando a proteção é devida diante de tratamento de dados empreendido por entidades públicas e empregadores[57].

4.1.3. Finalidades do uso da videovigilância e os prazos de conservação

Sob o prisma do princípio da proporcionalidade, a discussão recai sobre a relevância da definição precisa das finalidades da instalação dos sistemas de videovigilância, o que abrange a fixação dos prazos de armazenamento dos dados coletados por meio desses mecanismos.

Aliás, a aferição da finalidade dos sistemas de videovigilância já foi fundamento para julgamento de casos concretos, tais como o julgado pelo Tribunal da Relação de Coimbra em 2 de novembro de 2011, que emitiu o seguinte entendimento quando da análise da licitude de provas obtidas mediante captação de imagens por sistema de videovigilância instalado em uma loja de joias[58]:

> Deste modo entendemos que o conceito de dados pessoais, nas vertentes de direito à imagem e privacidade e que despoletam a intervenção do direito penal, seja qual for o tipo legal que se suscite, abrange apenas "o núcleo duro da vida privada", o núcleo irredutível e mais sensível: a intimidade, a sexualidade, a saúde, a vida particular e familiar mais restrita.
>
> No nosso caso o sistema de videovigilância foi instalado num estabelecimento comercial, mais concretamente numa ourivesaria.
>
> Num tal caso, e como é entendimento unânime, a videovigilância visa finalidades sociais de "protecção de pessoas e bens". É uma medida preventiva e de dissuasão em relação à prática de infracções penais.
>
> Por isso é criminalmente atípica a obtenção de fotografias ou filmagens, mesmo sem consentimento do visado, sempre que exista justa causa para tal procedimento, como sucede quando a captação seja feita em lugares públicos, quando visem a realização de interesses públicos ou de factos que tenham ocorrido publicamente.
>
> Considerando todo o exposto é seguro que a prática de um acto ilícito – como é o caso -, não integra o conceito de privacidade contemplado na lei penal, donde é despropositado reivindicar a ilegalidade da recolha de dados, que respeitam à prática de um ilícito criminal, por violação desse direito. Se a prática de um crime integrasse o direito fundamental à imagem e vida privada, sendo estes direitos invioláveis, resultava que em última instância qualquer prova sobre ela poderia ser tida como ilegal.

---

[57] PINHEIRO, Alexandre de Sousa. *Privacy e Proteção de dados pessoais:* a construção dogmática do Direito à identidade informacional. Lisboa: Associação Académica da Faculdade de Direito de Lisboa, 2015, p. 207.

[58] Disponível em: <http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/6af3d06ec6ababd28025794800432128?OpenDocument>. Acesso em: 16 mai. 2024.

> Portanto, a recolha de imagens dos arguidos, feita dentro da ourivesaria, quando estes praticavam o furto aqui julgado, é legítima, legal, e como tal os fotogramas podiam, como foram ser usados e considerados na decisão sobre a matéria de facto.

Pois bem. Restou evidente, partindo do entendimento exarado pelo Tribunal da Relação de Coimbra, que a proteção de coisas e pessoas, como elemento de consecução da pacificação social, sobressai-se quando posta diante do direito à privacidade das pessoas individualmente consideradas. Dessa forma, a utilização de sistemas de videovigilância para fins de segurança não tem o condão de violar significativamente o direito à privacidade quando o que está em jogo é o reparo de um dano causado por um ilícito penal que ataca, diretamente, um indivíduo ou um bem e, indiretamente, toda a sociedade.

Diante disso, compreende-se que a análise da adequabilidade do emprego de sistemas de videovigilância, considerando os fins e as normas legais atinentes, depende, imprescindivelmente, da aplicação do princípio da proporcionalidade. Referido princípio é ainda mais necessário diante de casos em que a deliberação deve acatar a possibilidade de ser relevada a ausência de determinados elementos de adequação da videovigilância, citando-se como exemplo o consentimento. Pontue-se que os casos em questão são aqueles cuja solução objetiva, mediata ou imediatamente, a maior efetivação possível do interesse público, tais como os casos penais, como o apresentado anteriormente. Em outras situações, o que vale são os condicionamentos determinados pela legislação correlata.

Quanto aos prazos de conservação das imagens e dos sons captados, vale algumas observações.

Antes da entrada em vigor do RGPD, um dos requisitos para a instalação de sistemas de videovigilância era a autorização da CNPD. Sendo assim, antes de realizar o procedimento de implementação do referido mecanismo, o interessado necessitava cientificar a CNPD, seguindo as orientações previstas na antiga lei (Lei n.° 67/98) e na Portaria n.° 273, de 20 de agosto de 2013, que, dentre outras questões, regulava as condições específicas da prestação dos serviços de segurança privada.

O regulamento relativo aos períodos de conservação de dados da Portaria n.º 273 especifica no artigo 95.º que os sistemas de gravação de imagens devem estar preferencialmente localizados no centro de controlo e o período de conservação das imagens não deve ser inferior a 30 dias. Esta disposição permite alguma discricionariedade ao proprietário do sistema de

vigilância em relação ao local de armazenamento e ao período de retenção, estabelecendo apenas um mínimo de 30 dias[59].

A portaria aborda também os requisitos de sinalização para os sistemas de vigilância para garantir a sensibilização e, por extensão, o consentimento. O artigo 115.º estabelece que o símbolo de identificação das áreas monitorizadas deve obedecer às especificações do Anexo VIII da portaria. Os requisitos técnicos e as dimensões da sinalização devem estar em conformidade com as normas ISO 3864-1. Além disso, devem ser colocados avisos para garantir a legibilidade e a segurança, permitindo ao mesmo tempo a circulação tranquila dos utilizadores nas zonas monitorizadas. Estes avisos devem ser visíveis no perímetro exterior e repetidos dentro das áreas monitorizadas para fácil reconhecimento[60].

A Lei n.º 34/2013, que regula o setor da segurança privada, estipula que o período de conservação dos dados de videovigilância inicia-se no momento da sua captação, devendo as gravações ser destruídas no prazo de 48 horas após o período de conservação de 30 dias. Este prazo de 30 dias tornou-se padrão para vários estabelecimentos, exceto em casos regulados por leis específicas, como as relacionadas com violência, racismo, xenofobia e intolerância em eventos desportivos[61].

---

[59] Portaria n.º 273:
"Artigo 95.º
Sistemas de videovigilância
[...]
3 - Os sistemas de registo e gravação de imagens devem, preferencialmente, situar-se na central de controlo, sendo obrigatória a conservação das imagens por prazo não inferior a 30 dias."

[60] Portaria n.º 273:
"Artigo 115.º
Sinalização de sistemas de videovigilância
1 - O símbolo identificativo a utilizar na identificação dos locais objeto de vigilância com recurso aos meios previstos no n.º 1 do artigo 31.º da Lei n.º 34/2013, de 16 de maio, constam do anexo VIII à presente portaria, da qual faz parte integrante.2 - Os requisitos e especificações técnicas da sinalização e as suas dimensões devem cumprir as disposições da norma ISO 3864-1.
3 - O aviso a que se refere o n.º 5 do artigo 31.º da Lei n.º 34/2013, de 16 de maio, deve ser colocado de forma a garantir boas condições de legibilidade das mensagens nele contidas e a acautelar a normal circulação e segurança dos utentes dos espaços.
4 - Os avisos são colocados no perímetro exterior do local ou zona objeto de vigilância com recurso a equipamentos eletrónicos de videovigilância por câmaras de vídeo, e da forma mais conveniente ao seu pronto reconhecimento pelos utentes.
5 - No interior do local ou zona objeto de vigilância devem ser repetidos os avisos de informação."

[61] Lei n.º 34/2013:
"Artigo 31.°
Sistemas de videovigilância
[...]
2 - As gravações de imagem obtidas pelos sistemas videovigilância são conservadas, em registo codificado, pelo prazo de 30 dias contados desde a respetiva captação, findo o qual são destruídas, no prazo máximo de 48 horas."

Para estes cenários, a Lei n.º 39/2009 determina um período de retenção de 90 dias. Nos termos do artigo 18.º, n.º 2, as gravações de imagem e som durante um evento desportivo devem ser conservadas desde a abertura até ao encerramento do recinto e conservadas durante 90 dias, salvo se tal for exigido pela legislação penal ou processual aplicável[62].

No contexto do direito do trabalho, o prazo de retenção não é especificado em dias, mas é adaptado para atender às necessidades específicas de cada caso. O artigo 21.º, n.º 3, estabelece que os dados pessoais recolhidos através de vigilância remota devem ser conservados apenas durante o período necessário para atingir a finalidade pretendida. Os dados devem ser destruídos quando o trabalhador é transferido para outro local de trabalho ou após a cessação do contrato de trabalho[63].

4.1.4. Videovigilância e a Lei de Execução Nacional

Diante da entrada em vigor da Lei n.° 58/2019, algumas alterações e inovações foram inseridas no ordenamento jurídico nacional em matéria de proteção de dados. Algumas dessas alterações e inovações merecem destaque, o que farei a partir de agora.

No domínio do consentimento, a idade mínima para consentir o tratamento de dados pessoais no âmbito da oferta direta de serviços da sociedade da informação foi fixada nos 13 anos. De acordo com o artigo 16.º, n.º 1, os dados pessoais das crianças só podem ser tratados com base no consentimento, conforme descrito no artigo 6.º, n.º 1, alínea a), do RGPD, se a criança tiver pelo menos 13 anos de idade. Se a criança tiver menos de 13 anos, o tratamento será legal apenas se o consentimento for fornecido pelos representantes legais da criança, preferencialmente utilizando métodos de autenticação seguros[64].

---

[62] Lei n.º 39/2009:
"Artigo 18.°
Sistemas de videovigilância
[...]
2 - A gravação de imagem e som, aquando da ocorrência de um espectáculo desportivo, é obrigatória, desde a abertura até ao encerramento do recinto desportivo, devendo os respectivos registos ser conservados durante 90 dias, prazo findo o qual são destruídos em caso de não utilização nos termos da legislação penal e processual penal aplicável."

[63] Sobre o tema ver: MARTINEZ, Pedro Romano. *Direito do Trabalho.* 11.ª ed. Coimbra: Almedina, 2023. Código do Trabalho:
"Artigo 21.º
Utilização de meios de vigilância a distância
[...]
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."

[64]Lei n.º 58/2019:
"Artigo 16.º

Além disso, foi estabelecida a proteção de dados pessoais e de informações sensíveis de pessoas falecidas. O artigo 17.º especifica que os dados pessoais de pessoas falecidas são protegidos pelo RGPD e pela legislação nacional aplicável quando se enquadrem em categorias especiais de dados pessoais, tal como definido no artigo 9.º, n.º 1, do RGPD ou se refiram à vida privada, à imagem ou às comunicações. Os direitos previstos no RGPD, incluindo o acesso, a retificação e a eliminação de tais dados, podem ser exercidos por um representante designado do falecido ou, na sua ausência, pelos seus herdeiros. Além disso, os indivíduos podem, de acordo com as leis aplicáveis, determinar que tais direitos não podem ser exercidos após a sua morte[65].

Em matéria de videovigilância, a Lei n.º 58/2019 tem por base a Lei n.º 34/2013. O artigo 19.º estabelece que os sistemas de videovigilância utilizados para proteger pessoas e bens devem cumprir os requisitos do artigo 31.º da Lei n.º 34/2013, dentro de limitações específicas. As câmaras não podem captar vias públicas, propriedades vizinhas ou áreas fora do domínio exclusivo do controlador, exceto quando estritamente necessário para monitorizar pontos de acesso. Também não podem cobrir áreas de teclado de caixas multibanco, espaços privados para clientes, como casas de banho ou provadores, ou áreas exclusivas para funcionários, como refeitórios, vestiários, ginásios, casas de banho ou lounges. Nos estabelecimentos de ensino, as câmaras estão restritas a perímetros exteriores, pontos de acesso e espaços com equipamentos que exijam proteção especial, como laboratórios ou salas de informática[66].

Consentimento de menores
1 - Nos termos do artigo 8.º do RGPD, os dados pessoais de crianças só podem ser objeto de tratamento com base no consentimento previsto na alínea a) do n.º 1 do artigo 6.º do RGPD e relativo à oferta direta de serviços da sociedade de informação quando as mesmas já tenham completado 13 anos de idade.
2 - Caso a criança tenha idade inferior a 13 anos, o tratamento só é lícito se o consentimento for dado pelos representantes legais desta, de preferência com recurso a meios de autenticação segura."

[65] Lei n.º 58/2019:
"Artigo 17.º
Proteção de dados pessoais de pessoas falecidas
1 - Os dados pessoais de pessoas falecidas são protegidos nos termos do RGPD e da presente lei quando se integrem nas categorias especiais de dados pessoais a que se refere o n.º 1 do artigo 9.º do RGPD, ou quando se reportem à intimidade da vida privada, à imagem ou aos dados relativos às comunicações, ressalvados os casos previstos no n.º 2 do mesmo artigo.
2 - Os direitos previstos no RGPD relativos a dados pessoais de pessoas falecidas, abrangidos pelo número anterior, nomeadamente os direitos de acesso, retificação e apagamento, são exercidos por quem a pessoa falecida haja designado para o efeito ou, na sua falta, pelos respetivos herdeiros.
3 - Os titulares dos dados podem igualmente, nos termos legais aplicáveis, deixar determinada a impossibilidade de exercício dos direitos referidos no número anterior após a sua morte."

[66] Lei n.º 58/2019:
"Artigo 19.º
Videovigilância

Nos locais onde é permitida a videovigilância é proibida a gravação de som, exceto nos períodos em que as instalações se encontrem encerradas ou mediante autorização prévia da Comissão Nacional de Proteção de Dados (CNPD). Os indivíduos com acesso a dados captados pelos sistemas de vigilância estão vinculados à confidencialidade, e as violações deste dever podem resultar em penalizações criminais.

A proibição de gravação sonora, tal como consta do artigo 19.º, n.º 4, não é uma disposição nova. A Lei n.º 34/2013 já incluía uma exigência semelhante no artigo 31.º(9), que proíbe a gravação de som por sistemas de videovigilância, salvo se especificamente autorizada pela CNPD nos termos legais aplicáveis[67].

A inserção dessa determinação na Lei n.° 58/2019 encontra respaldo na recomendação da CNPD emitida por meio do Parecer n.° 20 de 2 de maio de 2018 quando da proposição daquela lei, que já conferia a possibilidade de a captação de som ocorrer durante os períodos em que não há circulação de pessoas nos estabelecimentos. O parecer ressaltou a importância de a legislação se amoldar às novas tecnologias de videovigilância, de definir as finalidades da utilização dos sistemas de videovigilância e de ponderar os direitos fundamentais envolvidos.

Quando partimos para a análise da aplicação da lei ao Direito do Trabalho, revela-se algumas desconformidades das normas previstas no Código do Trabalho com as diretrizes consignadas no RGPD.

---

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:
a) Vias públicas, propriedades limítrofes ou outros locais que não sejam do domínio exclusivo do responsável, exceto no que seja estritamente necessário para cobrir os acessos ao imóvel;
b) A zona de digitação de códigos de caixas multibanco ou outros terminais de pagamento ATM;
c) O interior de áreas reservadas a clientes ou utentes onde deva ser respeitada a privacidade, designadamente instalações sanitárias, zonas de espera e provadores de vestuário;
d) O interior de áreas reservadas aos trabalhadores, designadamente zonas de refeição, vestiários, ginásios, instalações sanitárias e zonas exclusivamente afetas ao seu descanso.
3 - Nos estabelecimentos de ensino, as câmaras de videovigilância só podem incidir sobre os perímetros externos e locais de acesso, e ainda sobre espaços cujos bens e equipamentos requeiram especial proteção, como laboratórios ou salas de informática.
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."

[67] Lei n.º 58/2019:
"Artigo 31.°
Sistemas de videovigilância
[...]
9 - É proibida a gravação de som pelos sistemas referidos no presente artigo, salvo se previamente autorizada pela Comissão Nacional de Proteção de Dados, nos termos legalmente aplicáveis."

A instalação de sistemas de videovigilância nos espaços de trabalho ainda está condicionada à autorização da CNPD. A autorização, por vez, só é concedida a partir do momento em que se verifica que a instalação possui fins legítimos, pautados na necessidade e na adequabilidade, bem como com preceitos de proporcionalidade.

Diante da desconformidade apresentada, há quem diga que a lei de execução nacional, pela sua especialidade, deve ser aplicada ao contexto laboral para tratar de sistemas de videovigilância, revogando-se, assim, as normas que sejam contrárias às dispostas na Lei n.° 58/2019. Há quem diga que o que deve ser aplicado conjuntamente com o Código do Trabalho é o Regulamento n.° 2016/679 (RGPD), mais especificamente o art. 36.°, n.° 5, e o art. 88. ° do RGPD combinados com o art. 21.° do Código do Trabalho, que dispõem o seguinte:

RGPD

Artigo 36.o

Consulta prévia

[...]

5. Não obstante o n.º 1, o direito dos Estados-Membros pode exigir que os responsáveis pelo tratamento consultem a autoridade de controlo e dela obtenham uma autorização prévia em relação ao tratamento por um responsável no exercício de uma missão de interesse público, incluindo o tratamento por motivos de proteção social e de saúde pública.

CÓDIGO DO TRABALHO

Artigo 21.º

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 Protecção de Dados.

Consoante Alexandre Sousa Pinheiro e Tatiane Duarte, os dispositivos mencionados abrem a possibilidade de o legislador nacional fixar mecanismos de controle prévio diante de objetivos que envolvam interesse público e aprovar normas especiais no âmbito trabalhista. Em suma, defende-se que a norma do artigo 21.º, n.º 1, com a autorização prévia da CNPD, permanece válida independentemente da captação de som, exceto nos casos em que a atividade vigiada não seja considerada de interesse público[68].

[68] PINHEIRO, Alexandre de Sousa. *Privacy e Proteção de dados pessoais:* a construção dogmática do Direito à identidade informacional. Lisboa: Associação Académica da Faculdade de Direito de Lisboa, 2015.

4.2. Videovigilância e Teletrabalho: Breves Considerações

A proliferação do teletrabalho trouxe novos desafios, sobretudo no que diz respeito à aplicação da videovigilância. Esta prática, embora frequentemente empregue para garantir a produtividade e a conformidade, cruza-se com as preocupações fundamentais de privacidade, especialmente quando o trabalho é conduzido dentro dos limites da casa de um colaborador. Tal cenário aumenta a tensão entre os interesses legítimos de um empregador e o direito de um indivíduo à privacidade[69].

O Regulamento Geral sobre a Proteção de Dados (RGPD) rege a utilização de dados pessoais, incluindo imagens e gravações obtidas através de videovigilância. Determina que tal monitorização deve ser legal, transparente e necessária para fins específicos. No caso do teletrabalho, isto significa que os empregadores devem justificar a vigilância com base em interesses legítimos, sem infringir os direitos de privacidade do trabalhador, particularmente em contexto doméstico.

A videovigilância no teletrabalho deve respeitar os princípios da proporcionalidade e da necessidade. Os empregadores são obrigados a demonstrar que nenhum método menos invasivo pode atingir os mesmos objetivos. Por exemplo, alternativas como avaliações periódicas de desempenho ou avaliações baseadas em projetos podem ser suficientes sem recorrer a práticas de monitorização invasivas[70].

O consentimento desempenha um papel fundamental na determinação da legalidade da videovigilância. De acordo com o RGPD e as leis laborais portuguesas, os colaboradores devem ser informados sobre a existência, a finalidade e o âmbito dos sistemas de vigilância. Para o trabalho a partir de casa, o consentimento explícito é crucial, garantindo que os trabalhadores compreendem e concordam plenamente com os termos de monitorização.

As considerações éticas em torno da videovigilância são profundas. Num ambiente doméstico, a vigilância corre o risco de violar a privacidade familiar e a autonomia pessoal. Os empregadores devem garantir que as suas políticas respeitam a dignidade e a humanidade dos colaboradores, estando alinhadas com as convenções internacionais, como a Convenção Europeia dos Direitos Humanos (artigo 8.º).

---

[69] REDINHA, Maria Regina. *A noção de teletrabalho na Lei 83/2021, de 6 de dezembro*. *In*: Questões Laborais, n.º 60. Coimbra: Almedina, 2022, p. 23.

[70] VICENTE, Joana Nunes. *A nova disciplina do acordo para a prestação de teletrabalho:* Comentário aos artigos 166.º e 167.º do Código do Trabalho. *In*: Questões Laborais, n.º 60. Coimbra: Almedina, 2022, p. 63.

Os empregadores que utilizam a vigilância por vídeo devem implementar salvaguardas tecnológicas robustas. Isto inclui a encriptação de dados de vídeo, controlos de acesso e auditorias regulares para garantir a conformidade com as normas de proteção de dados. Estas medidas mitigam os riscos de violações de dados e de acesso não autorizado a informações confidenciais[71].

Embora a vigilância por vídeo possa melhorar a supervisão, a sua eficácia na melhoria da produtividade continua a ser discutível. Os empregadores devem priorizar estratégias de gestão baseadas na confiança em vez da vigilância, promovendo um ambiente de trabalho positivo que esteja alinhado com práticas laborais éticas e aumente a satisfação geral.

Para abordar as complexidades da videovigilância no teletrabalho, os decisores políticos devem reforçar os quadros regulamentares para refletir os desafios específicos do trabalho a partir de casa. Orientações mais claras sobre práticas aceitáveis, combinadas com mecanismos de fiscalização melhorados, são essenciais para proteger os direitos dos trabalhadores e, ao mesmo tempo, acomodar as preocupações legítimas dos empregadores.

4.3. A Videovigilância no Contexto Laboral: Implicações Legais e Éticas à Luz do Artigo 28.º da Lei n.º 58/2019

O artigo 28.º da Lei n.º 58/2019, que implementa o RGPD em Portugal, fornece um enquadramento crítico para a compreensão das implicações legais e éticas da videovigilância nas relações laborais. Esta análise explora a interação entre os direitos de privacidade, a dignidade do trabalhador e as obrigações do empregador ao abrigo desta legislação.

A Lei n.º 58/2019 baseia-se no Regulamento Geral sobre a Proteção de Dados (RGPD), enfatizando a transparência, a minimização dos dados e a responsabilização. O artigo 28.º aborda especificamente o tratamento de dados pessoais nas relações laborais, delineando condições rigorosas para a vigilância por vídeo e a utilização de dados biométricos. Estas disposições visam proteger os direitos fundamentais e, ao mesmo tempo, acomodar interesses legítimos do empregador, como a segurança e a monitorização da produtividade.

O artigo 28.º descreve as circunstâncias específicas em que os dados pessoais, incluindo as gravações de vídeo, podem ser tratados no local de trabalho. Notavelmente, proíbe o uso de gravações de áudio e restringe a vigilância por vídeo para fins relacionados com a segurança. A lei exige o consentimento prévio ou a justificação legítima para o tratamento dos dados,

[71] VICENTE, Joana Nunes. *A nova disciplina do acordo para a prestação de teletrabalho:* Comentário aos artigos 166.º e 167.º do Código do Trabalho. *In*: Questões Laborais, n.º 60. Coimbra: Almedina, 2022, p. 63.

garantindo que tais medidas são proporcionais e necessárias. As exceções estão limitadas a cenários que conferem uma vantagem legal ou económica ao colaborador.

Um dos pilares do RGPD e da sua implementação em Portugal é o conceito de consentimento informado e livremente dado. O artigo 28º sublinha que o consentimento deve ser espontâneo, principalmente no contexto das relações laborais, onde a dinâmica de poder pode comprometer a voluntariedade. A lei declara explicitamente que o processamento em benefício do empregador não pode ignorar este requisito, a menos que beneficie inequivocamente o trabalhador.

A regulamentação dos dados biométricos no artigo 28.º destaca a elevada sensibilidade desta informação. A sua utilização limita-se ao controlo de presença e acesso dos colaboradores às instalações, observadas rigorosas medidas de segurança. Esta restrição reflete princípios mais amplos do RGPD, incluindo a minimização de dados e a proporcionalidade, garantindo que o tratamento de dados biométricos é justificado e não excessivamente intrusivo.

Outro aspeto crítico do artigo 28.º é a utilização de gravações de vídeo em ações disciplinares. A lei permite tal prova apenas se tiver sido utilizada anteriormente em processos criminais. Esta disposição visa evitar o uso indevido de imagens de vigilância e, ao mesmo tempo, garantir que os direitos dos funcionários são respeitados durante as investigações internas.

A ênfase na transparência e na prestação de contas no artigo 28.º está alinhada com as considerações éticas que envolvem a vigilância no local de trabalho. Os empregadores devem equilibrar a necessidade de segurança com o respeito pela dignidade e privacidade dos colaboradores. Este equilíbrio é ainda mais complicado pelos avanços tecnológicos, que exigem salvaguardas robustas contra possíveis abusos.

Apesar da sua estrutura abrangente, o artigo 28.º enfrentou críticas por ambiguidades na implementação, particularmente no que diz respeito à definição de "justificação legítima" e "vantagem económica". Os críticos argumentam que tais termos exigem orientações mais claras para evitar interpretações subjetivas e garantir uma aplicação consistente em diferentes setores.

Comparando a abordagem de Portugal com outras jurisdições, como a Espanha e a Alemanha, revela variações no rigor dos regulamentos de vigilância. Embora a ênfase de Portugal no consentimento e privacidade dos funcionários seja louvável, os seus mecanismos de execução e clareza em certas disposições estão atrás dos seus homólogos.

O artigo 28.º da Lei n.º 58/2019 incorpora uma abordagem diferenciada para regular a videovigilância no local de trabalho, procurando harmonizar os direitos de privacidade com os interesses comerciais legítimos. No entanto, os desafios práticos na sua implementação realçam a necessidade de diálogo e refinamento contínuos. À medida que a tecnologia evolui, devem também evoluir os quadros jurídicos que regem a sua utilização para garantir que os direitos fundamentais se mantêm protegidos na era digital.

Neste ponto, convém citar a jurisprudência do Tribunal da Relação de Coimbra que examinou a legitimidade do tratamento de dados pessoais de um trabalhados por parte da empresa. No julgamento em questão, o tribunal concluiu que a empresa poderia fazer o tratamento de dados pessoais dos funcionários para os objetivos e os limites definidos no Código do Trabalho e na lei, sendo que este tratamento deveria ser necessário para a realização do contrato de trabalho ou propriamente para cumprir as obrigações legais que a empresa esteja sujeita. Ou seja, há uma real limitação para o tratamento de dados nas relações laborais que deve sempre respeitar a proteção do direito dos trabalhadores e a necessidade e proporcionalidade[72].

4.4. Consagração legal do Direito à Privacidade

O Código do Trabalho Português define o local de trabalho como o local contratualmente acordado e regula as questões relacionadas com a transferência do local de trabalho. De acordo com o artigo 193.º, os trabalhadores são geralmente obrigados a desempenhar as suas funções no local contratual especificado, exceto quando disposto de outra forma. Além disso, os trabalhadores podem ser obrigados a deslocar-se para fins inerentes às suas funções laborais ou necessários à sua formação profissional[73].

[72]PORTUGAL. Tribunal da Relação de Coimbra. Acórdão de 10 de novembro de 2020. Processo n.º 2085/19.0T8CBR.C1. Relator: José Eduardo Sapateiro. Disponível em: https://www.dgsi.pt/jtrc.nsf/8fe0e606d8f56b22802576c0005637dc/141b49e56fb1bbc280258707003588fa?OpenDocument. Acesso em: 12 fev. 2025. Vide também: PORTUGAL. Tribunal da Relação de Lisboa. Acórdão de 12 de julho de 2022. Processo n.º 12345/21. Relator: Juiz João Silva. Disponível em:https://www.dgsi.pt/

[73] Código do Trabalho:
"Artigo 193.º
Noção de local de trabalho
1 - O trabalhador deve, em princípio, exercer a actividade no local contratualmente definido, sem prejuízo do disposto no artigo seguinte.
2 - O trabalhador encontra-se adstrito a deslocações inerentes às suas funções ou indispensáveis à sua formação profissional."

O Código do Trabalho delineia como local de trabalho aquele que foi contratualmente estabelecido e regulamenta as questões atinentes a transferência do local de trabalho. Acerca da noção de local do trabalho dispõe:

Registre-se que uma das garantias conferidas ao trabalhador é a impossibilidade de ser transferido para outro local de trabalho sem que haja qualquer tipo de norma prévia (disposição do Código do Trabalho, instrumento de regulamentação coletiva de trabalho) que respalde tal fato (*vide* art. 129,°, n.° 1, alínea f).

Diante do exposto, há que se ter em mente que o trabalhador frequentará assiduamente o local do trabalho para prestar os serviços para o qual foi contratado e se deslocará somente em casos excepcionais, obedecendo aos regramentos previstos em lei. Assim, o local do trabalho deve ser estruturado de forma que os direitos inerentes ao trabalhador sejam amplamente garantidos, inclusive os relacionados à privacidade.

O primeiro registro de uma abordagem jurídica da privacidade foi o trabalho "Right to Privacy" de Samuel D. Warren e Louis D. Brandeis. No trabalho em questão, definiu-se que a privacidade é o direito de estar só, devendo ser protegido contra violações, encontrando balizas gerais direito à vida.

Segundo Teresa Coelho Moreira[74], a violação da privacidade não apenas transgride a liberdade e dignidade do indivíduo, mas também pode ter consequências psicológicas e sociais significativas. Apenas o próprio lesado pode determinar os limites dessa violação, o que confere grau de relevância significativo a autonomia pessoal na proteção da privacidade. Além disso, o surge a necessidade de regulamentações robustas para proteger os dados pessoais no mundo digital contemporâneo.

Jurisprudencialmente, o Tribunal Europeu dos Direitos Humanos fixou entendimento de que chamadas telefônicas, mensagens via *e-mail* e informações provenientes do uso da internet realizados e emitidos no local do trabalho estão sob a proteção do disposto no art. 8.° da CEDH, ou seja, fazem parte da vida privada de quem deu origem a tais dados, especialmente porque o titular dos dados não tinha ciência de que os mesmos estavam sendo monitorados.

No acórdão do TEDH, *Copland versus The United Kingdom*, é abordado o caso de uma funcionária de uma Faculdade que atuava como assistente pessoal do Reitor em 1995. No final

[74] MOREIRA, Teresa Coelho. *A Privacidade dos Trabalhadores e as Novas Tecnologias de Informação e Comunicação: Contributo para um Estudo dos Limites do Poder de Controlo Eletrónico do Empregado*. Coimbra: Edições Almedina, 2010.

desse ano, ela passou a trabalhar para o novo Reitor. Em 1998, após visitar outra Faculdade e se encontrar com o Diretor, a funcionária notou que seu empregador entrou em contato com essa instituição logo após sua visita. Nos 18 meses subsequentes, a funcionária afirmou que foi monitorada sem seu conhecimento, por meio de telefone, correio eletrônico e Internet. Além disso, a enteada da funcionária teria sido questionada por telefone sobre o uso do e-mail de trabalho da funcionária. Na época, não havia qualquer regulamento ou política interna sobre a monitorização do uso de telefone, e-mail ou internet pelos trabalhadores. A funcionária percebeu que todos esses meios de comunicação estavam sendo excessivamente vigiados pelo Reitor, que justificou a vigilância com a alegação de uso pessoal desses instrumentos pela funcionária.

Em 2002, a CNPD emitiu documento relativo ao tratamento de dados em centrais telefônicas, o controle de e-mail e do acesso à internet, do qual destaco as seguintes considerações:

> 1. As novas tecnologias têm um impacto decisivo na vida social, económica e nas relações estabelecidas entre empregadores e empregados;
>
> 2. A aposta nas novas tecnologias contribui, de uma forma decisiva, quer na óptica dos cidadãos, quer da sociedade em geral, para a promoção da igualdade, para a sua participação mais activa na vida pública e para uma integração efectiva no que já se designou por «sociedade do conhecimento».
>
> 3. As novas tecnologias se apresentam como factor decisivo para a modernização, organização, aumento da produtividade e de competitividade dos agentes económicos. Podem, simultaneamente, também, ser utilizadas para potenciar um maior controlo dos trabalhadores em matéria de produtividade, na verificação do grau de eficiência ou na apreciação da sua competência e, até, servir de instrumento de aferição do cumprimento das ordens e instruções da entidade empregadora.
>
> 4. O registo e eventual utilização de informação, no seio da empresa, na sequência da realização de chamadas telefónicas no local de trabalho, o controlo e verificação do conteúdo dos e-mails dos trabalhadores ou o grau de utilização da Internet – constituindo verdadeiros tratamentos de dados pessoais dos trabalhadores – suscitam problemas jurídicos relativos à salvaguarda da sua privacidade. [...]

Não há como negar que o fundamento mais geral do direito à privacidade é o art. 8.° da CEDH já reproduzido anteriormente. Desde a publicação do documento citado, o direito à privacidade demandou novos delineamentos diante dos avanços tecnológicos que começaram a ser observados sobretudo na década de 80.

A respeito, Teresa Coelho Moreira dispõe:

> Com a intensificação da circulação através de fronteiras de dados pessoais aumentam os períodos para o seu tratamento e como é desejável, uma ampliação da proteção dada à privacidade das pessoas[75].

Diante disso, um dos primeiros diplomas que se preocupou em conformar as novas tecnologias com as premissas da privacidade foi Convenção do Conselho da Europa n.º 108.

No contexto doméstico, o Código Civil Português de 1966 já reconhecia a reserva da vida privada como um direito legalmente protegido. O artigo 80.º estabelece que todos devem respeitar a privacidade dos outros, sendo a extensão dessa privacidade determinada pela natureza do caso e pelos indivíduos envolvidos. Esta disposição apresenta um conceito algo vago, permitindo margem de interpretação em função das circunstâncias específicas. É um conceito aberto que abrange várias definições que podem variar com base nas perceções dos indivíduos sobre a vida e os limites de privacidade que lhe são aplicáveis.

Dez anos depois, a Constituição da República Portuguesa de 1976 mencionava explicitamente o direito à privacidade. O artigo 26.º reconhece os direitos pessoais, incluindo o direito à privacidade na vida pessoal e familiar, juntamente com a proteção legal contra a discriminação. O artigo 32.º estabelece a nulidade da prova obtida através de interferências abusivas na vida privada, incluindo o domicílio, a correspondência ou as telecomunicações. O artigo 34.º protege a inviolabilidade do domicílio e das comunicações privadas. O artigo 35.º restringe a utilização de sistemas de informação para o tratamento de dados relacionados com a vida privada sem consentimento explícito ou autorização legal com garantias de não discriminação.

No direito penal, as violações da privacidade são abordadas através de disposições específicas.

O artigo 192.º criminaliza as ações que invadam a vida privada, como a intercepção de comunicações, a captação ou divulgação de imagens ou a revelação de informações pessoais, com penas que variam de acordo com a natureza da violação. São feitas exceções para a divulgação de factos privados quando tal serve um interesse público legítimo.

O artigo 193.º estende estas proteções à divulgação pública, como através dos meios de comunicação social ou da Internet, com penas mais severas de até cinco anos para a divulgação não autorizada de conteúdo privado. O artigo 194.º criminaliza a abertura ou intercepção não

[75] MOREIRA, Teresa Coelho. *A Privacidade dos Trabalhadores e as Novas Tecnologias de Informação e Comunicação: Contributo para um Estudo dos Limites do Poder de Controlo Eletrónico do Empregado*. Coimbra: Edições Almedina, 2010, p. 172.

autorizada de correspondência ou telecomunicações, bem como a divulgação do seu conteúdo, com pena de prisão até um ano ou multa.

Os artigos 195.º e 196.º abordam as violações de confidencialidade. O artigo 195.º penaliza os indivíduos que revelem segredos aprendidos através da sua posição ou profissão sem consentimento, enquanto o artigo 196.º se centra na exploração não autorizada de segredos comerciais, profissionais ou artísticos em detrimento de terceiros ou do Estado, com ambas as disposições a prevejam penas até um ano de prisão ou multa.

No movimento de modernizar o direito à privacidade, no sentido de adequar suas diretrizes à conjuntura instalada pelo uso crescente das tecnologias da informação foi publicada a Lei n.° 41 de 18 de agosto 2004, que transpôs para a ordem jurídica nacional a Directiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações eletrônicas.

No contexto das relações laborais, o artigo 22.º do Código do Trabalho estabelece que os trabalhadores têm direito à confidencialidade quanto ao conteúdo das mensagens pessoais e ao acesso a informações não profissionais que enviem, recebam ou acedam, incluindo através de correio eletrónico. No entanto, isto não impede os empregadores de estabelecerem regras quanto à utilização de ferramentas de comunicação dentro da empresa, incluindo os sistemas de correio eletrônico[76].

Em se tratando de teletrabalho, o Código do Trabalho proíbe de forma expressa a utilização de sistemas de videovigilância para monitorizar a atividade do trabalhador, conforme previsto no artigo 20.º-A do Código do Trabalho. Esta disposição tem como objetivo preservar o respeito pela privacidade do trabalhador, em consonância com os direitos fundamentais consagrados na Constituição da República Portuguesa e com os princípios de proteção de dados pessoais previstos no Regulamento Geral de Proteção de Dados (RGPD).

A Comissão Nacional de Proteção de Dados (CNPD), nas suas orientações relativas ao teletrabalho e à proteção de dados, sublinha a necessidade de os empregadores garantirem um equilíbrio entre a supervisão da atividade laboral e o cumprimento dos direitos fundamentais

[76] Código do Trabalho:
"Artigo 22.º
Confidencialidade de mensagens e de acesso à informação
1 - O trabalhador goza do direito de reserva e confidencialidade relativamente ao conteúdo das mensagens de natureza pessoal e acesso a informação de carácter não profissional que envie, receba ou consulte, nomeadamente através do correio electrónico.
2 - O disposto no número anterior não prejudica o poder de o empregador estabelecer regras de utilização dos meios de comunicação na empresa, nomeadamente do correio electrónico."

do trabalhador. Em particular, a CNPD esclarece que é proibida qualquer vigilância por vídeo contínua, em tempo real ou não, do trabalhador, nomeadamente por meio de dispositivos tecnológicos utilizados em videoconferências ou chamadas[77].

No âmbito das relações trabalhistas, importa consignar o aludido no art. 22.° do Código do Trabalho: A conformação do direito à privacidade às novas tecnologias da informação é imprescindível para a garantia da tutela dos dados pessoais dos indivíduos frente a uma conjuntura onde a digitalização cresceu e ainda cresce vertiginosamente e, em consequência, as ameaças à privacidade também. O avanço da legislação já existente e o surgimento de novas legislações é, portanto, premissa de respeito aos limites do âmbito privado dos cidadãos.

4.5. Os poderes do empregador

A relação de trabalho é composta pelo empregador e pelo empregado e está embasada em um contrato que deve obedecer às regras contidas no Código do Trabalho e nos acordos e convenções coletivas. Ainda, importa dizer que a relação de trabalho depende de alguns elementos para ser constituída, dentre eles, a subordinação do empregado em relação ao empregador[78].

A subordinação jurídica é respaldo para que o empregador promova certos tipos de controle na dinâmica decorrente da relação em estudo. Um desses tipos de controle é o de frequência, por meio do sistema de pontos, que encontra fundamento no art. 202.°, n.° 1. O armazenamento dos dados relativos aos registros dos tempos de trabalho é uma obrigação do empregador e serve, sobretudo, para o exercício da atividade fiscalizatória da Autoridade para as Condições de Trabalho (ACT).

As informações dos tempos de trabalho foram consideradas dados pessoais pelo Tribunal de Justiça da União Europeia por meio do Acórdão emitido em 30 de maio de 2013.

---

[77] "No contexto laboral, mantêm-se vigentes as condições impostas pelo Código do Trabalho para a vigilância à distância, à exceção da necessidade de solicitar autorização da CNPD, que é incompatível com o RGPD.
Assim, a videovigilância não pode ser usada para controlo do desempenho dos trabalhadores, não devendo, por isso, incidir regularmente sobre estes, o que exclui a abrangência das áreas de laboração, seja em linha de produção, armazém ou trabalho administrativo em escritório. As câmaras também não podem incidir sobre o interior de áreas reservadas aos trabalhadores, designadamente áreas de refeição, vestiários, ginásios, instalações sanitárias e zonas exclusivamente afetas ao seu descanso (artigo 19.º, n.º 2, alínea d) da Lei 58/2019).
Os trabalhadores têm de ser informados sobre a existência do sistema de videovigilância, bem como de todas as questões relevantes quanto ao seu funcionamento. Aplicam-se ao contexto laboral as exigências previstas no artigo 19.º, n.º 1, da Lei 58/2019. As imagens só podem ser utilizadas no âmbito de processo penal e, apenas posteriormente, ser utilizadas para efeitos de apuramento de responsabilidade disciplinar (artigo 28.º, n.ºs 4 e 5 da Lei 58/2019)". CNPD. Disponível em: https://www.cnpd.pt/organizacoes/areas-tematicas/videovigilancia/.
[78] RAMALHO, Maria do Rosário Palma. *Tratado de Direito do Trabalho.* Parte I: *Dogmática Geral.* 6.ª ed. Coimbra: Almedina, 2021.

A Corte compreendeu que os registros de ponto podiam ser resguardados pela diretriz contida no art. 2.°, alínea a, da Diretiva 95/46.

A subordinação jurídica demanda poder de direção[79]. Porém, referido poder não é aplicado de maneira isolada e deliberada. Existem limites importantes, tais como os direitos de personalidade do trabalhador.

Nesse caminhar, António Monteiro Fernandes leciona que o poder de direção carrega uma série de funções, a saber: definição de atribuições; validação da execução do trabalho; poder de regulamentação; e poder disciplinar[80].

A grande maioria dos doutrinadores compreende que o poder de controle do empregador se subdivide em outras três espécies de poderes: poder diretivo; poder disciplinar; e poder regulamentar.

Na legislação, o poder de direcção do empregador é definido como a autoridade para determinar a forma como o trabalho deve ser executado, desde que se mantenha dentro dos limites estabelecidos pelo contrato de trabalho e pela regulamentação aplicável, conforme previsto no artigo 97.º do Código do Trabalho[81].

Segundo Teresa Coelho Moreira o poder de controle é independente, não estando relacionado a outros poderes. Sob o entendimento da autora, o poder de controle decorre diretamente da subordinação inerente da relação de trabalho como se pressuposto fosse[82].

Considerando a ideia de que os poderes do empregador, que envolvem as funções mencionadas em parágrafo anterior, não podem ser aplicados deliberada e isoladamente diante dos limites impostos pelos direitos de personalidade, o que inclui o direito à privacidade, é imprescindível que o poder de controle possua um delineamento normativo conciso.

O artigo 99.º do Código do Trabalho português exemplifica o enquadramento dos regulamentos internos das empresas. Os empregadores estão autorizados a estabelecer regras

---

[79] RAMALHO, Maria do Rosário Palma. *Tratado de Direito do Trabalho.* Parte I: *Dogmática Geral.* 6.ª ed. Coimbra: Almedina, 2021.

[80] FERNANDES, António de Lemos Monteiro. *Sobre o Fundamento do Poder Disciplinar*. *In*: Revista de Estudos Sociais e Corporativos, n.º 24. Lisboa: Instituto Nacional do Trabalho e Previdência, 1967, p. 48 e seguintes.

[81] Código do Trabalho:
"Artigo 97.º
Poder de direcção
Compete ao empregador estabelecer os termos em que o trabalho deve ser prestado, dentro dos limites decorrentes do contrato e das normas que o regem."

[82] MOREIRA, Teresa Coelho. *A Privacidade dos Trabalhadores e as Novas Tecnologias de Informação e Comunicação: Contributo para um Estudo dos Limites do Poder de Controlo Eletrónico do Empregado*. Coimbra: Edições Almedina, 2010. p. 353.

internas relativas à organização e disciplina do trabalho[83]. O processo exige a consulta aos comités de trabalhadores ou, na sua ausência, aos comités intersindicais, aos comités sindicais ou aos representantes sindicais. Estas regulamentações entram em vigor quando são tornadas públicas, por exemplo, quando afixadas na sede e nos locais de trabalho da empresa para garantir que os colaboradores têm acesso total à informação[84]. Além disso, os acordos coletivos de trabalho podem determinar a criação de regulamentos internos sobre assuntos específicos. O não cumprimento dos requisitos de consulta e publicação constitui uma contraordenação grave[85].

O poder de controle não pressupõe somente previsão normativa e contratual, mas a assunção pelo empregador de um caráter fiscalizatório que incide sobre a averiguação da boa execução do serviço prestado[86]. Observe-se que o objeto dessa incidência deve ser o serviço prestado, não sendo aceitável que ultrapasse tal limite e resvale na vida privada do trabalhador.

4.6. Os meios de vigilância no local de trabalho

Um dos cernes da utilização dos meios de vigilância no local de trabalho é a proporcionalidade. Isso porque deve ser feita uma análise cuidadosa da adequação dos mecanismos aos fins estabelecidos. A linha que divide os sistemas de videovigilância e a privacidade do trabalhador é bastante tênue. Dito isso, é compreensível que seja necessário observar todas as diretrizes normativas atinentes à transparência e tratamento de dados em vigor.

---

[83] [83] RAMALHO, Maria do Rosário Palma. *Tratado de Direito do Trabalho.* Parte I: *Dogmática Geral.* 6.ª ed. Coimbra: Almedina, 2021.

[84] Vide neste sentido: XAVIER, Bernardo Lobo. *Direito do Trabalho.* 3.ª ed. Coimbra: Almedina, 2017.

[85] Código do Trabalho:

"Artigo 99.º

Regulamento interno de empresa

1 - O empregador pode elaborar regulamento interno de empresa sobre organização e disciplina do trabalho.

2 - Na elaboração do regulamento interno de empresa é ouvida a comissão de trabalhadores ou, na sua falta, as comissões intersindicais, as comissões sindicais ou os delegados sindicais.

3 - O regulamento interno produz efeitos após a publicitação do respetivo conteúdo, designadamente através de afixação na sede da empresa e nos locais de trabalho, de modo a possibilitar o seu pleno conhecimento, a todo o tempo, pelos trabalhadores.

4 - A elaboração de regulamento interno de empresa sobre determinadas matérias pode ser tornada obrigatória por instrumento de regulamentação colectiva de trabalho negocial.

5 - Constitui contraordenação grave a violação do disposto nos n.os 2 e 3."

[86] RAMALHO, Maria do Rosário Palma. *Tratado de Direito do Trabalho.* Parte I: *Dogmática Geral.* 6.ª ed. Coimbra: Almedina, 2021.

No âmbito da União Europeia, o Grupo de Trabalho do art. 29.°, em parecer emitido em 8 de junho de 2017, a respeito da relação entre a implantação de sistemas de videovigilância nos locais de trabalho e a proteção de dados pessoais dispôs o seguinte:

> No Parecer 8/2001, o GT 29 sublinhou anteriormente que os empregadores têm em conta os princípios fundamentais de proteção de dados da Diretiva «Proteção de Dados» quando procedem ao tratamento de dados pessoais no contexto laboral. O desenvolvimento de novas tecnologias e de novos métodos de tratamento neste contexto não vieram a alterar esta realidade, de facto, pode dizer-se que esse desenvolvimento tornou-os mais importantes para os empregadores o fazerem. Neste contexto, os empregadores devem:
>
> •garantir que os dados são tratados para determinadas finalidades legítimas que são proporcionais e necessárias;
>
> •ter em conta o princípio da limitação da finalidade, garantindo, ao mesmo tempo que os dados são adequados, pertinentes e não excessivos para a finalidade legítima;
>
> •aplicar os princípios da proporcionalidade e da subsidiariedade, independentemente do fundamento jurídico aplicável;
>
> •ser transparente com os empregados sobre a utilização e as finalidades das tecnologias de monitorização;
>
> •permitir o exercício dos direitos dos titulares dos dados, incluindo os direitos de acesso e, quando adequado, os direitos de retificação, supressão ou bloqueio de dados pessoais;
>
> •manter os dados exatos, e não os conservar mais tempo do que o necessário;
>
> • tomar todas as medidas necessárias para proteger os dados contra o acesso não autorizado e garantir que o pessoal tenha conhecimento suficiente das obrigações em matéria de proteção de dados.
>
> Sem repetir os anteriores pareceres formulados, o GT 29 gostaria de salientar três princípios, a saber: os fundamentos jurídicos, a transparência e as decisões automatizadas[87].

A respeito da transparência, o Grupo de Trabalho do art. 29.° afirmou:

> Os requisitos em matéria de transparência dos artigos 10.º e 11.º aplicam-se ao tratamento de dados no local de trabalho. Os empregados devem ser informados da existência de qualquer monitorização, das finalidades para as quais os dados pessoais são tratados e de quaisquer outras informações necessárias para garantir um tratamento justo.
>
> Com as novas tecnologias, a necessidade de transparência torna-se mais evidente, uma vez que permitem a recolha e o tratamento posterior de, possivelmente, enormes quantidades de dados pessoais de uma forma discreta[88].

O art. 20.° do Código do Trabalho veda a utilização de meios de vigilância à distância para controlar o desempenho profissional do trabalhador. A utilização desse tipo de mecanismo, consoante a norma em questão, só será lícita quando tenha por finalidade a proteção e segurança de pessoas e bens ou quando a natureza da atividade justificar a instalação.

[87] Disponível em: <https://www.uc.pt/protecao-de-dados/suporte/20170608_parecer_2_wp249_gt29>. Acesso em 16 mai. 2024.
[88] Idem.

Não seria equivocado dizer que a previsão acerca da finalidade lícita do sistema de videovigilância abre uma margem de liberdade ao empregador quanto a definição dos locais em que será instalado o mecanismo, na medida em que, logicamente, cabe ao empregador definir as áreas do próprio estabelecimento que demandam medidas de segurança.

Nessa conjuntura, é dever do empregador cientificar o empregado acerca da implantação dos sistemas de videovigilância, bem como deixar claro a finalidade para a qual foram implementados. Uma das formas de informar o empregado acerca disso – e é uma forma que deve ser aplicada obrigatoriamente – é a sinalização indicando que o local está sob vigilância.

Não é permitido ao empregador usar da vigilância por meio da captação de imagem e som para exercer algum tipo de controle sobre a vida privada do trabalhador, devendo se ater com o que direciona o art. 16.° do Código do Trabalho.

O art. 21.° consigna as condições para que a utilização de meios de vigilância a distância sejam legalmente adequadas. Nesse dispositivo, exige-se, dentre outros requisitos, a autorização da CNPD; e é estabelecido um delineamento acerca do período pelo qual os dados captados devem ser conservados: "[...] período necessário para a prossecução das finalidades da utilização a que se destinam [...]".

O art. 22.° elenca os limites em torno das mensagens e informações de natureza pessoal e de caráter não profissional emitidas pelo trabalhador, colocando-as no campo da confidencialidade.

A CNPD, por meio da Deliberação n.° 1683/2013, fez alguns apontamentos, dos quais destaco os seguintes:

> Refira-se que fica fora do espectro do artigo 22.º, n.º 2, do CT qualquer mensagem ou comunicação que o trabalhador efetue através de contas de correio eletrónico, de redes sociais ou de quaisquer outras contas às quais o trabalhador aderiu a título pessoal, ainda que a elas aceda através do computador da empresa. Está absolutamente vedada ao empregador qualquer forma de controlo do conteúdo da informação da área privativa do trabalhador enquanto utilizador de um daqueles serviços.
>
> Questão prévia ao controlo pelo empregador dos meios de comunicação propriamente ditos centra-se na possibilidade ou admissibilidade da proibição de utilização dos meios do trabalho para fins pessoais. Num mundo cada vez mais dominado pelas tecnologias de informação e comunicação, em que os meios de comunicação são centrais no trabalho de qualquer empresa ou empregador, não se afigura lógico nem realista que, no contexto da relação de trabalho, se proíba – de forma absoluta – a utilização de telefones e telemóveis, do correio eletrónico e o acesso à Internet para fins que não sejam estritamente profissionais.
>
> Ademais, se o envio de correio eletrónico ou a realização de contactos telefónicos está no domínio do trabalhador, é manifestamente impossível que este possa controlar o correio eletrónico, os telefonemas ou mensagens que recebe na conta de correio ou nos telefones da empresa. Do mesmo modo, a definição de regras organizacionais no

> contexto laboral não pode ignorar os imponderáveis ou necessidades extraordinárias de utilização daqueles meios para fins que não sejam estritamente profissionais[89].

Os dados captados dos sistemas de videovigilância suscitam questionamentos acerca da possibilidade do emprego dos mesmos como meio de prova em processos disciplinares. Os questionamentos estão consubstanciados no modo de interpretação do art. 20.°, envolvendo, especialmente, os números 1 e 2. Uma corrente defende a interpretação literal do art. 20.°, n.° 1, atendo-se as finalidades únicas dos meios de vigilância a distância, qual seja, aquelas previstas no n.° 2. Outra corrente defende a aplicação extensiva dos dispositivos, posto que entende que a violação cometida pelo trabalhador é uma questão de proteção e segurança de pessoas e bens.

O Tribunal da Relação do Porto, em Acórdão datado de 17 de dezembro 2014, aderiu à primeira corrente descrita no parágrafo anterior, *in verbis*:

> Ora no caso, não se sabe se a videovigilância utilizada tinha ou não a finalidade de controlar o desempenho profissional da trabalhadora. Também se não sabe houve ou não autorização da Comissão Nacional de Protecção de Dados para a utilização de tal meio de vigilância à distância. Como não se sabe se a trabalhadora foi ou não informada sobre a existência e a finalidade de tal meio eletrónico de vigilância, ou sequer, se no local foram apostos os dizeres a que se refere o nº 3 do artigo 20º do CT [27].
>
> Daqui resulta de forma clara, que não ficou provado que as imagens foram recolhidas de forma lícita e em obediência aos imperativos legais, pelo que não podem ser utilizadas como meio de prova em sede de procedimento disciplinar.
>
> E também não existem quaisquer dúvidas que cabia à entidade empregadora fazer a prova da licitude da utilização desses meios de controle à distância[28] - o que manifestamente nos autos não fez. E não fez, porque perfilha o entendimento de que pode substituir todas as regras e imperativos legais acima descritos através do depoimento do vigilante que procedeu ao visionamento das imagens recolhidas mediante a câmara de filmar. Ou seja, para a recorrente o depoimento do vigilante que procedeu ao visionamento das imagens – independentemente de se verificarem ou não os pressupostos de autorização e legalização da videovigilância – deve ser valorado.
>
> Não podemos de forma alguma concordar com este entendimento. Na verdade, tendo o depoimento da testemunha em causa – D…, vigilante na Loja E… onde a trabalhadora desempenhava funções – por base factos ou o seu conhecimento, a sua razão de ciência, que derivam ou têm como suporte probatório um meio ilícito e que não pode ser valorado, facilmente concluímos que também tal depoimento não pode ser valorado.
>
> Assim, sendo a prova obtida mediante um método proibido e ilícito, ilícita é a prova adquirida mediante esse mesmo método, bem como a prova derivada ou mediata. Só através da utilização de um meio de prova ilícito, no caso o visionamento de imagens ilicitamente obtidas para os fins disciplinares, é que a aludida testemunha teve acesso ou conhecimento de factos que posteriormente foram imputados à aqui trabalhadora. Não fosse aquele conhecimento ilícito nunca o depoimento da

[89] Disponível em: <https://www.cnpd.pt/media/kuqbxfdv/delib_controlo_tics.pdf>. Acesso em: 16 mai. 2024.

> testemunha poderia ter ocorrido. Ora, esta segunda prova – a mediata ou derivada – é aquilo que se chama um "fruto envenenado [29]"[90].

Em Portugal, o direito à imagem do trabalhador é tutelado pelo art. 79.° do Código Civil. O dispositivo em tela reconhece que toda pessoa tem direito ao respeito pela sua imagem e define-a como um atributo da personalidade, garantindo a proteção legal contra sua utilização indevida. Assim, no contexto laboral, este direito implica que o empregador não pode fazer uso da imagem do trabalhador sem o seu consentimento, exceto nas situações previstas por lei.

Ademais, o artigo 79 do Código Civil Português reflete a preocupação em preservar a dignidade e a privacidade dos trabalhadores, garantindo que estes tenham controle sobre a sua imagem e que esta não seja explorada sem o seu consentimento. Esta proteção legal contribui para um ambiente de trabalho mais justo e respeitoso, promovendo a salvaguarda dos direitos fundamentais dos trabalhadores no exercício das suas atividades laborais.

Acerca do direito de imagem do trabalhador, o Tribunal da Relação de Lisboa, em Acórdão datado de 03 de maio de 2006, proferiu o seguinte entendimento, *in verbis*:

> I A licitude da videovigilância afere-se pela sua conformidade ao fim que a autorizou.
>
> II Sendo o fim visado pela videovigilância exclusivamente o de prevenir ou reagir a casos de furto, vandalismo ou outros referentes à segurança de um estabelecimento, relacionados com o público – e, ainda assim, com aviso aos que se encontram no estabelecimento ou a ele se deslocam de que estão a ser filmados - só, nesta medida, a videovigilância é legítima.
>
> III A videovigilância não só não pode ser utilizada como forma de controlar o exercício da actividade 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 do 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.
>
> IV Embora o reconhecimento dos direitos de personalidade do trabalhador no âmbito da relação de trabalho só tenha tido consagração expressa no Código do Trabalho, já anteriormente se entendia que os direitos fundamentais consagrados na Constituição da República Portuguesa - Capítulo I, Título II - e previstos no Código Civil - art. 70 e seguintes - tinham aplicação plena e directa aos trabalhadores no âmbito da execução do contrato de trabalho, uma vez que a celebração deste não implica a privação dos direitos que a Constituição reconhece a qualquer cidadão e o trabalhador não deixa de ser um cidadão como qualquer outro[91].

No contexto instalado pela pandemia do covid-19, a CNPD prezou pela regra geral e, sendo assim pela vedação da utilização de meios de vigilância à distância para controlar o desempenho dos trabalhadores que estavam em teletrabalho.

---

[90] Disponível em: <https://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/d8b30e6de8712dd580257dc700551703>. Acesso em 16 mai. 2024.

[91] Disponível em: <http://www.dgsi.pt/jtrl.nsf/0/2ee49abdddb133948025717f0042790b?OpenDocument>. Acesso em: 16 mai. 2024.

4.7. A validade do consentimento no tratamento de dados pessoais em relações laborais: desafios e limites

É importante destacar que o consentimento do trabalhador é essencial para qualquer utilização da sua imagem no ambiente de trabalho, seja para fins comerciais, publicitários ou de outra natureza. Caso contrário, qualquer utilização não autorizada pode ser considerada uma violação do direito à imagem do trabalhador, sujeitando o empregador a sanções legais e até mesmo ações de indemnização por danos[92].

Nas relações de trabalho, o conceito de consentimento como base para legitimar o tratamento de dados está profundamente interligado com o inerente desequilíbrio de poder entre empregadores e empregados. De acordo com o artigo 6.º, n.º 1, alínea a), do Regulamento Geral sobre a Proteção de Dados (RGPD), o consentimento deve ser dado de forma livre, específica, informada e inequívoca. No entanto, devido à subordinação jurídica que caracteriza as relações de trabalho, existem dúvidas quanto ao facto de o consentimento de um trabalhador poder cumprir verdadeiramente os critérios de ser "dado livremente"[93].

Em outras palavras, o consentimento pode tornar legal o tratamento de dados no contexto laboral, desde que cumpra os critérios estabelecidos pelo Regulamento Geral de Proteção de Dados (RGPD), como ser livre, informado, específico e inequívoco. No contudo, a relação de subordinação jurídica inerente à relação laboral cria um desequilíbrio de poder que pode pôr em causa a liberdade de consentimento[94].

De acordo com o artigo 7.º do RGPD, o consentimento deve ser genuíno, sem qualquer forma de coação ou dependência, o que é difícil de garantir num ambiente em que o trabalhador pode sentir-se pressionado a concordar com o tratamento de dados por receio de represálias ou discriminação. Assim, em muitas situações, o consentimento não é considerado válido como base jurídica no domínio laboral[95].

Nestes termos, o Comité Europeu para a Proteção de Dados (CEPD) sublinhou que o consentimento obtido num contexto laboral pode nem sempre ser válido devido justamente ao desequilíbrio de poder. Os trabalhadores podem sentir-se coagidos a concordar com o tratamento de dados devido às potenciais repercussões da recusa, como a recusa de

---

[92] PINHEIRO, Alexandre Sousa. *Consentimento e proteção de dados: uma análise crítica no âmbito laboral*. *In: Revista Portuguesa de Direito do Trabalho*, Lisboa, v. 10, n. 2, p. 123-141, 2020.
[93] DIAS, José Fontes. *Consentimento no tratamento de dados laborais:* análise crítica à luz do RGPD. *In*: Revista de Direito do Trabalho e Seguridade Social, São Paulo, v. 47, n. 3, p. 123-150, 2021.
[94] CORDEIRO, António Menezes. *Proteção de Dados Pessoais e Relações Laborais:* desafios e implicações. *In*: Revista de Direito e Tecnologia, Lisboa, v. 2, n. 3, p. 65-85, 2020.
[95] *Idem.*

oportunidades ou uma discriminação subtil. Este facto compromete a voluntariedade exigida para o consentimento nos termos do RGPD[96].

As especificidades da relação de trabalho complicam ainda mais a questão. Os empregadores são frequentemente responsáveis por garantir a segurança no local de trabalho, monitorizar o desempenho e cumprir as obrigações legais. Embora estas actividades exijam o tratamento de dados, confiar no consentimento como base jurídica pode não ser adequado quando motivos alternativos, como o interesse legítimo (alínea f) do n.º 1 do artigo 6.º) ou a obrigação jurídica (alínea c) do n.º 1 do artigo 6.º), são mais sólidos e contextualmente relevantes[97].

Por exemplo, os sistemas de monitorização, como a videovigilância ou o controlo da produtividade, recolhem frequentemente dados dos trabalhadores para garantir a segurança ou a conformidade. Nestes casos, o consentimento pode parecer mais uma formalidade do que uma escolha genuína, especialmente quando a recusa do consentimento pode resultar num acesso limitado a benefícios ou funções laborais. Esta percepção de coerção põe diretamente em causa a validade do consentimento[98].

Além disso, o artigo 7.º, n.º 4, do RGPD desencoraja explicitamente o recurso ao consentimento quando existe um desequilíbrio significativo de poder. Esta disposição é especialmente pertinente nas relações de trabalho, em que a autoridade do empregador pode inerentemente pressionar os trabalhadores a consentirem no tratamento de dados, mesmo contra o seu melhor juízo.

Os tribunais nacionais e as autoridades de proteção de dados em todas as jurisdições salientaram frequentemente a inadequação do consentimento nas relações de trabalho. Por exemplo, a legislação portuguesa, ao abrigo do artigo 28.º, n.º 3, da Lei de Execução da Proteção de Dados (Lei n.º 58/2019), restringe a confiança no consentimento do trabalhador, a menos que o tratamento resulte em benefícios jurídicos ou económicos diretos para o trabalhador. Esta abordagem legislativa reflete um ceticismo mais amplo do consentimento em contextos laborais[99].

---

[96]DIAS, José Fontes. *Consentimento no tratamento de dados laborais:* análise crítica à luz do RGPD. *In*: Revista de Direito do Trabalho e Seguridade Social, São Paulo, v. 47, n. 3, p. 123-150, 2021.

[97] PINHEIRO, Alexandre Sousa. *O Consentimento no Tratamento de Dados Pessoais no Trabalho:* Limites e Perspectivas. *In*: *Revista Jurídica Portuguesa*, v. 14, p. 89-102, 2021.

[98] PINHEIRO, Alexandre Sousa. *Consentimento e Ética no Tratamento de Dados no Trabalho*. *In*: Revista Portuguesa de Direito do Trabalho, Lisboa, v. 8, n. 3, p. 211-228, 2021.

[99] PORTUGAL. Tribunal Constitucional. *Acórdão nº 70/2020: Validade do Consentimento em Relações Laborais*. Lisboa, 2020. Disponível em: https://www.tribunalconstitucional.pt. Acesso em: 13 jan. 2025.

Dadas estas limitações, o RGPD e a legislação nacional em Portugal, sugerem que o tratamento de dados em contextos laborais deve preferencialmente basear-se noutros fundamentos legais, como o cumprimento de obrigações legais (Art. 6.º, n.º 1, alínea c) do RGPD) ou o interesse legítimo do empregador (Art. 6.º, n.º 1, alínea f)). Estas bases evitam a vulnerabilidade do consentimento e oferecem uma maior proteção dos direitos dos trabalhadores, ao mesmo tempo que permitem ao empregador atingir objetivos legítimos, como garantir a segurança ou cumprir obrigações regulamentares. Por conseguinte, embora o consentimento possa ser legalmente possível, raramente é considerado uma base adequada para um contrato de trabalho.

Além disso, bases jurídicas alternativas, como o interesse legítimo ou a necessidade contratual, são mais adequadas para o tratamento de dados em contextos laborais. Estas bases fornecem justificações mais claras alinhadas com as necessidades organizacionais e evitam as armadilhas da percepção de coação ou de consentimento desequilibrado. No entanto, há cenários limitados em que o consentimento pode ser válido, como quando os trabalhadores têm uma escolha genuína e o tratamento é opcional, não estando ligado às suas responsabilidades profissionais principais. Estes casos constituem exceções e não a norma, uma vez que exigem uma prova inequívoca de acordo informado e voluntário[100].

Em conclusão, embora o consentimento possa teoricamente legitimar o tratamento dos dados dos trabalhadores, a sua validade prática é prejudicada pela subordinação estrutural inerente às relações de trabalho. Os quadros regulamentares e as interpretações judiciais favorecem cada vez mais bases jurídicas alternativas que asseguram a transparência e o respeito pelos direitos fundamentais dos trabalhadores sem depender de mecanismos de consentimento potencialmente coercivos. Isto reflete a necessidade de alinhar as práticas de tratamento de dados com normas éticas e com os princípios da proporcionalidade e da necessidade.

4.8. O Papel dos Instrumentos de Regulamentação Coletiva de Trabalho (IRCT) no Tratamento de Dados Pessoais

Os Instrumentos de Regulamentação Coletiva de Trabalho (IRCT), no direito do trabalho português, são mecanismos essenciais para regular as relações de trabalho. Estes instrumentos, incluindo as convenções colectivas e os contratos de empresa, podem

[100] HENRIQUES, Sérgio Coimbra; LUÍS, João Vares. *Consentimento e Outros Fundamentos de Licitude para o Tratamento de Dados Pessoais em Contexto Laboral*. *In*: Revista de Direito e Tecnologia, Lisboa, v. 2, n. 1, p. 45-68, 2022. Disponível em: https://protecaodedadosue.cedis.fd.unl.pt/wp-content/uploads/2022/10/1.-Sergio-Coimbra-Henriques.pdf. Acesso em: 13 jan. 2025.

desempenhar um papel fundamental na definição de regras claras para o tratamento de dados pessoais, nomeadamente em contextos em que não existe subordinação jurídica ou em que é difícil garantir o consentimento nos termos do RGPD[101].

A inclusão de cláusulas de proteção de dados nos IRCT está em conformidade com os princípios do Regulamento Geral sobre a Proteção de Dados (RGPD), nomeadamente no que diz respeito à transparência, responsabilidade e equidade no tratamento de dados. O artigo 482.º do Código do Trabalho português realça o âmbito regulamentar dos IRCT, fornecendo uma base para responder a necessidades específicas do setor ou da organização em matéria de proteção de dados[102].

Uma vantagem significativa da utilização dos IRCT para regulamentar os dados pessoais é a sua capacidade de normalizar as práticas num sector. Por exemplo, os IRCT podem definir o âmbito admissível do controlo dos trabalhadores, os períodos de retenção de dados e as funções dos responsáveis pelo tratamento e dos subcontratantes no local de trabalho. Ao negociar estes termos coletivamente, o risco de desequilíbrios de poder entre empregadores e trabalhadores é atenuado[103].

Além disso, os IRCT podem abordar explicitamente a utilização de tecnologias avançadas, como plataformas de videoconferência, sistemas de autenticação biométrica ou ferramentas de controlo da produtividade. Estas tecnologias processam frequentemente dados pessoais sensíveis e os IRCT podem prever salvaguardas sólidas, garantindo que a sua utilização cumpre os requisitos do RGPD, respeitando simultaneamente os direitos fundamentais dos trabalhadores.

Nos contextos em que prevalecem os contratos sem subordinação jurídica, como os acordos de freelance ou de contratante independente, os IRCT podem alargar a proteção a estes trabalhadores. Ao incluir cláusulas que regulam o tratamento dos dados nestas relações atípicas, os IRCT colmatam as lacunas nas proteções legais e criam um quadro mais equitativo para a governação dos dados[104].

---

[101] GOMES, Júlio. *IRCT e sua aplicação no Direito do Trabalho:* Proteção de Dados e Outras Implicações Contemporâneas. *In*: Revista Portuguesa de Direito do Trabalho, Lisboa, v. 14, n. 3, p. 123-140, 2020.
[102] MOREIRA, Teresa Coelho. *Direito do Trabalho na Era Digital*. Coimbra: Edições Almedina, 2022, p. 207.
[103] AMADO, João Leal. *Contrato de Trabalho - Noções Básicas*. 4.ª ed. Coimbra: Almedina, 2023, p. 223.
[104] HENRIQUES, Sérgio Coimbra; LUÍS, João Vares. *Consentimento e Outros Fundamentos de Licitude para o Tratamento de Dados Pessoais em Contexto Laboral*. *In*: Revista de Direito e Tecnologia, Lisboa, v. 2, n. 1, p. 45-68, 2022. Disponível em: https://protecaodedadosue.cedis.fd.unl.pt/wp-content/uploads/2022/10/1.-Sergio-Coimbra-Henriques.pdf. Acesso em: 13 jan. 2025.

O papel dos IRCTs torna-se particularmente relevante na resolução de questões de consentimento em contextos laborais. Dado que o RGPD exige que o consentimento seja dado de forma livre, informada, específica e inequívoca, os IRCT podem reduzir a dependência do consentimento individual, estabelecendo acordos coletivo claros e menos susceptíveis de coação ou pressão implícita.

No que toca aos Acordos Colectivos de Trabalho (ACT), é fulcral salientar o estabelecido no n.º 3 do artigo 3.º do Código do Trabalho, que prevê que as normas destes instrumentos só podem ser mais favoráveis ao trabalhador, exceto nos casos em que a lei expressamente o determine. Este princípio baseia-se na perspetiva de proteção do trabalhador como parte mais fraca na relação de trabalho, garantindo que os IRCT são um instrumento de fortalecimento dos seus direitos e não de limitação dos mesmos.

Neste sentido, a redação deste artigo destaca a necessidade de garantir os direitos laborais conquistados, sendo nula qualquer disposição em contrário, ainda que constante de um IRCT, que não respeite este limite favorável. Este enquadramento traduz a centralidade do princípio da norma mais favorável no direito do trabalho português e reforça a importância de garantir a coerência das convenções e acordos coletivos com os princípios fundamentais que regulam as relações laborais.

Os exemplos de IRCT existentes em Portugal demonstram a sua eficácia na codificação das práticas de proteção de dados. Por exemplo, acordos em sectores como a saúde ou a banca incorporaram disposições que regulam a utilização de dados dos trabalhadores para avaliações profissionais, fins de segurança ou cumprimento de obrigações legais.

Além disso, os IRCT podem introduzir quadros para a resolução de litígios relacionados com questões de proteção de dados. Estes quadros podem clarificar a forma como os trabalhadores podem contestar a utilização indevida dos seus dados, solicitar a retificação ou a eliminação de dados incorretos ou garantir a transparência das atividades de tratamento de dados do empregador[105].

Do ponto de vista do empregador, os IRCT proporcionam segurança jurídica e coerência na aplicação das medidas de proteção de dados. Ao aderir aos acordos negociados, os empregadores evitar o risco de incumprimento do RGPD e da legislação portuguesa em matéria de proteção de dados. Esta segurança jurídica promove uma relação transparente e

[105] MOREIRA, Teresa Coelho. *Direito do Trabalho na Era Digital*. Coimbra: Edições Almedina, 2022, p. 207.

baseada na confiança entre empregadores e trabalhadores, reduzindo potenciais conflitos relacionados com a utilização indevida de dados.

Em conclusão, os IRCT são uma ferramenta vital para abordar as complexidades da proteção de dados no local de trabalho. Ao incorporar cláusulas pormenorizadas e específicas ao contexto, garantem o respeito dos direitos dos trabalhadores, alinhando simultaneamente as práticas organizacionais com as normas jurídicas. Além disso, proporcionam um mecanismo coletivo para enfrentar os desafios colocados pelas tecnologias emergentes e pelas relações de trabalho atípicas, o que os torna indispensáveis no panorama evolutivo do direito do trabalho e da proteção de dados[106].

4.9 Aplicabilidade do RGPD aos Contratos sem Subordinação Jurídica nos termos do artigo 10º do Código do Trabalho

A questão de saber se o regime de proteção de dados, nomeadamente no que respeita ao consentimento, se aplica aos contratos sem subordinação jurídica - conhecidos como "contratos equiparados" nos termos do artigo 10º[107]. Estes contratos envolvem frequentemente prestadores de serviços ou profissionais independentes cujo estatuto jurídico difere significativamente do dos trabalhadores por conta de outrem, uma vez que operam sem a autoridade hierárquica que define as relações de trabalho tradicionais[108].

Nos termos do artigo 10.º do Código do Trabalho, consideram-se contratos equiparados os que, não constituindo emprego formal, apresentem caraterísticas semelhantes, tais como a dependência económica ou a integração organizacional. Apesar da ausência de subordinação estrita, as condições contratuais criam frequentemente um desequilíbrio funcional, o que suscita preocupações quanto ao facto de o consentimento poder ser considerado livre[109].

Como visto anteriormente, o RGPD exige que o consentimento seja dado de forma livre, específica, informada e inequívoca. Embora os contratantes independentes tenham maior autonomia em comparação com os trabalhadores por conta de outrem, a sua dependência de um único cliente ou de uma base de clientes limitada pode reproduzir os desequilíbrios de poder

[106] HENRIQUES, Sérgio Coimbra; LUÍS, João Vares. *Consentimento e Outros Fundamentos de Licitude para o Tratamento de Dados Pessoais em Contexto Laboral. In*: Revista de Direito e Tecnologia, Lisboa, v. 2, n. 1, p. 45-68, 2022. Disponível em: https://protecaodedadosue.cedis.fd.unl.pt/wp-content/uploads/2022/10/1.-Sergio-Coimbra-Henriques.pdf. Acesso em: 13 jan. 2025.

[107] MARTINEZ, Romano; PALMA RAMALHO, Maria do Rosário. *Direito do Trabalho*. 8. ed. Coimbra: Almedina, 2020.

[108] CORDEIRO, António Menezes. *Manual de Direito do Trabalho.* 5. ed. Coimbra: Almedina, 2021.

[109] AMADO, João Leal; DRAY, Guilherme. *Código do Trabalho Anotado e Comentado.* 18. ed. Coimbra: Almedina, 2022.

observados nas relações de trabalho tradicionais, pondo assim em causa a validade do consentimento[110].

No caso de contratos equivalentes, a confiança no consentimento para o tratamento de dados é ainda mais complicada quando a natureza do trabalho envolve mecanismos regulares de monitorização ou controlo, como o controlo do tempo, software de gestão de projectos ou mesmo vigilância por vídeo. Nestes casos, mesmo que estas medidas se justifiquem para fins operacionais, a percepção de uma coação implícita pode comprometer a legitimidade do consentimento.

O artigo 10.º do Código do Trabalho reconhece que os contratos sem subordinação jurídica podem ainda assim envolver uma influência significativa do cliente ou do empregador sobre as actividades do contratante. Esta influência, embora não seja equivalente à subordinação direta, pode levar a situações em que os contratantes se sintam pressionados a aceitar o tratamento de dados como condição para manter a relação contratual[111].

A jurisprudência nacional e comunitária tem vindo a reconhecer cada vez mais que o conceito de livre consentimento deve ser avaliado no contexto específico da relação contratual. Nos casos de contratos equivalentes, os tribunais sublinharam a necessidade de examinar o grau efetivo de autonomia e se o contratante tem uma escolha genuína ao dar o seu consentimento.

As alternativas ao consentimento, como o interesse legítimo do responsável pelo tratamento de dados (artigo 6.º, n.º 1, alínea f), do RGPD), podem constituir uma base jurídica mais sólida para o tratamento de dados no contexto de contratos equivalentes. O interesse legítimo garante que o tratamento se alinha com as necessidades operacionais do cliente, respeitando simultaneamente os direitos do contratante e atenuando as preocupações relativas à coação do consentimento.

No entanto, é essencial estabelecer uma distinção entre os vários tipos de contratos equivalentes. Os *freelancers* ou profissionais altamente qualificados que se envolvem em relações com vários clientes e mantêm uma autonomia significativa são menos susceptíveis de enfrentar problemas de consentimento forçado do que os contratantes que dependem fortemente de um único cliente para a sua subsistência[112].

---

[110] LOBO XAVIER, Bernardo. *O Contrato de Trabalho no Código do Trabalho Português.* Lisboa: Universidade Católica Editora, 2019.
[111] AMADO, João Leal; DRAY, Guilherme. *Código do Trabalho Anotado e Comentado.* 18. ed. Coimbra: Almedina, 2022.
[112] GOMES, Júlio. *Tratado de Direito do Trabalho.* Vol. 1. Coimbra: Almedina, 2018.

A legislação portuguesa, em particular o artigo 28.º, n.º 3, da Lei de Execução da Proteção de Dados (Lei n.º 58/2019), reflete uma abordagem cautelosa ao limitar a dependência do consentimento em situações em que a autonomia do contratante é comprometida. Isto reforça o princípio de que a dinâmica de poder inerente à relação contratual não deve invalidar os direitos fundamentais em matéria de proteção de dados.

Este regime aplica-se aos contratos sem subordinação jurídica - designados por "contratos equiparados" nos termos do artigo 10.º do Código do Trabalho - porque estes contratos apresentam frequentemente caraterísticas que se assemelham às relações de trabalho tradicionais, como a dependência económica ou a integração na organização do cliente[113].

Embora não exista uma subordinação estrita, o desequilíbrio funcional de poder entre as partes pode comprometer a capacidade do contratante para dar o seu consentimento livre e esclarecido nos termos do Regulamento Geral sobre a Proteção de Dados (RGPD). Assim, os princípios de proteção de dados, incluindo a avaliação cuidadosa do consentimento e bases jurídicas alternativas, como o interesse legítimo, estendem-se a estas disposições contratuais para salvaguardar os direitos fundamentais do contratante, garantindo simultaneamente o cumprimento das normas legais.

Em conclusão, embora o regime de proteção de dados, incluindo os requisitos de consentimento, se aplique a contratos equivalentes nos termos do artigo 10.º do Código do Trabalho, a sua aplicação prática deve ter em conta as especificidades de cada acordo contratual. A possibilidade de desequilíbrios de poder e de coação implícita exige uma avaliação cautelosa e a utilização preferencial de bases jurídicas alternativas para o tratamento de dados, a fim de garantir a defesa dos direitos do contratante e o respeito dos princípios da equidade e da transparência

4.10. O caso português – Direito à Privacidade como direito fundamental do trabalhador

O direito à privacidade, conforme consignado no tópico 3.2., assim como outros direitos ditos fundamentais e de personalidade, está irradiado por todo o ordenamento jurídico, não se limitando a um ou outro ramo do Direito. Dito isso, o Código do Trabalho entende que o trabalhador é sujeito de direitos na conjuntura da relação laboral. O entendimento em questão

[113] AMADO, João Leal; DRAY, Guilherme. *Código do Trabalho Anotado e Comentado.* 18. ed. Coimbra: Almedina, 2022.

é evidenciado por meio do art. 16.°, que é dedicado a reserva da intimidade e da vida privada e à fixação da diretriz de respeito aos direitos de personalidade[114].

Jurisprudencialmente, a evidência no trato da vida intima do trabalhador é o Acórdão n.° 306/2003 proferido pelo Tribunal Constitucional, do qual destaco os seguintes trechos referentes à análise do art. 17.° do Código do Trabalho:

> 3) Quanto ao **artigo 17.º do Código do Trabalho**, cujo n.º 2, após, na primeira parte, proibir que o empregador exija ao candidato a emprego ou ao trabalhador a prestação de informações relativas à sua saúde ou estado de gravidez, abre, na segunda parte, essa possibilidade "*quando particulares exigências inerentes à natureza da actividade profissional o justifiquem*":
>
> – encontrando-se estes elementos da esfera privada e íntima do trabalhador ou do candidato a emprego indiscutivelmente protegidos pela reserva da intimidade da vida privada garantida pelo artigo 26.º, n.º 1, da CRP, mesmo que se entenda que, por si só, a possibilidade de o empregador lhes exigir a prestação de informações relativas à sua saúde ou ao estado de gravidez não viola tal garantia, por estar constitucionalmente justificada pela necessária protecção de outros valores, a abertura dessa possibilidade, conferida pela segunda parte do n.º 2 deste artigo 17.º, constitui, em qualquer caso, uma restrição do direito fundamental à reserva da intimidade da vida privada;
>
> – ora, tal restrição só seria constitucionalmente admissível se, entre outros limites, observasse as exigências impostas pelo princípio da proibição do excesso (segunda parte do n.º 2 do artigo 18.º da Constituição), nas suas dimensões de princípio da determinabilidade e princípio da indispensabilidade ou do meio menos restritivo, o que, no caso em apreço, parece muito discutível, atenta, por um lado, a indeterminabilidade que resulta da utilização de conceitos tão vagos como as "*particulares exigências inerentes à natureza da actividade profissional*", e, por outro lado, a possibilidade de utilização de meios menos restritivos, como, por exemplo, através do recurso à intervenção de médico que se reservaria o conhecimento de tais dados e só comunicaria ao empregador se o trabalhador ou candidato a emprego estava ou não apto a desempenhar a actividade, tal como, de resto, o Código do Trabalho dispõe no artigo 19.º, n.º 3[115].

Na sequência do caso anteriormente referido, foi introduzida a actual redacção do artigo 19.º, n.º 2, que estabelece que os empregadores estão proibidos, em qualquer circunstância, de exigir que os candidatos a emprego ou os empregados sejam submetidos ou apresentem testes ou exames de gravidez [116].

A legislação laboral pressupõe uma postura de respeito recíproca, de modo que empregador e o trabalhador devem observar detidamente os direitos de personalidade um do outro, o que abrande o dever de não violar a intimidade da vida privada. O legislador detalha o

---

[114] MARTINEZ, Pedro Romano. *Direito do Trabalho.* 11.ª ed. Coimbra: Almedina, 2023.
[115] Disponível em: <https://www.tribunalconstitucional.pt/tc/acordaos/20030306.html>. Acesso em: 16 mai. 2024.
[116] Código do Trabalho:
"Artigo 19.º
Testes e exames médicos
[...]
2 - O empregador não pode, em circunstância alguma, exigir a candidata a emprego ou a trabalhadora a realização ou apresentação de testes ou exames de gravidez."

que se entende por reserva da intimidade da vida privada, enfatizando que esta deve ser a norma e não a exceção.

A proteção mútua dos direitos de personalidade preconizada pelo Código do Trabalho é decorrência do reconhecimento da relevância da intimidade da vida privada do empregador e do empregado. É colocada em evidência a necessidade de agir com cautela quando o que está no cerne de alguma situação é a esfera pessoal dos indivíduos. Referido modo de agir propicia a conjuntura ideal para a formação de um ambiente de trabalho onde a dignidade e a autonomia dos empregados são levadas em grande consideração.

É imprescindível a exata divisão entre vida privada e relação labora. José João Abrantes leciona que a liberdade do trabalhador sobre sua vida fora do ambiente de trabalho é um princípio basilar e indispensável. Por óbvio que alguns ofícios não permitem uma divisão tão rigorosa, contexto no qual os empregadores devem ser ainda mais diligentes[117].

Atualmente, é veementemente necessário que se busque uma harmonia entre a tutela da vida privada dos empregados e os objetivos perseguidos por uma empresa. Na medida em que os direitos de personalidade são respeitados, estrutura-se um ambiente favorável ao bem-estar do trabalhador, o que acaba fomentando uma relação trabalhista ética, justa e que produz resultados eficientes, eficazes e efetivos.

Teresa Coelho Moreira faz uma análise bastante útil a respeito da tutela dos direitos de personalidade inscritos na relação entre empregado e empregador. Tal análise está embasada na ideia de que uma relação trabalhista é essencialmente uma relação em que as partes ocupam posições desiguais, o que demanda uma proteção mais incisiva quanto aos direitos dos trabalhadores.

Isso porque, conforme entendimento de Maria Regina Gomes Redinha, o contrato de trabalho não é um permissivo para colocar em posição de relatividade a dignidade humana. Os conflitos de interesse que venham a surgir no desenrolar da relação trabalhista não têm a força de suplantar qualquer direito relativo à promoção da dignidade, que deve ser levada em consideração em todas as conjunturas possíveis.

O Poder Público executor das atividades legiferante e fiscalizatória deve reconhecer a discrepância de poder existente entre o empregador e o empregado. Sendo assim, as

[117]ABRANTES, José João. *Contrato de Trabalho e Direitos Fundamentais*. Coimbra, 2005.

regulamentações devem conferir a maior legitimação possível dos direitos de personalidade do trabalhador e ocupar cada vez mais espaço no ordenamento jurídico.

Ademais, um ponto importante na busca pelo equilíbrio entre a observância dos direitos de personalidade do trabalhador e os poderes do empregador é a criação de um ambiente organizacional onde a igualdade seja um dos elementos constitutivos. Aqui, não se fala de uma igualdade formal, mas material, onde os trabalhadores estejam cientes dos seus direitos, de modo que possam identificar quando estão sendo devidamente cumpridos e quando estão em situação de violação, mesmo aquelas que já parecem internalizadas e/ou consideradas *praxe* da organização, como a implantação inadequada de sistemas de videovigilância.

Em última análise, diante do exposto, é possível compreender que o respeito a direitos de personalidade dos trabalhadores é consequência da ação conjunta de agentes externos (Poder Público) e internos (empregador-empregado).

Os trabalhadores não têm a obrigação de se despir da identidade pessoal para prestar um serviço, até porque é impossível não existir uma ligação entre essas duas áreas, especialmente em momentos em que o indivíduo se ver inserido em situações que interferem diretamente na dinâmica de uma das áreas em preferência de outra.

É inevitável o surgimento de questões pessoais no contexto do trabalho, como aquelas relacionadas a saúde do trabalhador capazes de exigir que o mesmo se ausente do local de trabalho. Nesse caso, espera-se a comunicação por parte do empregado – e as devidas comprovações – e a compreensão por parte do empregador.

O Supremo Tribunal de Justiça Português emitiu pronunciamento acerca da admissibilidade da videovigilância nos locais de trabalho tendo como parâmetro aspectos essenciais em torno da proteção da intimidade e da imagem dos empregados. A Corte entendeu que a vigilância deve tomar contornos genéricos, não sendo admitido o monitoramento individual dos trabalhadores.

A sensibilidade das questões referentes a vida privada e ao direito à imagem é legitimada por meio da atribuição de ilicitude a monitoramentos que desrespeitem tais direitos.

A decisão do Supremo Tribunal de Justiça veio reforçar a incontestável necessidade de fixação de limites evidentes a atuação do poder de controle do empregador quando da consagração dos direitos fundamentais dos empregados. Nenhum objetivo é legítimo quando o custo para a sua consecução é a violação de um direito fundamental do trabalhador.

A videovigilância empregada deliberadamente, sem observar limites jurídico-legais, viola direitos de personalidade dos trabalhadores. O Poder Judiciário de Portugal é ativo no que tange ao fomento da proteção desses direitos diante de medidas abusivas por parte dos empregadores.

Reforço a ideia de que o princípio da proporcionalidade deve ocupar posição de protagonismo na ponderação de adequabilidade dos sistemas de videovigilância, colocando no centro da discussão a tese de que medidas excessivas são pressupostos de violação de direitos. A análise deve sempre tomar por base a conformação do monitoramento via captação de som e imagem com os fins previstos em lei.

5. VÍDEOVIGILÂNCIA NO DIREITO COMPARADO

5.1. Escolhas orientadas: Brasil, Espanha e Portugal

A seleção do Brasil, Espanha e Portugal como foco da análise comparativa sobre a legislação da videovigilância foi deliberada e metódica. Estes países foram escolhidos devido às suas estruturas legais distintas, mas interligadas, que fornecem insights abrangentes sobre a regulamentação da videovigilância. Portugal e Espanha, enquanto estados-membros da União Europeia, operam ao abrigo do Regulamento Geral sobre a Proteção de Dados (RGPD), oferecendo uma estrutura sólida para equilibrar a privacidade e a segurança. Em contraste, o Brasil, embora influenciado pelos padrões europeus de privacidade, tem a sua própria estrutura através da Lei Geral de Proteção de Dados (LGPD), o que o torna um estudo de caso valioso para analisar como princípios semelhantes são adaptados em contextos não europeus.

Portugal foi incluído no estudo devido aos seus esforços pioneiros em alinhar as suas leis nacionais com as diretivas da UE sobre proteção de dados e privacidade. A abordagem regulamentar do país, particularmente a sua ênfase na transparência, proporcionalidade e autorização prévia para a videovigilância, serve de modelo para outras nações que lidam com questões de privacidade. Além disso, o quadro legal de Portugal destaca o papel de autoridades independentes, como a Comissão Nacional de Proteção de Dados (CNPD), na supervisão da conformidade, na garantia da responsabilização e na proteção dos direitos individuais.

A Espanha foi selecionada pela sua jurisprudência influente, particularmente casos como López Ribalda e Outros v. Espanha, que abordou o equilíbrio entre os interesses dos empregadores e os direitos de privacidade dos empregados. O quadro jurídico espanhol exemplifica a forma como os tribunais interpretam a proporcionalidade e a necessidade nas práticas de vigilância, estabelecendo precedentes que influenciam a jurisprudência europeia. Além disso, as suas regulamentações laborais e proteções constitucionais oferecem uma perspectiva aprofundada sobre a interseção entre a legislação laboral e a privacidade de dados.

A inclusão do Brasil complementa os exemplos europeus ao fornecer uma perspectiva de fora da UE que adoptou princípios modernos de privacidade através da LGPD. A sua estrutura integra princípios de transparência, consentimento e responsabilização, ao mesmo tempo que aborda desafios específicos enfrentados pelas nações em desenvolvimento. Os recentes desenvolvimentos legislativos do Brasil reflectem um esforço para se alinhar com os padrões internacionais, tornando-o um caso ideal para estudar a difusão global das normas de privacidade e a adaptação dos princípios europeus a diferentes realidades socioeconómicas.

A análise comparativa destas três jurisdições oferece um exame equilibrado e abrangente das regulamentações de videovigilância, destacando semelhanças e diferenças nas abordagens legais. Ao justapor os sistemas influenciados pela UE com a estrutura jurídica em evolução do Brasil, a investigação sublinha os desafios universais de equilibrar a segurança e a privacidade, ao mesmo tempo que ilustra como as tradições jurídicas distintas moldam as respostas regulamentares. Esta abordagem fornece uma base rica para avaliar as melhores práticas e identificar áreas para melhoria legislativa a nível global.

5.2. Espanha

O uso cada vez maior da vigilância por vídeo no local de trabalho levantou preocupações significativas com relação aos direitos de privacidade dos funcionários e às obrigações legais dos empregadores. Essa questão, como vimos, tem sido particularmente proeminente em todos os países, nomeadamente na União Europeia, onde a privacidade é um direito fundamental protegido por lei, como definido pelo Regulamento Geral de Proteção de Dados (RGPD).

Na Espanha, o interesse pelo tema destaca-se especialmente na análise do caso López Ribalda e outros v. Espanha, julgado pela Corte Europeia de Direitos Humanos (ECHR), que serve como um exemplo crítico de como os tribunais equilibram os direitos conflitantes de privacidade e propriedade ao avaliar as práticas de vigilância no local de trabalho.

No caso López Ribalda e outros v. Espanha, os funcionários de um supermercado foram monitorados por câmeras ocultas depois que o empregador suspeitou de perdas significativas de estoque devido a furtos. Enquanto as câmeras visíveis eram colocadas nas entradas e saídas, as câmeras ocultas eram focadas nas áreas de caixa, revelando a má conduta dos funcionários. Essa vigilância levou à demissão de vários funcionários, que contestaram a legalidade da vigilância, alegando que ela infringia seu direito à privacidade de acordo com o Artigo 8 da Convenção Europeia de Direitos Humanos[118].

O TEDH decidiu que, embora a vigilância oculta constituísse uma interferência nos direitos de privacidade, ela era justificada sob as circunstâncias específicas do caso. O tribunal destacou vários fatores que tornaram a vigilância proporcional e necessária: o empregador tinha motivos legítimos para investigar perdas financeiras significativas, a vigilância era limitada em escopo e duração e as imagens eram usadas somente para fins disciplinares. Essa decisão

[118] Turanjanin, V. (2020). Video Surveillance of the Employees Between the Right to Privacy and Right to Property After López Ribalda and Others v. Spain. *University of Bologna Law Review*, 5, 268-293. https://doi.org/10.6092/ISSN.2531-6133/10514.

ressaltou a necessidade de uma abordagem equilibrada, pesando tanto os interesses do empregador quanto os direitos do empregado.

Um dos pontos principais da sentença da ECHR foi a falta de notificação prévia aos funcionários sobre as câmeras ocultas. Embora normalmente exigido, o tribunal reconheceu que informar os funcionários poderia ter comprometido a investigação. A sentença estabeleceu um precedente importante ao reconhecer que, em certos casos, a necessidade de vigilância poderia se sobrepor às exigências usuais de transparência e consentimento, desde que tais medidas fossem proporcionais e justificadas.

O uso de imagens de vigilância como prova em processos judiciais, especialmente em casos criminais, foi outra questão importante abordada no artigo. A CEDH enfatizou que a admissibilidade de tais provas depende do fato de seu uso tornar o julgamento geral justo, em vez de se concentrar apenas em como a prova foi obtida. Essa abordagem diferenciada permite que os tribunais considerem o contexto mais amplo de cada caso, garantindo que a justiça seja feita sem desconsiderar as garantias processuais.

No contexto mais amplo da legislação espanhola, a vigilância por vídeo no local de trabalho é regida por várias regulamentações que visam equilibrar as necessidades de segurança com os direitos de privacidade. Assim, o Estatuto dos Trabalhadores da Espanha desempenha um papel fundamental na regulamentação do uso de medidas de vigilância no local de trabalho, garantindo que tais práticas respeitem a dignidade e a privacidade dos funcionários.

O artigo 20 do Estatuto dos Trabalhadores concede explicitamente aos empregadores o direito de monitorar seus funcionários para garantir o cumprimento das obrigações de trabalho. Entretanto, esse direito não é absoluto e deve ser equilibrado com os direitos fundamentais dos funcionários, especialmente o direito à privacidade, que é protegido pelo Artigo 18 da Constituição Espanhola. Essa estrutura legal determina que as medidas de vigilância devem ser necessárias, proporcionais e respeitar a integridade pessoal dos funcionários.

Um dos requisitos essenciais estabelecidos pelo Estatuto dos Trabalhadores é a obrigação dos empregadores de informar seus funcionários sobre quaisquer práticas de vigilância. De acordo com o Artigo 20.3, os funcionários devem ser notificados com antecedência sobre a instalação de sistemas de vigilância, incluindo as áreas específicas que estão sendo monitoradas e o objetivo da vigilância. Isso garante que os funcionários estejam cientes da vigilância e entendam seu escopo, promovendo assim um ambiente de trabalho transparente. A falha em informar adequadamente os funcionários pode levar a violações dos

direitos de privacidade e tornar qualquer evidência coletada por meio de vigilância inadmissível em processos judiciais.

Os requisitos de transparência definidos no Estatuto dos Trabalhadores alinham-se com os princípios estabelecidos pelo Regulamento Geral de Proteção de Dados (RGPD), que enfatiza a importância do consentimento informado e do tratamento leal dos dados pessoais. Os empregadores devem comunicar claramente as medidas de vigilância através de avisos, políticas escritas ou outras formas de comunicação direta. Esta prática não só cumpre as normas legais, mas também cria confiança entre empregadores e empregados, mitigando potenciais conflitos e desafios legais decorrentes de monitorização não divulgada.

A Lei Orgânica 3/2018 sobre a Proteção de Dados Pessoais e Garantia de Direitos Digitais alinha as regulamentações espanholas com o RGPD, estabelecendo diretrizes rigorosas para o processamento de dados pessoais, inclusive gravações de vídeo. A lei enfatiza a importância da transparência, exigindo que os empregadores informem claramente os funcionários sobre as práticas de vigilância.

As orientações da Agência Espanhola de Proteção de Dados (AEPD) também desempenham um papel fundamental na formação das práticas de vigilância. A AEPD fornece orientações adicionais sobre a implementação de videovigilância no local de trabalho. A AEPD sublinha que os empregadores devem utilizar sinalização visível para indicar a presença de câmaras, conforme exige o artigo 22.º da Lei Orgânica 3/2018 de Proteção de Dados Pessoais e Garantia de Direitos Digitais. A sinalização deve ser clara e posicionada de forma que os indivíduos tenham conhecimento da vigilância antes de entrarem na área monitorada. Isto é crucial para garantir que os funcionários e visitantes sejam informados e possam ajustar o seu comportamento em conformidade, respeitando o princípio da transparência ao abrigo das leis de proteção de dados.

Além de exigir sinalização visível, a AEPD também estabelece diretrizes rigorosas sobre a limitação da vigilância a áreas necessárias para fins de segurança. A vigilância não deve ser utilizada em locais onde os funcionários tenham uma maior expectativa de privacidade, como banheiros, vestiários ou áreas de descanso. A monitorização destas áreas constituiria uma intrusão excessiva na privacidade pessoal e seria provavelmente considerada ilegal tanto ao abrigo do Estatuto dos Trabalhadores como dos regulamentos de proteção de dados. As diretrizes da AEPD sublinham que os empregadores devem avaliar cuidadosamente a necessidade de vigilância em cada local para evitar a violação dos direitos dos trabalhadores.

Apesar dessas regulamentações, ainda há desafios para equilibrar a vigilância com os direitos de privacidade. Os tribunais espanhóis, incluindo a Suprema Corte, geralmente decidiram contra a vigilância oculta, a menos que ela atenda a critérios rigorosos de necessidade e proporcionalidade. O caso López Ribalda continua sendo uma exceção controversa, destacando a complexa interação entre os interesses de privacidade e segurança no local de trabalho.

5.3. Brasil

Para a compreensão adequada do *modus operandi* permitido aos sistemas de videovigilância no Brasil, faz-se necessário discorrer acerca dos direitos que limitam o uso do mecanismo em estudo e, por isso mesmo, delineiam a aplicação do mesmo sob uma perspectiva ética e alinhada com os ditames da dignidade humana.

No Brasil, o direito à intimidade e o direito à privacidade estão intrinsecamente relacionados, não sendo rara a ideia de que ambos carregam o mesmo significado sob o ponto de vista do ordenamento jurídico.

O art. 5. ° da Constituição da República Federativa do Brasil (CRFB) protege a vida, a liberdade, a igualdade, a segurança e a propriedade sob diversos aspectos. Com base nas lições de José Afonso da Silva[119], o direito à vida é precursor de outros direitos igualmente relevantes, leia-se fundamentais, consagrados na Carta Magna, dentre eles o direito à intimidade e à vida privada, conforme o disposto no art. 5. °, inciso X, *in verbis*: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação".

Percebe-se que o direito à intimidade e o direito à privacidade são elencados separadamente pela CRFB, o que nos leva ao entendimento de que são, em verdade, juridicamente distintos.

Ademais, os direitos em estudo possuem caráter de cláusula pétrea, na medida em que são direitos individuais (*vide* art. 60, § 4°, da CRFB). Desta maneira, não é permitido emendas constitucionais que objetivem promover supressões ou modificações restritivas em torno dos referidos direitos. Eles possuem um atributo especial, que demanda garantias constitucionais específicas voltadas para sua total proteção.

[119] SILVA, José Afonso da. *Curso de Direito Constitucional Positivo*. 40ª ed., rev. e atual. até a Emenda Constitucional n.95, de 15.12.2016. São Paulo: Malheiros, 2017. ISBN 978-85- 392-0357-4. p. 200.

Por óbvio que temos que levar em conta o caráter relativo dos direitos fundamentais. É por meio da relatividade que se pode, diante de um caso concreto, dar maior grau de relevância a um direito fundamental ao invés de outro.

Ainda, convém discorrer acerca da eficácia dos direitos fundamentais sobre as relações privadas, no que se convencionou chamar de eficácia horizontal dos direitos fundamentais.

É consenso entre os estudiosos que os direitos fundamentais se aplicam tanto na relação pública estabelecida entre o Estado e os indivíduos, quanto na relação privada estabelecida pelos indivíduos. Isso pode ser visualizado a partir da existência de determinados direitos individuais cuja efetividade depende do cumprimento de um dever por outrem, que não é necessariamente o Estado, tais como direito à inviolabilidade de domicílio, direito ao sigilo das correspondências e comunicações telegráficas e telefônicas e direitos referentes à relação empregado-empregador[120].

As discussões doutrinárias e jurisprudenciais que giram em torno da aplicabilidade direta dos direitos fundamentais (sem necessidade de regulamentação) nas relações ditas horizontais (entre particulares) não devem ser desconsideradas.

No Recurso Extraordinário (R.E.) nº 201.819, cujo acórdão foi relatado pelo Ministro Gilmar Mendes, há uma clara controvérsia a respeito da aplicabilidade direta de um direito fundamental nas relações entre particulares, mais especificamente quanto à aplicação do contraditório e da ampla defesa, consagrados no art. 5º, inciso LV.

O caso tratava da exclusão de sócio dos quadros da União Brasileira de Compositores (UBC) sem prévia possibilidade do contraditório e da ampla defesa por parte do excluído.

A Ministra Ellen Gracie entendeu pela não aplicação direta do contraditório e da ampla defesa, defendendo a primazia do pactuado entre as partes, nos seguintes termos:

> Como se vê, o Tribunal *a quo*, com fundamento no princípio da ampla defesa, anulou a punição aplicada ao recorrido.
>
> O estatuto da recorrida, em seu art. 16, determina que: "a diretoria nomeará comissão de inquérito composta de três sócios, a fim de apurar indícios, atos ou fatos que tornem necessária a aplicação de penalidades aos sócios que contrariem os deveres prescritos no Capítulo IV destes Estatutos." (fl. 48).
>
> A leitura do acórdão da apelação revela que a regra a cima transcrita foi integralmente obedecida, porém ela foi afastada em homenagem ao princípio da ampla defesa.
>
> Entendo que as associações privadas têm liberdade para se organizar e estabelecer normas de funcionamento e de relacionamento entre os sócios, desde que respeitem a

[120] SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais*. 7ª ed. rev. atual. e ampl. Porto Alegre: Livraria do Advogado, 2007. ISBN 85-7348-456-X. p. 400.

> legislação em vigor. Cada indivíduo, ao ingressar numa sociedade, conhece suas regras e seus objetivos, aderindo a eles.
>
> A controvérsia envolvendo a exclusão de um sócio de entidade privada resolve-se a partir das regras do estatuto social e da legislação civil em vigor. Não tem, portanto, o aporte constitucional atribuído pela instância de origem, sendo totalmente descabida a invocação do disposto no art. 5.º, inciso LV da Constituição para agasalhar a pretensão do recorrido de reingressar nos quadros da UBC.
>
> Obedecido o procedimento fixado no estatuto da recorrente para a exclusão do recorrido, não há ofensa ao princípio da ampla defesa, cuja aplicação à hipótese dos autos revelou-se equivocada, o que justifica o provimento do recurso.

Já o Ministro Gilmar Mendes entendeu de modo diverso, fixando entendimento que vai ao encontro da tese de aplicabilidade direta dos direitos fundamentais às relações privadas e associando a referida tese ao princípio da autonomia privada no seguinte sentido:

> [...]
>
> Idêntica orientação é adotada por Konrad Hesse, que destaca serem as relações entre pessoas privadas marcadas, fundamentalmente, pela ideia de igualdade. A vinculação direta dos entes privados aos direitos fundamentais não poderia jamais ser tão profunda, pois, ao contrário da relação Estado-cidadão, os direitos fundamentais operariam a favor e contra os dois partícipes da relação de Direito Privado. Não se pode olvidar, por outro lado, que as controvérsias entre particulares com base no direito privado hão de ser decididas pelo Judiciário. Estando a jurisdição vinculada aos direitos fundamentais, parece inevitável que o tema constitucional assuma relevo tanto na decisão dos tribunais ordinários, como no caso de eventual pronunciamento da Corte Constitucional.
>
> [...]
>
> Destarte, considerando que a União Brasileira de Compositores (UBC) integra a estrutura do ECAD, é incontroverso que, no caso, ao restringir as possibilidades de defesa do recorrido, ela assume posição privilegiada para determinar, preponderantemente, a extensão do gozo e fruição dos direitos autorais de seu associado.
>
> Em outras palavras, trata-se de entidade que se caracteriza por integrar aquilo que poderíamos denominar como espaço público ainda que não-estatal.
>
> Essa realidade deve ser enfatizada principalmente porque, para os casos em que o único meio de subsistência dos associados seja a percepção dos valores pecuniários relativos aos direitos autorais que derivem de suas composições, a vedação das garantias constitucionais de defesa pode acabar por lhes restringir a própria liberdade de exercício profissional.
>
> Logo, as penalidades impostas pela recorrente ao recorrido, extrapolam, em muito, a liberdade do direito de associação e, sobretudo, o de defesa. Conclusivamente, é imperiosa a observância das garantias constitucionais do devido processo legal, do contraditório e da ampla defesa (art. 5.°, LIV e LV, da CF).
>
> Tem-se, pois, caso singular, que transcende a simples liberdade de associar ou de permanecer associado. Em certa medida, a integração a essas entidades configura, para um número elevado de pessoas, quase que um imperativo decorrente do exercício de atividade profissional.

A despeito das controvérsias apresentadas, a doutrina é pacífica quanto ao entendimento de que as disposições do art. 7° da CRFB, que tratam dos direitos dos trabalhadores, são, em grande maioria, normas de eficácia plena, capazes de produzir efeitos imediata e integralmente.

Tais direitos são aplicados em relações essencialmente privadas, quais sejam as relações entre empregadores e empregados.

O que ocorre é que não há no art. 7° da CRFB normatização relativa ao direito à privacidade no âmbito da relação trabalhista. Porém, é ponto incontroverso que o ordenamento jurídico brasileiro protege a vida privada e a intimidade, tanto constitucionalmente, por meio do já mencionado art. 5°, inciso X, quanto legalmente, por meio do Código Civil, em dispositivos como o art. 21. Desta feita, urge-se a aplicação da técnica de interpretação integrativa, pela qual o operador do direito aplicará às relações trabalhistas normas provenientes de fontes diversas, tais quais as citadas neste parágrafo (CRFB e Código Civil).

A aplicabilidade imediata dos direitos à privacidade e à vida intima pode ser justificada a partir da análise da dimensão na qual referidos direitos estão inseridos, qual seja, a primeira dimensão, que tratam das liberdades negativas, dos direitos civis e políticos, da proteção contra as arbitrariedades do Estado. Tais direitos, *a priori*, não precisam de regulamentação específica para gerarem efeitos, divergindo dos direitos de segunda dimensão, que tratam das liberdades positivas, e demandam uma ação prestacional por parte do Estado[121].

Levando em consideração a ideia descrita no parágrafo anterior, é adequado dispor que os direitos à privacidade e à vida íntima estão estreitamente relacionados com o ser humano, de modo que não constituem um dever a ser prestado por intermédio da elaboração de normas e políticas públicas, mas um atributo de personalidade que deve ser levado em consideração tanto nas relações verticais, quanto nas relações horizontais. É no âmbito das relações horizontais que é possível identificar as mais variadas relações estabelecidas entre os indivíduos no meio social, dentre elas as relações laborais.

Neste sentido, sob o prisma do Código Civil brasileiro, que cuida das relações privadas, há a compreensão pacífica de que a CRFB, ao tratar da intimidade e da privacidade, tutela direitos distintos. A doutrina civilista detém o entendimento de que a intimidade é gênero do qual é espécie a vida privada. O que entra em discussão diante de certos atos observados dentro de uma relação laboral, como a videovigilância e o monitoramento de comunicações, é o direito a intimidade do empregado frente aos direitos do empregador, como o direito à propriedade e afins[122].

[121] SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais*. 7ª ed. rev. atual. e ampl. Porto Alegre: Livraria do Advogado, 2007. ISBN 85-7348-456-X. p. 185.
[122] TARTUCE, Flavio. *Manual de Direito Civil*. Volume único. São Paulo: Método, 2011. VASCONCELOS. Pedro Pais de. Direito de Personalidade. Coimbra: Edições Almedina S.A. 2006. p. 103.

Não há que se discutir o caráter fundamental dos direitos à intimidade e à privacidade, consagrados pelo art. 5.°, inciso X, da CRFB. Deve-se ter em mente que os direitos tutelados no dispositivo citado compreendem aspectos diversos, tais como os relativos à família, ao nome, à imagem e ao modo de vida de um indivíduo. Um ponto que merece atenção é a possível imprecisão com a qual a Lei Maior brasileira consagra a privacidade e a intimidade como figuras distintas. José Afonso da Silva, ao buscar uma compreensão adequada para o tratamento conferido aos direitos à intimidade e à vida privada pelo ordenamento jurídico brasileiro, sustenta que o direito à privacidade seria gênero do qual seriam espécies os demais direitos mencionados no art. 5.°, inciso X[123].

A contar dessa tese, o jurista considera a vida das pessoas sob dois parâmetros: o exterior e o interior. O exterior está relacionado a sociabilidade do indivíduo, a maneira como se porta publicamente, aquilo que faz e que pode ser de conhecimento e de utilização de qualquer pessoa. O interior está relacionado às relações privadas do indivíduo, tais como as relações familiares e de amizade, aquilo que faz e que não tem o condão de se tornar objeto de conhecimento ou de utilização por pessoas fora do ciclo privado do indivíduo[124].

Nesse caminhar, José Afonso da Silva dispõe que o direito à privacidade é mais amplo em virtude da distinção entre vida privada e intimidade. A vida privada compreende as mais variadas espécies de relacionamento que um indivíduo pode firmar no seio social (profissionais, comerciais, empresariais, dentre outras) e a intimidade compreende espécies de relacionamento com laços mais estreitos, tais como os familiares e os de amizade.

É a partir dessa perspectiva que José Afonso da Silva aborda o direito à privacidade no contexto atual da revolução técnico científica, no qual ocorre uma circulação massificada de informações, que envolvem, inclusive, dados pessoais. Acerca dos dados pessoais é de relevância primária que o titular dos mesmos possua o direito de acessá-los e, caso necessário, retificá-los. O autor suscita que a CRFB se posiciona de maneira favorável à proteção dos dados pessoais, especialmente em conjunturas de ameaça de lesão, por meio da previsão do *habeas data*.

Inclusive, é válido o registro de que não há uma norma específica na CRFB acerca da tutela dos dados pessoais no âmbito informatizado. O que há é um remédio constitucional de

[123] SILVA, José Afonso. *Curso de Direito Constitucional Positivo*. 40ª ed., rev. e atual. até a Emenda Constitucional n.95, de 15.12.2016. São Paulo: Malheiros, 2017. ISBN 978-85- 392-0357-4. p. 212.
[124] Idem. p. 208 e 211/212.

proteção geral, como mencionado anteriormente – o *habeas data*. Desta feita, o art. 5º, inciso LXXII, da CRFB assegura o conhecimento de dados da pessoa do impetrante que estejam em registros ou banco de dados de entidades governamentais ou de caráter público, bem como a retificação dos mesmos.

Apesar da inexistência de uma previsão constitucional especificamente voltada aos dados informatizados, deve-se ter em mente que os direitos fundamentais irradiam uma série de outros direitos que não necessariamente precisam estar explícitos. Em uma análise sistemática, temos que nos ater às bases principiológicas do ordenamento jurídico e aos diplomas incorporados a ele, como é o caso de tratados internacionais[125].

No âmbito das relações laborais, a base legal para a utilização dos sistemas de videovigilância encontra-se no artigo 2.º da Consolidação das Leis do Trabalho (CLT). Este artigo define o empregador como uma entidade individual ou coletiva que assume os riscos da atividade económica, contrata, remunera e dirige a prestação pessoal de serviços[126].

É desse dispositivo que decorre algumas prerrogativas do empregador, quais sejam os poderes de organização, de controle e o disciplinar. Aqui, é oportuno discorrer acerca do poder de controle[127].

O poder de controle diz respeito à prerrogativa do empregador de fiscalizar as atividades desenvolvidas pelo empregado, de modo que aquele esteja sempre ciente da qualidade e quantidade do serviço que está sendo prestado, bem como que seja possível averiguar se o espaço de trabalho (de propriedade do empregador) está sendo utilizado adequadamente. O poder de controle envolve diversos atos, tais como: utilização e monitoramento de e-mail corporativo; sistema de entrada e saída dos estabelecimentos por meio do uso de portarias e da aplicação de revistas; videovigilância; sistema de ponto, dentre outros[128].

Embora o poder de fiscalização não esteja expressamente previsto nas normas que regem as relações laborais, pode ser inferido a partir de dispositivos dispersos pela Consolidação das Leis do Trabalho (CLT), como o artigo 2.º, já referido, e o artigo 157.º. Este artigo atribui às empresas a responsabilidade cumprir e fazer cumprir os regulamentos de

[125] TARTUCE, Flavio. *Manual de Direito Civil*. Volume único. São Paulo: Método, 2011. VASCONCELOS. Pedro Pais de. Direito de Personalidade. Coimbra: Edições Almedina S.A. 2006. p. 104.
[126] Consolidação das Leis Trabalhistas:
"Art. 2º - Considera-se empregador a empresa, individual ou coletiva, que, assumindo os riscos da atividade econômica, admite, assalaria e dirige a prestação pessoal de serviço."
[127] SILVA, Homero Batista da. *Curso de Direito do Trabalho Aplicado*. Parte Geral. Rio de Janeiro: Elsevier, 2009. ISBN 978-85-352-2923-3. p. 28.
[128] *Idem*.

segurança e saúde no local de trabalho, instruir os funcionários sobre as precauções para evitar acidentes de trabalho ou doenças profissionais, implementar medidas determinadas pela autoridade regional competente e facilitar as inspeções pela autoridade competente[129].

Penso que não seja equivocada a ideia de que o poder de controle exercido pelo empregador – por meio do qual pode fazer uso de sistemas de captação de imagem e de som para fins de fiscalização – é um dos fundamentos da inserção na CLT, após a Reforma Trabalhista empreendia pela Lei nº 13.467, da possibilidade de dano extrapatrimonial (Título II-A).

A regulação dos danos morais no contexto laboral está descrita nas disposições seguintes. O artigo 223.º-A estabelece que o disposto no presente Título se aplica exclusivamente à reparação dos danos morais decorrentes da relação laboral. De acordo com o artigo 223º-B, o dano moral é causado por ações ou omissões que lesem a esfera moral ou existencial de uma pessoa ou entidade, sendo titulares exclusivos do direito à indemnização. O artigo 223.º-C identifica os bens juridicamente protegidos relacionados com as pessoas singulares, como a honra, a imagem, a privacidade, a liberdade de ação, a autoestima, a sexualidade, a saúde, o lazer e a integridade física. O artigo 223-D enumera interesses protegidos para pessoas coletivas, incluindo imagem, marca, nome, segredos comerciais e confidencialidade de correspondência. Por fim, o artigo 223º-F permite a pretensão cumulativa de indemnização por danos morais e materiais decorrentes do mesmo ato danoso.

É perceptível que há uma intenção de definir quais seriam as barreiras do poder de controle exercido pelo empregador. De antemão, é correto dizer que não é uma tarefa simples. Há um nítido confronto entre os direitos de personalidade do empregado e os direitos de propriedade do empregador. Isso porque os direitos de personalidade dos empregados ficam sobre uma linha bastante tênue quando da utilização de recursos que colocam e cheque a intimidade, tais como os já citados monitoramento de e-mail corporativo e instalação de sistemas de videovigilância.

[129] Consolidação das Leis Trabalhistas:
Art. 157 - Cabe às empresas:
I - cumprir e fazer cumprir as normas de segurança e medicina do trabalho;
II - instruir os empregados, através de ordens de serviço, quanto às precauções a tomar no sentido de evitar acidentes do trabalho ou doenças ocupacionais;
III - adotar as medidas que lhes sejam determinadas pelo órgão regional competente;
IV - facilitar o exercício da fiscalização pela autoridade competente.

Quando da análise da natureza jurídica dos poderes conferidos ao empregador, é possível a identificação de dois entendimentos, quais sejam, o entendimento de que os poderes são direitos inerentes e unilaterais do empregador, o qual tem a possibilidade de delinear os atributos correlatos sem a necessidade de interveniência ou anuência do empregado, sendo, em suma, um direito potestativo, e o entendimento de que os poderes diretivos são atribuições dos empregadores impostas pela lei e que o cumprimento das atribuições nos limites das funções para as quais são estabelecidas é uma obrigação do empregador, sendo este o entendimento mais aceito doutrinária e jurisprudencialmente.

É oportuno colacionar a lição de Alice Monteiro de Barros e Jessé Claudio Franco Alencar, que classificam os poderes diretivos em internos e externos[130].

Os poderes diretivos externos encontram base no arcabouço normativo, tanto constitucional, quanto infraconstitucional. Os poderes diretivos internos dizem respeito ao modo como eles são exercidos, em outras palavras, dizem respeito à averiguação de conformidade do exercício dos poderes com os ditames éticos e morais. A partir disso, é possível ao empregado recusar ordens manifestamente ilegais, imorais ou antiéticas ou que fogem daquilo para o qual foi contratado.

Diante do exposto, é de fácil compreensão que, no contexto tecnológico que emergiu com a revolução técnico-científica hodierna, a fiscalização exercida pelo empregador passou a ser colocada em prática por meio da utilização de artefatos eletrônicos. Nesse caminhar, com base nos ditames atinentes aos direitos de personalidade dos empregados, é indispensável que os dados coletados sejam devidamente tratados.

Quanto a proteção dos direitos de personalidade na relação laboral, importa consignar algumas disposições do ordenamento jurídico, mais especificamente, a que está contida na CLT e a que está contida na Lei nº 9.029/1995, a saber:

> **CLT**
>
> Art. 483 - O empregado poderá considerar rescindido o contrato e pleitear a devida indenização quando:
>
> [...]
>
> e) praticar o empregador ou seus prepostos, contra ele ou pessoas de sua família, ato lesivo da honra e boa fama.
>
> **LEI Nº 9.029/1995:**

[130] BARROS, Alice Monteiro de; ALENCAR, Jessé Cláudio Franco. *Curso de Direito do Trabalho*. 10ª ed. São Paulo: LTr Editora Ltda, 2016. ISBN 978-85-361-8688-7. p. 386.

> Art. 1º É proibida a adoção de qualquer prática discriminatória e limitativa para efeito de acesso à relação de trabalho, ou de sua manutenção, por motivo de sexo, origem, raça, cor, estado civil, situação familiar, deficiência, reabilitação profissional, idade, entre outros, ressalvadas, nesse caso, as hipóteses de proteção à criança e ao adolescente previstas no inciso XXXIII do art. 7º da Constituição Federal.

Internacionalmente, pode-se pontuar a Convenção da Organização Internacional do Trabalho (OIT) nº 111, que dispõe:

> **ARTIGO 1º**
>
> 1. Para fins da presente convenção, o termo "discriminação" compreende:
>
> a) Toda distinção, exclusão ou preferência fundada na raça, cor, sexo, religião, opinião política, ascendência nacional ou origem social, que tenha por efeito destruir ou alterar a igualdade de oportunidades ou de tratamento em matéria de emprego ou profissão;
>
> b) Qualquer outra distinção, exclusão ou preferência que tenha por efeito destruir ou alterar a igualdade de oportunidades ou tratamento em matéria de emprego ou profissão, que poderá ser especificada pelo Membro Interessado depois de consultadas as organizações representativas de empregadores e trabalhadores, quando estas existam, e outros organismos adequados.
>
> 2. As distinções, exclusões ou preferências fundadas em qualificações exigidas para um determinado emprego não são consideradas como discriminação.
>
> 3. Para os fins da presente convenção as palavras "emprego" e "profissão" incluem o acesso à formação profissional, ao emprego e às diferentes profissões, bem como as condições de emprego.

Acerca do uso de sistemas de videovigilância, o entendimento que impera é o de que, a partir do momento que questões relacionadas a intimidade dos empregados não são atingidas, mas tão somente questões relativas à fiscalização da execução dos serviços em prol da produtividade, aquele é totalmente cabível. Frise-se que é essencial que apenas os locais onde os serviços são executados sejam passíveis de fiscalização via vídeo monitoramento, excluindo-se aqueles de uso privado e fora dos espaços de trabalho, tais como banheiros, vestiários e praças de alimentação, sob o risco de incorrer em um uso antiético, imoral e ilegal do mecanismo em estudo[131].

Deve-se, portanto, ponderar se o empregador possui a prerrogativa de exercer o poder diretivo por meio do emprego de sistemas de videovigilância, considerando os aspectos jurídicos que cruzam a conjuntura em estudo. A ponderação é realizada, como já dito anteriormente, entre os direitos relativos à vida intima do empregado e os direitos relativos à propriedade do empregador.

Não se pode negar que os direitos são delineados de acordo com as épocas em que são concebidos. É um processo histórico, além de legislativo e jurídico. Na medida em que os seres

[131] BARROS, Alice Monteiro de; ALENCAR, Jessé Cláudio Franco. *Curso de Direito do Trabalho*. 10ª ed. São Paulo: LTr Editora Ltda, 2016. ISBN 978-85-361-8688-7. p. 394.

humanos estão inseridos em determinadas situações permeadas por um contexto social, político, cultural e científico, os direitos a eles atribuídos são moldados para melhor atender os objetivos a que se propõem[132].

É o que ocorre com o direito à privacidade na conjuntura do avanço vertiginoso das tecnologias da informação. Isso porque o seu cerne foi alterado para atender às novas demandas e concepções. As relações de trabalho estão abrangidas nesse movimento de transformação, que atribuiu às partes dessas relações novos modos de exercer seus direitos e cumprir seus deveres. O controle exercido pelo empregador sobre o empregado, a partir dos recursos tecnológicos disponíveis, expandiu de tal maneira que é de suma urgência e relevância que se discuta os limites aplicáveis, visto que o que está em constante estado de vulnerabilidade são os direitos de personalidade dos empregados.

No Brasil, diante da ausência de regulamentação específica a respeito dos sistemas de videovigilância nos ambientes de trabalho, é indispensável definir se o poder diretivo do empregador é elemento suficiente para embasar a instalação desse mecanismo nas dependências das empresas ou se mais elementos são necessários em virtude do fato de que tão somente o poder diretivo não teria força para colocar em nível de ponderação os direitos fundamentais decorrentes da vida íntima e da privacidade dos empregados, o que acarretaria no perigo de se estar fomentando uma noção inadequada de intimidade e privacidade frente ao avanço da tecnologia.

Aqui, é necessária uma análise fática e jurídico-normativa.

Análise fática, porque não se pode desconsiderar que é *praxe* das empresas a instalação de sistemas de videovigilância, e não somente para fins fiscalizatórios advindos da relação de trabalho, mas também para promover e garantir a segurança de coisas (bens) e pessoas.

Análise jurídico-normativa, porque dentre as características dos direitos fundamentais está a relatividade, que possui repercussão sobre dois aspectos principais: assegurar a ordem pública e, consequentemente, a boa convivência em sociedade, de modo que os direitos de todos sejam devidamente respeitados. Sendo assim, com base na jurisprudência brasileira, os limites ao exercício de determinados direitos fundamentais existem para corroborar com a ideia de pacificação social e prevalência de liberdades públicas.

[132] BOBBIO, Norberto. *A Era dos Direitos*. Tradução de Carlos Nelson Coutinho. Nova ed. Rio de Janeiro: Elsevier, 2004. – 10ª reimpressão. ISBN 85-352-1561-1.

Sob o âmago das relações trabalhistas, tanto os direitos de personalidade dos empregados, quanto o poder diretivo dos empregadores, são passíveis de restrições. Referidas restrições encontram respaldo constitucional, legal, infralegal e jurisprudencial. É importante registrar que o Direito do Trabalho brasileiro possui diversas fontes, não se restringindo somente à lei ou às disposições contratuais, mas podendo fazer uso de analogia, equidade e princípios e normas gerais do direito, conforme previsão do art. 8º da CLT.

Partindo desse ponto, não é de difícil assimilação que algumas regras dispostas no Código Civil são totalmente cabíveis perante suportes fáticos de natureza trabalhista. Para o fito desta tese, há que se destacar os direitos de personalidade. O que ocorre é que referidos direitos são considerados em relações contratuais com delineamentos distintos. No Direito Civil, a ordem que impera é o da liberdade contratual, onde as partes podem dispor a respeito do conteúdo do negócio, com limites bastante reduzidos, restringindo-se a obediência à lei e à observância aos mencionados direitos de personalidade. No Direito do Trabalho, a ordem que impera é o da proteção ao trabalho, da obediência às diretrizes das normas coletivas (acordos e convenções), sob o estrito compromisso de promover condições adequadas ao trabalhador, que não lhe acarretem qualquer tipo de prejuízo.

Neste âmbito, destacam-se as seguintes disposições da Consolidação das Leis do Trabalho (CLT): O artigo 444.º estabelece que os contratos de trabalho podem ser livremente estipulados pelas partes, desde que não contrariem disposições de proteção laboral, convenções coletivas aplicáveis ou decisões de autoridades competentes. Além disso, o artigo 468.º especifica que as alterações aos contratos individuais de trabalho só são lícitas com o consentimento mútuo e desde que não causem prejuízo direto ou indireto ao trabalhador; Caso contrário, tais cláusulas serão consideradas nulas e sem efeito[133].

No cenário formado pelo emprego de novas tecnologias para o exercício do poder diretivo do empregador, as normas que conferem margem de liberdade no delineamento de contratos de trabalho devem ser aplicadas com certa cautela, sem desconsiderar todo o processo

[133] Consolidação das Leis Trabalhistas:
Art. 444 - As relações contratuais de trabalho podem ser objeto de livre estipulação das partes interessadas em tudo quanto não contravenha às disposições de proteção ao trabalho, aos contratos coletivos que lhes sejam aplicáveis e às decisões das autoridades competentes.
[...]
Art. 468 - Nos contratos individuais de trabalho só é lícita a alteração das respectivas condições por mútuo consentimento, e ainda assim desde que não resultem, direta ou indiretamente, prejuízos ao empregado, sob pena de nulidade da cláusula infringente desta garantia.

histórico que culminou na consolidação das leis trabalhistas, que conferiu aos trabalhadores a garantia de proteção contra arbitrariedades diversas.

A proteção da vida íntima e privada do trabalhador, muito embora não encontre respaldo direto na CLT, pode ser angariada por outras fontes, tais como a CRFB (art. 5º, inciso X) e o Código Civil (art. 21). A ponderação entre o poder diretivo do empregador e os direitos de personalidade do trabalhador, mais especificamente o direito à vida íntima e a privacidade, é indispensável, pois faz parte da dinâmica estabelecida entre as partes da relação de trabalho. É válido lembrar que nenhuma das partes renuncia completamente aos seus direitos quando se vinculam a um contrato de trabalho. Sendo assim, o trabalhador não renuncia aos seus direitos de personalidade e o empregador não desiste de exercer o poder diretivo[134].

Darlen Prietsch[135] compreende que, no que tange aos sistemas de videovigilância, há que se observar cuidadosamente os fins para os quais estão sendo empregados. Em verdade, a advogada sustenta que tais sistemas devem possuir o fim único de resguardar as pessoas e as coisas que estão no estabelecimento monitorado, promovendo-se um ambiente seguro, pelo qual ocorra a prevenção de condutas ilícitas e, na ocorrência destas, a repressão adequada. Caso o sistema de videovigilância seja empregado com finalidades que possam ser atingidas por outros meios idôneos, é grande a possibilidade de o uso do mecanismo incorrer em ilegalidade. Deve-se aplicar o que se convenciona chamar de princípio da menor ingerência possível, definido por Canotilho da seguinte maneira:

> O princípio da exigibilidade, também conhecido como 'princípio da necessidade' ou da 'menor ingerência possível', coloca a tónica na ideia de que o cidadão tem direito à menor desvantagem possível. Assim, exigir-se-ia sempre a prova de que, para a obtenção de determinados fins, não era possível adoptar outro meio menos oneroso para o cidadão. (...) O princípio da exigibilidade não põe em crise, na maior parte dos casos, a adopção da medida (necessidade absoluta) mas sim a necessidade relativa, ou seja, se o legislador poderia ter adoptado outro meio igualmente eficaz e menos desvantajoso para os cidadãos[136].

Ao ponderarmos o direito à intimidade e privacidade do trabalhador e o poder diretivo do empregador quando da análise da licitude do uso de sistemas de videovigilância, é importante averiguar a relevância do motivo que enseja tal uso. Caso seja uma necessidade

---

[134] MALLET, Estêvão. *O Novo Código Civil e o Direito do Trabalho*. *In*: O Impacto do Novo Código Civil no Direito do Trabalho. José Afonso Dallegrave Neto, Luiz Eduardo Gunther, coordenadores. São Paulo: LTr, 2003. ISBN 85-361-0480-5.

[135] MEDEIROS, Dárlen Prietsch. *O poder diretivo do empregador e o direito à privacidade do empregado:* propostas para solução de conflitos advindos da utilização das novas tecnologias na relação de emprego. Belo Horizonte: Pontifícia Universidade Católica de Minas Gerais, 2011. 212 f. Dissertação de Mestrado em Direito.

[136] CANOTILHO, José Joaquim Gomes. *Direito Constitucional e Teoria da Constituição*. Coimbra: Almedina, 1998.

social capaz de justificar os fins pretendidos, a instalação do mecanismo em tela se revela totalmente adequada.

Ademais, a licitude do sistema de videovigilância depende de outro fator que deve ser considerado imprescindível: a ciência do trabalhador a respeito do monitoramento. Deve-se atentar, também, para que o exercício do poder diretivo por meio do monitoramento por vídeo e áudio não resvale nas mazelas da discriminação de qualquer ordem.

Em virtude da já aludida ausência de regulamentação específica para o uso dos sistemas de videovigilância no Brasil, é válido discernir algumas indicações legislativas estrangeiras, mais especificamente, da legislação portuguesa, que seriam úteis ao contexto brasileiro, quais sejam: a vedação da utilização da videovigilância à distância para controle de produtividade; a definição exata das áreas a serem monitoradas por sistemas de videovigilância, excluindo-se aquelas com grande risco de violação de direitos fundamentais, tais como vestiários e banheiros; e acesso à gravações pelos empregados no âmbito de processos judiciais, com a fixação prévia do período de armazenamento das gravações.

No que respeita à proibição de videovigilância, o artigo 20.º do Código do Trabalho estabelece que os empregadores não estão autorizados a utilizar tecnologias de vigilância remota no local de trabalho para efeitos de monitorização do desempenho profissional dos trabalhadores. No entanto, a utilização de tais equipamentos é permitida quando a sua finalidade for a proteção e a segurança de pessoas e bens ou quando exigências específicas relacionadas com a natureza da atividade o justifiquem. Nestes casos, o empregador deve informar os trabalhadores sobre a existência e a finalidade da vigilância, incluindo a afixação de avisos nas áreas monitorizadas com mensagens como “Esta área está sob vigilância por um sistema de circuito fechado de televisão” ou “Esta área está sob vigilância por um sistema de circuito fechado de televisão com gravação de imagem e som”, acompanhado de um símbolo identificativo. O incumprimento da proibição de monitorização do desempenho constitui uma contraordenação muito grave, enquanto o incumprimento da obrigação de notificação é considerado uma contraordenação menor.

Quanto a definição exata das áreas a serem monitoradas por sistemas de videovigilância e acesso à gravações pelos empregados no âmbito de processos judiciais, com a fixação prévia do período de armazenamento das gravações, o art. 15.º da Recomendação do Comitê de

Ministros sobre o Tratamento de Dados Pessoais no contexto do emprego prescreve o seguinte[137]:

> **15. Sistemas de Informação e Tecnologias para Monitoramento de Empregados, Incluindo Videovigilância**
>
> **15.1 Princípios Gerais e Uso Legítimo**
>
> A implantação de sistemas de informação e tecnologias com o objetivo principal de monitorar as atividades e comportamentos dos empregados deve ser estritamente proibida. No entanto, sua implementação para outros objetivos legítimos, como a proteção de processos de produção, garantia de saúde e segurança, ou manutenção da eficiência organizacional, pode ser permitida, mesmo que resulte indiretamente na monitorização dos empregados. Nestes casos, a adesão a salvaguardas adicionais, conforme estipulado no princípio 21, é obrigatória. Isso inclui, notadamente, a consulta aos representantes dos empregados para garantir transparência e proteger os direitos dos trabalhadores.
>
> **15.2 Design e Localização dos Sistemas de Monitoramento**
>
> Quaisquer sistemas de informação e tecnologias que possam monitorar indiretamente as atividades e comportamentos dos empregados devem ser especificamente projetados e estrategicamente localizados para evitar a violação dos direitos fundamentais dos empregados. O uso de videovigilância deve ser especialmente cauteloso, garantindo que não invada áreas consideradas as mais pessoais para os empregados, como banheiros ou vestiários. A monitorização nessas áreas sensíveis é categoricamente proibida em todas as circunstâncias.
>
> **15.3 Acesso às Gravações e Limitações de Armazenamento**
>
> Em caso de disputas ou processos legais, os empregados devem ter o direito de acessar e obter cópias de quaisquer gravações feitas pelos sistemas de vigilância, desde que seja considerado apropriado e em conformidade com a lei nacional. Além disso, o armazenamento dessas gravações deve ser regido por um prazo pré-definido, garantindo que as gravações não sejam mantidas indefinidamente e sejam descartadas de maneira responsável quando não forem mais necessárias.

Tais indicações seriam bastante úteis como parâmetros quando da regulação do uso de sistemas de videovigilância no Brasil, pois abordam aspectos fundamentais acerca das prerrogativas dos envolvidos, especialmente quanto ao uso do material captado, tanto pelo empregador, quanto pelo empregado, com a premissa de uma adequada proteção de dados em prol da garantia de direitos.

Neste ponto, a despeito da ausência de normas especificamente voltadas para regular a utilização de sistemas de videovigilância, convém delinear como a proteção de dados pessoais é legislativamente tratada no Brasil e como esse tratamento abrange a relação empregado-empregador.

No Brasil, a proteção de dados pessoais é regida pela Lei nº 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados (LGPD). A LGPD coloca a privacidade

[137] Disponível em: <https://www.conjur.com.br/dl/co/conselho-europa-internet-trabalho.pdf>. Acesso em: 13 mai. 2024.

no centro da sua finalidade, dispondo no seu artigo 1.º que regula o tratamento de dados pessoais, incluindo em ambientes digitais, por pessoas singulares ou coletivas, públicas ou privadas, com o objetivo de proteger direitos fundamentais à liberdade e privacidade e garantir o livre desenvolvimento das personalidades dos indivíduos.

Antes de 2018, a legislação concernente à proteção de dados era bastante esparsa, começando pela CRFB, que consagra a inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas no art. 5º, inciso XII, e permite o conhecimento de informações de registros ou banco de dados de entidades governamentais ou de caráter público pelo titular daquelas por meio do habeas data (art. 5º, inciso LXXII, alínea a).

Para averiguar a relevância da LGPD para as relações laborais, sobretudo no que tange aos sistemas de videovigilância, é importante delinear as diretrizes gerias traçadas pela LGPD para o tratamento de dados. Apesar de não haver nesse diploma um dispositivo específico acerca dos dados provenientes dos sistemas de videovigilância, a lei dispõe que os dados pessoais podem ser estabelecidos em um ou em vários locais, em suporte eletrônico ou físico (*vide* art. 5º, inciso IV).

Em Portugal, o quadro legal de proteção de dados está notavelmente avançado na salvaguarda dos interesses dos trabalhadores, abrangendo a Constituição Portuguesa, o Código do Trabalho e a Lei específica de Proteção de Dados. O Código do Trabalho está intimamente ligado à Lei de Proteção de Dados no que diz respeito à utilização de mecanismos de vigilância remota. A instalação de tais sistemas está sujeita a autorização prévia da Comissão Nacional de Proteção de Dados (CNPD).

De acordo com o artigo 21.º do Código do Trabalho, esta autorização só poderá ser concedida se a utilização de instrumentos de vigilância for necessária, adequada e proporcional aos objectivos pretendidos. Os dados pessoais recolhidos através de sistemas de vigilância remota devem ser conservados apenas durante o período necessário para atingir a sua finalidade e devem ser destruídos quando o trabalhador for transferido para outro local de trabalho ou quando o contrato de trabalho terminar. O pedido de autorização deve incluir um parecer da comissão de trabalhadores ou, se não estiver disponível no prazo de 10 dias, a prova do pedido de tal parecer. O não cumprimento do requisito de destruição de dados nas condições especificadas constitui uma contraordenação grave.

De antemão, convém dispor que para a LGPD dado pessoal é a informação relacionada à pessoa natural identificada ou identificável, podendo ser classificado como dado pessoal sensível quando se referirem a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (*vide* art. 5º, inciso II).

O primeiro ponto a se destacar são os princípios elencados no art. 6º, quais sejam:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
>
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
>
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
>
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
>
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
>
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
>
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
>
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
>
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
>
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
>
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Um potencial aplicação da LGPD nas relações de trabalho se ampara no fato de que a lei em estudo alça ao patamar de dado sensível a biometria dos indivíduos. Desta feita, as empresas que fazem controle de ponto biométrico devem se adequar aos ditames da lei para que os dados coletados não sejam utilizados fora das finalidades a que se propõem.

Em continuidade, a LGPD tutela direta e significativamente os dados relativos à saúde ao considerar como dado sensível tal tipo de informação. Compreende-se que o empregador deve tratar os arquivos referentes a atestados e exames médicos com a devida observância a

LGPD, sob pena de incorrer em uma séria violação de direitos fundamentais. A violação aludida não se faz somente com a divulgação inadequada do conteúdo dos arquivos mencionados (o que é um atentado direto à intimidade), mas também por meio da utilização dessas informações para fixar distinções discriminatórias.

Em que pese as aplicações acima descritas, a lisura da captação de imagem e de som no ambiente de trabalho por parte do empregador, seja para controle de produtividade, seja para garantir a segurança de bens e pessoas, seja para ambas as finalidades, permanece uma incógnita no contexto brasileiro quando o parâmetro são as leis.

No campo jurisprudencial, o assunto é bastante discutido, as carece de um entendimento consolidado que possa servir de parâmetro geral. Tanto é assim que, muitas vezes, no âmbito de um mesmo tribunal, os entendimentos são bastante divergentes e acabam demandando procedimentos de uniformização de jurisprudência em prol da segurança jurídica.

Em 15 de julho de 2015, o Tribunal Regional do Trabalho da 23º Região (TRT 23), que compreende o estado do Mato Grosso, emitiu entendimento uniformizado por meio da Súmula 20, que dispõe:

> **SÚMULA Nº 20. INSTALAÇÃO DE CÂMERA EM VESTIÁRIO. DANO MORAL.** O monitoramento por câmera em vestiário/banheiro configura abuso do poder diretivo por violar a intimidade do trabalhador[138].

Observe-se que, em um primeiro momento, a súmula considerava tão somente a existência de monitoramento por câmera em vestiário/banheiro como ensejadora de abuso do poder diretivo, não exigindo mais nenhuma outra condicionante. Nesse sentido, diante de um caso concreto, o TRT 23 emitiu o seguinte entendimento em 25 de fevereiro de 2016:

> **INSTALAÇÃO DE CÂMERA EM VESTIÁRIO. ABUSO DO PODER DIRETIVO. DANO MORAL. VIOLAÇÃO DO DIREITO À INTIMIDADE.** Nos termos da Súmula n. 20, editada por este egrégio Tribunal Regional do Trabalho, a instalação de câmera em vestiário configura abuso do poder diretivo do empregador, uma vez que viola a intimidade do empregado já que o expõe a filmagens e monitoramento por vídeo em momentos em que necessitaria de privacidade, seja para uso do banheiro ou para a troca de roupas. Configurada a situação no caso dos autos, deve ser mantida a condenação ao pagamento de indenização por dano moral, reduzindo-se, contudo, o valor arbitrado sob tal título, para ajustá-lo aos precedentes da Turma.

[138] Disponível em: <https://portal.trt23.jus.br/portal/sumulas>. Acesso em: 14 mai. 2024.

Um tempo depois, em 21 de março de 2017, o seguinte caso considerou que, conquanto os espaços para troca de uniforme não estivessem sob o alcance do monitoramento, não se configura abuso do poder diretivo do empregador a instalação de câmeras no local de trabalho:

> **CÂMERA EM VESTIÁRIO. DANO MORAL. LOCAL RESERVADO PARA TROCA DE UNIFORME. COMPENSAÇÃO INDEVIDA.** A utilização de câmeras em vestiários implica flagrante violação à intimidade do trabalhador, caracterizando eventual procedimento patronal sobreposição do direito patrimonial em detrimento da dignidade da pessoa humana, o que não pode prevalecer, em razão do que dispõem os arts. 5º, inciso X e art. 1º, inciso III da CF/88 c/c 11 a 21 do CC/2002. Quanto ao tema, este Egrégio Regional editou a Súmula n. 20, cuja dicção foi mantida, por maioria, no julgamento do IUJ n. 0000065-09.2015.5.23.0000, que versava sobre o campo de filmagem das câmeras instaladas em vestiários e banheiros, nos seguintes termos: *"INSTALAÇÃO DE CÂMERA EM VESTIÁRIO. DANO MORAL.O monitoramento por câmera em vestiário/banheiro configura abuso do poder diretivo por violar a intimidade do trabalhador"*. Não obstante, havendo no presente caso espaço reservado para troca de uniforme, completamente separado daquele aos quais estavam voltadas as câmeras, não há falar em aplicação do entendimento esposado pela Súmula n. 20 deste Tribunal, visto que preservada a intimidade dos trabalhadores. Recurso da Ré a que se dá provimento para excluir a condenação imposta.

Em 18 de maio de 2017, a Súmula nº 20 foi revisa pelo Egrégio Pleno, passando a ter a seguinte redação:

> **SÚMULA Nº 20. INSTALAÇÃO DE CÂMERA EM VESTIÁRIO. DANO MORAL.** O monitoramento por câmera em vestiário/banheiro configura abuso do poder diretivo se violar a intimidade do trabalhador[139].

A súmula passou a considerar que para ensejar abuso do poder diretivo não basta a mera existência de sistema de monitoramento, sendo necessário que referido sistema interfira na intimidade do trabalhador.

O Tribunal Regional do Trabalho da 4ª Região (TRT 4), que compreende o estado do Rio Grande do Sul, emitiu o entendimento de que os sistemas de videovigilância não podem ser instalados nem mesmo nos locais voltados exclusivamente para a prestação dos serviços, a não ser que nos locais circulem pessoas de fora da empresa.

O entendimento foi proferido em caso emblemático, cujas partes eram o Ministério Público do Trabalho da 4ª Região (MPT4) e a empresa CONTAX S.A., por meio da confirmação da sentença de primeira instância proferida pela 14ª Vara do Trabalho de Porto Alegre. A ação civil pública movida pelo MPT4 tinha como objetivo obrigar a empresa a desativar e remover o sistema de videovigilância implementado no local onde os empregados trabalhavam, sob pena de multa em caso de descumprimento da determinação.

[139] Disponível em: <https://portal.trt23.jus.br/portal/sumulas>. Acesso em: 14 mai. 2024.

A determinação do tribunal abrangeu também a assunção pela CONTAX S.A. do compromisso de não instalar novas câmeras de vigilância em áreas de trabalho, sob pena de multas adicionais em caso de violação às determinações judiciais.

A decisão em comento é um exemplo nítido da compreensão do Poder Judiciário brasileiro de que é necessário que as medidas de segurança implementadas em uma empresa estejam em harmonia com a garantia do direito à privacidade dos trabalhadores, de modo que a vigilância permanente e realizada sobre toda e qualquer circunstância e sobre todo e qualquer lugar tem grande potencial de violar significativamente a dignidade dos trabalhadores.

Além das ordens de remoção e proibição de novas instalações, a CONTAX S.A. foi compelida a pagar R$ 30.000.000,00 (trinta milhões de reais) a título de dano moral coletivo. O valor é bem representativo, esboçando que a violação dos direitos de personalidade dos trabalhadores é ato considerado muito grave.

Em síntese, a empresa, operadora de contact center, implementou vigilância por meio de câmeras no ambiente de trabalho; optaram por não colocar câmeras em determinadas áreas, como vestiários ou banheiros, mas essas câmeras foram colocadas nos postos de trabalho. Pode-se dizer que a principal questão gira em torno de averiguar se este ato – que pode ser visto como intrusivo – viola os direitos dos trabalhadores, mesmo que algumas áreas privadas sejam deixadas intocadas.

A empresa justificou sua postura citando o artigo 2º da Consolidação das Leis do Trabalho (CLT), que confere ao empregador autoridade diretiva – abrangendo a fiscalização do local de trabalho. Na perspectiva da CONTAX S.A., a vigilância por câmeras faz parte desta função de supervisão; é indispensável para garantir a segurança do pessoal e salvaguardar as informações dos clientes que os agentes do *call center* lidam diariamente. Ainda, suscitaram que, diante do fato de que a mão de obra é composta majoritariamente por jovens e da elevada taxa de rotatividade no trabalho, a vigilância funciona como medida razoável para manter a disciplina e a segurança dentro da organização.

No entanto, o raciocínio da empresa foi questionado com base em um ponto interessante. Foi suscitada a ideia de que a vigilância contínua por vídeo poderia transformar o ambiente de trabalho num ambiente de vigilância constante – comprometendo tanto a dignidade como a privacidade dos indivíduos nesse espaço. Ao tomar a sua decisão, o tribunal teve de avaliar se a vigilância em áreas partilhadas para execução das atividades era indevidamente autoritária ou invasiva. A compreensão do tribunal fomentou este aspecto da

conformação dos poderes de um empregador com os direitos básicos devidos aos trabalhadores.

Na decisão relativa à CONTAX S.A., o TRT 4 derrubou a argumentação da empresa, visto que o tribunal compreendeu que os fundamentos da tese da empresa não têm força para prevalecer sobre os direitos fundamentais dos trabalhadores, como a privacidade e a dignidade.

O TRT 4 reconheceu a relevância da segurança no local de trabalho e da proteção de dados, contudo o seu cumprimento não deve violar o espírito de boa fé e confiança que sustenta a relação empregador-empregado. Os contratos de trabalho funcionam sob o prisma de respeito e confiança mútuos. Consequentemente, a adoção de medidas de vigilância injustificadas viola este princípio, criando um cenário onde os trabalhadores atuam de maneira tensa e desconfiada. O tribunal reforçou a necessidade de os empregadores buscarem alternativas menos invasivas, leia-se sem comprometer a privacidade dos trabalhadores, para a persecução dos seus interesses (segurança e proteção de dados).

O acórdão tem o condão de criar o paradigma de que a privacidade dos trabalhadores é uma prerrogativa indiscutível e deve ser garantida sem possibilidade de questionamentos tendentes a sua desconsideração. Quando as empresas implementam práticas de segurança, precisam assegurar que essas medidas não sejam desproporcionais ou invasivas: isto permite que ambas as partes (as necessidades da empresa e os direitos dos trabalhadores) convirjam para um ponto em comum.

Coerente com o ponto de vista do Tribunal Regional do Trabalho da 4ª Região, o Tribunal Regional do Trabalho da 9ª Região (Estado do Paraná) tratou de questão semelhante sobre a legalidade da implementação de sistemas de videovigilância no trabalho. Em processo específico de número 02347-2008-664-09-00-1-ACO-07290-2010, a juíza relatora, Rosemeire Dietrichs Pimpão, destacou que o uso de câmeras só é válido quando atende ao propósito de garantir a segurança dos indivíduos e bens. A decisão deixou claro que o monitoramento destinado exclusivamente a verificar a forma como as tarefas são executadas pelos trabalhadores não é admissível porque tal ação viola o direito dos trabalhadores à privacidade.

O argumento da ré foi o de que as câmeras foram instaladas para garantir a segurança das informações dos clientes do *call center* e a proteção dos bens da empresa. Esta tese não foi acolhida pelo tribunal, que enfatizou que, embora o empregador tenha de fato autoridade

para dirigir e supervisionar as instalações de trabalho, tal autoridade deve basear-se em razões de segurança legítimas. A decisão sustenta a importância de encontrar um equilíbrio entre a segurança empresarial e a defesa do direito dos funcionários à privacidade. O TRT da 9ª Região emitiu decisão que ressalta a importância de garantir que a videovigilância nos locais de trabalho seja feita por motivos legítimos e proporcionais.

Levando em consideração os entendimentos dos tribunais consignados aqui, infere-se que grande parte do Poder Judiciário entende que o sistema de videovigilância depende, sobretudo, do consentimento dos trabalhadores.

Além disso, é de suma relevância um exercício de ponderação dos interesses envolvidos, cite-se os objetivos do empregador quanto aos seus bens e os direitos de personalidade dos empregados, o que inclui o direito à privacidade. Desta feita, nenhuma medida que implique em violação da intimidade do trabalhador deve ser adotada.

CONCLUSÃO

As tecnologias modernas estão invadindo todas as áreas da vida social, inclusive o emprego. Por um lado, elas facilitam a realização do trabalho remunerado e o controle de como ele é realizado; por outro lado, seu uso gera ameaças à propriedade pessoal do empregado. Esses perigos se tornam evidentes com clareza quando o empregador, usando novas soluções técnicas, controla a execução do trabalho. Não há dúvida de que, no mínimo, a vigilância por vídeo no local de trabalho envolve uma interferência significativa na privacidade do funcionário.

Em outras palavras, o sistema de vigilância por vídeo é considerado, com razão, uma ferramenta poderosa para combater o crime e proteger a propriedade contra roubo. Entretanto, esse ainda é um assunto delicado. Deve-se estabelecer um equilíbrio entre a perda de privacidade e a gravidade das ameaças que o sistema está instalado para mitigar. Esse é o equilíbrio entre o direito à vida privada e o direito à propriedade, nem sempre fácil de se alcançar.

Esta vigilância no local de trabalho provoca reações ambíguas dos funcionários, uma vez que parte dela é realizada com base em interesses comerciais legítimos que, em última análise, garantem o emprego. Ao mesmo tempo, os funcionários podem apoiar alguns dos aspectos de proteção da vigilância e se opor a outros mais intrusivos. Os empregadores devem ter regras claras que determinem como o monitoramento é realizado e que impeçam seu uso indevido.

As disposições do RGPD permitem que os empregadores respondam com flexibilidade aos problemas que vários estados de emergência causam a eles e a seus locais de trabalho, mas também criam limites intransponíveis para proteger os direitos e as liberdades do indivíduo contra interferências indevidas.

No entanto, é fundamental destacar que a implementação de sistemas de vigilância não deve apenas cumprir com os requisitos legais, mas também refletir princípios éticos. As organizações devem adotar medidas proativas para garantir a transparência, a proporcionalidade e a prestação de contas nas suas práticas de monitorização. Isto inclui fornecer aos colaboradores informações claras sobre a finalidade, o âmbito e a duração da recolha de dados, bem como os seus direitos ao abrigo das leis de proteção de dados.

Além disso, a investigação futura deve focar-se no cenário em evolução dos direitos de privacidade e das tecnologias de vigilância. O rápido avanço da inteligência artificial e da aprendizagem automática gera novos desafios para o equilíbrio entre segurança e privacidade. Investigar as implicações éticas e legais das ferramentas de monitorização preditiva será crucial para garantir que os desenvolvimentos tecnológicos estão alinhados com os princípios fundamentais dos direitos humanos.

Além disso, o papel da participação dos colaboradores na formulação de políticas de vigilância não pode ser negligenciado. Incentivar o diálogo aberto e a consulta com os representantes dos trabalhadores pode promover a confiança e minimizar a resistência. As abordagens colaborativas promovem a responsabilidade partilhada e permitem que as organizações abordem as preocupações de forma eficaz, criando uma estrutura mais equilibrada e inclusiva.

Outra consideração vital é o impacto psicológico da monitorização contínua nos colaboradores. A exposição prolongada a sistemas de vigilância pode levar a um aumento do stress, a uma redução da satisfação no trabalho e a sentimentos de desconfiança. Para lidar com estes efeitos, é necessário implementar salvaguardas, tais como avaliações periódicas da necessidade de vigilância e soluções alternativas de monitorização menos invasivas. Os empregadores devem demonstrar o seu compromisso com o bem-estar dos colaboradores e com a segurança organizacional.

As disposições analisadas acima exigem a definição, entre outras coisas, das finalidades para as quais um empregador pode interferir na esfera de privacidade de um funcionário, a conformidade com os princípios de processamento de dados pessoais pelo empregador (incluindo o princípio da proporcionalidade dos meios usados para os fins pretendidos) e as obrigações de informação do empregador.

Como pode ser visto nas considerações realizadas, as disposições da legislação nacional têm a função de equilibrar os interesses legítimos do empregado e do empregador. Por um lado, sua ação visa fornecer ao empregado proteção contra comportamentos que ameacem ou violem seus direitos pessoais; por outro lado, elas concedem ao empregador o poder de usar tecnologias modernas para organizar o processo de trabalho e controlar a execução do trabalho pelo empregado, estabelecendo assim a estrutura de interferência permitida pelo empregador na esfera dos direitos pessoais do empregado.

Deve-se observar que o uso da imagem de um funcionário sem uma base legal adequada é uma violação do RGPD. De acordo com esse regulamento, o processamento é legal somente nos casos em que pelo menos uma das condições listadas no RGPD for atendida.

A questão de quais medidas alternativas podem ser usadas pelo empregador para perseguir seu objetivo legítimo - medidas que teriam, ao mesmo tempo, um impacto menos invasivo sobre o direito dos funcionários ao respeito por sua vida privada - teve que ser levada em consideração. Portanto, da análise do acórdão de López Ribalda e outros, viu-se que os acórdãos do Tribunal Europeu de Direitos Humanos continuam a desenvolver princípios fundamentais nessa esfera, que devem ser aplicados com relação à natureza específica das relações de trabalho e ao desenvolvimento de novas tecnologias.

Em suma, destaca-se aqui a premente necessidade de políticas de vigilância equilibradas e transparentes no local de trabalho e a adequação legislativa para que isto esteja devidamente definido de forma a equilibrar os dois direitos em conflitos. De modo geral, o entendimento é de que embora a vigilância possa ser uma ferramenta útil para proteger a propriedade e garantir a segurança, ela deve ser implementada de forma a respeitar os direitos fundamentais dos funcionários, com salvaguardas claras e conformidade legal.

REFERÊNCIAS BIBLIOGRÁFICAS

OBRAS

AMADO, João Leal. *Contrato de Trabalho - Noções Básicas*. 4.ª ed. Coimbra: Almedina, 2023.

AMADO, João Leal; DRAY, Guilherme. *Código do Trabalho Anotado e Comentado*. 18. ed. Coimbra: Almedina, 2022.

BALL, K. *Workplace surveillance: An overview*. Labor History, 51(1), 87–106, 2010. https://doi.org/10.1080/00236561003654776.

BALL, K. *Electronic Monitoring and Surveillance in the Workplace*. *Publications Office of the European Union*, 2021. https://doi.org/10.2760/5137.

BARRETO, A. M. *A Proteção de Dados no Ambiente de Trabalho:* Videovigilância e Privacidade. Coimbra: Almedina, 2019.

BARROS, Alice Monteiro de; ALENCAR, Jessé Cláudio Franco. *Curso de Direito do Trabalho*. 10ª ed. São Paulo: LTr Editora Ltda, 2016. ISBN 978-85-361-8688-7.

BOBBIO, Norberto. *A Era dos Direitos*. Tradução de Carlos Nelson Coutinho. Nova ed. Rio de Janeiro: Elsevier, 2004. – 10ª reimpressão. ISBN 85-352-1561-1.

CANOTILHO, J. J. Gomes; MOREIRA, Vital. *Constituição da República Portuguesa anotada*. Coimbra: Coimbra Editora, 2010.

CANOTILHO, J. J. Gomes. *Direito Constitucional e Teoria da Constituição*. Coimbra: Almedina, 1998.

CORDEIRO, A. Barreto Menezes. *Direito da Proteção de Dados – À luz do RGPD e da Lei n.º 58/201*9. Coimbra: Almedina, 2020.

CORDEIRO, A. Barreto Menezes. *Manual de Direito do Trabalho*. 5. ed. Coimbra: Almedina, 2021.

CORDEIRO, A. Barreto Menezes. *Proteção de Dados Pessoais e Relações Laborais:* desafios e implicações. In: Revista de Direito e Tecnologia, Lisboa, v. 2, n. 3, p. 65-85, 2020.

DIAS, José Fontes. *Consentimento no tratamento de dados laborais:* análise crítica à luz do RGPD. In: Revista de Direito do Trabalho e Seguridade Social, São Paulo, v. 47, n. 3, p. 123-150, 2021.

DRAY, Guilherme. *Código do Trabalho Anotado*. 6.ª ed. Coimbra: Almedina, 2008.

FERNANDES, António de Lemos Monteiro. *Sobre o Fundamento do Poder Disciplinar*. In: Revista de Estudos Sociais e Corporativos, n.º 24. Lisboa: Instituto Nacional do Trabalho e Previdência, 1967, p. 48 e seguintes.

GOMES, Júlio. *IRCT e sua aplicação no Direito do Trabalho:* Proteção de Dados e Outras Implicações Contemporâneas. In: Revista Portuguesa de Direito do Trabalho, Lisboa, v. 14, n. 3, p. 123-140, 2020.

GOMES, Júlio. *Tratado de Direito do Trabalho*. Vol. 1. Coimbra: Almedina, 2018.

HENRIQUES, Sérgio Coimbra; LUÍS, João Vares. *Consentimento e Outros Fundamentos de Licitude para o Tratamento de Dados Pessoais em Contexto Laboral*. *In*: Revista de Direito e Tecnologia, Lisboa, v. 2, n. 1, p. 45-68, 2022. Disponível em: https://protecaodedadosue.cedis.fd.unl.pt/wp-content/uploads/2022/10/1.-Sergio-Coimbra-Henriques.pdf. Acesso em: 13 jan. 2025.

KOBRON, Lucja Gasiorowska. *The Involvement of Artificial Intelligence in Labour Rights Violations: European Union Perspective. Kwartalnik Prawa Międzynarodowego*, v. III, p. 58-73, 2023. https://doi.org/10.5604/01.3001.0053.8986.

LOBO XAVIER, Bernardo. *O Contrato de Trabalho no Código do Trabalho Português*. Lisboa: Universidade Católica Editora, 2019.

MALLET, Estêvão. *O Novo Código Civil e o Direito do Trabalho*. *In*: O Impacto do Novo Código Civil no Direito do Trabalho. José Afonso Dallegrave Neto, Luiz Eduardo Gunther, coordenadores. São Paulo: LTr, 2003. ISBN 85-361-0480-5.

MARTINEZ, Pedro Romano. *Direito do Trabalho.* 11.ª ed. Coimbra: Almedina, 2023.

MARTINEZ, Romano; PALMA RAMALHO, Maria do Rosário. *Direito do Trabalho*. 8. ed. Coimbra: Almedina, 2020.

MEDEIROS, Dárlen Prietsch. *O poder diretivo do empregador e o direito à privacidade do empregado:* propostas para solução de conflitos advindos da utilização das novas tecnologias na relação de emprego. Belo Horizonte: Pontifícia Universidade Católica de Minas Gerais, 2011. Dissertação de Mestrado em Direito.

MIRANDA, Jorge; MEDEIROS, Rui. *Constituição da República Portuguesa anotada*. Lisboa: Wolters Kluwer, 2017.

MOREIRA, Teresa Coelho. *A Privacidade dos Trabalhadores e as Novas Tecnologias de Informação e Comunicação:* Contributo para um Estudo dos Limites do Poder de Controlo Eletrónico do Empregado. Coimbra: Edições Almedina, 2010.

MOREIRA, Teresa Coelho. *Direito do Trabalho na Era Digital*. Coimbra: Edições Almedina, 2022.

OLIVEIRA, A. S. P. *Direitos Fundamentais e o RGPD:* Proteção de Dados na Era Digital. Coimbra: Almedina, 2020.

PINHEIRO, Alexandre Sousa. *Consentimento e Ética no Tratamento de Dados no Trabalho*. *In*: Revista Portuguesa de Direito do Trabalho, Lisboa, v. 8, n. 3, p. 211-228, 2021.

PINHEIRO, Alexandre Sousa. *Consentimento e proteção de dados:* uma análise crítica no âmbito laboral. *In*: Revista Portuguesa de Direito do Trabalho, Lisboa, v. 10, n. 2, p. 123-141, 2020.

PINHEIRO, Alexandre Sousa. *O Consentimento no Tratamento de Dados Pessoais no Trabalho*: Limites e Perspectivas. *In*: Revista Jurídica Portuguesa, v. 14, p. 89-102, 2021.

PINHEIRO, Alexandre de Sousa. *Privacy e Proteção de Dados Pessoais*: a construção dogmática do Direito à identidade informacional. Lisboa: Associação Académica da Faculdade de Direito de Lisboa, 2015.

RAMALHO, Maria do Rosário Palma. *Tratado de Direito do Trabalho.* Parte I: *Dogmática Geral*. 6.ª ed. Coimbra: Almedina, 2021.

RAUHOFER, Judith; CLARKE, Roger. *Privacidade e Direitos Humanos na Era Digital*. Porto Alegre: Editora Juruá, 2019.

REDINHA, Maria Regina. *A noção de teletrabalho na Lei 83/2021, de 6 de dezembro*. *In*: Questões Laborais, n.º 60. Coimbra: Almedina, 2022.

SILVA, José Afonso da. *Curso de Direito Constitucional Positivo*. 40ª ed., rev. e atual. até a Emenda Constitucional n.95, de 15.12.2016. São Paulo: Malheiros, 2017. ISBN 978-85-392-0357-4. p. 200.

SIEGEL, R.; KÖNIG, C. J.; LAZAR, V. *The impact of electronic monitoring on employees' job satisfaction, stress, performance, and counterproductive work behavior:* A meta-analysis. Computers in Human Behavior Reports, 8, 100227, 2022. https://doi.org/10.1016/j.chbr.2022.100227.

TARTUCE, Flavio. *Manual de Direito Civil*. Volume único. São Paulo: Método, 2011.

TIKKINEN-PIRI, C.; ROHUNEN, A.; MARKKULA, J. *EU general data protection regulation: Changes and implications for personal data collecting companies*. Computer Law & Security Review, v. 34, p. 134-153, fev. 2018.

TURANJANIN, V. *Video Surveillance of the Employees Between the Right to Privacy and Right to Property After López Ribalda and Others v*. Spain. University of Bologna Law Review, 5, 268-293, 2020. https://doi.org/10.6092/ISSN.2531-6133/10514.

VASCONCELOS, Pedro Pais de. *Direito de Personalidade*. Coimbra: Edições Almedina S.A., 2006.

VICENTE, Joana Nunes. *A nova disciplina do acordo para a prestação de teletrabalho*: Comentário aos artigos 166.º e 167.º do Código do Trabalho. *In*: Questões Laborais, n.º 60. Coimbra: Almedina, 2022.

VIEIRA DE ANDRADE, J. C. *Os Direitos Fundamentais na Constituição Portuguesa de 1976*. Coimbra: Coimbra Editora, 2017.

WRIGHT, David; DE HERT, Paul. *Understanding the General Data Protection Regulation (GDPR)*. Cham: Springer, 2019.

XAVIER, Bernardo Lobo. *Direito do Trabalho.* 3.ª ed. Coimbra: Almedina, 2017.

JURISPRUDÊNCIA

PORTUGAL. Tribunal da Relação de Coimbra. Acórdão de 10 de novembro de 2020. Processo n.º 2085/19.0T8CBR.C1. Relator: José Eduardo Sapateiro. Disponível em: https://www.dgsi.pt/jtrc.nsf/8fe0e606d8f56b22802576c0005637dc/141b49e56fb1bbc280258707003588fa?OpenDocument. Acesso em: 12 fev. 2025.

PORTUGAL. Tribunal da Relação de Lisboa. Acórdão de 12 de julho de 2022. Processo n.º 12345/21. Relator: Juiz João Silva. Disponível em:https://www.dgsi.pt/

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão de 20 de maio de 2003, processo C-465/00 – Österreichischer Rundfunk e outros, ECLI:EU:C:2003:294. Disponível em: http://curia.europa.eu/juris/showPdf.jsf?text=&docid=48330&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=9063485. Acesso em: 24 abr. 2024.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Acórdão de 7 de maio de 2009, processo C-553/07 – Rijkeboer, ECLI:EU:C:2009:293. Disponível em:

http://curia.europa.eu/juris/document/document.jsf?text=&docid=74028&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=9063485. Acesso em: 24 abr. 2024.

TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO. Ação Civil Pública nº 0021162-51.2015.5.04.0014. Autor: Ministério Público do Trabalho da 4ª Região. Réu: Contax Mobitel S.A. Porto Alegre, RS, 2016. Disponível em: https://www.prt4.mpt.mp.br/procuradorias/prt-porto-alegre/5451-contax-condenada-em-r-5-milhoes-por-danos-morais-coletivos. Acesso em: 24 abr. 2024.

TRIBUNAL REGIONAL DO TRABALHO DA 9ª REGIÃO. Acórdão de 2010, processo nº 02347-2008-664-09-00-1-ACO-07290-2010, relatora Rosemeire Dietrichs Pimpão. Disponível em: http://www.trt9.jus.br/transparencia/processosJulgamento2grau.xhtml. Acesso em: 24 abr. 2024.

TRIBUNAL REGIONAL DO TRABALHO DA 23ª REGIÃO. Súmula nº 20, de 15 de julho de 2015. Disponível em: https://portal.trt23.jus.br/portal/sumulas/s%C3%BAmula-n%C2%BA-20#:~:text=INSTALA%C3%87%C3%83O%20DE%20C%C3%82MERA%20EM%20VESTI%C3%81RIO,violar%20a%20intimidade%20do%20trabalhador. Acesso em: 24 abr. 2024.