PROTEÇÃO DE DADOS E USO DA TECNOLOGIA NO MONITORAMENTO DO TRABALHADOR: DA EXPERIÊNCIA PORTUGUESA ÀS PROJEÇÕES NO BRASIL

Célio Pereira Oliveira Neto

RESUMO: Baseando-se na comprovação de que o Direito Português se encontra mais estruturado diante de uma cultura da proteção de dados pessoais, inclusive no campo das relações laborais, parte-se dessa vivência, mediante análise, por meio da pesquisa bibliográfica da doutrina, legislação e jurisprudência lusitana, diretivas e recomendações da União Europeia, além de acórdãos que marcaram importantes posições no âmbito do Tribunal Europeu de Direitos Humanos, propondo-se uma reflexão, por vezes comparativa, no que tange ao uso das tecnologias, parte das vezes ambivalentes - pois representam ao mesmo tempo instrumento de trabalho e controle – que permitem a vigilância à distância, geolocalização e monitoramento do correio eletrônico e seus impactos nos direitos à privacidade e intimidade, destacadamente no que se refere à tutela dos dados pessoais do trabalhador, analisando o momento atual da doutrina e da jurisprudência, a fim de traçar projeções e apresentar caminhos quanto ao uso dessas tecnologias à luz da Lei Geral de Proteção de Dados no Brasil no campo das relações de trabalho.

PALAVRAS-CHAVE: Proteção de dados; vigilância à distância; geolocalização; monitoramento; correio eletrônico; proporcionalidade.

ABSTRACT: Based on the evidence that Portuguese law is more structured in the face of a culture of personal data protection, including in the field of labor relations, this experience is based on an analysis, trough bibliographical research of Portuguese doctrine, legislation and jurisprudence, directives and recommendations of the Federal

Célio Pereira Oliveira Neto

Membro da Academia Brasileira de Direito do Trabalho (titular da cadeira 75). Pós-Doutorando pela Faculdade de Direito da Universidade do Porto; Doutor e Mestre pela PUC/SP; Pesquisador GETRAB/USP, Professor convidado PUC/SP, PUC/PR, UCAM/RJ, EmatraIX, ABDConst, Sócio-fundador Célio Neto Advogados. E-mail: celio@celioneto.com.br, https://orcid.org/0000-0002-0844-5923.

Union, in addition to judgments that marked important positions in the scope of the European Court of Human Rights, proposing a reflection, sometimes comparative, regarding the use of technologies, sometimes ambivalent – because they represent, at the same time, an instrument of work and control – which allow remote surveillance, geolocation and monitoring of electronic mail and their impacts on the rights to privacy and intimacy, especially with regard to the protection of the worker's personal data, analyzing the current moment of doctrine and jurisprudence, in order to draw projections and present paths regarding the use of these technologies in the light of the General Data Protection Law in Brazil in the field of labor relations.

KEY WORDS: Data protection; remote surveillance; geolocation; monitoring; e-mail; proportionality.

SUMÁRIO:

1. Introdução

Há aproximadamente vinte anos, Maria Regina Redinha e Maria Raquel Guimarães, já apontavam a informação como motor do crescimento, e não mais o setor energético, alertando inclusive que a informação tendia a ser um bem apropriável.[1]

A previsão se realizou em meio à sociedade da informação, onde de um lado, o dado aparece como direito e patrimônio; de outro a disponibilização de informações pessoais de forma inocente em sites de navegação e redes sociais, seja para "ganhar uma curtida", exibindo-se no mundo dos heróis, seja em troca de mínimos descontos ou mesmo para ter acesso a produtos, serviços e informações.[2]

Ocorre que a coleta e combinação de dados de diferentes fontes representa elevado risco de desnude do indivíduo, ao ponto de influenciá-lo em suas decisões. Os episódios envolvendo a *Cambridge Analytica* na eleição americana e no *Brexit* bem mostraram a força do uso dos dados quando de modo dirigido, observadas as preferências individualizadas.

Nessa linha, imagine-se o risco desse desnude ao tratar do setor de saúde, onde já se tem notícias da internet das coisas de saúde (*IoHt – Internet of Healthcare Things*) combinando sensores ao ponto de permitir a emissão de alerta sobre os níveis de poluição para uma pessoa asmática.[3]

Nas relações de trabalho a situação não é diversa, na medida em que o uso da tecnologia se faz diuturnamente presente no curso do contrato de trabalho, possibilitando inclusive a combinação de dados com potencial para definição de perfis.

Ainda que não tenha por escopo a coleta de dados, tal acaba por ocorrer, do que são meros exemplos as câmeras de segurança instaladas nas organizações, as imagens gravadas em evento do empregador ainda que limitadas à divulgação interna, a geolocalização de veículos da empresa ou mesmo computadores utilizados pelos trabalhadores no desempenho das atividades.[4]

1 Maria Regina Gomes Redinha / Maria Raquel Guimarães, «O uso do correio electrónico no local de trabalho – algumas reflexões», *in* **Estudos em homenagem ao Professor Doutor Jorge Ribeiro de Faria**, Faculdade de Direito da Universidade do Porto, Coimbra Editora, Coimbra, 2003, pp. 647-671, in https://repositorio-aberto.up.pt/bitstream/10216/24325/2/49769.pdf, p. 647 e 648.

2 Dom Total, A LGPD e o Direito como limite ao determinismo tecnológico, 2020, in https://domtotal.com/noticia/1481541/2020/11/a-lgpd-e-o-direito-como-limite-ao-determinismo-tecnologico (18.05.2023).

3 Carlos André Ferreira Dias, **A Privacidade na era da Internet das Coisas:** Direitos de Personalidade e Proteção de Dados. Dissertação de Mestrado, Faculdade de Direito da Universidade do Porto, 2019, in https://hdl.handle.net/10216/140094 (15.05.2023), p. 8 e p.28.

4 Duarte Abrunhosa e Sousa / Rui Coimbra Gonçalves, «Cessação do contrato de trabalho e

E quando se tratam de dados pessoais, por evidente, estes não só estão sujeitos à proteção, como também representam risco de avanço nos direitos da personalidade, amplificados pela ambivalência da tecnologia, na medida em que o equipamento de trabalho não só representa o meio de execução da atividade, como, ao mesmo tempo, pode ser o instrumento utilizado para o controle.

Nesse contexto, a vigilância à distância, o monitoramento de correio eletrônico e a geolocalização estão expressamente regradas no Código de Trabalho (CT), somando-se a existência de cultura inclusive jurisprudencial, tanto no Direito Português como no Tribunal Europeu de Direitos Humanos (TEDH), servindo de referência ao Brasil, onde essas questões são incipientes e não regulamentadas.

2. O paradigma português

De um lado, amparado no direito constitucional da livre iniciativa, previsto no art. 61.º, n. 1, o empregador possui o direito de verificar o cumprimento da atividade laboral, além de tomar ciência e acompanhar o que ocorre na sede da empresa, no âmbito do seu poder de gerenciamento da atividade, diante da relação de subordinação do trabalhador, forte do art. 11.º, CT e art. 80.º, alínea "c" da CRP.

Soma-se que o empregador detém a propriedade dos equipamentos de trabalho, custeando a atividade e tendo preocupação com a segurança da informação, sobretudo interesse em prevenir danos relativos à quebra de confidencialidade, preservação do *know-how*, prevenção de danos a terceiros, inclusive de modo a cumprir princípios da proteção de dados pessoais. De outro lado, o empregado possui o direito à reserva da intimidade, privacidade e proteção de dados pessoais, mantendo os seus direitos laborais inespecíficos, que, por sinal se atrelam diretamente à dignidade da pessoa humana.

Nesse cenário, todo e qualquer monitoramento só poderá ser levado a efeito se observar os princípios que regem a coleta de dados, sobretudo da finalidade legítima que funciona como princípio orientador dos demais[5], na medida em que os dados devem ser adequados, pertinentes, não excessivos, completos e atualizados

conservação de dados pessoais dos trabalhadores», in **O Regulamento Geral de Proteção de Dados e as Relações de Trabalho – Estudos APODIT 6**, Maria do Rosário Palma Ramalho e Teresa Coelho Moreira (coord.), Associação Portuguesa de Direito do Trabalho, Livraria AAFDL, Lisboa, 2020, p. 209.

5 Teresa Coelho Moreira, **A privacidade dos trabalhadores e as novas tecnologias de informação e comunicação:** contributo para um estudo dos limites do poder de controlo electrónico do empregador, Coimbra, Livraria Almedina, 2010, p. 818.

em conformidade com a finalidade, só sendo conservados pelo tempo necessário para o cumprimento da finalidade. E claro, levados ao conhecimento do trabalhador, diante da transparência que se impõe, e a fim de que o empregado possa fazer uso do direito à autodeterminação informativa.

2.1. Vigilância à distância

A pandemia da Covid-19 acelerou sobremaneira o reconhecimento da sociedade quanto às facilidades e benefícios do teletrabalho. Nesse cenário, parte dos gestores reconheceram a autonomia de suas equipes e passaram a gerir resultados, porém, outra parte passou a preocupar-se com o monitoramento de seus subordinados[6], fazendo inclusive uso de programas para tal fim.

Softwares diversos foram postos no mercado internacional com a finalidade de controlar entrega, produtividade, períodos de inatividade e sites navegados.

On line, o programa *Teramind* propõe o monitoramento de trabalhadores, inclusive abrindo opção para o modo furtivo, para ter certeza de que está monitorando o verdadeiro comportamento do empregado, anuncia o programa.[7]

Mediante uso da tecnologia, há ainda o *Peeking*, que consiste em sensores de cadeira que medem e registram o tempo em que o trabalhador permanece sentado no seu posto de trabalho.[8]

Fato a ser notado é que a mesma tecnologia utilizada para o exercício da atividade pode ser usada para o monitoramento do trabalhador, o que conduz à preocupação quanto à definição de perfis do trabalhador que fica desnudado, na medida em que o uso dos computadores e programas deixa rastros digitais, sendo possível verificar quem fez, quando e o que fez, colhendo-se interesses e preferências do trabalhador.[9]

Na lição de Maria Regina Gomes Redinha, "homens e mulheres, no tempo e local de trabalho, não abandonam a sua qualidade de cidadãos nem se despem dos

6 Célio Pereira Oliveira Neto. **Trabalho em ambiente virtual:** causas, efeitos e conformação, 2ª ed., São Paulo, LTr, 2022, p. 295.

7 "perhaps most importantly, you'll want the option to run the software in a stealth mode, so you can be sure you're monitoring employee's true behavior ... Further, it can be deployed both in silent and transparent mode."Teramind, Detecção de ameaças internas e monitoramento de funcionários, 2023, in https://www.teramind.co/ (31.05.2023).

8 Maria Regina Gomes Redinha, «Os direitos de personalidade no Código do Trabalho: actualidade e oportunidade da sua inclusão», in **A Reforma do Código do Trabalho**, Coimbra, Coimbra Editora, 2005, in https://repositorio-aberto.up.pt/bitstream/10216/18699/2/49726.pdf (15.05.2023), p. 2.

9 Teresa Coelho Moreira, A privacidade dos trabalhadores..., op. cit., pp. 39-43.

atributos jurídicos da sua humanidade."[10]

A análise dos sites de navegação combinada com o cruzamento de dados permite conhecer preferências sexuais, religião, preocupações relativas à saúde (dados sensíveis) aos quais se somam esporte de preferência e outros, isso porque tudo fica armazenado no computador, seja por meio de *browsers* que permitem verificar as conexões, páginas visitadas, tempo da visita e datas, seja por meio dos *cookies* que permitem guardar a informação da visita a um determinado site, ou mesmo mediante o uso de *firewalls* para proteger a rede que, nessa missão, acabam realizando registro das atividades.

O Código de Trabalho de Portugal[11], forte do art. 20.º veda o uso de meios de vigilância à distância no local de trabalho, mediante o emprego de equipamento tecnológico, com a finalidade de controlar o desempenho profissional do trabalhador, só considerando tal procedimento como lícito quanto tenha por finalidade resguardar a proteção e segurança de pessoas e bens ou quando particulares exigências inerentes à natureza da atividade o justifiquem.

Maria Regina Gomes Redinha chama a atenção quanto à invisibilidade do controle, pois estabelece-se "um controlo difuso e ausente que não possibilita o acompanhamento pelo trabalhador da fiscalização que sobre si é exercida", de maneira que "não sabe nem tem possibilidade de saber por quem, quando e como está a ser vigiado."[12]

Talvez por isso que o código português preveja que o empregador deve informar sobre a existência e finalidade dos meios de vigilância, com o que se dá cumprimento ao princípio da transparência, que implica na garantia do oferecimento de informações claras, precisas e facilmente acessíveis ao titular.

Nota-se, pois, o dever de informação imposto ao empregador no sentido de comunicar ao trabalhador o regime de exceção que decorre do resguardo da proteção e segurança de pessoas e bens ou quando particulares exigências ou justifiquem.

Nesse sentido, a jurisprudência lusitana, consoante acórdão do STJ, de lavra do Relator Sousa Grandão, de 27.05.2010:

10 Maria Regina Gomes Redinha, Os direitos de personalidade..., op. cit., p. 1.

11 Portugal, Código do Trabalho – CT Lei 7/2009, in https://dre.pt/dre/legislacao-consolidada/lei/2009-34546475 (15.05.2023).

12 Maria Regina Gomes Redinha, **Da protecção da personalidade no código do trabalho**, Coimbra Editora, Coimbra, 2004, p. 880.

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

Maria Regina Redinha aponta que nos termos do n. 2 do art. 20.º, a obrigatoriedade de informar ao trabalhador não é prévia ao monitoramento, podendo a comunicação ocorrer *a posteriori*, desde que enquadrada nas disposições de exceção autorizantes[13] e, com base na boa-fé que rege as relações contratuais, informada no menor espaço de tempo.[14]

Outra decisão que também norteia os contornos da videovigilância no local de trabalho em Portugal, é o acórdão de 08.02.2006, STJ, de relatoria de Fernandes Cadilha, estabelecendo que há de existir um razoável risco de delitos a justificar a finalidade de proteção e segurança de pessoas e bens, exercida de modo geral e impessoal, não dirigido e, ainda assim sempre observado o princípio da proporcionalidade.

Acresça-se que o uso associado de som e vídeo possibilita uma intromissão ainda maior nos direitos à privacidade, intimidade e autodeterminação informativa do trabalhador, consoante Parecer 4/2004 do Grupo de Trabalho do art. 29 (GT29) sobre o Tratamento de Dados Pessoais por meio de Videovigilância, de 11 de fevereiro de 2004, orientando a minimização não só da coleta, como também do número de pessoas que tenham acesso aos dados, como corolário da proteção à privacidade e autodeterminação informativa – vedando ainda, de forma expressa, o controle quanto à qualidade e quantidade da atividade laboral.

Visando a autodeterminação informativa, a Organização Internacional do Trabalho (OIT), por meio do Repertório de recomendações práticas sobre proteção de dados pessoais dos trabalhadores, de 1997, estabeleceu, entre outros, a necessidade de prévio conhecimento por parte dos trabalhadores quando estes sofrem controles de medida e vigilância, assim como no que tange às razões que motivam o controle, horas em que o controle será levado a efeito, técnicas utilizadas para tanto e dados a serem

13 Maria Regina Gomes Redinha, Os direitos de personalidade..., op. cit., p. 9.

14 Maria Regina Gomes Redinha, Da protecção..., op. cit., p. 895.

coletados, sempre observada a menor invasão à privacidade.

Orienta ainda que a vigilância só pode ocorrer por motivo de segurança, saúde e proteção de bens, observada a vedação quanto ao controle oculto, salvo se previsto em legislação nacional ou se existentes fundadas suspeitas de atividades criminosas ou infrações graves.[15]

Tais orientações constam também do Parecer 2/2017 GT29, garantindo que os dados sejam tratados para finalidades legítimas, que sejam adequados, necessários e proporcionais, não excessivos para a finalidade, e o empregador seja transparente para com os empregados quanto à utilização e finalidade das tecnologias de monitoramento.

Ao sublinhar os riscos decorrentes do uso das novas tecnologias, o parecer aponta vez mais para o necessário equilíbrio entre o interesse legítimo dos empregadores, propondo avaliação da proporcionalidade das medidas adotadas nos diferentes cenários antes do início do tratamento, a fim de verificar se de fato este é necessário para atingir uma finalidade legítima, bem como as medidas a serem adotadas para mitigar as restrições do direito à vida privada e à confidencialidade das comunicações, tendo ainda em conta o princípio da minimização dos dados, conservando as informações pelo prazo mínimo e necessário, sendo em seguida excluídas.

A prova obtida por meio de controle oculto encontra óbice no art. 32.º, n. 8 da CRP, que expressamente prevê a nulidade, dentre outras, da prova obtida por abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações, constituindo violação à autodeterminação informativa.

De forma semelhante, em Itália, o *Statuto dei Lavoratori*[16] é expresso em seu art. 4.º ao estabelecer a proibição do uso de instrumentos audiovisuais ou de outros aparelhos com a finalidade de controle à distância da atividade dos trabalhadores, só o permitindo por meio de negociação com os representantes sindicais, e ainda assim com a finalidade de atender às razões de organização da empresa devidamente justificadas.

15 André Franco de Oliveira Passos / Edésio Passos / Sandro Lunard Nicoladeli, Anexo VII – Repertório de recomendações práticas sobre a proteção dos dados pessoais dos trabalhadores, Conferência da OIT, 1997 in https://vlex.com.br/vid/anexo-vii-repertorio-recomendacoes-718495325 (15.05.2023).

16 Italy, Legge 20 maggio 1970, n. 300 (Statuto dei lavoratori), Norme sulla tutela della libertà e dignità del lavoratori, della libertà sindacale e dell'attività sindacale nel luoghi di lavoro e norme sul collocamento, in https://www.cgil.unimi.it/wp-content/uploads/2014/01/l_300_70.pdf (15.05.2023).

Pois bem, nas hipóteses de monitoramento à distância, faz-se mister o uso do princípio da proporcionalidade e seus subprincípios da adequação, necessidade e proporcionalidade em sentido estrito. Logo, a coleta tem que ter aptidão para cumprir a sua finalidade, inexistindo outro meio menos gravoso com a mesma eficácia, e gerando menos prejuízos do que vantagens, sempre preservado o núcleo essencial do direito preterido.

O próprio Considerando 4 do RGPD enuncia que o direito à proteção de dados deve ser apreciado em relação à sua função na sociedade, prevendo a sua ponderação com outros direitos fundamentais via princípio da proporcionalidade.

Nessa condição, a visualização de traços ou dados não necessários para a finalidade pretendida implica descumprimento ao princípio da minimização da coleta, representando excesso que torna o ato ilícito, ainda que a finalidade original fosse lícita, salvo se advier benefício ao trabalhador, consoante Recomendação 89 do Conselho da Europa (CE)[17], que prevê a inexistência de incompatibilidade se a finalidade diversa da original gerar benefício ao trabalhador.

Teresa Coelho Moreira defende a inexistência de ilicitude quando da coleta da imagem para fins de segurança das pessoas e bens ou razões de organização da produção, de forma não intencional, ocorra alguma espécie de controle, sem relação com o motivo da coleta e indesejado – controle preterintencional, desde que tal não represente a aceitação do proveito do conteúdo captado, ou seja, ficando de todo vedado seu uso para prova de descumprimentos contratuais, salvo se os fatos forem particularmente gravosos, podendo constituir ilícitos penais.[18]

Durante a Covid-19, diante do isolamento social e da envergadura que ganhou o teletrabalho, objeto à época do Decreto-Lei n. 10-A/2020[19], a Comissão Nacional de Proteção de Dados (CNPD) se posicionou quanto às questões relativas ao controle pelo empregador, tanto dos tempos de trabalho quanto da própria atividade prestada pelo empregado, com o escopo de "garantir a conformidade do tratamento de dados pessoais dos trabalhadores com o regime jurídico de proteção de dados e minimizar o impacto sobre a privacidade em regime de teletrabalho."

Para a CNPD, "independentemente da propriedade dos instrumentos de

17 Agências dos direitos fundamentais da União Europeia / conselho da Europa, Manual da Legislação Europeia sobre Proteção de Dados, 2014, in https://www.echr.coe.int/Documents/Handbook_data_protection_Por.pdf (15.05.2023).

18 Teresa Coelho Moreira, A privacidade dos trabalhadores..., op. cit., pp. 507-509.

19 Portugal, Decreto-Lei 10-A/2020, de 13 de março, in https://dre.pt/dre/detalhe/decreto-lei/10-a-2020-130243053 (15.05.2023).

trabalho, o empregador mantém os poderes de direção e de controlo da execução da prestação laboral", contudo, considerando a inexistência de disposição legal que regule o controle à distância, aplica-se a regra geral.

Tomando, pois, por base a expressa previsão do art. 20.º do Código de Trabalho de Portugal (CT), a CNPD redigiu orientações sobre o controle à distância em regime de teletrabalho, enunciando que a "regra geral de proibição de utilização de meios de vigilância à distância, com a finalidade de controlar desempenho profissional do trabalhador, é plenamente aplicável à realidade do teletrabalho", rejeitando soluções tecnológicas para o controle à distância do desempenho.

Prosseguiu inadmitindo impor ao trabalhador que mantenha a câmera de vídeo permanentemente ligada, vedando *a priori* a possibilidade de gravação de teleconferências entre o empregador (ou dirigentes) e os trabalhadores.

Concluiu o primeiro item, reafirmando a possibilidade de o empregador manter o poder de controlar a atividade do trabalhador, por meio da fixação de objetivos, criação de obrigações de reporte na periodicidade que julgar adequada, ou mesmo agendando reuniões em teleconferência.

Já no que se refere ao registro da jornada de trabalho, a CNPD admite que tal seja levada a efeito por meios tecnológicos, desde que nos mesmos moldes da marcação presencial, de tal arte que as ferramentas que registram os horários sejam desenhadas, desde a concepção e por padrão, de modo a observar o princípio da minimização na coleta de dados, ou seja, não obtendo mais dados do que o necessário à finalidade proposta.

E, caso o empregador não disponha de ferramentas que atendam a tanto, de forma excepcional, entende a CNPD, que:

> "é legítimo ao empregador fixar a obrigação de envio de e-mail, SMS ou qualquer outro modo similar que lhe permita, para além de controlar a disponibilidade do trabalhador e dos tempos de trabalho, demonstrar que não foram ultrapassados os tempos máximos de trabalho permitidos por lei".

Dispõe ainda que o controle da disponibilidade do trabalhador e do cumprimento dos horários de trabalho pode ser levado a efeito "por via de contacto telefônico ou eletrónico por parte do empregador."

Retornando, a vigilância à distância em sentido *lato*, quando preenchidos os requisitos do art. 20.º do CT – ou seja, destinada à proteção e segurança de pessoas e

bens ou quando particulares exigências inerentes à natureza da atividade o justifiquem –, ainda assim antes do RGPD haveria de se cumprir previamente com a regra prevista pelo art. 21.º do mesmo diploma legal, que consiste em obter autorização da CNPD, que só seria concedida se de fato a vigilância à distância fosse necessária, adequada e proporcional.

Portanto, vez mais presente a aplicação do princípio da proporcionalidade no caso concreto, que diante da minimização do tempo de manutenção dos dados conduz à limitação da conservação ao período necessário para o atingimento das finalidades a que se destinam, devendo ser posteriormente destruídos.

Mas aqui releva observar que o pedido de autorização dirigido à CNPD[20] não é mais necessário, tendo em vista a tácita e parcial revogação do art. 21.º do CT por antinomia com o RGPD, a partir do momento em que este entrou em vigor. Isso porque o sistema legal deixou de ser heterônomo, sendo uniformizadas as regras de proteção de dados da Comunidade Europeia, passando as autoridades locais a deterem competência de fiscalização[21], mas não de normatização. Por sinal, a Lei 58/2019 dispõe no art. 3.º que a CNPD "é a autoridade de controlo nacional para efeitos do RGPD e da presente lei".

Na mesma esteira, o controle que era prévio, com o RGPD pressupõe tratamento autônomo, sem a necessidade de autorização das autoridades legais. No entanto, o art. 21.º do CT mantém a redação pós-RGPD, não sofrendo alteração com a recente modificação legislativa, promovida pela Lei 13/2023, em vigor desde 01.05.2023. Percebe-se, pois, que o legislador português perdeu a oportunidade de alterar o texto do art. 21.º do CT, especialmente ns. 1, 2 e 4.

Outrossim, cumpre mencionar que nos termos do art. 192.º do Código Penal[22], a captação, registro ou divulgação de imagens das pessoas, sem consentimento, e com a intenção de devassar a vida privada, designadamente a vida familiar ou sexual, constitui

20 Que deveria vir acompanhado do parecer da comissão de trabalhador, sendo que, se este não estivesse disponível no prazo de dez dias, o pedido de autorização poderia ser instruído mediante comprovação do pedido de parecer.

21 Nesse sentido, a própria CNPD aponta: "A CNPD controla e fiscaliza o cumprimento do RGPD, da Lei 58/2019, da Lei 59/2019 e da Lei 41/2004, bem como das demais disposições legais e regulamentares em matéria de proteção de dados pessoais, a fim de defender os direitos, liberdades e garantias das pessoas singulares no âmbito dos tratamentos dos seus dados pessoais.
CNPD – Comissão Nacional de Proteção de Dados, O que somos e quem somos, 2023, in https://www.cnpd.pt/cnpd/o-que-somos-e-quem-somos/ (15.05.2023).

22 Portugal, Código Penal – CP. Decreto-Lei 48/1995, in https://dre.pt/dre/legislacao-consolidada/decreto-lei/1995-34437675 (15.05.2023)

crime previsto com pena de prisão de até 1 ano ou pena de multa de até 240 dias.

A Recomendação do Comitê de Ministros sobre o Tratamento de Dados Pessoais no contexto do emprego CM/REC (2015/5) é no sentido de que não sejam permitidos sistemas e tecnologias de informação que tenham por escopo principal monitorar a atividade e comportamento de empregados, e quando tal ocorrer indiretamente sempre ter em consideração os direitos fundamentais, reforçando a vedação de videovigilância em locais de uso pessoal dos colaboradores.

O Parecer 2/2017 do GT29 apresenta reflexão de que o empregador pode pensar existir uma justificação para implantar pacote de softwares com a capacidade de registrar digitação no teclado, movimento do mouse, capturas de ecrã, registrar as aplicações utilizadas e o tempo de uso, ou mesmo coletar imagens por câmeras web, no entanto, diz o parecer, que o tratamento seria desproporcional, possivelmente sem fundamento jurídico.[23]

A Lei de Execução do Regulamento Geral de Proteção de Dados – Lei 58/2019 – disciplinando regras de aplicação ao RGPD em Portugal, em seu art. 28.º, n. 4 e n. 5, tutela a vedação do uso de imagens coletadas por meio de sistemas de vídeo ou outros meios de vigilância à distância, só os admitindo para uso no âmbito do processo penal, e condicionando a apuração de responsabilidade disciplinar (trabalhista) à utilização no âmbito do processo penal.

E ainda, forte do art. 19.º, estabeleceu a proibição da videovigilância em áreas destinadas aos trabalhadores, não só vestiários e instalações sanitárias, mas também locais reservados a práticas esportivas, refeitórios e ambientes destinados ao repouso e descanso, procurando, assim, garantir a privacidade do trabalhador também durante o lazer e descanso.

2.2. Geolocalização

A Recomendação do Comitê de Ministros sobre o Tratamento de Dados Pessoais no contexto do emprego CM/REC (2015/5) é no sentido de admitir o monitoramento por meio de equipamentos que revelem a localização dos seus empregados apenas para proteção da produção, segurança e bom funcionamento da organização, assim como saúde e segurança do trabalhador.

23 European Data Protection Board, Article 29 Data Protection Working Party. 17/EN WP 249. Opinion 2/2017 on data processing at work. Adopted on 8 June 2017, in https://www.pdpjournals.com/docs/88772.pdf (15.05.2023).

O art. 17.º da Carta Portuguesa de Direitos Humanos na Era Digital[24] tutela a proteção contra a coleta e tratamento de informações relativas à localização a partir de qualquer equipamento, só tendo lugar mediante o consentimento ou autorização legal do titular.

Na mesma esteira, releva observar que o direito à reserva de intimidade da vida privada está na categoria dos direitos disponíveis, de sorte que o consentimento do lesado exclui eventual ilicitude, consoante art. 340.º, n. 1, do Código Civil de Portugal (CC)[25].

O enquadramento ou não do uso da geolocalização no conceito de vigilância à distância de que tratam os arts. 20.º e 21.º do CT ainda é tema em aberto. A favor do enquadramento, acórdão do Tribunal da Relação do Porto, de 22.04.2013, no sentido de que o GPS constitui equipamento eletrônico de vigilância e controle, e o seu tratamento implica limitação ou restrição à reserva da intimidade da vida privada, violando o art. 26.º, n. 1 da CRP, de modo que a prova daí obtida para efeitos disciplinares é nula.

No mesmo sentido acórdão de 5.12.2016 do Tribunal de Guimarães, que veda a coleta de dados pessoais e registros 24 horas por dia, 7 horas por semana, aplicando à espécie os arts. 20.º e 21.º do CT.

A matéria, no entanto, é controvertida, consoante se observa do acórdão do STJ, de 13.11.2013, que entende que o poder de direção do empregador autoriza o uso do GPS diante das necessidades de serviço, não podendo ser qualificado como meio de vigilância à distância e inexistindo ofensa aos direitos da personalidade do trabalhador, não permitindo a captação ou registro de imagem ou som.[26]

Anteriormente à decisão supramencionada, por sinal, cabe destacar outro acórdão do STJ, de 22.05.2007, de relatoria de Pinto Hespanhol, também não qualificando GPS instalado em automóvel na dicção do art. 20.º do CT, haja vista que o sistema "não permite a captação das circunstâncias, duração e os resultados das visitas efetuadas aos seus clientes, nem identificar os respectivos intervenientes".

Por sinal, na compreensão de que o uso do sistema de geolocalização não constitui meio de vigilância à distância, pode ser usado inclusive para efeito de justa causa

24 Portugal, Carta Portuguesa de Direitos Humanos na Era Digital, Lei 27/2021, in https://dre.pt/dre/legislacao-consolidada/lei/2021-164870244 (15.05.2023).

25 Portugal, Código Civil – CC, Decreto-Lei 47344, in https://dre.pt/dre/legislacao-consolidada/decreto-lei/1966-34509075 (15.05.2023).

26 STJ – Supremo Tribunal de Justiça, Acórdão do STJ de (Mário Belo Morgado) n.º 73/12.3TTVNF.P1.S1, in http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/e32eab3444364cb980257c2300331c47?OpenDocument (15.05.2023).

para despedimento, tal como Acórdão proferido pelo Tribunal de Relação de Évora, de 26.10.2017, diante da adulteração pelo trabalhador do sistema de geolocalização para efeito de esconder as distâncias percorridas ao total de 97.357 quilômetros sem registro em atividades extralaborais, gerando, por consequência, elevados gastos adicionais para a empregadora.

Cumpre notar a existência de acórdãos que entenderam como lícito até mesmo o controle do desempenho profissional do trabalhador, validando o uso como meio de prova das imagens captadas em processo disciplinar, ao argumento de que a finalidade da coleta não foi exclusivamente a de controlar o desempenho profissional. Tratam-se dos Acórdãos do Tribunal da Relação do Porto de 26 de junho de 2017, cujo relator foi o Des. Jerônimo Freitas, assim como de 5.3.2018 e 23.4.2018, ambos de relatoria do Des. Nelson Fernandes – e objeto da crítica de Teresa Coelho Moreira.

A autora sustenta que se o veículo é utilizado para fins laborais e extralaborais, caberá ao empregador o ônus de criar mecanismos que permitam a separação das atividades, de modo a não violar a privacidade e intimidade do trabalhador, mediante a previsão do art. 25.º do RGPD, adotando-se a proteção de dados desde a concepção e por padrão, por meio do uso de técnicas organizativas adequadas, como a pseudonimização, de modo a limitar o tratamento aos dados estritamente necessários, de acordo com a finalidade indicada na coleta, assim como observância ao prazo mínimo de conservação e ao direito à autodeterminação informativa[27] e vedado o uso para controle do desempenho profissional, haja vista que a geolocalização, no seu entender se enquadra no conceito de vigilância à distância de que trata o art. 20.º, n. 2 do Código do Trabalho, não representando medida necessária para a execução do contrato.[28]

De toda sorte, é ponto comum a vedação do monitoramento da geolocalização quando o veículo está sendo utilizado para fins privados, devendo, pois, existir mecanismo que permita a desconexão ainda que temporária do dispositivo, tal como direciona o Parecer 2/2017 GT29, fazendo referência inclusive à proibição quanto a áreas sensíveis como locais religiosos, espaços sanitários e de convívio, ou mesmo consultas médicas, tomando-se ainda cautela quanto ao tempo de amostragem, evitando-se o monitoramento contínuo.[29]

27 Em observância também ao Considerando 78 do RGPD.

28 Teresa Coelho Moreira, Direito do Trabalho na Era Digital, Livraria Almedina, Coimbra, 2022, p. 246-247 e 251.

29 European Data Protection Board, Article 29 Data Protection..., op. cit.

A mesma linha de raciocínio vale para dispositivos de identificação por radiofrequência, tais como *microchips*, cada vez mais utilizados ante o barateamento da tecnologia utilizada, especialmente quando do descanso e fora dos tempos de trabalho, dando-se conhecimento ao trabalhador dos dados coletados e a finalidade da coleta em observância ao princípio da transparência e em cumprimento do direito à autodeterminação informativa, assim como minimizando-se a quantidade de dados e o tempo de conservação destes ao estritamente necessário. Há situações, contudo, que justificam plenamente o uso de dispositivos dessa natureza, por razões objetivas, lícitas, tal como no caso de mineiros cujos *microchips* são inseridos nas roupas de trabalho[30].

Mas jamais no próprio corpo, tal como adotado com ênfase durante a pandemia da Covid-19 em empresas no estado de Michigan, nos Estados Unidos da América. Com efeito, os microchips, aproximadamente do tamanho de um grão de arroz, eram implantados nas mãos dos empregados a fim de cumprir as funções de crachás de identificação, cartões de ponto, nomes de usuário e senhas para liberação de segurança e até cartões de crédito. Com isso, os empregados podiam abrir as portas, entrar e sair do trabalho, fazer *login* e *logoff*, ou pagar pela comida na lanchonete sem usar as mãos.

Claro que durante a crise sanitária, a medida tinha o seu valor, a questão, no entanto, tem de ser avaliada à luz do princípio da proporcionalidade, e nessa esteira, quer parecer que o legislador no Estado de Michigan entendeu pela existência de possível violação em demasia aos direitos à intimidade, privacidade e proteção de dados, tanto que a Câmara dos Deputados de Michigan aprovou o Projeto de Lei 5672, denominado *Microchip Protection Act* com vistas a proteger a privacidade dos trabalhadores de qualquer "tipo de vigilância do empregador ou da empresa" e impedir a obrigatoriedade de implantação de *microchips*.[31]

Na mesma linha de raciocínio, quer parecer abusivo aos direitos personalíssimos, o monitoramento contínuo por toda a empresa, obtendo a localização do trabalhador durante o período inteiro de trabalho, tal como a pulseira patenteada pela *Amazon* – ainda não disponível no mercado –, que identifica a localização dos empregados, monitorando os trabalhadores, inclusive vibrando se a movimentação indicar lado incompatível com as atividades laborais exercidas.[32]

Quer parecer lícito, no entanto, o uso da geolocalização para efeito de gestão da

30 Teresa Coelho Moreira, Direito do Trabalho..., op. cit., pp. 249 e 261.

31 Michigan, Microchip Protection Act passes Michigan House, Data Guidance, 30.06.2020, in https://www.dataguidance.com/news/michigan-microchip-protection-act-passes-michigan-house (02.05.2023).

32 Giovanna Sutto, «Amazon registra patente que rastreia funcionários durante horário de trabalho», InfoMoney, 05.08.2018, in https://www.infomoney.com.br/carreira/amazon-registra-patente-que-rastreia-funcionarios-durante-horario-de-trabalho/ (15.05.2023).

frota e assistência técnica, em hipóteses como tratamento de dados para distribuição de bens, transporte de valores, transporte de mercadorias, segurança privada, assim como a proteção de bens e segurança pessoal diante do transporte de materiais perigosos,[33] informando-se ao trabalhador na forma do Parecer 2/2017 GT29 quanto à instalação do dispositivo, movimentos registrados, inclusive possível modo de condução e forma da coleta.

Por sinal, o Parecer 13/2011 GT29 *sobre serviços de geolocalização em dispositivos móveis inteligentes* orienta que tais dispositivos não são de localização do pessoal, tendo por função determinar ou monitorar a localização dos veículos, não devendo ser considerados para localizar ou monitorar o comportamento dos condutores ou outros empregados.[34]

Portanto, em Portugal, linhas gerais, a geolocalização pode ser usada para fins legítimos, buscar a melhor eficiência e qualidade do serviço, otimização de recursos, assim como proteção de bens e pessoas, e jamais para efeito de obter mera localização injustificada do trabalhador, supervisionar ou controlar o rendimento do trabalho. E isso mediante o uso dos meios menos intrusivos de acordo com a necessidade, assim como observada a finalidade legítima apontada para o tratamento.

A limitação do direito do trabalhador no que tange à intimidade e privacidade deve ser avaliada à luz do princípio da proporcionalidade, apreciadas no caso concreto as medidas a serem adotadas para fazer frente aos riscos à privacidade, intimidade e proteção de dados do titular, realizando-se relatório de impacto nos termos do art. 35.º do RGPD, que prevê a descrição do tratamento acompanhada da avaliação da necessidade e proporcionalidade.

2.3. Monitoramento do correio eletrônico e outras redes

O art. 34.º da CRP[35] que contempla a inviolabilidade do domicílio e da correspondência abarca (n. 1), não só o domicílio e o sigilo da correspondência, como também outros meios de comunicação privada, assim como proíbe toda ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais

33 Nuno Cerejeira Namora, «RGPD y la vigilancia del trabajador por medios tecnológicos», in Adaptland, Diapositivas y pósteres presentados en el 2º Congresso Mundial Comunidad CIELO Laboral, in https://moodle.adaptland.it/mod/folder/view.php?id=22815 (15.05.2023).

34 GPDP – Gabinete para a Protecção de Dados Pessoais, Documentos adoptados pelo Grupo de Trabalho do Artigo 29.º para a Protecção dos Dados da Comissão Europeia, 26.05.2022, in https://www.gpdp.gov.mo/pt/references_detail/article/l3mqmkcr.html (15.05.2023).

35 Portugal, Constituição da República Portuguesa, VII Revisão Constitucional, 2005, in https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx (15.05.2023).

meios de comunicação, ressalvados os casos previstos na lei em matéria de processo criminal (n. 4).

Na lição de Teresa Coelho Moreira, o conteúdo do sigilo de correspondência e outros meios de comunicação privada de que trata a norma constitucional, não faz distinção entre gênero de correspondência, abarcando "toda correspondência pessoa a pessoa, como as cartas postais, os impressos e mesmo os casos de encomendas que não contém qualquer comunicação escrita, assim como todas as telecomunicações, abrangendo ainda o e-mail". Nessa linha, aponta a autora, o art. 18.º, n. 3 da CE, possui caráter aberto, incluindo as comunicações eletrônicas através da rede de informática, o que engloba os e-mails, até porque, o segredo tem caráter formal, independente de seu cunho íntimo ou não.[36]

Antes da atual redação do art. 22.º do CT, ainda à luz do CC, em 2003, Maria Regina Gomes Redinha e Maria Raquel Guimarães publicaram artigo contemplando importantes reflexões no uso do correio eletrônico no local de trabalho, apontando que as disposições dos arts. 75.º e 78.º do CC "estabelecem requisitos de licitude para a divulgação e a publicação de cartas-missivas, distinguindo consoante se tratem de cartas confidenciais ou não confidenciais e estendendo o regime das primeiras às memórias familiares e 'outros escritos confidenciais'." Contudo, no que se refere ao correio eletrônico, a questão coloca-se na "esfera de segredo, na medida em que se pretende, precisamente, apurar qual a extensão dessa reserva relativamente à correspondência enviada e recebida por via electrónica no local de trabalho".[37]

Valendo-se da doutrina de Orlando de Carvalho relativa às três zonas de proteção da privacidade: privada, pessoal e de segredo, à época as autoras já suscitavam o enquadramento da proteção da privacidade aos recônditos mais íntimos. Partindo dessa "demarcação", passaram a investigar "se é legítima a tomada de conhecimento pela entidade patronal do conteúdo das mensagens electrónicas trocadas entre o mesmo trabalhador e terceiros"[38], tomando por pressuposto que o simples conhecimento do conteúdo por terceiro não autorizado já seria de per se ilícito.

As autoras trataram então de fazer a demonstração à luz da Carta Portuguesa, do amplo caráter que se deve dar ao termo "correspondência", mormente em cenário

36 Teresa Alexandra Coelho Moreira, A privacidade dos trabalhadores..., cit., pp. 745-746.

37 Maria Regina Gomes Redinha / Maria Raquel Guimarães, «O uso do correio electrónico no local de trabalho ...», cit., p. 657.

38 Maria Regina Gomes Redinha / Maria Raquel Guimarães, «O uso do correio electrónico no local de trabalho ...», cit., p. 658.

de progresso tecnológico e linguagem informática, e mais adiante apresentaram série de indagações com o objetivo de avaliar situações práticas com o objetivo de sopesar de um lado os direitos à privacidade e intimidade do trabalhador, de outro os direitos decorrentes dos poderes empresariais de direção e fiscalização.[39]

Mencionaram as pegadas digitais deixadas no e-mail que não são apagadas com o mero uso da tecla "*delete*", e apontaram a necessidade de primeiro verificar a natureza do correio eletrônico, se pessoal ou coletiva, desde logo se posicionando quanto à legitimidade de acesso ao conteúdo dos correios compartilhados por vários trabalhadores, assim como aos e-mails de caráter profissional, desde que não o sejam de modo abusivo. Já no que se refere às comunicações pessoais, ainda que por meio de equipamentos empresariais e durante a jornada, no desenvolvimento das atividades laborais e no local de trabalho, a posição externada foi em sentido diverso, vedando-se o conhecimento do empregador sem o consentimento do empregado ou ordem judicial.[40]

Considerando essas primeiras posições, Maria Regina Gomes Redinha e Maria Raquel Guimarães se autoprovocaram quanto ao modo como se daria a fiscalização, haja vista que na prática se abriria a possibilidade de o empregador ter acessso ao conteúdo pessoal, afinal "só após o conhecimento efectivo do seu conteúdo poderá o empregador avaliar da sua natureza pessoal ou profissional", respondendo à autoindagação "se a conta de correio electrónico é comum e exclusivamente destinada às comunicações empresariais, então o ilícito reside na sua utilização particular", isentando o empregador de responsabilidade contratual, extracontratual e criminal, pois ausente o dolo.[41]

Retornando ao sopesamento no que tange ao correio de uso privativo do trabalhador, as autoras sustentaram que "perante a desigual natureza e qualificação jurídica dos direitos em presença", prevalece o direito de reserva e confidencialidade, acrescentando que o consentimento deverá ser prévio à intromissão, expresso e livremente revogável a todo o tempo (art. 81.º, n. 2, CC), não podendo ser presumido (art. 340.º, n. 3, CC).[42]

39 Maria Regina Gomes Redinha / Maria Raquel Guimarães, «O uso do correio electrónico no local de trabalho ...», cit., p. 659.

40 Maria Regina Gomes Redinha / Maria Raquel Guimarães, «O uso do correio electrónico no local de trabalho ...», cit., p. 660 e 661.

41 Maria Regina Gomes Redinha / Maria Raquel Guimarães, «O uso do correio electrónico no local de trabalho ...», cit., p. 662-665.

42 Maria Regina Gomes Redinha / Maria Raquel Guimarães, «O uso do correio electrónico no local

Diante dessas apreciações, as autoras fizeram alusão ao direito comparado, no que tange à adoção de uma política empresarial clara e transparente a regrar a matéria, a fim de que os trabalhadores fossem esclarecidos quanto aos seus direitos, inclusive apontando que nos EUA a instituição de políticas dessa natureza vinham sendo fator de exoneração de responsabilidade empresarial, e provocaram: "talvez se a nossa contratação colectiva tomasse este precedente em consideração se viessem a prevenir conflitos de interesses cuja harmonização e equilíbrio se podem revelar intangíveis", sustentando: "... se é inquestionável que o empregador não pode franquear a privacidade do trabalhador, não deixa de, paralelamente, dispor do direito de estabelecer os parâmetros da utilização do *e-mail* na sede da empresa", e propondo ainda que "estas directrizes referentes ao correio electrónico, estendem-se com proveito também à utilização da internet".[43]

O legislador português parece ter abraçado as linhas mestras da doutrina de Maria Regina Gomes Redinha e Maria Raquel Guimarães, ao disciplinar a matéria no art. 22.º, tratando do direito de reserva e confidencialidade do trabalhador, e prevendo inclusive a possibilidade de o empregador estabelecer regras de utilização dos meios de comunicação.

Com efeito, o art. 22.º do CT, n. 1 trata da confidencialidade de mensagens e acesso à informação, contemplando o direito do trabalhador de reserva e confidencialidade quanto ao conteúdo das mensagens de natureza pessoal e acesso à informação de caráter não profissional que envie, receba ou consulte por meio do correio eletrônico, e o n. 2 é claro ao disciplinar que "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 eletrônico".

Bem se nota que a regra legal voltada à reserva e confidencialidade da mensagem e à proibição do acesso tutela o livre desenvolvimento da personalidade, destacadamente o direito de expressão e reserva da vida privada e intimidade, mas ao mesmo tempo, sopesando valores, permite ao empregador estabelecer regras de uso para o correio eletrônico, dentre as quais pode figurar o controle do conteúdo das mensagens corporativas.

Nessa esteira de raciocínio, Teresa Coelho Moreira leciona que:

de trabalho ...», cit., p. 666.

43 Maria Regina Gomes Redinha / Maria Raquel Guimarães, «O uso do correio electrónico no local de trabalho ...», cit., p. 666-669.

> "parece-nos excessivo abranger dentro da proteção do sigilo das comunicações os e-mails profissionais, no caso de existir uma política clara acerca da sua utilização e contas separadas de e-mails. Entende-se que, no caso dos e-mails profissionais há uma relação comitente-comissário em que o empregador pode controlar o conteúdo destas mensagens, respeitando todos os requisitos para o exercício correto do seu poder de controlo, principalmente o requisito da proporcionalidade, na medida em que não nos parece que o empregador seja um terceiro para efeitos de uma prévia autorização judicial".[44]

Ademais, a tutela dispensada pelo artigo analisando é voltada ao conteúdo de mensagens pessoais, portanto, ainda que inexistente vedação ao uso do correio ou outras redes corporativas de comunicação, não se pode proibir o acesso por parte do empregador, se não houver identificação que permita distinguir que se trata de assunto relativo à reserva da intimidade e vida privada.

Quando o texto se refere a mensagens de natureza pessoal (n. 1) deve-se por tal entender não só os correios eletrônicos, mas também outras formas de consulta e acesso a informações não profissionais, preservando-se outros modelos de mensagens, sejam escritas, visuais, telefônicas ou audiovisuais, ou mesmo consultas *on line*, dados recolhidos, conservados ou reencaminhados, tornando-os, pois, invioláveis, independentemente da forma de transmissão utilizada ou meio de acesso.[45]

O consentimento, no entanto, autoriza que se ingresse na esfera da reserva e intimidade na hipótese que se está a tratar, desde que seja expresso, livre e revogável, não se podendo presumi-lo, mormente diante da relação de desequilíbrio material própria do contrato de trabalho.

A questão do monitoramento do correio eletrônico e outras redes pode ser dividida, pois, em três possibilidades: i) uso exclusivamente pessoal; ii) uso corporativo com vedação de uso pessoal; iii) uso corporativo, com permissão para uso pessoal neutro.

Pela primeira das possibilidades, a empresa permite o uso de correio eletrônico e outras redes pessoais por meio dos equipamentos corporativos, sobre o qual o trabalhador não poderá sofrer qualquer fiscalização de conteúdo, somente quanto aos aspectos formais.

Pela segunda conjetura, o empregador veda qualquer uso pessoal dos meios

44 Teresa Coelho Moreira, Direito do Trabalho..., op. cit., p. 270.

45 Maria Regina Gomes Redinha, Da protecção..., op. cit., pp. 899-902.

de comunicação corporativos da organização, observando que, ainda que proibido, se utilizado para fins pessoais, tal não franqueia ao empregador o acesso ao conteúdo das mensagens.

Já pela terceira possibilidade, o empregador permite o uso do e-mail e outras redes corporativas para fins pessoais, desde que de modo neutro, de tal arte a não prejudicar o serviço.

É fundamental distinguir o correio eletrônico com fins corporativos do correio utilizado para fins pessoais, demarcando os e-mails de caráter pessoal ainda que encaminhados por correio corporativo quando autorizado. Isso porque o art. 18.º, n. 3 da CE veda qualquer ato de controle das mensagens, ainda que o conteúdo não seja íntimo – só podendo ser permitido o acesso por meio de autorização judicial.

Seguindo essa linha, Acórdão do Tribunal da Relação do Porto, de 15.12.2016, relativo à disponibilização ao trabalhador de conta de correio eletrônico corporativo, sem, entretanto, o estabelecimento de regras para uso, compreendendo o Tribunal pela proibição de acesso do empregador ao conteúdo dos e-mails, ainda que não delimitados como pessoais, restringindo o empregador a obtenção de informações quanto à data e hora do envio do e-mail, dados externos dos anexos (não conteúdo), e sem direito de acesso ao endereço do remetente ou destinatário quando terceiro.[46]

Nessa hipótese, o empregador não fica sem qualquer controle, todavia, limitado ao aspecto formal. Significa que lhe é vedado o acesso ao conteúdo, só podendo ser aferido o número de mensagens enviadas e recebidas, extensão da mensagem e tempo de permanência na rede, havendo alguma divergência na doutrina quanto à possibilidade de acesso aos endereços dos destinatários ou emissários dos correios quando terceiros.

Segundo Teresa Coelho Moreira, o empregador poderá se eximir da responsabilidade de que trata o art. 500.º do Código Civil, em razão de difamação ou assédio sexual cometido por empregado, se tiver adotado política interna que discipline o uso das tecnologias, e o conteúdo do e-mail for estritamente pessoal. Isso porque, em razão da proteção constitucional de sigilo de que goza o e-mail, não poderia o empregador ser responsabilizado por ato do qual – por determinação constitucional – não pode tomar conhecimento.[47]

Ao mesmo tempo, o empregado possui o direito ao uso do correio, seja pessoal,

46 Bruno Mestre, «O RGPD, o TEDH e as Relações Laborais: um equilíbrio complexo», in: **Prontuário de Direito do Trabalho**, n. 2, 2018, pp. 157-193, p. 188.

47 Teresa Coelho Moreira, A privacidade dos trabalhadores..., op. cit., pp. 435-437.

seja corporativo, para comunicar-se com o sindicato, tal como expressamente previsto no CT, art. 169.º, n. 2 e n. 3, que tutelam expressamente o uso das tecnologias de informação e comunicação para reuniões com a representação de trabalhadores.

De igual sorte, importante estabelecer regras para acesso ao correio corporativo e outras redes quando da ausência do trabalhador em razão de férias ou outros, a fim de que o empregador possa dar continuidade às atividades.

O Parecer 2/2017 GT29 aborda a necessidade de clareza quanto à existência do monitoramento e as consequências daí advindas, posicionando-se no sentido de que:

> "na ausência de uma política de monitorização no local de trabalho de fácil compreensão e facilmente acessível, os empregados podem não ter conhecimento da existência e das consequências da monitorização que está a ser realizada e, por conseguinte, estão impossibilitados de exercer os seus direitos."[48]

O Parecer acrescenta que a titularidade dos meios eletrônicos por parte do empregador não torna letra morta o direito dos empregados à confidencialidade das suas comunicações e dos dados relativos à localização e à correspondência.

O art. 14.º da Recomendação 2005, de 04/2015 do Conselho da Europa[49] orienta ao empregador a instituição de política de utilização da internet, por meio da qual informe previamente ao trabalhador os filtros utilizados, as prevenções e proibições quanto aos sites visitados, e as diretrizes para separação das mensagens privadas, sobre as quais o empregador não terá acesso de conteúdo.

Ao referir-se à regra do art. 22.º do CT, Bruno Mestre leciona que a generalidade da doutrina aceita e a lei permite que o empregador regulamente o uso dos meios de comunicação na empresa, sobretudo correio eletrônico, contudo, salienta, amparado em Júlio Gomes, que a proibição de uso para fins privados é irrealista, devendo-se, pois, respeitar o conteúdo das mensagens de caráter pessoal e não profissional, e orienta que os empregadores não controlem os sites visitados pelos trabalhadores.[50]

Na linha de todo o exposto, é recomendável a criação de política de uso de

48 European Data Protection Board. Article 29 Data Protection..., op. cit.

49 Council of Europe, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223), in https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223 (15.05.2023).

50 Bruno Mestre, O RGPD, o TEDH..., op. cit., pp. 157-193.

recursos eletrônicos, contemplando, no que tange aos e-mails, internet e outras redes de comunicação, os seguintes itens:

> i) expresso conhecimento de que o correio eletrônico, outras redes corporativas de comunicação e internet estão sujeitos a monitoramento impessoal e generalizado com a finalidade de prevenir danos a organização e terceiros, os descrevendo;
> ii) possibilidade de uso dos meios pessoais ou mesmo corporativos – este último mediante expressa distinção por parte do empregado, quando para fins pessoais;
> iii) vedação do uso de modo a prejudicar terceiros, estabelecendo-se cláusula de responsabilidade;
> iv) regulamentar o acesso do empregador ou outro empregado ao correio corporativo e outras redes de comunicação do trabalhador em razão de férias ou ausências deste;
> v) possibilidade de uso dos equipamentos telemáticos corporativos para fins de comunicação com o sindicato.

2.4. Casos Barbulescü, López Ribalda e Mirković

a) Caso Barbulescü

Na Europa, o monitoramento de correio eletrônico tem o seu norte no caso envolvendo o empregado Bogdan Mihai Barbulescü e a Romênia, levado à apreciação do TEDH.

O Acórdão TEDH Barbulescu I, de 12.01.2016 – proferido pela Câmara da Quarta Sessão, no processo n.º 61496/2008, analisou a despedida de um empregado em razão de ter violado normas da empresa que proibiam o uso para fins pessoais de equipamentos tecnológicos postos à disposição dos trabalhadores durante o horário de trabalho.

No caso, o trabalhador teria utilizado o serviço *Yahoo Messenger*, por meio do computador da empresa, durante o horário de trabalho, a fim de manter contato com familiares.

O trabalhador argumentou que os dados interceptados pela empresa são de cunho pessoal, e, portanto, protegidos à época pela Diretiva 95/46/CE, assim como pela lei de proteção de dados romena, configurando dados sensíveis, só podendo ser coletados mediante consentimento prévio – tese não acolhida pelas instâncias nacionais, nem pelo Tribunal Europeu.

Para o TEDH, não há expectativa de privacidade do trabalhador no uso das

ferramentas corporativas, que estão fora do âmbito pessoal, consoante disciplinado em política interna da empresa, de tal arte que concluiu por adequado, legítimo e proporcional o acesso do empregador às comunicações do empregado no âmbito de procedimento disciplinar, até porque o uso da conta do *Yahoo Messenger* pressupunha atividade profissional.

Prevaleceu, pois, em contagem de seis votos contra um, a possibilidade de monitoramento de comunicações privadas dos trabalhadores, de forma condicionada, no tempo e local de trabalho.

Insatisfeito com a decisão, o trabalhador recorreu ao Tribunal Pleno, tendo sido proferido o Acórdão Barbulescü II, de 05.09.2017, que por maioria de votos (onze contra seis) entendeu que houve violação ao art. 8.º da Convenção para Proteção de Direitos Humanos e Liberdades Fundamentais.

A Corte observou que no decorrer do processo disciplinar, o empregador gravou e arquivou o conteúdo das mensagens, não se limitando ao fluxo destas, assim como que o monitoramento das mensagens foi levado a efeito logo após o comunicado do empregador de que monitoraria o trabalho e a má conduta de seus empregados.

O Tribunal Pleno baseou-se na noção de que o trabalhador tem uma expectativa razoável de privacidade, devendo ser municiado com informações prévias e claras quanto às medidas de controle que podem ser utilizadas, assim como ao alcance destas medidas, não se limitando à informação geral de que o trabalhador pode estar sujeito a medidas de vigilância.

Soma-se que, para a Corte, o empregador não demonstrou quais seriam as razões específicas que teriam o condão de justificar as medidas de monitoramento adotadas, nem esclareceu o grau de intrusão. Compreendeu-se que mediante uso do princípio da proporcionalidade, a medida de vigilância a ser adotada deve ser a menos invasiva, assim como a vigilância não pode ser subsequente ao início do processo disciplinar.

b) Caso López Ribalda

A questão envolvendo López Ribalda e outros *versus* Espanha teve início com o Acórdão da Vara Social n. 1 da Granollers, confirmado pelo Superior Tribunal de Justiça da Catalunha, tendo sido considerada lícita a prova obtida mediante videovigilância pela empresa para efeito de despedimento de trabalhadores que teriam levado a efeito possíveis furtos que geraram prejuízo de mais de 80.000 euros ao empregador.

Insatisfeitos com o julgado, os trabalhadores recorreram ao TEDH, tendo a 3ª Seção do órgão, em 09.01.2018 proferido acórdão em favor da existência do direito de os trabalhadores serem previamente informados de forma expressa, precisa e inequívoca acerca do monitoramento, assim como da existência de fichário ou tratamento de dados pessoais, bem como a finalidade da coleta e a respeito dos destinatários da informação.

Para a 3ª Seção, foi violado o direito à proteção de dados pessoais, conclusão a que chegou mediante aplicação do princípio da proporcionalidade. O cerne da questão é que os trabalhadores foram informados da existência das câmeras visíveis, mas houve a inserção de câmeras ocultas, sem que de tais tenha sido dado conhecimento aos empregados que atuavam nos caixas e que teriam levado a efeito os possíveis furtos.

Para melhor compreensão, vale rápida passagem pela legislação espanhola, que oferece regramento expresso à videovigilância, geolocalização e monitoramento digital, tanto na *Ley Orgánica de Protección de Dados* (LOPD), quanto no Estatuto dos Trabalhadores (ET)[51] – este último consoante art. 20.º *bis* nos seguintes termos:

> "Os trabalhadores têm direito à privacidade na utilização dos dispositivos digitais que lhes sejam disponibilizados pela entidade patronal, à desconexão digital e à privacidade na utilização dos dispositivos de videovigilância e geolocalização nos termos estabelecidos na legislação em vigor sobre proteção de dados pessoais e garantia dos direitos digitais".[52]

Na lição de Juan Pascual, a norma do art. 20.º do ET tem caráter amplo, na medida em que se refere à legislação da proteção de dados, nesta, portanto, compreendido todo o arcabouço jurídico de proteção de dados pessoais, de modo que o descumprimento pode conduzir inclusive a inspeção do Trabalho e da Segurança a aplicar as sanções do Real Decreto Legislativo 5/2000, que expressamente prevê a penalização de atos do empregador que sejam contrários ao respeito à intimidade e à consideração devida à dignidade dos trabalhadores.[53]

51 Espanha, Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social, in https://www.boe.es/buscar/act.php?id=BOE-A-2000-15060 (15.05.2023).

52 Tradução livre – "Artículo 20 bis. Derechos de los trabajadores a la intimidad en relación con el entorno digital y la desconexión. Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales".

53 Juan Pascual, «López Ribalda II, la utilización de cámaras de video-vigilancia en las relaciones

Nessa esteira, a LOPD regula o tratamento com fins de videovigilância no art. 22.º, permitindo-o para preservar a segurança das pessoas e bens, assim como das suas instalações (n. 1), limitando a coleta ao mínimo indispensável para cumprimento desta finalidade (n. 2).

Dentre as suas inúmeras disposições, o n. 4 prevê que o dever de informação previsto no RGPD se entenderá cumprido mediante a inserção de um dispositivo informativo em lugar suficientemente visível, indicando ao menos a existência do tratamento, identidade do responsável, e possibilidade de exercer os direitos previstos nos arts. 15.º a 22.º do RGPD, ao passo que o n. 8 remete o tratamento pelo empregador dos dados obtidos através de sistemas de câmeras e videocâmeras ao disposto no art. 89.º da mesma lei (LOPD).

A seu turno, o art. 89.º – intitulado *Derecho a la Intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en lugar de trabajo* – em seu n. 1 prevê a possibilidade de o empregador tratar as imagens obtidas através de câmeras ou videocâmeras para o controle dos trabalhadores ou empregados públicos, nos termos do art. 20.3.º do ET e na legislação pública aplicável, sempre que tais se exerçam dentro do marco legal e nos limites deste, prevendo que a informação do uso do recurso deve ser prévia, de forma expressa, clara e concisa aos trabalhadores e aos representantes destes.

Prevê ainda que o requisito para a captação de um ato flagrantemente ilícito pelos trabalhadores ou empregados públicos se entenderá cumprido – quanto ao dever de informação –, quando existir ao menos o dispositivo a que se refere o item 22.4.º da LOPD (informativo em lugar suficientemente visível, e indicando ao menos a existência do tratamento, identidade do responsável, e possibilidade de exercer os direitos previstos nos arts. 15.º a 22.º do RGPD).

O n. 2 do art. 89.º reforça a proibição quanto à instalação de sistemas de gravação de som e videovigilância nos lugares destinados ao descanso ou lazer, tais como vestiários, banheiros, refeitórios e análogos.

Já o n. 3 do art. 89.º, em apertada síntese, disciplina que a utilização de sistemas similares aos referidos nos itens anteriores para a gravação de sons no lugar de trabalho se admitirá somente quando existirem relevantes riscos para a segurança das instalações, bens e pessoas, sempre respeitando o princípio da proporcionalidade,

.....
laborales: ¿se puede prescindir del deber de información?», Diario la Ley, 20.12.2019, in https://diariolaley.laleynext.es/dll/2020/01/17/lopez-ribalda-ii-la-utilizacion-de-camaras-de-video-vigilancia-en-las-relaciones-laborales-se-puede-prescindir-del-deber-de-informacion (15.05.2023).

a intervenção mínima e as garantias previstas nos itens anteriores.

Considerando, pois, que o art. 89.º, n. 1 exige que o empregador cumpra com o dever de informação, à luz da literalidade do ordenamento espanhol, quer parecer que o dever de informação é requisito para licitude da coleta da imagem e consequente uso da prova em procedimento de despedimento.

Ocorre que em 17 de outubro de 2019, a Grande Câmara do TEDH proferiu o acórdão López Ribalda II alterando o julgado da 3ª Seção, ao entendimento de que inexistiu violação à proteção de dados, e que os tribunais espanhóis tinham valorado a questão de modo a aplicar corretamente o juízo de ponderação no conflito entre a liberdade de empresa e os direitos fundamentais dos trabalhadores.

Na compreensão da Grande Câmara, a não prestação de informações prévias aos trabalhadores acerca dos sistemas ocultos de videovigilância se mostrou justificada na espécie, diante das razoáveis suspeitas de furtos.

Juan Pascual aponta mudança de norte da jurisprudência do TEDH ao permitir o uso de câmeras ocultas temporárias quando existam razoáveis suspeitas de ilícito, o que vai de encontro ao texto legal espanhol. Para o autor, a empresa sempre terá um meio de defender os seus interesses, como o anúncio da gravação das imagens indicando a finalidade da coleta a fim de proteger o seu patrimônio, defendendo que a câmera oculta só poderá ser utilizada mediante autorização judicial na linha do voto proferido por três dos julgadores no caso López Ribalda II.

c) Caso Antović e Mirković

O Conselho da Agência de Proteção de Dados Pessoais de Montenegro analisou reclamação apresentada por Nevenka Antović e Jovan Mirković diante da instalação de equipamento de videovigilância, sem o consentimento destes, nos auditórios da Universidade de Montenegro.[54]

Os professores haviam sido informados quanto ao monitoramento, cujo objetivo seria a segurança de bens e pessoas, entretanto, segundo o Conselho reponsável pela proteção de dados no país, inexistia perigo para a segurança de pessoas e bens nos auditórios, de modo que proferiu decisão determinando a retirada das câmeras.

Antović e Mirković ingressaram então com ação pleiteando indenização pela violação das suas vidas privadas diante da coleta e tratamento de dados seus não

54 Croner-i. Antović and Mirković v Montenegro [2017] ECHR 1068, in https://app.croneri.co.uk/law-and-guidance/case-reports/antovi-and-mirkovi-v-montenegro-2017-echr-1068?product=8 (17.05.2023).

autorizados, tendo tanto a Primeira Instância quanto a Segunda proferido decisão no sentido de que a Universidade é um local público, não se cogitando de direito à vida privada, e entendendo que inexistiu prova de violação do direito vindicado.

Insatisfeitos com o resultado dos julgamentos, os requerentes não interpuseram recurso constitucional, mesmo diante das disposições dos arts. 40.º, 43.º e 24.º, § 1.º da Constituição de Montenegro, que preveem o direito ao respeito pela vida privada e familiar, à informação quanto aos dados coletados e proteção contra o uso indevido, à garantia de que os direitos e liberdades humanos só podem ser restringidos diante de lei que assim preveja, respectivamente.

Optaram por levar a questão à apreciação do TEDH, que entendeu em decisão de 28.11.2017, por maioria simples (4x3), que houve violação ao art. 8.º da CEDH, na medida em que os professores possuíam razoável expectativa de privacidade, a videovigilância no local não se mostrava necessária para o resguardo de bens ou pessoas, assim como o controle da prestação laboral não se enquadrava como situação legítima de videovigilância à luz da legislação montenegrina, de tal sorte a concluir pela violação ao direito à vida privada.[55]

3. Projeções no cenário brasileiro

3.1. Vigilância à distância

À luz do direito lusitano, o monitoramento do trabalhador e a videovigilância para controle do desempenho profissional representa clara violação ao art. 20.º do CT, ao passo que sob o olhar do Direito Brasileiro, se o controle for incisivo e contínuo, flerta-se perigosamente com a invasão desmedida da privacidade, em possível violação aos direitos da intimidade e vida privada.[56]

Com efeito, como se sabe, o poder diretivo é limitado, não estando autorizado o ingresso na esfera dos direitos personalíssimos, dos quais o trabalhador não se despe no curso de uma relação laboral, seja em Portugal, seja no Brasil.

A observância dos direitos da personalidade não significa, contudo, que estes adquiram caráter absoluto perante outro direito fundamental ou de âmbito

55 Europen Court of Human Rights. Case of Antović and Mirković v. Montenegro. Application no. 70838/13, in https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-178904%22]} (18.05.2023).

56 Célio Pereira Oliveira Neto / Ricardo Calcini, «Adequação à LGPD no recrutamento e seleção de candidatos a emprego», Consultor Jurídico, 24.09.2020, in https://www.conjur.com.br/2020-set-24/pratica-trabalhista-adequacao-lgpd-recrutamento-selecao-candidatos-emprego (15.05.2023).

constitucional. Mesmo as liberdades protegidas não são definitivas, afinal inexistem direitos absolutos.[57]

Seguindo nessa esteira de raciocínio, observa-se o teor do Enunciado n.º 139 da III Jornada de Direito Civil[58] que ao tratar da limitação dos direitos da personalidade, disciplina que "os direitos da personalidade podem sofrer limitações, ainda que não especificamente previstas em lei, não podendo ser exercidos com abuso de direito de seu titular, contrariamente à boa-fé objetiva e aos bons costumes".[59]

Os direitos da personalidade, regulados de maneira não exaustiva pelo Código Civil, são expressões da cláusula geral de tutela da pessoa humana, contida no art. 1.º, inc. III, da Constituição (princípio da dignidade da pessoa humana)[60]. Em caso de colisão entre eles, como nenhum pode sobrelevar os demais, deve-se aplicar a técnica da ponderação.

Significa dizer, no Brasil, ante a ausência do mesmo comando do código de trabalho lusitano, o empregador pode monitorar resultados e metas, mas não tem a faculdade de fiscalizar o trabalhador em si durante todo o curso do trabalho, auferindo pari passo a execução das atividades, haja vista que a vigilância à distância pode invadir a esfera da privacidade, e as novas tecnologias combinadas com aplicativos, permitem que o controle por vezes vá além inclusive daquele presencialmente exercido.[61]

Nesse sentido, quanto à possibilidade de exercício do poder de fiscalização, desde que não avance sobre a intimidade do trabalhador, decisão da 5ª Turma do Tribunal Superior do Trabalho de lavra do Min. Guilherme Caputo Bastos:

> "o exercício do poder fiscalizatório, realizado de modo impessoal, geral, sem contato físico ou exposição da intimidade, não submete o trabalhador a situação vexatória nem caracteriza humilhação, vez que decorre do poder diretivo do empregador, revelando-se lícita a prática desse ato".

As câmeras de vigilância – tal como em Portugal – podem ser usadas, pois, para garantir a segurança das pessoas e bens, e indo além, inclusive para monitoramento

57 Célio Pereira Oliveira Neto, Trabalho em ambiente virtual..., op. cit., p. 311.

58 Não vinculativo.

59 Brasil. Conselho da Justiça Federal, in https://www.cjf.jus.br/enunciados/enunciado/222 (15.05.2023).

60 Brasil, Constituição da República Federativa do Brasil, de 1988, in https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm (15.05.2023)

61 Célio Pereira Oliveira Neto, Trabalho em ambiente virtual..., op. cit.

do desempenho profissional, no entanto não ao ponto de colocar os empregados sob constante e permanente vigilância.

Portanto, em respeito aos direitos da personalidade, e fazendo uso de aprendizados a partir da experiência lusitana, se houver monitoramento, é recomendável que o empregador adote os seguintes procedimentos:

> i) informar ao trabalhador acerca do monitoramento;
> ii) justificar o motivo do monitoramento, sem abuso de poder;
> iii) controlar metas e resultados, mas não os momentos de inatividade;
> iv) criar política de teletrabalho, impondo ao empregado a obrigação de colocar um fundo de tela se desejar preservar a intimidade do seu lar;
> v) implementar política de adequação à LGPD, visando a tutela dos dados dos trabalhadores.

No que se refere à possibilidade de as câmeras de vídeo manterem-se ligadas durante reunião com o empregador, clientes, fornecedores ou *stakeholders*, alia-se à posição externada pela autoridade francesa[62] de proteção de dados — *Commission Nationale de l'Informatique et des Libertés* (CNIL — Comissão Nacional de Informática e Liberdades), para quem a abertura da câmera confere maior fluidez à comunicação e contribui para o convívio, no entanto, constitui processamento de dado pessoal, e com potencial para divulgação de informações íntimas. Nesse sentido, orienta a adoção de soluções tecnológicas que desfoquem o fundo, preservando a casa ou local onde está o teletrabalhador.[63]

A autoridade francesa de proteção de dados, por sinal, quando questionada se "o empregador pode controlar a atividade dos empregados em casa?", em apertada síntese responde que sim, pois possui o poder de supervisionar e controlar a execução das tarefas, alerta, no entanto, para que não haja abuso de poder, de modo que o empregador deve sempre justificar que as medidas implementadas são proporcionais ao objetivo perseguido, assim como respeitam os direitos e liberdades dos empregados, especialmente a vida privada.[64]

62 Célio Pereira Oliveira Neto, Trabalho em ambiente virtual..., op. cit., p. 297.

63 CNIL – Comissão Nacional de Informática e Liberdades, «Les questions-réponses de la CNIL sur le télétravail», CNIL, 08.09.2021, in https://www.cnil.fr/fr/les-questions-reponses-de-la-cnil-sur-le-teletravail (15.05.2023).

64 CNIL – Comissão Nacional de Informática e Liberdades, «Télétravail : les règles et les bonnes pratiques à suivre», CNIL, [s.d], in https://www.cnil.fr/fr/teletravail-les-regles-et-les-bonnes-pratiques-suivre (15.05.2023).

No que tange às câmeras de videovigilância, sopesando o respeito à intimidade, privacidade e proteção de dados do trabalhador, é recomendável seguir os seguintes procedimentos:

i) promover a instalação nas entradas e saídas dos edifícios ou sedes das organizações empresariais, assim como saídas de emergência e locais de maior tráfego na organização, de modo a coletar imagens gerais, de forma impessoal, sem focar em pessoa determinada ou posto de trabalho específico, visando a saúde e segurança das pessoas e bens;

ii) utilizar câmeras em locais de maior risco, como estoque e caixas, de modo impessoal, não focando na pessoa que exerce a atividade, mas visando a preservação da segurança do local, dos bens e dos empregados que desempenham a atividade;

iii) por evidente, não coletar imagens em locais de acesso privado, sobretudo banheiros, assim como em regra nos espaços de recreação ou descanso;

iv) evitar a combinação de som e imagem, só o fazendo em situações justificadas e ponderadas, mediante aplicação do princípio da proporcionalidade, avaliando o grau de afetação do direito fundamental à privacidade, intimidade e proteção de dados do trabalhador;

v) limitar o acesso às imagens coletadas, no que se refere às pessoas que tenham tal atividade no escopo de suas funções, v.g. segurança, e tempo de guarda, observado o princípio da minimização da coleta;

vi) capacitar as pessoas que tenham acesso às câmeras de videovigilância para que procedam em observância aos direitos do titular dos dados;

vii) empregados, parceiros, *stakeholders* e visitantes da organização devem ser informados nos locais onde há filmagem, por meio de placa afixada de modo permanente, em local visível;

viii) ao lado da placa informativa da filmagem, afixar aviso de privacidade contemplando as seguintes informações: viii.1) finalidade do tratamento dos dados; viii.2) período de retenção das imagens; viii.3) nome, cargo e número de telefone do encarregado pela proteção de dados; viii.4) direitos dos titulares – servindo de paradigma o art. 22.4.º da LOPD.

3.2. Geolocalização

No Brasil, o uso de GPS ou similares para controle da jornada de trabalho, tempos de direção e intervalo na condução é comum, e possui supedâneo na Lei 13.103, aplicável aos motoristas nos setores econômicos de transporte de carga e/ou coletivo de passageiros.

Igualmente a geolocalização passou recentemente a ser utilizada como meio de prova judicial, diante de requerimento de uma das partes ou mesmo ante a determinação do juiz condutor do caso de quebra da geolocalização do trabalhador a fim de aferir a existência ou não de horas extras.

A título exemplificativo, em demanda individual numa das varas do trabalho do TRT da 12ª Região, a empresa requereu e o juízo deferiu a expedição de ofício para a operadora telefônica a fim de que esta fornecesse dados de geolocalização do ex-empregado a fim de demonstrar o período em que o reclamante esteve na empresa a fim de produzir prova de que não havia a prestação de horas extras.[65]

O magistrado entendeu que o meio de prova requerido teria maior eficácia do que a tradicional coleta de depoimentos testemunhais, tendo o cuidado de determinar que a obtenção dos dados fosse limitada aos dias úteis e restrita à localização da ex-empregada.

Em processo perante a 4ª Vara do Trabalho de Diadema, a juíza da causa autorizou a produção da prova por meio de geolocalização, com o objetivo de verificar se a ex-empregada se encontrava no endereço do trabalho nos períodos em que alegou labor sem registro de jornada, entre os meses de agosto de 2016 e 2021.

O deferimento da magistrada foi objeto de mandado de segurança da ex-empregada, apreciado e negado pela Des. Doris Ribeiro Torres Prina, da 7ª Seção Especializada em Dissídios Individuais do TRT2, para quem o juízo agiu dentro da liberdade que lhe cabe na condução do processo, complementando que o art. 22.º do Marco Civil da Internet outorga ao juiz a possibilidade de ordenar ao responsável o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet, assim como o art. 7.º da LGPD[66] que prevê o exercício regular de direitos em processo judicial como uma das bases legais de tratamento.

65 Marcus Vinicius R. Gonçalves / Nadyne Melo, «LGPD e a geolocalização como meio de prova trabalhista», Migalhas, 15.06.2022, in https://www.migalhas.com.br/depeso/368015/lgpd-e-a-geolocalizacao-como-meio-de-prova (15.05.2023).

66 Brasil, Lei 13.709, de 14 de agosto de 2018, in https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm (15.05.2023).

De forma diversa, com base nos princípios que regem a LGPD, ao analisar o pedido de uso da geolocalização, decisão do TRT da 3ª Região, de lavra do Des. Marco Antonio Paulinelli Carvalho, nos autos 0011155-59.2021.5.03.0000, foi no sentido de que ofende o direito líquido e certo ao sigilo telemático e à privacidade a decisão que determina a requisição de horários, lugares e posições do ex-empregado, durante largo período de tempo, vinte e quatro horas por dia para suprir prova que deveria ser trazida aos autos pela empresa.[67] Aqui a decisão parece ter observado o princípio que rege a minimização da coleta, e mesmo o princípio da adequação, na medida em que coletadas informações extralaborais, portanto, sem pertinência com a finalidade informada.

Por mencionar o princípio da adequação, na condução dos autos 1000695-07.2021.5.02.0264, o juízo da 48ª Vara do Trabalho de São Paulo entendeu que além de representar tumulto ao processo, a prova por meio do uso da geolocalização traz em seu bojo informações privadas do trabalhador – e acresenta a possibilidade de produção de provas digitais mais adequadas, tais como acessos aos sistemas internos e câmeras de segurança.

Com a devida vênia à compreensão do juízo, é necessário verificar antes a finalidade da coleta das imagens, pois o uso para efeito de prova em processo judicial poderia representar violação à LGPD por desvio da finalidade, valendo como paradigma o Direito Português que só admite o uso das câmeras de videovigilância para prova de descumprimento contratual em se tratando de ilícito penal.

Particularmente, na qualidade de advogado, tive atuação em demanda que envolveu perícia relativa à geolocalização de ex-empregado, justamente para efeito de aferir a (in)existência da prestação de horas em regime extraordinário. Com efeito, nos autos 0000462-15.2022.5.09.0129, foi realizada perícia que teve por escopo analisar o banco de dados do histórico de localização do celular do ex-empregado, por meio do *Google Takeout*®, cuja coleta foi levada a efeito pelo *Google Maps*®. Passa-se a breve narrativa de pontos cardeais da perícia judicial, consoante elencado pelo perito:

i) a capacidade de captura da geolocalização ocorre em intervalo mínimo de 1 segundo, ficando gravado na memória do celular;

ii) tanto a data, quanto a hora, minutos e segundos são obtidos pela operadora mesmo na ausência de internet;

67 Letícia Paiva, «Juízes quebram sigilo de geolocalização de trabalhadores para checar horas extras», Jota, 11.08.2022, in https://www.jota.info/especiais/juizes-quebram-sigilo-de-geolocalizacao-de-trabalhadores-para-checar-horas-extras-11082022 (15.05.2023).

iii) quando há internet, a sincronização é feita através de servidores NTP (*Network Time Protocol*) da própria *Google*®, que possuem extrema exatidão;

iv) a margem de erro da geolocalização é de 13 metros, dentro de um círculo;

v) são coletados todos os registros de local, data, hora, minutos e segundos, sendo que qualquer alteração fica registrada;[68]

vi) "a prova de geolocalização é identificada pelo histórico de localização coletado pelo *Google Maps*® instalado no celular";

vii) com a ferramenta *Google Takeout*® é possível selecionar o tipo de dado a ser coletado, selecionando apenas o histórico de navegação – o que observa o princípio da necessidade, regendo a minimização da coleta;

viii) a cópia do documento é incluída no repositório próprio do TRT da 9ª Região, com acesso apenas às partes, ficando em segredo de justiça, e o perito recebendo o documento por e-mail;

ix) é possível a ocorrência de erros grosseiros de aquisição de sinais de satélite, especialmente em estacionamentos nos subsolos ou elevadores prediais, sobretudo em celulares mais antigos;

x) visando preservar a privacidade do ex-empregado, foi reduzido o volume de dados para processamento, limitando-se ao intervalo de data da vigência do contrato e as posições geográficas em um quadrante no local de trabalho do ex-empregado – o que gera uma margem de erro de 200 metros por 200 metros;

xi) fez-se uso do método de animação *Google Earth*® para efeito de traçar uma rotina de como era o dia a dia do ex-empregado, o que facilita a compreensão de saídas e entradas durante o horário de trabalho;

xii) "em estudos efetuados anteriormente, havia inviabilidade de produção de um algoritmo para tratar grandes volumes de dados. Durante os últimos meses, foram desenvolvidos algoritmos utilizando a biblioteca Pandas para Python onde existem métodos já prontos para tratar grandes volumes de dados nos formatos JSON e KML";

xiii) a análise é feita por repetição e rotina, inclusive de outros pontos de trabalho, tais como filiais ou locais com potencial relação de trabalho, especialmente se a geolocalização ocorrer no horário de trabalho;

xiv) o perito orientou o servidor público na coleta *on line* em tempo real, assitindo a extração de dados pelo ex-empregado, confirmando a base originária da *Google*®, assim como a inexistência de manipulação, gerando código HASH segundos depois da coleta, a fim de garantir a integridade dos dados.

68 Nos dizeres do perito: "Observe que a renomada Google® teve o cuidado de preservar a autenticidade de horários e datas do banco de dados original de histórico de localização (Records.json), não permitindo que informações possam ser manipuladas ou fraudadas".

Após todas as análises e demonstrações, em apertadíssima síntese, o perito concluiu, dentre outras, que: (i) "as geolocalizações foram eficientes para demonstrar a real rotina da reclamante, verificando as informações elencadas na inicial, cruzando as informações com as narrativas da audiência e os cartões pontos acostados aos autos"; (ii) "marcações de ponto compatíveis com a geolocalização encontrada nas amostras analisadas, coletadas pelo sensor de GPS do celular do reclamante"; (iii) "a grande maioria das marcações do ponto estavam altamente compatíveis com o GPS".

Como se percebe, a geolocalização obtida através do celular pode ser um meio hábil para a produção da prova quanto à existência ou não de horas extras, tanto que algumas empresas se tornaram contumazes requerentes de pleitos nesse sentido.

Nesse momento é importante uma releitura dos princípios que regem a LGPD, analisando no caso concreto, se o princípio da proporcionalidade está sendo cumprido, especialmente se o meio utilizado seria o menos intrusivo para a produção da prova. Lembra-se, porém, que só podem ser comparadas duas medidas que tenham a mesma eficácia, de sorte que se a prova oral não tem a mesma eficácia, quer parecer que a comparação não pode ser estabelecida.

Por sinal, um dos argumentos do Banco Santander é de que vem sofrendo condenações sucessivas com base em depoimentos de testemunhas arroladas pelos trabalhadores, sem dispor de pessoas que tenham acompanhado os fatos, aptas a contraprova, especialmente quando a alegação é de que o trabalhador registrou o ponto, porém continuou trabalhando.[69]

Entretanto, sempre terá de ser analisado se a limitação ao direito à privacidade, intimidade e proteção de dados é proporcional ao fim atingido à luz do subprincípio da proporcionalidade em sentido estrito, e especialmente se o direito *prima facie* preterido não está sendo ferido de morte.

E ainda, antes, observância a todos os princípios que regem o tratamento de dados, sobretudo minimização da coleta, de tal arte a limitar o uso da geolocalização ao necessário para a produção da prova, não colhendo informações de períodos de férias, afastamentos ou em horários que não são objeto da controvérsia instaurada.

3.3. Monitoramento do correio eletrônico e outras redes

Quando se trata da manutenção do saudável meio ambiente do trabalho, não é difícil pensar em hipóteses que possam gerar prejuízos à higidez do local, como o empregado que posta comentários maliciosos sobre um(a) colega de trabalho, manifesta

69 Letícia Paiva, Juízes quebram sigilo..., op. cit.

opiniões sobre a orientação sexual de um par de trabalho, ou mesmo comete assédio sexual ou moral – ações contrárias às regras mais elementares do direito, e sobre as quais, por evidente, o empregador não deve se manter inerte.[70]

Nessas hipóteses de abuso de direito, por evidente, se de um lado o empregado tem o direito à manifestação do pensamento; de outro o empregador possui o direito à preservação da sua imagem, reputação, e manutenção do saudável ambiente de trabalho, com ainda mais ênfase quando do uso de correios eletrônicos, serviços de mensagens e redes sociais, dada a amplitude que pode ser alcançada pela informação.

Conforme lição de Alexandre Agra Belmonte, "cuida-se da atuação dos princípios do juízo de ponderação e da dimensão de peso e importância".[71] A antinomia jurídica ou colisão de direitos torna necessária a aplicação do juízo de ponderação, de modo a impor o mínimo sacrifício aos direitos violados e máxima eficácia do direito protegido.

Nessa mesma esteira, vale-se dos ensinamentos de Lélia Guimarães Carvalho Ribeiro,

> "por isso mesmo, havendo colisão de direitos fundamentais, deve o julgador, em regra, atentar para o princípio da unidade do ordenamento jurídico, o que o obriga a uma tarefa de otimização para com os bens periódicos em conflito, sugerindo, sempre que, por meio de um critério de proporcionalidade, seja dado e reconhecido como prevalente o bem de maior envergadura jurídica e que não fira a dignidade da pessoa do trabalhador".[72]

Acresça-se a obrigação de o empregador preservar o ambiente de trabalho seguro e hígido, e a responsabilidade pelos atos de seus prepostos nos termos do art. 932.º do CC, sendo inócua qualquer cláusula de isenção de responsabilidade. Por outro lado, o art. 52.º do CC também determina a aplicação dos direitos da personalidade, no que couber, à pessoa jurídica, e a Lei 13.467/2017 inclui o art. 223.º -G da CLT, que trata do dano à pessoa jurídica.

Políticas preventivas têm o condão de estabelecer regras que podem alcançar momentos em que o trabalho não está sendo prestado, no que tange à possível limitação dos direitos de expressão do empregado até o necessário à proteção dos

70 Célio Pereira Oliveira Neto, Trabalho em ambiente virtual..., op. cit., p. 313.

71 Alexandre Agra Belmonte, O monitoramento da correspondência eletrônica nas relações de trabalho, São Paulo, LTr, 2009. p. 77.

72 Lélia Guimarães Carvalho Ribeiro, A monitoração audiovisual e eletrônica no ambiente de trabalho e seu valor probante, São Paulo, LTr, 2007. p. 66.

direitos do empregador e à manutenção do saudável meio ambiente do trabalho, sem que isso represente ferir o núcleo essencial dos direitos da personalidade do empregado.

Portanto, a limitação das manifestações na forma apontada não se restringe ao horário de trabalho, alcançando, com supedâneo nas cláusulas gerais da boa-fé objetiva e função social do contrato, não só os períodos em que o labor não está sendo prestado, como até mesmo o momento *post pactum finitum*.

O estabelecimento de regras empresariais é crucial para o negócio, e amplamente justificado, para prevenir a ocorrência de violações de direito, tais como: ofensas a clientes, fornecedores ou parceiros; abusos sexuais e discriminação; danos morais e materiais a terceiros; proteção de informações confidenciais e o próprio *know how* do negócio; prevenção de fraudes; disseminação de vírus e congestionamento da rede interna — que podem ser violados por meio do correio eletrônico, ou mesmo através das redes sociais.[73]

No Brasil, a jurisprudência é guiada por decisão proferida pelo TST, no ano de 2004, ao analisar o monitoramento de correios eletrônicos em caso envolvendo o HSBC, cuja relatoria do acórdão coube ao Ministro Oreste Dalazén.

Segundo o acórdão, o correio corporativo pode ser comparado a um papel timbrado da empresa, já que o empregado está fazendo uso de equipamentos fornecidos para o trabalho, de propriedade do empregador, no horário de trabalho.[74]

Nesse sentido, quando do uso do correio corporativo, o empregado não tem expectativa de privacidade, até porque e-mail e redes sociais corporativos não se equiparam ao conceito constitucional de correspondência, de tal sorte que não se cogita de violação ao direito de sigilo das correspondências.[75]

Isso não quer dizer que o empregador tenha livre e desmedido acesso ao conteúdo dos correios corporativos, na medida em que a fiscalização material deve ser geral e impessoal, exercida de preferência por meio de palavras-chave.

A empresa pode e deve exercer o poder de vigilância e fiscalização, desde que de modo generalizado e impessoal, somente fazendo uso da verificação de conteúdo em caso de necessidade de acesso a determinada informação institucional na ausência do empregado, ou em razão de fundadas suspeitas de má utilização.[76]

73 Célio Pereira Oliveira Neto, Trabalho em ambiente virtual..., op. cit., p. 315.

74 Célio Pereira Oliveira Neto, Trabalho em ambiente virtual..., op. cit., p. 316.

75 TST — RR 613/2000-013-10-00 — 1ª T. — Rel. Min. João Oreste Dalazen — DJU 10.06.2005 — p. 901. JCF.5 JCF.5.X JCF.5.XII JCF.5.LVI. Repositório eletrônico autorizado Juris Síntese IOB. (15.05.2023).

76 Alexandre Agra Belmonte, O monitoramento da correspondência..., op. cit., p. 86.

Já o uso do correio pessoal ou outras tecnologias da informação, mesmo no ambiente de trabalho mediante recursos do empregador, não está sujeito ao monitoramento material, somente formal. Pode-se até punir, se proibido o uso, mas ao conteúdo das mensagens o empregador não terá acesso direto, na medida em que o correio pessoal só pode ser vasculhado mediante autorização judicial ou inequívoca autorização do empregado.

Vale mencionar decisão da 3ª Vara do Trabalho de São Leopoldo/RS, confirmada pela 5ª Turma do TRT da 4ª Região, que condenou a empregadora em danos morais de pequena monta – R$ 3.000,00 (três mil reais) – e reverteu a justa causa que havia sido aplicada pela empregadora em razão do conteúdo das mensagens enviadas pelo trabalhador fora do horário de trabalho a um grupo composto por colegas de trabalho, através do aplicativo *WhatsApp*, de uso pessoal.

A decisão foi no sentido de que o acesso e o uso dos dados obtidos pela empresa por meio de aplicativo de mensagens representa violação à privacidade e intimidade do empregado, observado o caráter pessoal das conversas, em aparelho celular particular, através de conta particular, fora do horário de trabalho.[77]

Analisando a possibilidade de acesso do empregador ao e-mail pessoal de empregado, a Subseção II Especializada em Dissídios Individuais do TST se debruçou sobre caso em que pendia suspeita de que o empregado estava repassando informações de cunho sigiloso a um terceiro, no caso escritório de advocacia, tendo a empresa ajuizado ação de indenização, onde também pleiteava liminarmente que o *Yahoo* fosse oficiado a fim de encaminhar todas as mensagens enviadas e recebidas pelo trabalhador.

Tudo teve início diante do deferimento do pedido liminar, de modo que o empregado impetrou mandado de segurança junto ao TRT da 15ª Região, que a seu turno, e fazendo juízo de ponderação, entendeu por não conferir às mensagens o sigilo constitucional de correspondência, não havendo que se falar em violação de direito líquido e certo do trabalhador.

Por meio do julgado de 03.10.2022, a SBDI-2 do TST deixou patente que a quebra de sigilo se limita aos metadados, tais como registros de datas, horários, contas e endereços de IP, não se podendo franquear acesso ao conteúdo das mensagens enviadas e recebidas de conta de e-mail pessoal, ainda que para fins de apuração

77 TRT4 – Tribunal Regional do Trabalho da 4ª Região, «Trabalhador que teve conversas de WhatsApp lidas pela empregadora deve ser indenizado», TRT4, 13.01.2023, in https://www.trt4.jus.br/portais/trt4/modulos/noticias/539477 (18.05.2023).

deato ilícito.[78]

A Corte Superior Trabalhista, por meio da SBDI-2 entendeu que a Lei 12.965/2014 – conhecida como Marco Civil da Internet – permite, forte do art. 22.º, o fornecimento de registros de conexão ou de acesso às aplicações da internet, mas não ao conteúdo.

A Relatora, Min. Maria Helena Mallmann, abordou a necessidade de se distinguir entre a requisição de registros e seus conteúdos, pontuando que o acesso ao conteúdo só poderia ocorrer, como regra geral, diante de processo criminal, enunciando que "ressalvadas situações extremas, em que há risco à vida ou à integridade física de pessoas, é inviável a quebra do sigilo do conteúdo de mensagens de e-mail privado para fins de instrução de demanda cível."

A decisão supramencionada tem cunho de mera demonstração quanto à possibilidade de monitoramento inclusive de comunicações privadas, desde que – mediante uso do princípio da proporcionalidade – haja prévio comunicado do alcance de eventual monitoramento, que deverá ser impessoal, o menos intrusivo possível e limitar-se aos metadados. O plano fático demonstra o interesse do empregador não só para tutelar segredos de negócio, como também para efeito do próprio cumprimento da LGPD.

Nesse norte, o TRT da 15ª Região enfrentou questão nos autos 1000612-09.2020.5.02.0043 em que o empregado havia assinado Termo de Confidencialidade e Adesão à Política de Segurança da Informação, por meio do qual obrigava-se a "tratar confidencialmente todas as informações e documentos aos quais tivesse acesso em decorrência do contrato de trabalho", assim como constava cláusula de confidencialidade do contrato de trabalho.

No caso, segundo narrado pela empresa, e contrariando normas internas desta, o empregado teria encaminhado para o seu e-mail pessoal planilha com mais de oito mil linhas de dados de cartões do cliente MRV.

O Tribunal Regional manteve inalterada a sentença que validou a justa causa aplicada ao trabalhador, fazendo constar do acórdão trechos da decisão primeira em que o extravio dos dados já autorizava a justa causa, independente de posterior transmissão, na medida em que havia inúmeros dados pessoais de clientes, tais como CPF, valores carregados no cartão alimentação, além de locais de lotação dos empregados.

Como se nota, também no Brasil é imperioso o estabelecimento de políticas claras

78 TST – Tribunal Superior do Trabalho, «TST limita quebra de sigilo de e-mail pessoal de empregado», TST, 03.10.2022, in https://www.tst.jus.br/web/guest/-/tst-limita-quebra-de-sigilo-de-e-mail-pessoal-de-empregado%C2%A0 (15.05.2023).

e transparentes, comunicando ao trabalhador que os equipamentos são fornecidos para a execução do trabalho, expressamente informando quanto à possibilidade de monitoramento, alcance, meio e forma deste controle, que deve ser geral e impessoal, não intrusivo, limitado ao mínimo necessário para o alcance da legítima finalidade apontada.

Nessa esteira, deve ficar igualmente expressa, de modo indene de dúvidas, a possibilidade de monitoramento formal e material dos correios eletrônicos e demais dispositivos de comunicação, quando corporativos, assim como o monitoramento formal quando do uso de equipamentos da empresa em correios pessoais.

Por sinal, na sociedade da informação, é bastante usual que o empregado faça uso das ferramentas digitais que lhe são disponibilizadas pelo empregador para efeito de arquivamento de fotos, vídeos e outros documentos pessoais, sendo recomendável que a política a ser instituída contemple o uso e identificação de pasta própria para uso pessoal, com regras relativas à distinção dos temas corporativos, limitação de espaço, tempo de uso, modo do arquivamento, dentre outras.

Tal orientação ganha maior relevo com o expresso reconhecimento da proteção de dados como direito fundamental, forte da EC 115, que incluiu tal garantia no inciso LXXIX do art. 5.º da CF (embora já se tratasse de direito fundamental implícito). Nesse contexto, o Parecer 2 GT29 serve de paradigma ao orientar que os empregados possam gozar de espaços privados, para os quais o empregador não tenha acesso, salvo em situações excepcionais, orientando que "se o empregado estabelece uma nomeação para 'privado' ou assinala isso na própria nomeação, os empregadores (e outros empregados) não devem ser autorizados a analisar o conteúdo da nomeação".[79]

Salutar prever ainda a segurança das informações e preservação de segredos, bem como o expresso cumprimento dos demais deveres atinentes à lealdade, boa-fé e função social do contrato, afinal o empregado é responsável pela guarda das informações recebidas do empregador, não podendo divulgá-las ou valer-se delas em proveito próprio ou de terceiro.

Após o estabelecimento das regras, estas devem ser objeto de palestras educativas apresentando os problemas, as medidas, casos práticos, a posição da doutrina e do judiciário, com o que não só se orienta o empregado, como também este se sente parte do processo, na medida em que inserido no meio.

79 European Data Protection Board. Article 29 Data Protection Protection..., op. cit.

4. Conclusão

Considerando que a cultura de proteção de dados em Portugal possui nível de maturidade bem superior à brasileira, ainda incipiente, e acrescendo que os temas aqui tratados não possuem regulamentação na seara trabalhista no Brasil, recomenda-se o uso do Direito Português como paradigma – claro que mediante as adaptações necessárias, seja em razão do momento experiencial de cada país, seja em razão das diferenças legislativas.

Nessa esteira, dos temas analisados neste estudo, compreende-se que, diferentemente do Direito Português, não há óbice legal à vigilância à distância do trabalhador no Brasil para avaliação ou medição do desempenho profissional, desde que não seja desmedida, desproporcional, contínua, invadindo, assim, a esfera da intimidade, privacidade e proteção de dados.

O enquadramento da geolocalização como instrumento de vigilância a distância ainda é tema não pacificado em Portugal, de toda sorte, tal só deve ocorrer para a preservação e segurança de bens e pessoas ou quando as circunstâncias inerentes à natureza da atividade a justifiquem; ao passo que no Brasil, ante a ausência de regulamentação no campo trabalhista, e inexistência de óbice para o monitoramento a distância, recomenda-se algumas cautelas, sobretudo quanto à minimização da coleta e respeito aos direitos personalíssimos.

A geolocalização tem sido utilizada com alguma frequência para a produção da prova, no Brasil, em ações judiciais relativas à (in)existência de horas extras, recomendando-se a análise da necessidade da medida, avaliando se há outro meio menos gravoso para obtenção de resultado com a mesma eficácia, além de perquirir se todos os princípios que regem a coleta de dados estão sendo observados.

Por fim, o monitoramento do correio eletrônico e outras redes possuem compreensões semelhantes nos países analisados, em que pese à luz do Direito Português, inclusive doutrina e jurisprudência, os e-mails se enquadrem como correspondência, gozando da proteção constitucional do sigilo, com as ressalvas do correio corporativo sobre os quais o empregador possui acesso, ainda que geral e impessoal, somam-se, contudo, algumas cautelas, pois podem envolver dados pessoais. Ponto comum é a necessidade de instituição de políticas claras regrando o uso dos correios e demais meios de comunicação.

No Brasil à luz da jurisprudência do caso HSBC, e considerada a ausência de comando legal, os e-mails corporativos são compreendidos como papel timbrado da

empresa, sujeitos ao monitoramento geral e impessoal, porém com menos cuidados, se comparados à prática lusitana, até porque não enquadrados no sigilo constitucional de correspondência, embora talvez o tema volte a ser debatido ante a inserção expressa da proteção de dados na ordem constitucional como direito fundamental e autônomo, o que pode provocar a incidência das mesmas cautelas já adotadas em Portugal e sugeridas neste estudo, adotando-se como modelo o Parecer 2 GT29.

Bibliografia

Belmonte, Alexandre Agra, *O monitoramento da correspondência eletrônica nas relações de trabalho*, São Paulo, LTr, 2009

Brasil, *Conselho da Justiça Federal*, *in* https://www.cjf.jus.br/enunciados/enunciado/222 (15.05.2023)

CNIL – Comissão Nacional de Informática e Liberdades, «Les questions-réponses de la CNIL sur le télétravail», *CNIL*, 08.09.2021, *in* https://www.cnil.fr/fr/les-questions-reponses-de-la-cnil-sur-le-teletravail (15.05.2023)

CNIL – Comissão Nacional de Informática e Liberdades, «Télétravail : les règles et les bonnes pratiques à suivre», *CNIL*, [s.d], *in* https://www.cnil.fr/fr/teletravail-les-regles-et-les-bonnes-pratiques-suivre (15.05.2023)

Council of Europe, *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (CETS No. 223), *in* https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223 (15.05.2023)

Croner-i. *Antović and Mirković v Montenegro [2017] ECHR 1068*, *in* https://app.croneri.co.uk/law-and-guidance/case-reports/antovi-and-mirkovi-v-montenegro-2017-echr-1068?product=8 (17.05.2023)

Europen Court of Human Rights, *Case of Antović and Mirković v. Montenegro. Application no. 70838/13, in* https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-178904%22]} (18.05.2023)

Gonçalves, Marcus Vinicius R. / Melo, Nadyne, «LGPD e a geolocalização como meio de prova trabalhista», *Migalhas*, 15.06.2022, *in* https://www.migalhas.com.br/depeso/368015/lgpd-e-a-geolocalizacao-como-meio-de-prova (15.05.2023)

GPDP – Gabinete para a Protecção de Dados Pessoais, *Documentos adoptados pelo Grupo de Trabalho do Artigo 29.º para a Protecção dos Dados da Comissão Europeia*, 26.05.2022, *in* https://www.gpdp.gov.mo/pt/references_detail/article/l3mqmkcr.html (15.05.2023)

Mestre, Bruno, «O RGPD, o TEDH e as Relações Laborais: um equilíbrio complexo», *in Prontuário de Direito do Trabalho*, n. 2, 2018, pp. 157-193

Michigan, «Microchip Protection Act passes Michigan House», *Data Guidance*, 30.06.2020, *in* https://www.dataguidance.com/news/michigan-microchip-protection-act-passes-michigan-house (15.05.2023)

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 electrónico do empregador*, Coimbra, Livraria Almedina, 2010

Moreira, Teresa Coelho, *Direito do Trabalho na Era Digital*, Coimbra, Livraria Almedina, 2022

Namora, Nuno Cerejeira, «RGPD y la vigilancia del trabajador por medios tecnológicos», *in Adaptland, Diapositivas y pósteres presentados en el 2º Congresso Mundial Comunidad CIELO Laboral, in* https://moodle.adaptland.it/mod/folder/view.php?id=22815 (15.05.2023)

Oliveira Neto, Célio Pereira / Calcini, Ricardo, «Adequação à LGPD no recrutamento e seleção de candidatos a emprego», *Consultor Jurídico*, 24.09.2020, *in* https://www.conjur.com.br/2020-set-24/pratica-trabalhista-adequacao-lgpd-recrutamento-selecao-candidatos-emprego (15.05.2023)

Oliveira Neto, Célio Pereira, *Trabalho em ambiente virtual*: causas, efeitos e conformação, 2ª ed., São Paulo, LTr, 2022

Paiva, Letícia, «Juízes quebram sigilo de geolocalização de trabalhadores para checar

horas extras», *Jota*, 11.08.2022, *in* https://www.jota.info/especiais/juizes-quebram-sigilo-de-geolocalizacao-de-trabalhadores-para-checar-horas-extras-11082022 (15.05.2023)

Pascual, Juan, «López Ribalda II, la utilización de cámaras de video-vigilancia en las relaciones laborales: ¿se puede prescindir del deber de información?», *Diario la Ley*, 20.12.2019, *in* https://diariolaley.laleynext.es/dll/2020/01/17/lopez-ribalda-ii-la-utilizacion-de-camaras-de-video-vigilancia-en-las-relaciones-laborales-se-puede-prescindir-del-deber-de-informacion (15.05.2023)

Passos, André Franco de Oliveira / Passos, Edésio / Nicoladeli, Sandro Lunard Nicoladeli, *Anexo VII – Repertório de recomendações práticas sobre a proteção dos dados pessoais dos trabalhadores*, Conferência da OIT, 1997, *in* https://vlex.com.br/vid/anexo-vii-repertorio-recomendacoes-718495325 (15.05.2023)

Redinha, Maria Regina Gomes, *Da protecção da personalidade no código do trabalho*, Coimbra Editora Coimbra, 2004

Redinha, Maria Regina Gomes, «Os direitos de personalidade no Código do Trabalho: actualidade e oportunidade da sua inclusão», *in A Reforma do Código do Trabalho*, Coimbra, Coimbra Editora, 2005, *in* https://repositorio-aberto.up.pt/bitstream/10216/18699/2/49726.pdf (15.05.2023)

Redinha, Maria Regina Gomes / Guimarães, Maria Raquel, «O uso do correio electrónico no local de trabalho – algumas reflexões», *in Estudos em homenagem ao Professor Doutor Jorge Ribeiro de Faria,* Faculdade de Direito da Universidade do Porto, Coimbra Editora, Coimbra, 2003, pp. 647-671, *in* https://repositorio-aberto.up.pt/bitstream/10216/24325/2/49769.pdf

Ribeiro, Lélia Guimarães Carvalho, *A monitoração audiovisual e eletrônica no ambiente de trabalho e seu valor probante*, São Paulo, LTr, 2007

Sousa, Duarte Abrunhosa e / Gonçalves, Rui Coimbra, «Cessação do contrato de trabalho e conservação de dados pessoais dos trabalhadores», *in O Regulamento Geral de Proteção de Dados e as Relações de Trabalho – Estudos APODIT* 6, Maria do Rosário

Palma Ramalho e Teresa Coelho Moreira (coord.), Associação Portuguesa de Direito do Trabalho, Livraria AAFDL, Lisboa, 2020

Sutto, Giovanna, «Amazon registra patente que rastreia funcionários durante horário de trabalho», *InfoMoney*, 05.08.2018, *in* https://www.infomoney.com.br/carreira/amazon-registra-patente-que-rastreia-funcionarios-durante-horario-de-trabalho/ (15.05.2023)
Teramind, *Detecção de ameaças internas e monitoramento de funcionários*, 2023, *in* https://www.teramind.co/ (31.05.2023)

TRT4 – Tribunal Regional do Trabalho da 4ª Região, «Trabalhador que teve conversas de WhatsApp lidas pela empregadora deve ser indenizado», *TRT4*, 13.01.2023, *in* https://www.trt4.jus.br/portais/trt4/modulos/noticias/539477 (18.05.2023)

TST – Tribunal Superior do Trabalho, «TST limita quebra de sigilo de e-mail pessoal de empregado», *TST*, 03.10.2022, *in* https://www.tst.jus.br/web/guest/-/tst-limita-quebra-de-sigilo-de-e-mail-pessoal-de-empregado%C2%A0 (18.05.2023)

Legislação

Agências dos direitos fundamentais da União Europeia / conselho da Europa, *Manual da Legislação Europeia sobre Proteção de Dados*, 2014, *in* https://www.echr.coe.intDocuments/Handbook_data_protection_Por.pdf (15.05.2023)

Brasil, *Constituição da República Federativa do Brasil*, de 1988, *in* https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm (15.05.2023)

Brasil, *Lei 13.709*, de 14 de agosto de 2018, *in* https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm (15.05.2023)

Espanha, *Real Decreto Legislativo 5/2000*, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social, *in* https://www.boe.es/buscar/act.php?id=BOE-A-2000-15060 (15.05.2023)

European Data Protection Board, *Article 29 Data Protection Working Party. 17/EN WP 260. Opinion 2/2017 on data processing at work. Adopted on 8 June 2017, in* https://www.

pdpjournals.com/docs/88772.pdf (15.05.2023)
Italy, *Legge 20 maggio 1970, n. 300* (Statuto dei lavoratori), Norme sulla tutela della libertà e dignità del lavoratori, della libertà sindacale e dell'attività sindacale nel luoghi di lavoro e norme sul collocamento, *in* https://www.cgil.unimi.it/wp-content/uploads/2014/01/l_300_70.pdf (15.05.2023)

Portugal, *Carta Portuguesa de Direitos Humanos na Era Digital*, *Lei 27/2021*, *in* https://dre.pt/dre/legislacao-consolidada/lei/2021-164870244 (15.05.2023)

Portugal, *Código Civil – CC*, *Decreto-Lei 47344*, *in* https://dre.pt/dre/legislacao-consolidada/decreto-lei/1966-34509075 (15.05.2023)

Portugal, *Código do Trabalho – CT, Lei 7/2009*, *in* https://dre.pt/dre/legislacao-consolidada/lei/2009-34546475 (15.05.2023)

Portugal, *Código Penal – CP*, Decreto-Lei 48/1995, *in* https://dre.pt/dre/legislacao-consolidada/decreto-lei/1995-34437675 (15.05.2023)

Portugal, *Constituição da República Portuguesa*, VII Revisão Constitucional, 2005, *in* https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx (15.05.2023)

Portugal, *Decreto-Lei 10-A/2020*, de 13 de março, *in* https://dre.pt/dre/detalhe/decreto-lei/10-a-2020-130243053 (15.05.2023)

Jurisprudência

Brasil

– 48ª Vara do Trabalho de São Paulo, 1000695-07.2021.5.02.0264
– TRT da 3ª Região (Marco Antonio Paulinelli Carvalho), 0011155-59.2021.5.03.0000
– TRT da 15ª Região, 1000612-09.2020.5.02.0043
– TST, 1ª Turma (João Oreste Dalazén), RR 613/2000-013-10-00, DJU 10.06.2005, p. 901
- TST, 2ª Turma (Maria Helena Mallmann), AIRR-597-43.2012.5.02.0009
– TST, 5ª Turma (Guilherme Caputo Bastos), RR-169000-71.2009.5.02.0011. Julgado em 04.05.2016

– Vara do Trabalho de São Miguel do Oeste, 0000876-17.2021.5.12.0015.

Espanha

– Acórdão da Vara Social n. 1 da Granollers

Portugal

– Acórdão do STJ de 08.02.2006 (Fernandes Cadilha)

– Acórdão do STJ de 22.05.2007 (Pinto Hespanhol)

– Acórdão do STJ de 27.05.2010 (Sousa Grandão)

– Acórdão do Tribunal da Relação do Porto, de 22.04.2013 (António José Ascensão Ramos)

– Acórdão do STJ de 13.11.2013 (Mário Belo Morgado) n.º 73/12.3TTVNF.P1.S1

– Acórdão do Tribunal de Guimarães de 05.12.2016

– Acórdão do Tribunal da Relação do Porto, de 15.12.2016 (Paula Leal de Carvalho)

– Acórdão Tribunal da Relação do Porto de 26.06.2017 (Jerônimo Freitas)

– Acórdão Tribunal de Relação de Évora, de 26.10.2017 (Mário Coelho)

– Acórdão do Tribunal da Relação do Porto de 05.03.2018 (Nelson Fernandes)

– Acórdão do Tribunal da Relação do Porto de 23.04.2018 (Nelson Fernandes)

– Acórdão do Tribunal Constitucional Portugal n.º 382/03 (Mário Torres)

TEDH

– Acórdão 3ª Seção, em 09.01.2018 (Linos-Alexandre Silicianos, *President*)

– Acórdão Barbulescu I, de 12.01.2016 – Câmara da 4ª Sessão, processo n.º 61496/2008 (András Sajó, *President*)

– Acórdão Barbulescü II, de 05.09.2017 (Guido Raimondi, *President*)

– Acórdão López Ribalda II, de 09.01.2019 (Helena Jäderblom, *President*)