Produtividade ou vigilância? A linha ténue da monitorização digital no trabalho

pmemagazine.sapo.pt/produtividade-ou-vigilancia-a-linha-tenue-da-monitorizacao-digital-no-trabalho

Estudos da OCDE e da Comissão Europeia mostram que as empresas estão a recorrer cada vez mais a *software* para monitorizar, organizar e avaliar trabalhadores. Especialistas ouvidos pela PME Magazine alertam, porém, que a fronteira entre segurança e vigilância abusiva continua a ser uma das zonas mais sensíveis do mundo laboral.

A utilização de *software* para monitorizar trabalhadores está a tornar-se uma realidade cada vez mais presente nas empresas, impulsionada pela digitalização, pelo trabalho híbrido e pela pressão para ganhar eficiência e produtividade.

Dois estudos recentes, **Gestão Algorítmica no local de trabalho da OCDE** e **Monitorização digital, gestão algorítmica e a plataformização do trabalho, da Comissão Europeia**, mostram que a chamada gestão algorítmica está a entrar de forma crescente no local de trabalho, através de ferramentas que organizam tarefas, registam horários, acompanham acessos e, em alguns casos, avaliam desempenho.

Software já gere tarefas, horários e monitorização

No estudo “Algorithmic Management in the Workplace: New Evidence from an OECD Employer Survey”, a OCDE define gestão algorítmica como o uso de *software,* com ou sem inteligência artificial, para automatizar parcial ou totalmente tarefas antes feitas por chefias humanas. Isso inclui desde a atribuição de horários e tarefas até à monitorização da atividade laboral e à avaliação do desempenho.

Os dados mostram que esta prática já está bastante disseminada. A adoção é especialmente elevada nos Estados Unidos, mas também relevante nos países europeus analisados pela organização.

Na Europa, a utilização tende a concentrar-se mais em ferramentas de instrução e monitorização básica, como registo de horas de trabalho, enquanto nos EUA há um uso mais intensivo de ferramentas de monitorização e avaliação, incluindo sistemas mais intrusivos.

A OCDE conclui ainda que cerca de 60% dos gestores inquiridos consideram que estas ferramentas melhoram a qualidade das decisões, sobretudo por permitirem acesso mais rápido a informação e maior capacidade de coordenação. Ao mesmo tempo, o estudo identifica preocupações significativas com responsabilidade em caso de erro, falta de transparência sobre a lógica dos sistemas e insuficiente proteção da saúde física e mental dos trabalhadores.

Na Europa, a monitorização já é comum

A tendência é corroborada pelo relatório da Comissão Europeia “Digital Monitoring, Algorithmic Management and the Platformisation of Work in Europe”, que conclui que a monitorização digital dos trabalhadores já está amplamente disseminada no espaço europeu.

Segundo o estudo, mais de 90% dos trabalhadores da UE usam dispositivos digitais no trabalho, enquanto 37% dizem ser monitorizados quanto ao horário de trabalho e 36% quanto a entradas e saídas do local de trabalho.

O relatório acrescenta que 24% dos trabalhadores afirmam que o seu tempo de trabalho é atribuído automaticamente, sinalizando a expansão de mecanismos de organização laboral baseados em software. Embora os autores reconheçam ganhos potenciais de eficiência e produtividade, alertam que esta transformação pode traduzir-se em perda de autonomia, maior pressão, mais stress e novos riscos de privacidade.

Segurança não é o mesmo que vigiar pessoas

Para Bruno Castro, fundador e CEO da VisionWare, especialista em cibersegurança e análise forense, a distinção entre monitorização técnica legítima e vigilância abusiva de trabalhadores é central.

“A monitorização é considerada legítima quando está diretamente ligada à proteção de infraestruturas, dados e sistemas críticos, funcionando como uma salvaguarda proporcional face aos riscos existentes. Isto significa que a organização recolhe apenas a informação necessária para detetar incidentes de segurança, como acessos suspeitos, anomalias de rede ou tentativas de intrusão, e não para observar ou avaliar comportamentos pessoais dos colaboradores”, afirma em resposta à PME Magazine.

Segundo o responsável, a linha vermelha é ultrapassada quando o foco deixa de estar nos sistemas e passa a estar nas pessoas.

“Para proteger dados, uma empresa precisa sobretudo de visibilidade sobre aquilo que acontece tecnicamente no sistema: registos de acesso, tentativas de login, movimentos de ficheiros sensíveis, comportamentos anómalos que indiciem risco, entre outros. Isto não exige observar o que o colaborador faz ao detalhe, mas sim captar sinais técnicos que permitam identificar padrões de risco, muitas vezes despersonalizados ou anonimizados. O excesso começa quando a monitorização ultrapassa esse âmbito e passa a recolher dados que não são necessários para a segurança, como capturas de ecrã contínuas, gravações de teclado, análise de mensagens pessoais ou métricas granulares da atividade diária”, sublinha.

Bruno Castro defende que é possível proteger sistemas sem transformar o ambiente laboral num espaço de vigilância permanente.

“Não só é possível, como é o que deve ser feito. Os modelos modernos de segurança funcionam com base em padrões técnicos e risco contextual, e não na vigilância humana individual. A grande evolução da segurança digital está precisamente na capacidade de monitorizar comportamentos do sistema, muitas vezes de forma agregada ou anonimizada, mantendo a privacidade do colaborador intacta. Só em situações excecionais, como um incidente de segurança claro, é necessário aprofundar a análise com maior detalhe num utilizador específico. No fundo a proteção eficaz dos sistemas não depende de vigiar pessoas, mas de proteger infraestruturas com mecanismos autónomos, inteligentes e tecnicamente fortes.”

IA e produtividade estão a empurrar o controlo

A pressão para automatizar processos e medir desempenho está também a acelerar esta tendência, alerta o especialista.

“Sim, e este é um dos fenómenos mais relevantes e também desafiantes no mundo laboral atual. A pressão competitiva para adotar IA e aumentar a produtividade tem levado algumas organizações a recolher cada vez mais dados para avaliação de performance dos colaboradores com detalhe excessivo, e isto sim é preocupante. Esta lógica de recolher dados para prever e avaliar comportamentos já é familiar nas redes sociais, e começa agora a infiltrar-se no contexto laboral.”

Em Portugal, a lei distingue segurança de controlo de desempenho

Do ponto de vista jurídico, Cristina Romariz, advogada da área laboral da Cuatrecasas, sublinha que a legislação portuguesa é particularmente sensível ao uso de meios tecnológicos de controlo à distância.

“Em Portugal, o empregador não pode utilizar meios de vigilância à distância, como sejam câmaras de vídeo, microfones ou mecanismos de escuta e registo telefónico, com o propósito de controlar o desempenho profissional. O bossware – tecnologia para vigiar a atividade dos trabalhadores (rastreamento de cliques, acesso remoto aos dispositivos, captura de ecrã, entre outros) – insere-se, precisamente, no âmbito desta proibição.”

A advogada recorda que, embora o empregador tenha poder de direção e supervisão, esse poder não é ilimitado.

“É inegável que o empregador detém a prerrogativa do poder de direção, que lhe confere o direito de supervisionar a execução da atividade laboral. Contudo, o uso de tecnologia para implementar um controlo impessoal (muitas vezes, sub-reptício) e tendencialmente ininterrupto ultrapassa os limites legais (e éticos) que devem reger a relação laboral. O facto de os equipamentos sob monitorização serem das empresas, não mitiga ou anula aquela proibição.”

Também o RGPD, acrescenta Cristina Romariz, impõe restrições claras à recolha e tratamento de dados neste contexto.

“O RGPD estabelece exigências claras, como a necessidade, proporcionalidade, transparência e minimização na recolha de dados. Ferramentas como keylogging ou capturas periódicas de ecrã revelam-se incompatíveis com estes princípios, ao recolherem informação excessiva e altamente intrusiva. O acesso a dados pessoais, credenciais e até eventuais comunicações privadas coloca em risco, desde logo, a privacidade do trabalhador.”

Zona cinzenta está a crescer nas empresas

A maior complexidade, explica Cristina Romariz, está muitas vezes em sistemas aparentemente neutros, mas que acabam por ser usados para medir produtividade de forma indireta.

“Há diferença entre controlo de segurança e vigilância de produtividade? Sim, essa diferença é, aliás, central na lei laboral. A regra é a de que o empregador não pode utilizar meios de vigilância à distância no local de trabalho, mediante equipamento tecnológico, para controlar o desempenho profissional. No entanto, salvaguarda-se a utilização de tecnologia que tenha por finalidade a proteção e segurança de pessoas e bens.”

Mas a jurista alerta que a finalidade real do *software* é o que determina a sua licitude.

“A distinção depende da finalidade real e do modo de utilização da tecnologia. Um software apresentado como ferramenta para controlo de segurança pode tornar-se ilícito se, na prática, servir para escrutinar hábitos, desempenho ou presença online do trabalhador.”

Sobre a ideia, por vezes invocada pelas empresas, de que o consentimento do trabalhador resolve o problema, a resposta é direta: “Não. O consentimento do trabalhador não é uma solução para legitimar a monitorização digital.”

E detalha porquê: “Aliás, o RGPD enfatiza que o consentimento deve ser dado de forma livre, sem pressão, condicionamento ou receio de consequências negativas em caso de recusa. Sucede que, no contexto da relação laboral, há uma desigualdade estrutural entre o empregador e o trabalhador que compromete a liberdade do consentimento que este possa dar.”

Na prática, diz, é precisamente no uso secundário dos dados que surgem muitos dos riscos legais mais relevantes.

“Diria que na ‘zona cinzenta’ encontramos, no mais das vezes, situações em que ocorre um desvio de finalidade, isto é, dados recolhidos por razões aparentemente legítimas – logs de acesso, tempos de login/logout, sistemas de tickets, ferramentas colaborativas, entre outros – que acabam depois por ser usados para inferir e escrutinar produtividade, assiduidade ou empenho. Esse desvio de finalidade é juridicamente sensível.”