Instituto Universitário de Lisboa

Secção Autónoma de Direito

Os meios de vigilância à distância no local de trabalho: em especial sobre o âmbito de aplicação do art. 20.º do Código do Trabalho

Marisa Ouro

Dissertação submetida como requisito parcial para obtenção do grau de

Mestre em Direito das Empresas
Especialização em
Direito do Trabalho

Orientador:
Doutor José João Abrantes, Professor Associado,
FDUNL

Junho, 2009

RELAÇÃO DE SIGLAS E ABREVIATURAS

Ac.	Acórdão
al.	alínea
AMA	American Management Association
Apud	Junto a
Art.	Artigo
BAG	Bundesarbeitsgericht – Tribunal Federal do Trabalho
B.F.D.U.C.	Boletim da Faculdade de Direito da Universidade de Coimbra
CC	Código Civil
CEDH	Convenção Europeia dos Direitos do Homem
Cfr.	Confere
CNIL	Commission Nationale de l' Informatique et des Libertés
CNPD	Comissão Nacional de Protecção de Dados
Consult.	Consultada
CT	Código do Trabalho
D.L.	Decreto-Lei
ECPA	Electronic Communications Privacy Act
Ed.	Edição
ET	Estatuto de los Trabajadores
GPS	*Global Positioning System;* Geolocalização
GT29	Grupo de Trabalho do Artigo 29
IDRF	Identificação por radiofrequência
Ibid.	Ibidem; no mesmo lugar
ICO	Information Commissioner's Office
LPDP	Lei de Protecção de Dados Pessoais
NTIC	Novas Tecnologias de Informação e Comunicação
OIT	Organização Internacional do Trabalho
ONU	Organização das Nações Unidas
Op. cit.	Obra já citada
p.	Página
pp.	Páginas
RF	Radiofrequência
SL	Statuto dei Lavoratori

ss.	seguintes
STJ	Supremo Tribunal de Justiça
TEDH	Tribunal Europeu dos Direitos do Homem
UE	União Europeia
UNI	Union Network International
Vd.	Vide
Vol.	Volume

Introdução

O presente trabalho tem como objecto os meios de vigilância à distância no local de trabalho e verificar de que modo a sua implementação está a ser conciliada com a reserva da intimidade da vida privada do trabalhador. Em especial, pretendemos verificar como está a ser aplicado e interpretado o art. 20.º do Código do Trabalho que regula a utilização destes meios, e cuja redacção se manteve inalterada no novo Código, tendo o nosso legislador procedido a meras alterações de sistematização.
Assim, ficam de fora do objecto deste estudo a protecção da reserva da intimidade da vida privada do empregador e situações laborais especiais, como sucede com o teletrabalho.

Quanto à metodologia seguida, em primeiro lugar, vamos proceder ao enquadramento dogmático da questão e que se insere na temática mais ampla da tutela dos direitos fundamentais no domínio das relações das relações laborais. Em particular, veremos que a implementação de meios de vigilância à distância no local de trabalho implica a colisão entre dois direitos constitucionalmente protegidos: liberdade de empresa, nomeadamente o poder directivo do empregador que irradia dessa liberdade, e o direito fundamental à reserva da intimidade da vida privada que o trabalhador conserva enquanto cidadão.

Em segundo lugar, tratamos do enquadramento legal dos meios de vigilância à distância no local de trabalho, quer ao nível de convenções internacionais aplicáveis, direito comunitário, direito constitucional, civil, penal, laboral, a lei de protecção de dados pessoais portuguesa e uma referência ao direito comparado alemão, espanhol, italiano, francês e americano e inglês.

Enquadrado o tema, vamos estabelecer critérios para definir o que se entende por meios de vigilância à distância no local de trabalho com recurso a equipamento tecnológico e, seguidamente, expor os resultados de uma pesquisa ao nível da jurisprudência, bem como analisar as principais Decisões e Orientações da Comissão Nacional de Protecção de Dados sobre a videovigilância, identificação por radiofrequência, geolocalização, controlo do uso da internet e do telefone.

Ao nível da análise jurisprudencial vamos centrar-nos na sensibilidade dos tribunais para a problemática dos meios de vigilância à distância e como os conciliam com os direitos fundamentais dos trabalhadores. Os tribunais admitem que alguns destes meios de vigilância possam constituir meios de prova, nomeadamente para despedir o trabalhador? Os tribunais consideram que a utilização destes meios pela entidade empregadora possa constituir justa causa de despedimento pelo trabalhador? E em caso afirmativo, em que circunstâncias?

Será que se em vez de analisarmos a potencialidade de cada um destes meios tecnológicos separadamente fizermos uma análise da totalidade dos meios tecnológicos existentes na empresa e da informação que resulta do cruzamento entre estes relativamente ao trabalhador vamos chegar a uma compreensão diferente em relação à sua interferência na reserva da intimidade da vida privada do trabalhador? Que consequências devemos retirar dessa conclusão?

Seguidamente, debruçamo-nos sobre o âmbito de aplicação do artigo 20.º do Código do Trabalho, recorrendo ao elemento histórico, sistemático, literal e teleológico da interpretação para perceber se a expressão do art. 20.º do Código do Trabalho relativamente aos "meios de vigilância à distância no local de trabalho, com recurso a equipamento tecnológico" remete apenas para formas de captação à distância de imagem, ou imagem e som, excluindo outras possibilidades proporcionadas pelas novas tecnologias. Deve este artigo ver a sua aplicabilidade limitada à videovigilância? Devemos incluir no seu âmbito todas as formas de vigilância à distância no local de trabalho com recurso a equipamento electrónico? Deverão ser efectuadas clarificações na lei laboral ou remetemos a resolução dos conflitos que possam resultar para a integração com a lei constitucional, civil, penal e de protecção de dados pessoais?

Ao longo desta tese pretendemos levantar novas questões, trazidas pela aplicação das novas tecnologias ao Direito do Trabalho, e apresentar algumas respostas possíveis.

Enquadramento dogmático:

Contrato de trabalho e direitos fundamentais

A relação entre o contrato de trabalho e os direitos fundamentais pressupõe uma concepção social do Estado de Direito que apareceu plasmada pela primeira vez na Constituição alemã de Weimar, de 11 de Agosto de 1919 e que marca a passagem do constitucionalismo liberal[1] para o constitucionalismo social[2].

Na sequência da Constituição de Weimar desenvolveram-se na Alemanha várias teorias que defendem a eficácia horizontal dos direitos fundamentais, isto é, a eficácia dos direitos fundamentais nas relações entre os particulares.

A primeira modalidade desta teoria deveu-se a um dos grandes nomes do juslaboralismo – Hans Carl Nipperdey[3] - que defendeu a eficácia directa ou imediata ("*unmittelbare Drittwirkung"*) dos direitos fundamentais sem necessidade de interposição legislativa. Esta tese tem como principal preocupação a protecção da liberdade individual contra os poderes sociais e a defesa da coerência interna do ordenamento, defendendo que os direitos fundamentais são normas de valor que devem valer também para o direito privado.

Outros autores, de que se destaca Günter Dürig, criticaram esta tese por a considerarem uma ameaça à autonomia privada e conduzir a uma compressão inaceitável do princípio do livre desenvolvimento da personalidade pelo que defenderam a teoria da eficácia indirecta, isto é, a apreciação dos comportamentos privados não teriam por base directa os preceitos constitucionais mas sim a lei e essa

[1] O constitucionalismo liberal é pautado por uma obrigatoriedade de abstenção, de não interferência nos direitos e liberdades dos cidadãos. A igualdade do constitucionalismo clássico liberal era uma igualdade meramente formal, que se limitava exclusivamente à atribuição de direitos fundamentais à vida, à liberdade e à propriedade e não se estendia às situações concretas.

[2] O constitucionalismo social traz consigo uma modificação no modo de encarar os direitos fundamentais, não apenas na sua dimensão subjectiva mas também com uma *dimensão objectiva*, *normas de valor* que percorrem toda a ordem jurídica, trespassando não só o direito público mas também o direito privado, ou seja, a pessoa tem direito a ver os seus direitos fundamentais protegidos não apenas contra o Estado mas também perante os outros cidadãos nomeadamente quando estamos a falar de relações em que uma das partes tem um poder económico ou social de facto que faz com que a outra parte seja um *contraente débil*.

[3] Sobre a teoria defendida por Hans Carl Nipperdey ver JOSÉ JOÃO ABRANTES, *Contrato de trabalho e direitos fundamentais*, Coimbra Editora, Coimbra, 2005, pp. 80-87

sim seria obrigada na sua conformação a obedecer a esses direitos[4]. Os direitos fundamentais funcionariam como princípios influenciadores da interpretação das cláusulas gerais de direito privado e não seriam tidos em conta nessa valoração todos os princípios mas apenas aqueles cuja violação choque com *a "consciência ou a sensibilidade das pessoas de sã formação"* ou com a *"consciência social"*[5].

Estas teorias conduziam quase sempre aos mesmos resultados práticos, embora nem sempre, e a sua aplicação pelos tribunais conduziu a uma aceitação generalizada da *Drittwirkung*.

No ordenamento jurídico português diz o art. 18.º, n.º 1 da Constituição da República Portuguesa: "Os preceitos constitucionais respeitantes aos direitos, liberdades e garantias são directamente aplicáveis e vinculam as entidades públicas e privadas." Apesar de a letra parecer apontar no sentido da aplicabilidade directa às entidades privadas há quem defenda a aplicabilidade mediata no nosso ordenamento argumentando que a Constituição não concretiza em que termos se processa essa vinculação. É o caso de Menezes Cordeiro[6] que fala a este propósito numa *eficácia reflexa* dos direitos fundamentais e alerta para o facto de "o recurso indiscriminado à Constituição para interferir nas posições privadas" poder "conduzir a banalizações que retirem impacto às intervenções constitucionais verdaadeiramente necessárias".

Para os defensores da teoria da eficácia directa não é necessária a intervenção ou mediação do legislador para que os direitos fundamentais sejam aplicados, tendo eficácia erga omnes. A este respeito, e argumentando contra a teoria da aplicabilidade mediata, Gomes Canotilho e Vital Moreira[7], escrevem: "a Constituição portuguesa faz aplicar expressamente os direitos fundamentais às relações entre entidades privadas, sem qualquer restrição ou limitação, não sendo portanto legítimo limitar essa eficácia apenas aos casos em que a doutrina estrangeira a admite quando nada nas respectivas leis fundamentais a impõe". Também José João Abrantes[8] e Ana Prata[9] defendem esta posição.

Um terceiro grupo de autores defende a aplicabilidade imediata dos direitos fundamentais no domínio das relações privadas apenas quando, como refere Vieira de Andrade[10], "se trate de situações em que pessoas colectivas (ou, excepcionalmente, indivíduos) disponham de *poder especial* de carácter privado sobre (outros) indivíduos".

---

[4] Sobre esta teoria ver GUILHERME DRAY, *O princípio da igualdade igualdade no Direito do Trabalho: sua aplicabilidade no domínio específico da formação de contratos individuais de trabalho*, Almedina, Coimbra, 1999, pp. 145-146.
[5] JOSÉ JOÃO ABRANTES, *Contrato de trabalho e direitos fundamentais…,* p. 131
[6] *Manual de Direito do Trabalho*, Almedina, Coimbra, 1991, *pp. 151-156*
[7] GOMES CANOTILHO e VITAL MOREIRA, *Constituição da República Portuguesa Anotada,* Vol I, 4.ª ed. revista, Coimbra Editora, 2007, pp. 385-387.
[8] *Contrato de trabalho e direitos fundamentais*, op. cit., pp. 131-134.
[9] *A tutela constitucional da autonomia privada*, Livraria Almedina, Coimbra, 1982, pp. 136-140
[10] *Os Direitos Fundamentais na Constituição Portuguesa de 1976, pp.* 262-264.

Defendem também esta posição Heinrich Hörster[11], João Caupers[12], Jorge Miranda[13], Vasco Pereira da Silva[14] e Teresa Moreira[15].

Em nosso entender, o conteúdo essencial de um direito fundamental, a que se reporta o art. 18.º, n.º 3 da Constituição, não coincide necessariamente com o conteúdo das cláusulas gerais de direito privado pelo que, nessas situações, *só a teoria da eficácia imediata responde de forma a cumprir o desiderato constitucional, ou seja, a intangibilidade do conteúdo mínimo essencial dos direitos fundamentais*[16]. A aplicação directa dos direitos fundamentais não é contudo uma aplicação automática porquanto há que ponderar em cada caso concreto os interesses e valores em presença e, caso exista algum direito fundamental em causa, recorrer às regras sobre conflitos de direitos (art 335.º do Código Civil) na sua resolução[17].

Na prática, acabam por não haver grandes diferenças entre estas teorias acabando todas por aplicar as regras dos conflitos de direitos, nomeadamente, os princípios da necessidade, da adequação e da proporcionalidade para delimitar a eficácia dos direitos fundamentais em cada caso concreto.[18]

Todas as teorias chegam à conclusão de que as entidades privadas "poderosas" não podem ser tratadas como quaisquer outros indivíduos e, por isso, na relação laboral, a eficácia dos direitos fundamentais surge como absolutamente "natural"[19] porque no plano das relações laborais verifica-se com maior acutilância uma desigualdade entre as partes, tanto no plano factual como contratual e desde o momento do processo de selecção até ao da execução do contrato[20], tendo sido aliás o reconhecimento da necessidade de limitar esse poder que levou à autonomização do Direito do Trabalho[21].

---

[11] *A parte geral do Código Civil português – Teoria Geral do Direito Civil*, Almedina, Coimbra, 1992, pp. 96-97

[12] *Os direitos fundamentais dos trabalhadores e a Constituição*, Almedina, Coimbra, 1985, pp. 167-174

[13] *Manual de Direito Constitucional*, Tomo IV, *Direitos Fundamentais*, 3.ª ed., Coimbra Editora, 2000, pp. 320-327. Jorge Miranda defende que a aplicação das normas sobre direitos liberdades e garantias nas relações entre particulares se faz por identidade de razão nas relações entre pessoas colectivas e os seus membros bem como entre particulares e poderes sociais de facto, e por analogia nas relações entre particulares em igualdade.

[14] *A vinculação das entidades privadas pelos direitos, liberdades e garantias*, in *R.D.E.S.* 1987, n.º 2, pp. 272-273.

[15] *Da esfera privada…, op. cit.,* p. 57

[16] JOSÉ JOÃO ABRANTES, *Contrato de trabalho e direitos fundamentais…,* p. 132

[17] Ibid., p. 135 e nota 261

[18] JOSÉ JOÃO ABRANTES, "O novo Código do Trabalho e os direitos de personalidade", in *Estudos sobre o Código do Trabalho*, pp.151-152 e nota 22 que refere que a única diferença entre as duas principais teorias é a de que a a tese da eficácia indirecta pode conduzir a uma interpretação mais restritiva dos direitos fundamentais.

[19] JOSÉ JOÃO ABRANTES, *Contrato de trabalho e direitos fundamentais…,* p. 17 e 141, do mesmo autor "O novo Código de Trabalho e os direitos de personalidade"…, p. 146. Ver também TERESA MOREIRA, *Da esfera privada do trabalhador e o controlo do…,* pp. 57-58 e nota 113.

[20] JOSÉ JOÃO ABRANTES, *Contrato de trabalho e direitos fundamentais…, op. cit.,* p. 36

[21] Ibid., p. 38 e TERESA MOREIRA, *Da esfera privada do trabalhador e o controlo do…,* p. 17

Como refere José João Abrantes[22], *o facto de o contrato de trabalho ter por objecto uma prestação pessoalíssima, com a pessoa do trabalhador intrinsecamente envolvida na troca contratual, sendo, além disso, o trabalho um valor essencial para a dignidade do homem e para o livre desenvolvimento da sua personalidade, aquele contrato é, provavelmente como nenhum outro, constitucionalmente condicionado, por valores e princípios subjacentes aos direitos fundamentais,* havendo mesmo quem afirme que é a própria pessoa do trabalhador que estabelece uma comunicabilidade directa entre a Constituição e o Direito do Trabalho[23].

A reserva da intimidade da vida privada do trabalhador

O que é o direito à reserva da intimidade da vida privada?

A origem do conceito "right to privacy" é reconduzida a um artigo de Samuel Warren e Louis Brandeis, publicado na Harvard Law Review, vol. IV, n.º 5, 15 December 1890[24] e apareceu na sua vertente de "right to be let alone" e tendo como objectivo estabelecer um limite jurídico às intromissões da imprensa na vida privada.

De todos os direitos humanos, a privacidade talvez seja o mais difícil de definir e circunscrever mas a falta de uma definição única não implica que não tenha importância porque, como Fernando Volio disse: *"in one sense, all human rights are aspects of the right to privacy"*[25].

O conceito de vida privada é um conceito aberto onde estão em causa aspectos que se prendem com as "experiências, lutas e paixões pessoais de cada um e que não devem, enquanto tal, ser objecto da curiosidade do público[26]". Dentro da esfera da vida privada, e na esteira da jurisprudência constitucional alemã que esteve na origem da "teoria das três esferas"[27], alguma doutrina nacional procura distinguir entre uma esfera

---

[22] *Contrato de trabalho e direitos fundamentais…,* op. cit., p. 48

[23] REY GUANTER, "Diritti fondamentali della persona e contratto di lavoro: appunti per una teoria generale", in *Quaderni di Diritto del Lavoro e delle Relazioni Industriali. Diritti della persona e contratto di lavoro,* Torino, 1994, p. 31 apud JOSÉ JOÃO ABRANTES, *Contrato de trabalho e direitos fundamentais…,* p. 48, nota 70

[24] Apud CATARINA SARMENTO E CASTRO, "A protecção dos dados pessoais dos trabalhadores", in *Questões Laborais*, 19, Ano IX, 2002, p.27 e DAVID FESTAS "O direito à reserva da intimidade da vida privada do trabalhador no Código do Trabalho", in *R.O.A.,* Ano 64, vol I/II, Novembro 2004, p. 3. Este último autor refere: "muito embora o direito à reserva da intimidade da vida privada já houvesse sido anteriormente reconhecido, é a Warren e Brandeis que se deve (…) o primeiro ensaio sobre a matéria".

[25] In "Legal personality, privacy and the family" in Henkin (ed) The International Bill of Rights, New York : Columbia University Press, 1981 apud PRIVACY INTERNATIONAL - **"**PRIVACY AND HUMAN RIGHTS An International Survey of Privacy Laws and Practice" in http://gilc.org/privacy/survey/intro.html [Consult. 28 Junho 2009]. Neste último artigo é referido também que a privacidade tem raízes históricas antigas, com referências numerosas na Biblia, nas origens da cultura hebraica, Grécia Clássica e antiga China. Ver também PAULO MOTA PINTO, "A protecção da vida privada e a Constituição", *in B.F.D.U.C.,* n.º 76, 2000, p. 164, que defende que "O reconhecimento da reserva da vida privada é uma condição de integridade da pessoa e a sua protecção deve ser considerada actualmente como um aspecto da protecção da "dignidade humana" ".

[26] TERESA MOREIRA, *Da esfera privada…,* p. 135

[27] Esta teoria distinguia três níveis ou graus de protecção em relação à vida privada: um respeitante à esfera intima (*intimsphäre*), que se identifica com a noção de intimo, protegendo a vida pessoal e familiar

pessoal, íntima e absolutamente protegida que compreende factos que objectivamente devem estar protegidos da curiosidade alheia, como comportamento sexuais, práticas religiosas e estado de saúde das pessoas. Uma outra esfera privada que compreende todos os factos que o titular tem interesse, subjectivamente, em conservar para si e que apenas cederia em caso de conflito com outro direito e, por último, uma esfera pública, abrangendo todos os factos do conhecimento público que se desenvolveriam perante a comunidade[28].

Como refere Rabindrananath Capelo de Sousa[29], *a reserva da vida privada abrange "não só o respeito da intimidade da vida privada, em particular a intimidade da vida pessoal, familiar, doméstica, sentimental e sexual e inclusivamente os respectivos acontecimentos e trajectórias, mas ainda o respeito de outras camadas intermédias e periféricas da vida privada, como as reservas de domicílio e de lugares adjacentes, da correspondência e de outros meios de comunicação privada, dos dados pessoais informatizáveis, dos lazeres, dos rendimentos patrimoniais, dos demais elementos privados da actividade profissional e económica, bem como também, last but not the least, a própria reserva sobre a individualidade do privada do homem no seu ser para si mesmo, v. g., sobre o seu direito a estar a só e sobre os caracteres de acesso privado do seu corpo, da sua saúde, da sua sensibilidade e da sua estrutura intelectiva e volitiva".*

Este conceito tem aplicação ao trabalhador?

Há quem defenda que a empresa é um espaço público e ainda hoje encontramos concepções nesse sentido e cuja visão é determinante na fundamentação de determinadas sentenças[30]: dentro do horário laboral e em cumprimento da actividade laboral não existe espaço de intimidade.

Outra corrente, baseada na defesa da cidadania na empresa, isto é, no reconhecimento da relevância dos direitos fundamentais não especificamente laborais, dos direitos do "cidadão-trabalhador", que os exercita enquanto "trabalhador-cidadão" na empresa[31], onde ele mantém em princípio todos os direitos de que são titulares todas

---

que se pretende reservada e fora do conhecimento dos demais; outro referente à esfera privada (*privatsphäre*), relativo ao que cada pessoa tem como secreto ou particular, cuja violação ocorre quando se conhecem factos ou noticias que não se desejam revelar; um outro relativo à esfera individual (*individualsphäre*), que é tudo aquilo que individualiza uma pessoa, como a honra, o nome, a imagem.

[28] TERESA MOREIRA, *Da esfera privada…,* p. 136 e para referências doutrinais vide nota 424

[29] *Direito Geral de Personalidade*, Coimbra Editora, 1995, pp. 316-325.

[30] Cristina SÁNCHEZ-RODAS NAVARRO, "Videocámaras y poder de vigilancia", *Arazandi Social*, Tomo IX, 1999, p. 1127 e R. LÓPEZ PARADA "Análisis jurisprudencial acerca de la instalación por el empresario de sistemas de videovigilância en los lugares de trabajo", *Información Laboral (Jurisprudencia)*, n.º 9, 1999, p. 5046 e ss apud JOSÉ LUÍS GOÑI SEIN, *La videovigilancia empresarial y la protección de datos personales*, Civitas / Colección Estudios de protección de datos, 2007, p. 28, nota 25 e 26.

[31] Expressões de ALONSO OLEA, *Las fuentes del Derecho, en especial del Derecho del trabajo,* Madrid (1982), p. 28 Apud JOSÉ JOÃO ABRANTES, "*Contrato de Trabalho e Direitos Fundamentais"…* p. 60 nota 88

as outras pessoas, sustenta que há lugar para o direito à reserva da intimidade da vida privada do trabalhador.

O trabalhador ao celebrar o contrato de trabalho está a limitar a sua esfera privada mas essa esfera não fica confinada às casas de banho ou cacifos. Abrange aspectos como as conversas pessoais com os seus companheiros de trabalho, a actividade sindical destes, o rendimento auferido, o seu estado de saúde. Como refere Menezes Cordeiro[32], a esfera privada dos trabalhadores corresponde "em termos latos ao círculo dos direitos de personalidade que só com o consentimento do próprio e nos limites da lei, podem ser restringidos".

A informática e o direito à autodeterminação informacional

Graças à informática e à enorme capacidade de tratamento automatizado, conexão, transmissão e utilização de dados pessoais operou-se uma *revolução coperniciana*[33] no direito à intimidade obrigando as pessoas a tomarem uma atitude mais activa designada de "direito à privaticidade"[34] ou direito à autodeterminação informacional. Como refere José Luís Goñi Sein[35], o direito à autodeterminação informacional é mais abrangente que o direito à intimidade, é o direito a dispor de todas as informações sobre a sua pessoa e o bem protegido não é apenas o espaço defendido da curiosidade alheia mas também o direito em geral de personalidade, a identidade, o património moral da pessoa, que dá a possibilidade de exercer um controlo sobre a totalidade da pessoa e que constitui em si mesmo um direito ou liberdade fundamental.

Assim, o poder directivo do empregador tem como limite não apenas o direito à reserva da vida privada do trabalhador mas também tem de respeitar o direito à autodeterminação informacional deste.

O poder de controlo do empregador

A liberdade de empresa encontra-se constitucionalmente tutelada quer através do art. 80.º, al. c) que estatui que a organização económico-social assenta no princípio da liberdade de iniciativa e de organização empresarial quer através do art. 86.º, n.º 1 que estabelece que o Estado incentiva a actividade empresarial.

---

[32] MENEZES CORDEIRO, "O respeito pela esfera privada do trabalhador", in *I Congresso Nacional de Direito do Trabalho _Memórias* (coord. António Moreira), Almedina, Coimbra, 1998, p. 36

[33] Expressão utilizada por VINCENZO FRANCESCHELLI, "La tutela dei dati personali. Introduzzione alla lege sulla privacy informática", in AA.VV., *La tutela della privacy informatica – Problema e prospettive* (coord. Vincenzo Franceschelli), Giuffré Editore, Milão, 1998, p. 4 Apud TERESA MOREIRA, *Da esfera privada…,* p. 22, nota 6

[34] Expressão de VIEIRA DE ANDRADE, *Os Direitos Fundamentais na Constituição…*, op. cit., p. 65

[35] *"La videovigilancia empresarial y la protección…"*, op. cit., pp. 60-61, nota 2

Para poder gerir a empresa e conformar a prestação laboral, o empregador tem o poder directivo para poder fixar os termos em que deve ser prestado o trabalho, nos termos previstos no art. 97.º do CT, ou seja, dentro dos limites que decorrem do contrato e das normas que o regem, e necessita que o trabalhador cumpra as ordens e instruções do empregador em tudo o que respeite à execução e disciplina do trabalho, conforme está previsto no art. 128.º, n.º1 al. e) do CT. Este "poder conformativo da prestação"[36] varia de âmbito e intensidade consoante a maior dependência técnica ou autonomia técnica do trabalhador (art. 116.º e 127 e) CT).

O exercício do poder de direcção tem limites, nomeadamente o direito à reserva de intimidade da vida privada do trabalhador (art. 26.º, n.º 1 CRP) ou o seu direito de personalidade (arts 70.º e ss do CC)[37].

O poder directivo compreende não apenas o poder de dar ordens ou instruções mas também outros aspectos como definir o organigrama da empresa, classificar postos de trabalho, determinar onde, quando e como deve o trabalhador desempenhar a sua actividade e, naturalmente, o empregador tem o poder de fiscalizar a actividade do trabalhador.

O poder de controlo exercido pela entidade empregadora, poder exercido com carácter imperativo, legitima que, legalmente, esta possa ser responsabilizada perante terceiros em situações de responsabilidade civil por *culpa in vigilando* e também nos termos previstos no art. 500.º CC para a responsabilidade do comitente[38].

As novas tecnologias e o poder de controlo do empregador

O modo com as empresas trabalham alterou-se muito devido às novas tecnologias. O mercado em que muitas empresas trabalham deixou de ser um espaço físico e passou a ser um espaço cibernético. Simultaneamente, a coordenação da actividade económica realiza-se através do computador, do email, do telemóvel. O poder do empregador tem de ser agora exercido neste novo espaço e é aqui que entra a cibervigilância. As técnicas de monitorização contribuem para que as novas tecnologias

---

[36] Expressão de MONTEIRO FERNANDES, *Direito do Trabalho,* 13.ª ed., Almedina, 2007, pp. 261-263. Monteiro Fernandes distingue quatro vectores na posição jurídica do empregador: poder determinativo da função; poder conformativo da função; poder regulamentar e poder disciplinar. O poder conformativo da função é a faculdade de determinar o modo de agir do trabalhador e o seu exercício tem como limites os próprios contornos da função sendo que, em funções de autonomia técnica o poder conformativo terá que limitar-se à definição do tempo e local de trabalho, bem como às regras gerais derivadas da disciplina e da organização da empresa.

[37] PEDRO ROMANO MARTINEZ, *Direito do Trabalho,* 4ª ed., Coimbra : Almedina, 2007, p. 628

[38] Nos termos do Art. 500.º, n.º 1 do Código Civil: *" Aquele que encarrega outrem de qualquer comissão responde, independentemente de culpa, pelos danos que o comissário causar, desde que sobre este recaia também a obrigação de indemnizar."*

possam fazer parte desta nova forma de organização dos factores produtivos, capital e trabalho, havendo quem fale a este respeito em "*società sorvegliata*"[39].

As novas tecnologias permitem uma maior efectividade do controlo por parte do empregador e a actual capacidade informática de recolha de dados leva a que hoje se utilize a expressão *"trabalhador-transparente"* ou *"trabalhador de vidro"*[40].

Outro aspecto importante é que a produtividade do trabalhador pode ser potenciada pelas novas tecnologias. Existem já estudos[41] que concluem que pequenos intervalos durante o trabalho para aceder à internet permitem ao trabalhador descansar a mente e, como tal, aumentar a produtividade. Já há empregadores[42] a defender que um uso livre da Internet no local de trabalho estimula a auto-formação dos trabalhadores na medida em que lhes permite ampliar os seus conhecimentos, que se podem revelar úteis no local de trabalho. A outra face da moeda é que um uso excessivo e não controlado da internet no local de trabalho pode levar a uma queda drástica na produtividade do trabalhador. Até que ponto a entidade empregadora pode monitorizar os sites visitados e monitorizar o conteúdo dos emails dos trabalhadores é uma questão cuja resposta varia de acordo com as políticas empresariais seguidas e com o quadro legal do país em que laboram.

O uso intensivo dos meios de controlo do trabalhador pode levar à redução da sua autonomia para níveis inexistentes, desumanizando o trabalhador[43].

Em conclusão, as novas tecnologias não só permitem um poder de controlo ilimitado como trouxeram novas vantagens e problemas para o local de trabalho cabendo ao empregador dosear o seu emprego, de acordo com as suas necessidades, mas sempre respeitando a dignidade humana e os direitos fundamentais do trabalhdor

---

[39] D. LYON, "La società sorvegliata.", Milão 2001, p. 127 apud ANDREA STANCHI, "L'utilizzo della Radio Frequency Identification (Rfid) e le implicazioni giuslavoristiche." in http://www.di-elle.it/consultazione/approfondimenti_4/radio_frequency_identification_790/view/790/ [Consult. 28 Junho 2009]

[40] Expressão de MARIAPAOLA AIMO, "I "lavoratori di vetro": regole di trattamento e meccanismi di tutela dei dati personali", in R.G.L.P.S., n.º 1, 2002 apud TERESA MOREIRA, *Da esfera privada…,* p. 26, nota 9

[41] MICHAEL SPECHT, "Internet usage at work makes you more productive" in http://specht.com.au/michael/2009/04/03/internet-usage-at-work-makes-you-productive/ [Consult. 28 Junho 2009] tem um artigo sobre um estudo que foi feito em 300 trabalhadores na Austrália e que conclui que pequenos intervalos durante o trabalho para aceder à internet permite ao trabalhador descansar a mente e, em consequência, aumen tar a produtividade.

[42] A este respeito, veja-se o artigo de PHIL JOHNSON, "A new policy for internet use in the workplace", (16 Março 2009) in http://adage.com/smallagency/post?article_id=135266 [Consult. 28 Junho 2009].

[43] A este respeito, veja-se o artigo publicado na edição de 8 de Junho de 2005 do Elmundo.es com o título "Vigilancia electrónica total a los trabajadores británicos de la distribución", in http://www.elmundo.es/navegante/2005/06/08/esociedad/1118217101.html [Consult. 28 Junho 2009]. Neste artigo é referido que, actualmente, os empregados de armazém em muitos supermercados britânicos são obrigados a transportar micro-computadores agarrados aos braços, que têm um dispositivo gps associado, limitando-se estes a seguir as instruções sobre os locais do armazém para que se devem dirigir. Estes dispositivos calculam exactamente quanto tempo se demora a ir de uma parte do armazém para a outra bem como as pausas, não se tolerando quaisquer desvios a estes tempos.

que não deixam de estar sujeitos à ordem constitucional pelo facto de terem um carácter privado. Existe neste campo uma *presunção de liberdade*[44] a favor do trabalhador pelo que o empregador só poderá limitar a liberdade do trabalhador quando tal lhe seja especificamente permitido e/ou se houver subjacentes à sua actuação interesses que, no caso concreto, se mostrem merecedores de uma tutela superior à daquela liberdade. *Cabendo, aliás, ao empregador o ónus da prova da legitimidade de introduzir limitações à referida liberdade do trabalhador e, mesmo assim, sempre dentro de critérios de necessidade e de proporcionalidade*[45].

[44] Expressão de JOSÉ JOÃO ABRANTES, "O novo Código de Trabalho e os direitos de…", p. 157
[45] JOSÉ JOÃO ABRANTES, *Contrato de trabalho e direitos fundamentais…*, p. 191, nota 402

Enquadramento legal - **Disposições legais genericamente aplicáveis à problemática dos meios de vigilância à distância no local de trabalho**

Direito Internacional

Nos termos do art. 8.º da Constituição, as normas e os princípios de direito internacional geral ou comum fazem parte integrante do direito português, as normas constantes de convenções internacionais regularmente ratificadas ou aprovadas vigoram na ordem interna, as normas emanadas dos órgãos competentes das organizações internacionais de que Portugal seja parte vigoram directamente na ordem interna desde que tal se encontre estabelecido nos respectivos tratados constitutivos. Quanto às disposições dos tratados que regem a União Europeia e às normas emanadas das suas instituições, no exercício das respectivas competências, são aplicáveis na ordem interna, nos termos definidos pelo direito da União.

Vamos seguidamente referir normas de Direito Internacional importantes na resolução do conflito existente entre o poder de controlo do empregador e a dignidade do trabalhador, nomeadamente na defesa da intimidade da sua vida privada, bem como normas que contêm os princípios por que se devem reger o tratamento dos dados pessoais.

Nações Unidas

Declaração Universal dos Direitos Humanos

Adoptada em 1948 pela Assembleia Geral da ONU e publicada no Diário da República a 9 de Março de 1978, a Declaração Universal dos Direitos Humanos encontra-se expressamente referida na nossa Lei Fundamental, no art. 16.º, n.º 2, e tem, como refere Jorge Bacelar Gouveia[46], um intenso significado simbólico-político no sentido do comprometimento do Estado português no movimento de protecção dos direitos do homem. Para a matéria dos meios de vigilância à distância no local de trabalho interessa-nos o art. 12.º que preceitua: "Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a protecção da lei."

[46] JORGE BACELAR GOUVEIA, "A Declaração Universal dos Direitos do Homem e a Constituição da República Portuguesa", *Perspectivas do Direito*, vol. IV, n.º 6, Julho de 1999, p. 59

Pacto Internacional sobre Direitos Civis e Políticos

Adoptada pela Assembleia Geral das Nações Unidas a 16 de Dezembro de 1966 e tendo entrado em vigor na ordem jurídica portuguesa a 15 de Setembro de 1978, o Pacto Internacional sobre Direitos Civis e Políticos estabelece no seu art. 17.º, n.º 1: "Ninguém poderá ser objecto de ingerências arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem de ataques à sua honra e reputação".

Recolha de Directivas Práticas sobre a Protecção de Dados Pessoais dos trabalhadores, OIT, 7/10/96

No âmbito das Nações Unidas, mais concretamente no domínio do direito laboral, destaca-se a Recolha de Directivas Práticas sobre a Protecção de Dados Pessoais dos trabalhadores efectuada pela Organização Internacional do Trabalhadores (OIT), que abrange o sector privado e o sector público, aplicável à recolha manual ou automatizada de dados pessoais do trabalhador. Este Código não tem força obrigatória, ao contrário das Convenções da OIT, nem gera obrigações procedimentais, como sucede com as Recomendações da OIT, mas destina-se a fornecer aos empregadores e trabalhadores regras-base de orientação prática nesta matéria.

Sobre a monitorização é de destacar o ponto 6.14 (1) que estabelece o dever de o trabalhador ser informado previamente sobre a monitorização e as suas finalidades, métodos e técnicas utilizadas bem como quais os dados que irão ser recolhidos devendo essa monitorização ser efectuada com um mínimo de intrusão na privacidade dos trabalhadores.

Em relação à monitorização oculta, o ponto 6.14 (2) estabelece que deve apenas ser permitida se estiver em conformidade com a legislação nacional ou se houver suspeitas fundadas de actividade criminosa ou outros delitos graves.

Quanto à monitorização contínua, nos termos do ponto 6.14 (3) deve ser permitida somente se for necessário por questões de saúde, segurança ou de protecção da propriedade.

Conselho da Europa

Convenção Europeia para a Protecção dos Direitos Humanos

Do Conselho da Europa emanam as principais fontes de direito europeu não comunitário e, com incidência para a matéria que nos prende, importa referir o art. 8.º da Convenção Europeia para a Protecção dos Direito Humanos (CEDH): "Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência."

O Tribunal Europeu dos Direitos do Homem, encarregue de assegurar o cumprimento dos direitos que a Convenção reconhece, considera que o respeito pela vida privada deve também englobar o direito de cada pessoa desenvolver relações com

os seus semelhantes e por isso não vê razão para não ser aplicado também às actividades comerciais e laborais[47].

Recomendação R (89)2 do Comité de Ministros do Conselho da Europa

Também é do Conselho da Europa, mais concretamente do Comité de Ministros, que emana a Recomendação sobre a protecção de dados pessoais no local de trabalho aplicável ao processamento automático de dados e que recomenda os princípios a que deve obedecer o legislador nacional na feitura das leis sobre esta temática bem como a difusão dos mesmos entre os empregadores e trabalhadores. A destacar o art 3.º n.º 1 que estabelece que as entidades empregadoras devem informar ou consultar os empregados ou os seus representantes antes da introdução ou adaptação de sistemas automatizados de recolha de dados pessoais dos trabalhadores sendo que este princípio também se aplica à introdução ou adaptação de tecnologias destinadas a monitorizar os movimentos ou a produtividade dos empregados. O art. 3.º, n.º2 recomenda que o procedimento de consulta seja efectuado antes da introdução desses dispositivos de modo a que a obtenção do acordo dos trabalhadores ou dos seus representantes seja feita no respeito pela vida privada e dignidade humana.

União Europeia

Carta dos Direitos Fundamentais da União Europeia

A Carta dos Direitos Fundamentais da União Europeia representa a síntese dos valores comuns dos Estados-Membros da UE e, pela primeira vez, reúne num único texto os direitos civis e políticos clássicos, bem como os direitos económicos e sociais. Os objectivos são explicados no preâmbulo: "é necessário, conferindo-lhes maior visibilidade por meio de uma Carta, reforçar a protecção dos direitos fundamentais, à luz da evolução da sociedade, do progresso social e da evolução científica e tecnológica". Os princípios delineados na Carta são aplicáveis não apenas no seio das instituições europeias mas também aos Estados-Membros (às autoridades centrais, bem como às autoridades regionais ou locais) sempre que apliquem a legislação comunitária. No art. 7.º da Carta é declarado que "Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações". E no art.º 8.º encontra-se estabelecido que todos têm direito à protecção dos dados de carácter pessoal que lhes digam respeito sendo que esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Também está previsto, no n.º 2 do mesmo artigo,

[47] Vd. Acs do T.E.D.H. *N. contra a Alemanha*, de 23 de Novembro de 1992, e *H. contra o Reino-Unido*, de 27 de Maio de 1997, citados pela Commission Nationale de l' Informatique et des Libertés no relatório "La Cybersurveillance sur les lieux de travail", p. 8 in http://www.cnil.fr/fileadmin/documents/approfondir/rapports/Rcybersurveillance-2004-VD.pdf [Consult. 28 Junho 2009]

o direito de acesso aos dados coligidos que lhes digam respeito e o direito de obter a respectiva rectificação.

A Directiva n.º 95/46/CE, de 24 de Outubro relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados

A Directiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, tem como objectivo, como diz no seu art. 1.º, assegurar "a protecção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais" e aplica-se "ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos num ficheiro ou a ele destinados".

Os dados pessoais são, como refere o art. 2.º, "qualquer informação relativa a uma pessoa singular identificado ou identificável" sendo que essa identificabilidade pode resultar de forma directa ou indirecta, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social.

Dos princípios que a Directiva estabelece, a destacar, quanto à qualidade dos dados: terão de ser objecto de um tratamento leal e lícito; recolhidos para finalidades determinadas, explícitas e legítimas, não serão posteriormente tratados de forma incompatível com essas finalidades; adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e para que são tratados posteriormente; exactos e, se necessário, actualizados; conservados de forma a permitir a identificação das pessoas em causa apenas durante o período necessário para a prossecução das finalidades para que foram recolhidos ou para que são tratados posteriormente.

Quanto aos requisitos para que esses dados sejam tratados de forma legítima, a regra é a da exigência do consentimento da pessoa em causa, que deve ser dado de forma inequívoca. Esse consentimento não será exigido quando estiverem preenchidas algumas das outras alíneas do art 7.º da Directiva, nomeadamente quando, nos termos da alínea f), "for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa". Quer isto dizer que os interesses legítimos da entidade empregadora poderão justificar o tratamento de dados pessoais dos trabalhadores, ponderados os interesses ou os direitos e liberdades fundamentais dos mesmos, nomeadamente o seu direito à reserva da intimidade da vida privada. Relativamente aos dados sensíveis (dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como dados relativos à saúde e à vida sexual), o seu tratamento é proibido pelo art. 8.º n.º 1 da Directiva salvo, entre outras situações, quando a pessoa em causa tiver dado o seu consentimento para esse tratamento.

A questão do consentimento é um dos fundamentos para que se defenda, como o faz Júlio Gomes[48], que deve ser considerada uma regulamentação própria em relação ao tratamento de dados pessoais dos trabalhadores, dado que o consentimento do trabalhador subordinado é uma barreira pouco significativa porque fácil de obter[49], dada a força contratual diversa das partes.

Obriga a Directiva, no seu art. 10.º e 12.º, que quando uma pessoa seja objecto de tratamento de dados deve-lhe ser fornecido pelo responsável pelo tratamento a identidade do responsável pelo tratamento; finalidades do tratamento a que os dados se destinam; e outras informações necessárias para garantir um tratamento leal dos dados, tais como os destinatários dos dados, o carácter obrigatório ou facultativo da resposta, bem como as possíveis consequências se não responder, a existência do direito de acesso aos dados que lhe digam respeito e o direito de os rectificar.

O responsável pelo tratamento dos dados deve pôr em prática medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição acidental ou ilícita, a perda acidental, a alteração, a difusão ou acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito. O nível de segurança deve ser adequado em relação aos riscos que o tratamento apresenta e à natureza dos dados a proteger e a realização de operações de tratamento em subcontratação deve ser regida por um contrato ou acto jurídico que vincule o subcontratante ao responsável pelo tratamento e que estipule, designadamente, que: o subcontratante apenas actuará mediante instruções do responsável pelo tratamento; as obrigações para protecção dos dados pessoais incumbem igualmente ao subcontratante.

Nos termos do art. 23.º da Directiva,"qualquer pessoa que tiver sofrido um prejuízo devido ao tratamento ilícito de dados ou a qualquer outro acto incompatível com as disposições nacionais de execução da presente directiva tem o direito de obter do responsável pelo tratamento a reparação pelo prejuízo sofrido".

Esta Directiva foi transposta pelas leis de protecção de dados pessoais dos Estados-membros da União Europeia. Para a ordem jurídica portuguesa foi transposta através da Lei de Protecção de Dados Pessoais, a Lei n.º 67/98, de 26 de Outubro.

---

[48] JÚLIO MANUEL VIEIRA GOMES, *Direito do Trabalho,* Coimbra Editora, Coimbra, 2007, pp. 354-356

[49] VINCENZO FERRANTE, *La privacy del lavoratore: brevi considerazioni alla luce delle fonti internazionali e della normativa comparata,* in La Tutela della privacy del Lavoratore, Quaderni di Diritto del Lavoro e delle Realzioni Industriali 24, UTET, Torino, 2000, págs 279 e ss Apud JÚLIO MANUEL VIEIRA GOMES, *Direito do Trabalho* …., p. 355, nota 948. Este autor chama também a atenção para o facto de o prejuízo para a pessoa do trabalhador em matéria de dados sensíveis derivar, desde logo, da sua simples revelação. O mais importante para o trabalhador nestes casos não é tanto controlar a circulação da informação mas sim fazer com que essa informação nunca chegue ao empregador.

Direito Comparado

Direito alemão

Constituição Alemã

Não há um explícito direito à privacidade na Constituição Alemã embora um genérico *direito de personalidade* tenha sido identificado pelo Tribunal Constitucional com base na interpretação combinada do Artigo 1, parágrafo 1 (protecção da dignidade humana contra o poder do Estado) com o Artigo 2, parágrafo 1 (direito ao livre desenvolvimento da personalidade) da Lei Fundamental Alemã. A interpretação que é feita dos princípios constantes destes dois artigos tem fundamentado a proibição de quaisquer formas de controlo do trabalhador contrárias à sua dignidade. Em tal proibição são abrangidos os usos de aparelhos ópticos de vigilância dos trabalhadores[50] e as escutas telefónicas[51].

Directa ou indirectamente aplicáveis, os direitos fundamentais dos trabalhadores têm por limites "interesses legítimos do empregador" ou "necessidades prementes da empresa", ligadas às funções em concreto exercidas pelo trabalhador e/ou motivos de segurança[52].

Em 1969, o Tribunal Constitucional sublinhou que a Lei Fundamental protege "uma esfera intocável da vida privada que escapa à influência do poder do Estado"[53] e em 1983 reconheceu o direito à autodeterminação informacional[54] como um direito fundamental e que garante ao indivíduo o direito a decidir a que informação pessoal sobre ele podem aceder e o usos que lhe podem dar.

Lei Federal de Protecção dos Dados Pessoais

O *Bundesdatenshutzgesetz (BDSG),* Lei Federal de Protecção dos Dados Pessoais, de 20 de Dezembro de 1990, cuja actualização mais recente é datada de 5 de Fevereiro de 2009, implementa a Directiva 95/46/CE relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação

[50] Cfr. Decisões do BAG referidas em JOÃO JOSÉ ABRANTES, *Contrato de trabalho e direitos fundamentais…*, p. 152 nota 296

[51] Cfr. Decisões do BAG referidas em JOÃO JOSÉ ABRANTES, *Contrato de trabalho e direitos fundamentais…*, p. 152 nota 297

[52] JOÃO JOSÉ ABRANTES, *Contrato de trabalho e direitos fundamentais…,* pp. 148-153

[53]*Entscheidungen des Bundesverfassungsgericht (BVerfGE)* (Decisões do Tribunal Constitucional Alemão), Decisão de 16 de Julho de 1969, citada na nota 3, p. 174 do Workers' privacy: Part II: Monitoring and surveillance in the workplace (1993), *Conditions of Work Digest*, Vol. 12.

[54] Verfassungsrechtliche Überprüfung des Volkszählungsgesetzes 1983, BVerfGE Urteil I Bv R 209/83, Julgamento de 15 Dezembro 1983, citado num livro da OIT, "Workers' privacy: Part II: Monitoring and surveillance in the workplace", *Conditions of Work Digest*, Vol. 12, No. 1, 1993, na nota 4, p. 174

desses dados e contribuiu para integrar os princípios da protecção de dados no seio das relações laborais[55].

Direito Laboral

A Bertriebsverfassungsgesetz (BetrVG), promulgada a 25 de Setembro de 2001, estabelece na sua Secção 87 (6) que a comissão de trabalhadores, quando não houver legislação específica ou convenção colectiva que abranja essas situações, tem o direito de co-decisão na introdução na empresa de aparelhos tecnológicos concebidos para monitorizar o comportamento ou o desempenho dos trabalhadores. O Tribunal Federal do Trabalho decidiu[56] que a expressão "concebido para" da Secção 87 (6) deve ser entendida como "adequada a" monitorizar o comportamento e desempenho dos trabalhadores, ou seja, mesmo que a intenção do empregador não seja a de monitorizar, se esses aparelhos são adequados a tal, então, deve ser chamada a comissão de trabalhadores a participar nessa decisão.

Direito Penal

O Código Penal Alemão também proíbe a escuta, gravação ou transmissão de discursos não-públicos na sua Secção 201, parágrafos 1, 2 e 3 pelo que o uso de microfones escondidos pelos empregadores para monitorizar as conversas dos trabalhadores constitui uma violação dos seus direitos de personalidade e está sujeito a procedimento criminal.

Direito espanhol

A Constituição espanhola

Nos termos do art.º 18 n.º 1 da Constituição espanhola: "Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen." E o art. 18.º, n.º 3

[55] Para exemplos da aplicação do BDSG à relação laboral ver a decisão de 17 de Março de 1987 do Tribunal do Trabalho Federal que decidiu que a Lei Federal de Protecção de Dados Pessoais deve ser considerada como uma lei que beneficia os trabalhadores pelo que, como de acordo com o disposto na Secção80(1)(2) do *Bundesgesetzblatt* a comissão de trabalhadores tem o dever de emitir recomendações sobre tudo o que possa beneficiar o estabelecimento e os trabalhadores, a entidade empregadora é obrigada a informar a comissão de trabalhadores sobre todas as formas de processamento dos dados pessoais dos trabalhadores. O empregador não fica liberto deste dever mesmo que os dados não sejam processados na empresa mas numa outra empresa que faça parte desse grupo de empresas.
Também a decisão de 22 Outubro de 1986 do mesmo Tribunal decidiu que os registos dos dados pessoais legalmente recolhidos são permitidos no seio das relações laborais dentro dos limites do direito consitucional à auto-determinação informacional.
Ambas as decisões judiciais são citadas pela OIT no "Workers' privacy: Part II: Monitoring and surveillance…" , p. 181

[56] BAGE, decisão de 9 de Setembro de 1975, 1 ABR 20/74, citada pela OIT no Workers' privacy: Part II: Monitoring and surveillance…", p. 180

garante o segredo das comunicações: "Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial." Adicionalmente, no art. 18.º, n.º 4 é consagrado o direito à intimidade informática: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

Lei de Protecção dos Dados Pessoais

A Lei Orgânica 15/99, de 13 de Dezembro é a Lei de Protecção de Dados Pessoais, que se destina a cumprir a Directiva 95/46/CE, e é regulamentada pelo Decreto Real 1720/2007, de 21 de Dezembro. Em ambas as leis não encontramos uma referencia à videovigilância nem a outras formas de monitorização no local de trabalho mas é óbvio que os seus princípios se aplicam a estas situações porquanto esta lei é "de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado", como refere o art 2.º, n.º 1 da Lei Orgânica. No que toca à videovigilância, a Agencia Española de Protección de Datos veio, em 2001, responder afirmativamente a esta questão no seu *informe jurídico* sobre a "Videovigilância no local de trabalho[57]".

Direito Laboral

O ordenamento jurídico espanhol caracteriza-se por uma ausência de regras especiais aplicáveis ao poder de controlo da entidade empregadora mas existe, não obstante, uma previsão de carácter geral, o art. 20.3 do Estatuto de los Trabajadores (ET) que autoriza o empresário a "adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso." José Luís Goñi Sein critica este artigo por exibir um grande "raquitismo jurídico" [58] na medida em que provoca uma grande insegurança jurídica porquanto deixa totalmente na mão dos empresários a decisão de adopção dos sistemas de controlo audiovisuais sendo que o único limite é o respeito da dignidade humana, conceito com um grande grau de indeterminação e que por isso não é garantia suficiente para evitar arbitrariedades.

Nos termos do art. 64.º , n.º 5, f) ET, a comissão de trabalhadores deve sempre ser informada e emitir parecer sobre a implantação ou alteração de sistemas de organização de controlo do trabalho, estudos de tempos e estabelecimento de sistemas de prémios ou incentivos e avaliação dos postos de trabalho.

---

[57] Disponível in https://www.agpd.es/portalweb/canaldocumentacion/informes_juridicos/videovigilancia/common/pdfs/2001-0000_Videovigilancia-en-el-lugar-de-trabajo.pdf [Consult. 28 Junho 2009]

[58] JOSÉ LUÍS GOÑI SEIN, *La videovigilancia empresarial y la protección…*, p. 21

Direito Penal

Nos termos da Secção 497 do Código Penal, quem interceptar comunicações telefónicas, escutar, gravar, transmitir ou utilizar aparelhos de reprodução de som para descobrir os segredos privados de outrém sem o seu consentimento, é susceptivel de procedimento criminal.

Direito Francês

A Constituição

Não há nenhum direito à privacidade mencionado explicitamente na Constituição. Um direito geral à privacidade é mencionado no art. 9.º do Código Civil: "Chacun a droit au respect de sa vie privée".

Lei de Protecção dos Dados Pessoais

A Lei de 6 de Janeiro de 1978, designada como a Lei relativa à informática, aos ficheiros e às liberdades, foi modificada a 6 de Agosto de 2004, para dar cumprimento à Directiva 95/46/CE sendo que a última modificação desta lei foi a 12 de Maio de 2009.

O incumprimento desta Lei de Protecção dos Dados Pessoais está sujeito a pesadas coimas bem como, em muitos casos, a procedimento criminal com penas que podem ir até aos 5 anos de prisão[59].

De destacar também o intensivo labor da Commission National de L'Informatique et dês Libertés (CNIL) neste campo, nomeadamente ao nível da aplicação da Lei de 6 de Janeiro de 1978 no âmbito das relações laborais tendo já produzido importantes deliberações ao nível da geolocalização[60], controlo dos telefonemas feitos pelos trabalhadores[61] e sobre a cibervigilância no local de trabalho[62].

A não comunicação à CNIL da introdução de meios de vigilância à distância no local de trabalho invalida que a entidade empregadora possa despedir o trabalhador com justa causa com base no facto de este se recusar a ser controlado por esses meios[63].

---

[59] Vide nossas pp. 24-25

[60] Deliberação n.º 2006-066 de 16 de Março de 2006 que produz uma recomendação relativa a dispositivos destinados a geolocalizar os veículos automóveis utilizados por empregados de organismos públicos ou privados

[61] Deliberação n.º 84-031de 18 de Setembro de 1984que produz uma recomendação relativa ao uso de autocomutadores telefónicos nos locais de trabalho

[62] HUBERT BOUCHET, "La cybersurveillance sur le lieu…", op. cit.

[63] Esta é a posição seguida pelos tribunais desde a Decisão de 6 de Abril de 2004 da Cour de Cassation, caso *Honeywell Longlaville c/ Miguel X: "*Il résulte de la combinaison des articles 16, 27 et 34 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, 226-16 du Code pénal, L. 121-8 et L. 432-2-1 du Code du travail, qu'à défaut de déclaration à la Commission nationale de l'informatique et des libertés d'un traitement automatisé d'informations nominatives concernant un salarié, son refus de déférer à une exigence de son employeur impliquant la mise en oeuvre d'un tel traitement ne peut lui être reproche". Texto integral da Decisão disponível in http://www.foruminternet.org/specialistes/veille-juridique/jurisprudence/cour-de-cassation-chambre-sociale-6-avril-2004.html [Consult. 28 Junho 2009]

Direito Laboral

Apesar de o Código do Trabalho francês ter sido modificado em 2008, mantiveram-se em vigor os princípios que devem presidir à utilização dos meios de vigilância à distância no local de trabalho, embora com numeração diferente.

O princípio da lealdade, emanação do princípio da boa fé na execução do contrato (art. L 1222-1), obriga a que o trabalhador seja expressa e previamente informado dos métodos e técnicas de avaliação profissionais (art. L1222-3) e a que nenhuma informação que diga respeito pessoalmente ao trabalhador possa ser recolhida por um dispositivo que não seja levado previamente ao seu conhecimento (art. L1222-4).

O princípio da proporcionalidade obriga, por sua vez, a que não possam ser impostas quaisquer limitações aos direitos e liberdades fundamentais que não sejam justificadas pela natureza das funções exercidas pelo trabalhador ou proporcionadas à finalidade que se pretende alcançar (art. L 1121.1), regra que é retomada no que respeita ao conteúdo do regulamento interno (art. L 1321-3, 2.º). Os métodos e técnicas de avaliação devem ser pertinentes face às finalidades prosseguidas (art. L1222-3).

Relativamente aos direitos colectivos, o *comité d'entreprise* tem de ser informado e consultado previamente à decisão de instalação na empresa de novas tecnologias que permitam um controlo da actividade dos trabalhadores (Art. L2323-13).

Direito Penal

Nos termos do 226-1 do Código Penal francês, é punido com pena até um ano de prisão e pena de multa até 45000 euros todo aquele que atentar contra a intimidade da vida privada de outrem ao captar, gravar ou transmitir, sem o consentimento do próprio, conversas privadas ou confidenciais bem como ao gravar ou transmitir imagens de outrem num local privado sem o seu consentimento.

O segredo da correspondência, escrita ou electrónica, também é tutelado pelo art. 226-15 e inclui a punição pela instalação de aparelhos destinados a interceptar as comunicações.

Desde 2004 que o Código Penal francês tem uma secção própria dedicada às violações dos direitos das pessoas resultantes de ficheiros ou de tratamentos informáticos (art. 226-16 a 226-24) e que pune quem proceder a tratamentos de dados pessoais sem observar as formalidades prévias previstas na Lei de Protecção de Dados Pessoais francesa, ainda que por mera negligência. As penas são bastante pesadas e vão até aos 3000 0000 euros de multa e 5 anos de prisão.

De destacar, uma inovação introduzida no Código Penal pela Lei n.º 2009-526 de 12 de Maio de 2009 e que possibilita a responsabilização penal das pessoas colectivas que violem os direitos resultantes dos tratamentos de dados pessoais (art.

226-24 do Código Penal) e que aplicam, entre outras sanções, o encerramento do estabelecimento da empresa nos quais foram praticados os factos constitutivos do crime e a divulgação pública da decisão judicial (art. 131-39 4.º e 9.º ex vi art 226-24).

Direito Italiano

A Constituição

A Constituição italiana tem um elenco de direitos especificamente laborais, considerados condição de exercício efectivo dos restantes direitos, comuns a todos os cidadãos, os quais, por seu turno, também são objecto de tutela reforçada[64].

O artigo 2.º indica que a República reconhece e garante os direitos humanos fundamentais dos indivíduos enquanto tal e no seio das organizações em que operam. O artigo 15.º garante a liberdade e o segredo da correspondência e de todas as outras formas de comunicação. O Artigo 32.º estabelece que em caso algum a lei pode violar os limites impostos pelo princípio do respeito pela pessoa humana e o artigo 41, n.º 2 estabelece como limite à iniciativa económica privada a segurança, liberdade e dignidade humana.

Lei de Protecção de Dados Pessoais

A Lei que tutela o tratamento de dados pessoais, e que entrou em vigor em Maio de 2004, é o Decreto Lei n.º 196, de 30 de Junho de 2003, conhecido como "Codice in materia di protezione dei dati personali". Este Código representa a primeira tentativa no mundo de compilar num único documento legislativo as inúmeras disposições relativas à privacidade, incluindo a Lei 675/1996 e outros decretos legislativos, regulamentos e códigos de conduta[65].

Em relação à monitorização à distância, o Código dispõe no seu artigo 114 que se mantêm em vigor as disposições do art. 4.º do Statuto dei Lavoratori, que proíbe a utilização de meios audiovisuais e outros aparelhos que tenham como finalidade o controlo à distância da actividade do trabalhador.

Este Código apela à adopção de Códigos de Conduta e de Práticas Profissionais aplicáveis ao tratamento de dados pessoais, nomeadamente na área da videovigilância (art. 134.º do Código).

---

[64] JOSÉ JOÃO ABRANTES, *Contrato de Trabalho e Direitos Fundamentais,* p. 160

[65] Como se pode ler no site da Comissão de Protecção de Dados italiana in http://www.garanteprivacy.it/garante/navig/jsp/index.jsp?folderpath=Normativa%2FItaliana [Consult. 28 Junho 2009]: "Il Testo unico è ispirato all' introduzione di nuove garanzie per i cittadini, alla razionalizzazione delle norme esistenti e alla semplificazione degli adempimenti e sostituirà la legge "madre" sulla protezione dei dati, la n. 675 del 1996."

Direito Laboral

A Lei 300/70, conhecida como *Statuto dei Lavoratori* estabelece no seu título 1 uma série de normas relativas à liberdade e dignidade do trabalhador, que funcionam como limites ao poder de controlo do empregador.

Desde logo, de acordo com o art. 2.º, o uso de guardas juradas só pode ocorrer "com fins de tutela do património do empregador", pelo que não podem supervisionar a actividade profissional dos trabalhadores por factos que não digam respeito à tutela do património do empregador, e esses guardas não podem aceder aos locais de trabalho durante o período de trabalho, a não ser, excepcionalmente, por exigências específicas atinentes a essas funções. É feita, pois, uma delimitação cuidadosa das competências do pessoal afecto à vigilância.

Com a intenção de proibir o controlo oculto, nos termos do art. 3.º, os nomes e funções específicas do pessoal envolvido na supervisão do trabalho devem ser comunicados aos trabalhadores em causa.

Sobre a matéria dos meios de vigilância à distância no local de trabalho temos especificamente o artigo 4.º que estabelece a proibição da utilização de equipamento audiovisual e outros equipamentos para fins de monitorização remota dos trabalhadores. Apenas é admissível a instalação de meios de vigilância à distância por exigências organizativas e/ou de segurança da empresa mas, resultando desses equipamentos a possibilidade de controlar o desempenho profissional dos trabalhadores, então, deve ser obtido o acordo do representante sindical da empresa (RSA). Na ausência de acordo, o empregador poderá pedir à Inspecção do Trabalho o estabelecimento do regime de utlização de tais equipamentos de vigilância à distância.

O Código Civil Italiano também contém normas relativas ao Direito do Trabalho nomeadamente o art. 2087.º que obriga o empregador a adoptar na empresa todas as medidas que, de acordo com as características da função, experiência e conhecimento técnico, forem necessárias à tutela da integridade física e da personalidade moral do trabalhador.

Direito Penal

Nos termos do artigo 617 e 617-bis do Código Penal, quem fraudulentamente tomar conhecimento de uma conversa ou comunicação, por telefone ou telégrafo, entre outros, ou a interromper, bem como aquele que instalar equipamentos destinados a interceptar uma comunicação ou conversa, são punidos com penas de prisão que podem ir até quatro anos.

O segredo das comunicações escritas ou electrónicas é protegido pelo art 616.

O artigo 623 bis estabelece que as disposições penais relativas às comunicações e conversações telegráficas, telefónicas, informáticas ou telemáticas aplicam-se a qualquer outra transmissão à distância de som, imagem ou outros dados.

Direito inglês

Não existem disposições normativas específicas relativamente à monitorização e vigilância dos trabalhadores.

Nos termos do Trade Union and Labour Relations (Consolidation) Act 1992, os empregadores têm o dever de informar os representantes do sindicato em matéria respeitante à empresa e outras informações que sejam necessárias para o processo negocial, o que poderá incluir a introdução de novas tecnologias (artigo 181).

Dado que as convenções colectivas e os contratos de trabalho individuais não se pronunciaram sobre esta matéria, os tribunais reconheceram as prerrogativas do empregador nesta área. Neste sentido, foi julgado no caso Cresswell[66] que o trabalhador tem o dever de aceitar a introdução de novas tecnologias no trabalho e de se adaptar ao novo trabalho, desde que fornecida a formação adequada. Porém, o direito do empregador introduzir novas tecnologias não é ilimitado e deve ser analisado no contexto particular de um trabalho específico.

A protecção da privacidade do trabalhador é feita sobretudo ao nível da protecção de dados pessoais com a *Data Protection Act de 1998*, que regula o tratamento de dados pessoais. Esta lei estabelece que todos aqueles que lidam com dados pessoais devem obedecer aos seguintes princípios: processamento leal e justo; finalidades determinadas; adequação, necessidade e proporcionalidade; dados correctos e actualizados; manutenção dos dados apenas pelo tempo necessário e processados de acordo com os direitos individuais; segurança dos dados; proibição da transferência de dados pessoais para outros países sem a adequada protecção.

No cumprimento desta lei, o Information Commissioner's Office (ICO) estabeleceu uma série de Códigos de Boas Práticas que pretendem orientar os empregadores no tratamento dos dados pessoais dos trabalhadores, quer para as pequenas empresas[67], quer para as empresas em geral[68], para que adequem as suas práticas aos princípios do *Data Protection Act* e ao art 8.º da CEDH.

A monitorização no trabalho, de acordo com o entendimento do ICO, abrange actividades como: videovigilância, abertura do email do trabalhador, verificação automática dos emails enviados, *Keystroke monitoring*, registo das chamadas telefónicas efectuadas e dos sites visitados. Para poder monitorizar os seus trabalhadores a entidade empregadora deve realizar previamente um *impact assessment*: estabelecer de modo claro as finalidades da monitorização dos empregados e os benefícios que vai trazer; identificar os aspectos negativos dos efeitos da monitorização; verificar se

---

[66] *Cresswell* v. *Inland Revenue* [1984] IRLR 190, Ch.D. citada no livro da OIT "Workers' privacy: Part II: Monitoring and surveillance…", p. 267

[67] *Quick Guide to the Employment Practices Code: Ideal for the Small Business* in http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/quick_guide_to_employment_practices_code.pdf [Consult. 28 Junho 2009]

[68] *The Employment Practices Code* in http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/employment_practices_code001.pdf [Consult. 28 Junho 2009]

existem meios de monitorização alternativos menos intrusivos; ter em conta as obrigações que advêm da monitorização (notificação dos trabalhadores e manutenção dos dados recolhidos em local seguro e com acesso restrito) e decidir se a monitorização é justificada. Salvo em casos de suspeita de actividades criminais graves, os empregadores devem tomar medidas para que os seus empregados saibam que estão a ser monitorizados e o que está a ser monitorizado. O consentimento individual dos empregados à monitorização pode ser dispensado se o empregador levar a cabo um adequado *impact assessment.*

Direito norte-americano

O fundamento constitucional do segredo da vida privada dos cidadãos perante o governo federal encontra-se na 4.ª Emenda[69] e perante os governos locais na invocação da 14.ª Emenda. Porém, embora a Constituição possa ser invocável pelos trabalhadores em empregos públicos, não protege os cidadãos perante empregadores do sector privado.

Muitos Estados norte-americanos têm previsões constitucionais semelhantes à 4.ª Emenda e, inclusivamente, pelo menos dez Estados garantem explicitamente nas suas Constituições o direito dos seus cidadãos à privacidade[70]. Porém, até ao momento, apenas os tribunais da California declararam expressamente que o direito constitucional à privacidade pode ser invocado perante entidades não-governamentais, incluindo empregadores e, mesmo neste caso, é necessário que o trabalhador demonstre claramente que o empregador poderia ter usado um meio menos instrusivo da privacidade[71].

A única lei federal potencialmente aplicável é a *Electronic Communications Privacy Act,* de 1986 (ECPA) que proíbe a intercepção, acesso, divulgação ou uso intencional das comunicações por fio, orais ou electrónicas. Na prática, devido à existência de três excepções que legitimam a intercepção de comunicações alheias, esta lei tem uma aplicação muito reduzida nas relações laborais. Trata-se da excepção do consentimento (§ 2511, (2) (d) e § 2702 (b) (3) da ECPA), sendo que os tribunais admitem o consentimento tácito quando o empregador divulga a sua política de

[69] A Quarta Emenda estabelece: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

[70] LARRY O. NATT GANTT, "An affront to human dignity: electronic mail monitoring in the private sector workplace" in *Harvard Journal of Law and Technology*, vol 8, number 2, spring 1995, pp. 389-390, notas 285 a 287.

[71] Ver 1994 California Supreme Court case of *Hill v. National Collegiate Athletic Ass'n* citado em LARRY O. NATT GANTT, "An affront to human dignity…". pp. 390-392. A este respeito e referindo-se particularmente à monitorização do email do trabalhador, este autor refere que esta oportunidade de prova dada ao trabalhador é meramente especulativa dado que o empregador pode facilmente provar que apenas a monitorização do e-mail pode servir os seus interesses.

monitorização[72]. Existe também a excepção do fornecedor de serviço (§ 2511 (2) (a) (I), § 2701 (c) (1) e § 2702 (b) da ECPA), que possibilita que o fornecedor do serviço de comunicações por fio ou electrónicas possa interceptar essas comunicações, ou seja, o empregador que fornece o correio electrónico ao trabalhador pode aceder livremente a este. Por último, a excepção que permite ao empregador efectuar escutas e intercepções de emails e telefonemas dos trabalhadores para assegurar o normal funcionamento da empresa ou para proteger os seus direitos de propriedade (§ 2510 (4) e § 2510 (5) (a) da ECPA).

Deste modo, a monitorização por parte de empresas privadas em relação aos seus trabalhadores não só é possível, como é realizada amplamente. Um estudo de 2007 conduzido pela American Management Association[73] (AMA) revelou que os meios de controlo dos trabalhadores vão desde a monitorização do email, bloqueio de websites, escutas telefónicas, localizadores GPS.

Um trabalhador do sector privado que pretenda defender-se de uma intromissão na sua vida privada tem de demonstrar que o local de trabalho é um lugar suficientemente privado e que a actuação empresarial traduziu um ingerência excessiva no âmbito privado pelo que é muito difícil obter decisões dos Tribunais favoráveis ao trabalhador neste campo[74].

Como refere Larry O. Natt Gantt[75] para que a legislação norte-americana proteja verdadeiramente a privacidade dos trabalhadores, as soluções legislativas devem abandonar as exigências de subordinação dos direitos de privacidade dos trabalhadores aos interesses dos seus empregadores e voltar às noções tradicionais de privacidade, como um direito legal independente criado para proteger a dignidade humana e o respeito pelos indíviduos.

[72] LARRY O. NATT GANTT, "An affront to human dignity: …", pp. 356-358
[73] Estudo disponível em http://www.amanet.org/ e que consistiu num inquérito feito a 304 companhias norte-americanas das quais: 27% representam companhias que empregam menos de 100 trabalhadores, 101–500 trabalhadores (27%), 501–1,000 (12%), 1,001–2,500 (12%), 2,501–5,000 (10%) e 5,001 ou mais (12%). Mais de um quarto dos empregadores despediram trabalhadores com base no uso indevido do e-mail e um terço dos empregadores despediram trabalhadores com base no uso abusivo da internet. Das 43% de empresas que monitorizavam o uso do email, 40% tinham uma pessoa encarregada especificamente de ler e monitorizar o conteúdo dos emails. O estudo concluiu que apenas dois Estados, Delaware e Connecticut, exigiam que os empregadores notificassem os empregados da monitorização do e-mail. 7% usavam a videovigilância unicamente para controlar o desempenho profissional dos trabalhadores e 45% monitorizavam o tempo gasto em telefonemas e 16% gravavam as conversas telefónicas.
[74] TERESA MOREIRA, "Da esfera privada….", p. 257
[75] LARRY O. NATT GANTT, "An affront to human dignity…", p.350

Direito nacional

A Constituição da República Portuguesa

A Constituição da República Portuguesa estabelece desde logo no art. 26.º, n.º 1 que : "A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à protecção legal contra quaisquer formas de discriminação". Para o efeito, preceitua o n.º 2 do mesmo artigo que: "A lei estabelecerá garantias efectivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias".

Outras normas importantes em sede de protecção da intimidade da vida privada do trabalhador são o art. 34.º, n.º 1, que prevê a inviolabilidade do sigilo da correspondência e dos outros meios de comunicação privada, e o art. 32.º, n.º 8, que estabelece a nulidade de todas as provas obtidas mediante ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, na correspondência ou nas telecomunicações.

No tocante ao direito à autodeterminação informacional e protecção de dados pessoais, estabelece o art. 35.º, n.º 3 que: "A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis", e nos termos do n.º 7 do mesmo artigo "Os dados pessoais constantes de ficheiros manuais gozam de protecção idêntica".

Código Civil

Os direitos de personalidade são tutelados pelo Código Civil e são direitos gerais (comuns a todos os seres humanos), oponíveis *erga omnes* e pessoais (insusceptíveis de avaliação pecuniária e intransmissíveis por vida e por morte). Estes direitos não estão na disponibilidade do seu titular, no sentido de que este não pode renunciar a eles, sem prejuízo do consentimento do lesado, desde que este não seja contrário aos princípios de ordem pública, e pode ser revogável a todo o tempo (art. 81.º CC).

O Código Civil, após enunciar o princípio da tutela geral da personalidade (artigo 70.º, n.º 1), prevê um conjunto exemplificativo de direitos de personalidade, entre os quais constam o direito ao nome (artigo 72.º), o direito à confidencialidade das cartas-missivas (artigo 75.º), o direito à imagem (artigo 79.º) e o direito à reserva sobre a intimidade da vida privada (artigo 80.º).

O direito à reserva da intimidade da vida privada é um direito especial de personalidade que não se confunde com o direito à imagem e à honra[76].

Código Penal

A devassa da vida privada das pessoas, realizada através da intercepção, gravação, registo, utilização de conversa, comunicação telefónica, mensagens de correio electrónico ou facturação detalhada, bem como a captação, fotografia, filmagem, registo ou divulgação da imagem das pessoas é punida com pena de prisão até um ano ou com pena de multa até 240 dias (art. 192.º do Código Penal).

Do mesmo modo quem criar, mantiver ou utilizar ficheiro automatizado de dados individualmente identificáveis e referentes a convicções políticas, religiosas ou filosóficas, à filiação partidária ou sindical, à vida privada, ou a origem étnica, é punido com pena de prisão até dois anos ou com pena de multa até 240 dias (art. 193.º do Código Penal)[77].

A violação de correspondência ou telecomunicações, quer tomando conhecimento destas sem o consentimento do destinatário, quer impedindo as comunicações ou intrometendo-se nelas, também são puniveis nos termos do art. 194.º do Código Penal.

Salvo no caso do artigo 193.º, o procedimento criminal por estes crimes depende de queixa ou de participação (art. 198.º Código Penal).

---

[76] Como refere TERESA MOREIRA, *Da esfera privada…,* p. 144, o direito à imagem tem como principal característica fazer referência ao que é puramente externo, enquanto o direito à reserva sobre a intimidade da vida privada tenta impedir que sejam revelados aspectos intrínsecos à própria esfera pessoal e familiar e pode ser agredido sem que seja violado o direito à imagem do mesmo modo que o direito à imagem pode ser violado fora da vida privada.

[77] A propósito do art. 192.º, n.º 1 do C. Penal, respeitante à devassa da vida privada, e do art. 193.º, respeitante à devassa por meio de informática, leia-se a decisão do Acordão do Tribunal da Relação do Porto de 31 de Maio de 2006 que decidiu que *" O patrão que no local de trabalho dos seus empregados instala um sistema electrónico que permite saber as vezes que cada empregado se desloca à casa de banho, as horas a que o faz e o tempo que aí demora não preenche o elemento objectivo do crime de devassa por meio de informática."* Isto porque*: "uma coisa é a incidência da tutela constitucional da reserva da vida, outra é a juscivilista, uma outra é a tutela administrativa ou a laboral e uma outra ainda é a tutela penal, que <u>são diversos modos de protecção da vida privada, cada um com um enfoque e âmbito distintos</u> (…) <u>a referência a vida privada existente no tipo legal de crime do art. 193.º, pretende-se apenas abranger "o núcleo duro da vida privada" e mais sensível de cada pessoa, como seja a intimidade, a sexualidade, a saúde, a vida particular e familiar mais restrita, que se pretende reservada e fora do conhecimento dos demais</u>. Ora e muito embora não tenhamos dúvidas que <u>a deslocação de uma pessoa ao quarto de banho, no seu local de trabalho, seja um acontecimento da sua vida privada, em sentido amplo, já não o é em sentido restrito</u>.(…) Com isto não se pretende dizer que seja lícito, para efeitos de tutela decorrente da Lei de Protecção de Dados – mas isso não está aqui em causa –, o registo informático do número de vezes e o lapso de tempo que uma certa pessoa, enquanto trabalhador de uma empresa, se desloca ao quarto de banho, ou que os mesmos não se possam opor a esse registo.*
O que se sustenta é que esse registo informático, não encontra tutela, pelas razões expostas, na tipificação expressa no art. 193.º do C. Penal."

Lei de Protecção de Dados Pessoais: Lei n.º 67/98, de 26 de Outubro

Esta é a lei que transpõe para a ordem jurídica portuguesa a Directiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais[78] e à livre circulação desses dados.

Esta lei é relevante para a matéria ora abordada dado o seu âmbito de aplicação: a LPDP aplica-se a uma entidade empregadora quando esta proceda ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros manuais ou a estes destinados, bem como quando esta recorra à videovigilância e outras formas de captação, tratamento e difusão de sons e imagens que permitam identificar pessoas (art. 4.º, n.º 1 e n.º 4 da Lei 67/98).

No tratamento de dados pessoais dos trabalhadores a entidade empregadora deve obedecer aos princípios estabelecidos no art. 5.º da LPDP: o princípio da legalidade e da boa fé no seu tratamento; o princípio da finalidade, isto é, estes devem ser recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser posteriormente tratados de forma incompatível com essas finalidades; o princípio da adequação, pertinência e proporcionalidade relativamente às finalidades para que são recolhidos e posteriormente tratados; o princípio da veracidade, isto é, os dados devem ser exactos e actualizados e apagados ou rectificados os inexactos ou incompletos e, por último, devem ser conservados de forma a permitir a identificação dos seus titulares apenas durante o período necessário para a prossecução das finalidades da recolha ou do tratamento posterior.

A LPDP no seu art. 6.º condiciona o tratamento de dados ao consentimento do titular dos dados ou se o tratamento for necessário para: "a) execução de contrato ou contratos em que o titular dos dados seja parte ou de diligências prévias à formação do contrato ou declaração da vontade negocial efectuadas a seu pedido; *b*) Cumprimento de obrigação legal a que o responsável pelo tratamento esteja sujeito; (…) *e*) Prossecução de interesses legítimos do responsável pelo tratamento ou de terceiro a quem os dados sejam comunicados, desde que não devam prevalecer os interesses ou os direitos, liberdades e garantias do titular dos dados".

[78] Ao abrigo da LPDP entendem-se como «Dados pessoais»: "qualquer informação, de qualquer natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável, sendo que é considerada identificável a pessoa que possa ser identificada directa ou indirectamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social." (art. 3.º, al. a) LPDP). A LPDP abrange todo o tratamento de dados pessoais sendo que este é "qualquer operação ou conjunto de operações sobre dados pessoais, efectuadas com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição" (art. 3.º, n.º 1 al. b) da LPDP).

Em nosso entender, a questão do consentimento não deve relevar em sede laboral, isto porque, ou a entidade patronal faz um tratamento de dados pessoais a que está obrigada expressamente por força da lei, nomeadamente para cumprimento das suas obrigações perante a segurança social e a administração fiscal, e o consentimento não é solicitado, ou existe um interesse legítimo no tratamento desses dados, interesse esse que não pode ser substituído pelo mero consentimento do trabalhador. Considerar que o consentimento para a celebração do contrato de trabalho inclui implicitamente o consentimento para a instalação de sistemas de vigilância à distância, e que por isso estaria dispensado por força da alínea a) do art 6.º, significaria aceitar que o poder de controlo da actividade laboral da entidade empregadora é ilimitado, admitir uma vigilância total, violadora da dignidade e da liberdade do trabalhador[79].

No que toca ao tratamento de dados pessoais referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica, bem como o tratamento de dados relativos à saúde e à vida sexual, incluindo os dados genéticos, é exigido o consentimento do titular dos dados sendo que, como refere Catarina Sarmento e Castro[80], dado que estamos perante uma relação subordinada, o consentimento não deveria ser a regra para os tratamentos de dados dos trabalhadores e a Lei deveria ser modificada quanto a esse aspecto.

A actual Lei de Protecção de Dados Pessoais (LPDP), não consagra disposições especiais em matéria de trabalhadores. Encontramos referências marginais no caso do tratamento de dados sensíveis, dado que nos termos do art. 7.º, n.º 1 é proibido o tratamento de dados pessoais referentes a filiação sindical e também encontramos referências no art. 13.º, dado que este artigo proíbe que a capacidade profissional de uma pessoa seja avaliada exclusivamente com base num tratamento automatizado de dados.

É de notar que, como refere Teresa Moreira[81], a LPDP "desconhece a singular posição do trabalhador subordinado e, por extensão, a dimensão colectiva da relação de trabalho" sendo que nada diz relativamente ao dever de informar os representantes dos trabalhadores aos quais não é reconhecido qualquer direito de controlo, seguimento ou informação sobre o funcionamento do tratamento de dados. Esta autora, inclusivamente, sugere que, dado a escassa "albabetização informática" do trabalhador, este deveria poder designar um representante que o assistisse no exercício dos seus direitos ou até que os exercesse em seu lugar sendo que o papel da negociação colectiva deveria ter sido tratado nesta Lei.

Porém, como refere Catarina Sarmento e Castro[82], a Constituição Portuguesa dá às comissões de trabalhadores alguns direitos na área da protecção de dados pessoais dos trabalhadores, dado que a Constituição obriga o empregador a fornecer às

[79] JOSÉ LUÍS GOÑI SEIN, "*La videovigilancia empresarial y la…",* pp. 110-111
[80] CATARINA SARMENTO E CASTRO - "A protecção de dados pessoais…", p.58
[81] TERESA MOREIRA, *"Da esfera privada…",* p. 238
[82] CATARINA SARMENTO E CASTRO - "A protecção de dados pessoais…", pp.57-58

comissões de trabalhadores informações importantes ao acompanhamento e intervenção na vida da empresa (art. 54.º, n.º 1 e n.º 5 al. a) da Constituição), como é o caso da introdução de novas tecnologias de monitorização e vigilância. Por outro lado, essas matérias devem constar de regulamentos internos sendo que estes, por sua vez, estão sujeitos ao parecer prévio da comissão de trabalhadores (art 99.º, n.º 2 da Lei 7/2009, de 12 de Fevereiro).

Código do Trabalho

O controlo da actividade do trabalhador pelo empregador encontra desde logo o seu fundamento na própria definição legal de contrato de trabalho: "é aquele pelo qual uma pessoa singular se obriga, mediante retribuição, a prestar a sua actividade a outra ou outras pessoas, no âmbito de organização e sob a autoridade destas" (Artigo 11.º CT).

É ao empregador que compete o poder de direcção, isto é, "estabelecer os termos em que o trabalho deve ser prestado, dentro dos limites decorrentes do contrato e das normas que o regem" (art. 97.º CT). Ao trabalhador compete cumprir as ordens e instruções do empregador respeitantes a execução ou disciplina do trabalho que não sejam contrárias aos seus direitos ou garantias (art.º 128.º, n.º1, al. e) CT).

O empregador tem o o poder de elaborar o regulamento interno da empresa sobre organização e disciplina do trabalho, regulando o modo como é feito o controlo da actividade do trabalhador e através de que tecnologias (Artigo 99.º, n.º 1 CT).

O dever do trabalhador guardar lealdade ao empregador, nomeadamente não negociando por conta própria ou alheia em concorrência com ele, nem divulgando informações referentes à sua organização, métodos de produção ou negócios (art.º 128.º, n.º1, al. f) CT) ganha maior importância dada a facilidade com que as novas tecnologias, nomeadamente o computador e a internet, permitem que o trabalhador passe informações para o exterior ou exerça actividade por conta própria durante o horário de trabalho. É perfeitamente legítimo que o empregador tome medidas para controlar e prevenir estas situações, dentro dos limites da lei.

O trabalhador deve também velar pela conservação e boa utilização de bens relacionados com o trabalho que lhe forem confiados pelo empregador (art. 128.º, n.º1, al. g) CT), nomeadamente computador, internet, telefone, viatura. O empregador pode controlar o modo como estes instrumentos de trabalho são utilizados e um uso indevido pode ser susceptível de procedimento disciplinar (art. 98.º CT).

Sempre que introduza novos meios de controlo no local de trabalho o empregador deve informar o trabalhador, dado que se trata de um aspecto relevante do contrato de trabalho (art. 106.º CT).

Os meios de vigilância à distância no local de trabalho e os meios de monitorização da actividade do trabalhador devem ser introduzidos ponderando-se até que ponto estes vão introduzir alterações nefastas no ambiente de trabalho, nomeadamente criando situações indutoras de stress e que violam o dever do

empregador de proporcionar boas condições de trabalho, do ponto de vista físico e moral ao trabalhador (art. 127.º, n.º 1 c) do CT).

O "poder conformativo da prestação"[83] da entidade empregadora, que aumentou exponencialmente com os novos desenvolvimentos tecnológicos, deve sempre respeitar a autonomia técnica do trabalhador que exerça actividade cuja regulamentação ou deontologia profissional a exija (art. 127.º, n.º 1 e) CT).

A introdução de dispositivos de vigilância à distância no local de trabalho, ainda que autorizados pela CNPD, pode colocar questões de assédio, no sentido de que podem ser instalados com o o objectivo ou o efeito de perturbar ou constranger a pessoa, afectar a sua dignidade, ou de lhe criar um ambiente intimidativo, hostil, degradante, humilhante ou desestabilizador (art. 29.º, n.º 1 e 4 CT). Basta pensar, a título de exemplo, na colocação de um dispositivo GPS numa única viatura utilizada por um determinado trabalhador, quando a empresa tem várias viaturas que fazem o mesmo tipo de serviço mas que não estão sujeitas a este controlo sendo que, antes da decisão de colocação do dispositivo o trabalhador foi pressionado para aceitar a diminuição da sua retribuição ou para chegar a um despedimento por acordo, e recusou-se.

No exercício dos seus direitos e cumprimento das suas obrigações ambas as partes devem proceder de boa fé e colaborar na obtenção da maior produtividade, bem como na promoção humana, profissional e social do trabalhador (art.º 126.º CT). O dever de proceder de boa fé no exercício dos direitos leva a que defendamos que a entidade empregadora, ainda que proíba a utilização da internet ou do telefone para fins pessoais, deva permitir a sua utilização em situações adequadas socialmente, como seja o trabalhador telefonar para casa a informar que vai ter de ficar a trabalhar até mais tarde ou procurar na internet um telefone de um médico para um filho que adoeceu repentinamente.

Regulamentação laboral específica relativamente aos direitos de personalidade do trabalhador e, em especial, quanto aos meios de vigilância à distância:

O Código do Trabalho, depois de definir contrato de trabalho e antes de entrar na regulação do poder de direcção e dos poderes e deveres da entidade empregadora e do trabalhador, regula os direitos de personalidade (Subsecção II), a igualdade e não discriminação (Subsecção III), a parentalidade (Subsecção IV) e só na Subsecção IX é que passa para "O trabalhador e a empresa" começando logo, à cabeça, com a referência ao poder de direcção. Esta sistemática, quanto a nós, valoriza o homem, o cidadão, antes do trabalhador e do seu dever de subordinação jurídica podendo, e devendo, ser entendida como estabelecida com o intuito de passar uma mensagem de limitação ao poder de direcção do empregador.

Assim, no âmbito dos direitos de personalidade (direitos inerentes ao homem, que existem unicamente porque é homem, e que não derivam da sua condição de

[83] Vd. nossa nota 36

trabalhador, ao contrário do que sucede no caso dos direitos do trabalhador-menor ou do trabalhador-estudante), o Código de Trabalho reconhece a liberdade de expressão e de opinião no âmbito da empresa (Art. 14.º CT), a integridade física e moral do trabalhador e do empregador (Artigo 15.º CT) e a reserva da intimidade da vida privada. Nos termos do art. 16.º do CT, o direito à reserva da intimidade da vida privada abrange quer o acesso, quer a divulgação de aspectos atinentes à esfera íntima e pessoal das partes, nomeadamente relacionados com a vida familiar, afectiva e sexual, com o estado de saúde e com as convicções políticas e religiosas.

No tocante à protecção dos dados pessoais estabelece o Código do Trabalho no seu art. 17.º, n.º 1 al. a) que o empregador não pode exigir ao trabalhador que preste informações relativas à sua vida privada, salvo quando estas sejam estritamente necessárias e relevantes para avaliar da respectiva aptidão no que respeita à execução do contrato de trabalho e seja fornecida por escrito a respectiva fundamentação. Os ficheiros e acessos informáticos utilizados pelo empregador para tratamento de dados pessoais do trabalhador ficam sujeitos à legislação em vigor relativa à protecção de dados pessoais (art 17.º, n.º 4 CT).

O Código do Trabalho trata dos meios de vigilância à distância no seu art. 20.º e estabelece desde logo que o empregador não pode utilizar meios de vigilância à distância no local de trabalho, mediante o emprego de equipamento tecnológico, com a finalidade de controlar o desempenho profissional do trabalhador constituindo contra-ordenação muito grave a violação desse preceito (art. 20.º, n.º 1 e n.º4 do CT).

O legislador permite a utilização destes meios quando a finalidade seja a da protecção e segurança de pessoas e bens ou quando particulares exigências inerentes à natureza da actividade o justifiquem (art. 20.º, n.º 2 CT) mas nesses casos o empregador tem de informar o trabalhador sobre a existência e finalidade dos meios de vigilância utilizados, devendo nomeadamente afixar nos locais sujeitos os seguintes dizeres, consoante os casos: «Este local encontra-se sob vigilância de um circuito fechado de televisão» ou «Este local encontra-se sob vigilância de um circuito fechado de televisão, procedendo-se à gravação de imagem e som», seguido de símbolo identificativo.

O artigo 21.º do Código do Trabalho estabelece que a utilização de meios de vigilância à distância no local de trabalho está sujeita à autorização da Comissão Nacional de Protecção de Dados mas, por força do art 4.º, n.º 4 da LPDP a videovigilância, já estava sujeita à autorização da CNPD. O n.º 2 do art 21.º do CT estabelece que a autorização só pode ser concedida se a utilização dos meios for necessária, adequada e proporcional aos objectivos a atingir, condição que já constava do art.º 5.º, n.º 1 al. c) da LPDP que exige que os dados pessoais devem ser adequados, pertinentes e não excessivos relativamente às finalidaeds para que são recolhidos. O n.º3 do art. 21.º estabelece que os dados pessoais recolhidos através dos meios de vigilância a distância são conservados durante o período necessário para a prossecução das finalidades da utilização a que se destinam, devendo ser destruídos no momento da transferência do trabalhador para outro local de trabalho ou da cessação do contrato de trabalho. A primeira parte do n.º 3 não acrescenta nada ao que já estava estabelecido no

art. 5.º, n.º 1 al. e) da LPDP e, a última parte não se consegue conceber qual a sua utilidade. Se uma autorização da CNPD para ser colocado um meio de vigilância à distância no local de trabalho tem por finalidade a protecção ou a segurança de pessoas e bens porque é que os dados pessoais recolhidos têm de ser destruídos no momento da transferência do trabalhador? Se esses dados têm um prazo de conservação é porque se considera que durante esse período são úteis à prossecução da finalidade, que é a protecção de pessoas e bens, e essa finalidade pode, ou não, cessar com a transferência do trabalhador de local de trabalho ou com o terminus da relação laboral.

O n.º 4 do art. 21.º do CT poderá ser o único número que acrescenta algo à LPDP dado que exige que o pedido de autorização seja acompanhado de parecer da comissão de trabalhadores, e isto sem prejuízo de concordarmos com Catarina Sarmento e Castro[84] quando refere que a obrigatoriedade de submeter a introdução de novas tecnologias de vigilância ao parecer da comissão de trabalhadores já resulta da própria Constituição, e do que entendemos que deve fazer parte do regulamento interno, também ele sujeito a parecer da comissão de trabalhadores (art. 99.º, n.º 2 do CT). O parecer da comissão de trabalhadores poderá alertar para alguma situação concreta que determine os termos em que a autorização vai ser concedida pela CNPD, ou até recusada, e, se repararmos bem, é a única altura em que os trabalhadores têm acesso, através da informação que é enviada à comissão pela entidade empregadora, dos termos em que vão ser instalados os meios de vigilância à distância, prevenindo assim uma oposição "a posteriori" destes, muito mais complicada porque teria de seguir a via judicial.

Após a regulação dos meios de vigilância à distância no local de trabalho, o CT trata da confidencialidade de mensagens e de acesso a informação, sendo estabelecido no art. 22.º que trabalhador goza do direito de reserva e confidencialidade relativamente ao conteúdo das mensagens de natureza pessoal e acesso a informação de carácter não profissional que envie, receba ou consulte, nomeadamente através do correio electrónico, embora isso não prejudique o poder de o empregador estabelecer regras de utilização dos meios de comunicação na empresa, nomeadamente do correio electrónico.

[84] Ver nossa referência nas pp. 33-34

Os meios de vigilância à distância no local de trabalho com recurso a equipamento tecnológico

O que são "meios de vigilância à distância no local de trabalho com recurso a equipamento tecnológico"?

Vamos procurar um critério para delimitar o que são meios de vigilância começando por definir o que é "vigilância". Definir uma coisa é *de+finire*, dar fins, *limites* ao objecto. A definição encontra-se pela oposição ao que lhe é semelhante mas não igual, isto é, vamos procurar características distintivas. Sendo assim, comecemos por distinguir os termos controlar, vigiar e monitorizar.

Controlar é "conferir; verificar; ter sob seu poder; orientar"[85]. Vigiar é o acto de "observar atentamente; espreitar; espiar; examinar; fiscalizar"[86]. Existe ainda um terceiro conceito que é o de monitorizar e que é definido como "controlar, supervisionar, acompanhar e avaliar"[87]. Podemos desde já concluir que vigiar e monitorizar são actividades instrumentais para o exercício do poder de controlo.

A entidade empregadora tem o poder de controlar a actividade do trabalhador e de controlar o que se passa na empresa[88]. Mas será que o poder de controlo da entidade empregadora permite a vigilância e monitorização do trabalhador com recurso a equipamento tecnológico?

Uma incursão pelas obras que tratam da introdução de novas tecnologias no local de trabalho como forma de controlar o trabalhador e vemos que vigilância e monitorização surgem lado a lado. A única distinção que é feita tem a ver com o facto de se designar por monitorização o controlo que é feito da utilização do email e da internet enquanto que se fala em vigilância para a videovigilância. O critério distintivo entre monitorização e vigilância está então no instrumento utilizado para controlar o trabalhador? Seria uma solução fácil mas o facto é que os autores na área do Direito Laboral que se debruçam sobre o tema, as uniões representativas de trabalhadores, a OIT e as próprias Comissões de Protecções de Dados da União Europeia também falam em cibervigilância e monitorização electrónica indiferentemente[89], acabando por

---

[85] Ibid., p. 391
[86] GRANDE DICIONÁRIO DA LÍNGUA PORTUGUESA, Porto Editora, Porto, 2004, p. 1588
[87] Ibid., p. 1043
[88] Ver páginas 10 a 13
[89] Veja-se, a título de exemplo, os próprios títulos das obras sobre este tema: da OIT "Workers' privacy: Part II: Monitoring and surveillance in the workplace…", op. cit.; da UNI "Electronic surveillance and monitoring at work", UNI Global Union Report, in http://www.uniglobalunion.org/Apps/UNIPub.nsf/vwLkpById/3A8CFDE3607D5CC5C125754C004FB7F9/$FILE/E-ELECTRONIC%20MONITORING.PDF [Consult. 28 Junho 2009]; da A.M.A. "2007 Electronic monitoring & Surveillance survey"

analisar as mesmas situações[90], isto é, a monitorização do uso do email e da internet, a videovigilância, as escutas telefónicas (tapping), controlo do uso do telefone e o uso de dispositivos de localização (tracking devices).

Nos países anglo-saxónicos encontramos uma tendência, que é a de considerar monitorização toda a actividade de controlo do trabalhador[91], o que inclui a vigilância por vídeocâmara mas que também passa por actividades tão diversas como registo das chamadas telefónicas nos call centers, examinar se os trabalhadores não fazem o download de conteúdos pornográficos da internet na empresa, ou até obter informação através de agências especializadas para saber se o trabalhador está com dificuldades financeiras. A legislação australiana, no *Workplace Surveillance Act 2005*[92], utiliza unicamente o termo "surveillance" fazendo apelo a uma distinção baseada no meio utilizado para a vigilância: "camera surveillance", "computer surveillance" ou "tracking surveillance". Os dispositivos de escuta, inclusivamente quando associados à videovigilância, são regulados numa lei à parte: o *Surveillance Devices Act 2007.*

Este uso indistinto dos termos monitorizar e vigiar, quando estamos a falar de meios electrónicos que possibilitam o controlo do trabalhador, não é mais do que um reflexo da falta de transparência da legislação nesta matéria, o que pode derivar da necessidade na prática de se aplicarem diferentes princípios e regras à sua utilização[93].

No Direito Laboral português não encontramos qualquer referência à monitorização sendo que os termos em que pode ser efectuada a utilização dos meios de vigilância à distância é limitada pela amplitude do poder de controlo do empregador, dado que este não pode utilizar estes meios para controlar o desempenho profissional do trabalhador (art. 20.º, n.º 1 CT) mas apenas por questões de protecção de pessoas e bens ou quando particulares exigências inerentes à actividade o justifiquem (art. 20.º, n.º 2 CT). Esta limitação ao poder de controlo encontra, por sua vez, justificação no princípio do respeito da reserva da intimidade da vida privada e, sobretudo, no respeito pela dignidade humana.

---

[90] Leia-se no estudo preparado para a Comissão Europeia de FRANK HENDRICKX, "Protection of worker's personal data in the European Union", Julho de 2002, p. 90: "The issue of 'electronic monitoring', which includes forms of surveillance and monitoring such as internet and e-mail monitoring, the use of cameras, recording devices, dataveillance etc.".

[91] Ver a este propósito a parte 3 do "Employment Practices Code" publicado pelo Information Commissioner's Office in http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/coi_html/english/employment_practices_code/part_3-monitoring_at_work_1.html [Consult. 28 Junho 2009]

[92] Disponível in http://www.austlii.edu.au/au/legis/nsw/consol_act/wsa2005245/ [Consult. 28 Junho 2009]. Desde 1998 que existe na Australia um *Workplace Video Surveillance Act* que regula a videovigilância dos trabalhadores. Em 2005 o Governo decidiu estender essas restrições a outros dispositivos através do *Workplace Surveillance Act* sendo que para os dispositivos que gravem conversas privadas ou quando as câmaras também tenham dispositivos de gravação de som incorporados, regula o *Surveillance Devices Act 2007.* A ideia principal a retirar desta legislação é a de que a vigilância tem de ser notificada com 14 dias de antecedência, bem como tem de ser dado conhecimento das respectivas políticas da empresa que lhe estão associadas aos trabalhadores. Porém, políticas de empresa bem delineadas permitem ao empregador fazer tudo o que queira.

[93] FRANK HENDRICKX "Protection of worker's personal...", p. 91

Independentemente da interpretação que se faça do âmbito de aplicação do art. 20.º do CT, ponto discutível e que analisaremos mais à frente, entendemos que são meios de vigilância à distância no local de trabalho com recurso a equipamento tecnológico os que obedecem cumulativamente aos seguintes critérios:

- observação executada com recurso a equipamento tecnológico, o que exclui, por exemplo, a situação dos vidros fumados, embora não coloquemos de parte a possibilidade de o art. 20.º do CT ser aplicado, mas por analogia.

- meios que ofereçam a possibilidade de observação de algum aspecto da vida do trabalhador no local de trabalho. Isto para significar que essa observação não tem de ser da totalidade da vida e nem só da actividade laboral do trabalhador, podendo abranger outros aspectos, ainda que de forma parcial, como é o caso dos lugares por onde o trabalhador se desloca ou o tempo que permanece nestes.

- tenham associado um tratamento de dados pessoais do trabalhador, isto é, quando esses meios tecnológicos forem utilizados em combinação com um sistema de tratamento de dados pessoais, na acepção dada pela LPDP. É este tratamento de dados pessoais que identifica ou torna identificável o trabalhador e que, por isso, torna perigoso o uso destas novas tecnologias, daí a introdução deste critério, para evitar uma atitude ludista na aplicação da lei, o que travaria sem fundamento a competividade das empresas. Deste modo, a videovigilância implica sempre um tratamento de dados pessoais, pelo registo que faz da imagem do trabalhador e que o torna identificável, mas o mesmo não acontece com outros meios tecnológicos de vigilância à distância no local de trabalho.

- meios que, tecnicamente, podem ser utilizados de forma contínua ou oculta. Critério introduzido para distinguir de outros meios tecnológicos em que também existe um tratamento de dados pessoais mas em que o trabalhador tem de ter sempre uma interferência directa no processo de registo dos dados pessoais, como sucede no tradicional "picar do ponto", mas que já não sucederia no caso de o trabalhador ter de usar um identificador por radiofrequência ou um dispositivo de geolocalização para registar a hora em que entra nas instalações da entidade empregadora. Esses dispositivos também podem ser accionados em qualquer altura sem que o trabalhador se aperceba e, em alguns casos, até fora do local e horário de trabalho.

Atendendo aos critérios expostos, a videovigilância, o GPS, a radiofrequência, a monitorização dos conteúdos acedidos e enviados através da internet, bem como as escutas telefónicas integram meios de vigilância à distância no local de trabalho. Se cabem todos, ou não, no âmbito do art. 20.º do CT é outra questão que iremos analisar.

Videovigilância:

Noção de videovigilância

Consiste na colocação de câmaras de gravação de vídeo com ou sem gravação de som que transmitem para um local específico, num conjunto limitado de monitores. Este sistema é designado por CCTV _ closed circuit television_ por oposição às trasnsmissões públicas de televisão. As gravações hoje em dia tendem a utilizar DVR's _ digital video recorder_ que permitem as gravações contínuas e por muitos anos bem como opções adicionais, como detector de movimento e envio por email de alertas. Um ramo em expansão também no CCTV é o das câmaras IP, cujas imagens podem ser consultadas remotamente através da internet ou de uma instalação de rede.

As novas tecnologias, com os meios actuais de consulta remota, tratamento e armazenamento de imagens, possibilitam uma aplicação prática muito abrangente dos dados que resultam da videovigilância[94].

Jurisprudência:

Para a videovigilância ser lícita, nos termos do art. 20.º do CT, a jurisprudência analisa se estão preenchidos os seguintes requisitos:

- **Informação ao trabalhador**: a videovigilância só é admitida em circunstâncias excepcionais mas, quando o seja, ainda assim tem de ser cumprido o dever de informar o trabalhador sendo necessário que sejam afixados nos locais sujeitos a vigilância os dizeres prescritos no n.º 3 do art. 20.º CT (Ac. da Relação de Lisboa de 3 de Maio de 2006, relator Carlos Sousa[95]).

---

[94]Veja-se por exemplo o artigo de JENNIFER ALSEVER, "Monitoring the staff pays off installing online cameras helped one restaurant owner boost profits by 40%", CNNMoney.com (3 Outubro 2008) in http://money.cnn.com/2008/10/03/smallbusiness/surveillance.fsb/index.htm [Consult. 28 Junho 2009], em que se relata a experiência de um gerente de um restaurante norte-americano que instalou um sistema de videovigilância controlado remotamente: "Elmore can log in online, view a receipt, and call up the video of that transaction. He can see whether employees cleaned the restaurant when they said they would. He knows whether they're smiling at customers. And if a customer's order arrives at the table late or if employees are helping themselves to meals, Elmore sees it."

[95] Disponível in http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/c35d3b6d630e466f80257199003ab4f2?OpenDocument&Highlight=0,videovigil%C3%A2ncia [Consult. 28 Junho 2009]. Neste Acordão foi analisada a colocação de uma câmara oculta numa gelataria tendo-se detectado pequenos furtos por parte do trabalhador. A Relação decidiu que a prova era nula porque não foi colocado qualquer aviso sobre a

Este dever de informação é essencial por uma questão de lealdade e boa fé nas relações laborais.

- **Finalidade legítima:** A licitude da videovigilância afere-se pela sua conformidade ao fim que a autorizou (Ac. do Tribunal da Relação de Lisboa de 18 de Maio de 2005[96]).

A videovigilância realizada pela entidade patronal ao abrigo do art.º 20.º CT deve destinar-se à protecção de pessoas e bens ou quando particulares exigências inerentes à natureza da actividade o justifiquem. É o que diz a lei, mas os tribunais apenas analisam e invocam a obrigação de a videovigilância ser instalada com a finalidade de protecção de pessoas e bens, talvez muito pela influência das leis anteriores neste campo, que regulam a videovigilância no âmbito da actividade de segurança privada.

O Acordão do Supremo Tribunal de Justiça, de 8 de Fevereiro de 2006[97], analisou precisamente quando é que se considera existir um interesse legítimo na protecção do património e refere que "o empregador pode utilizar meios de vigilância à distância sempre que tenha por finalidade a protecção e segurança de pessoas e bens, devendo entender-se, contudo, que essa possibilidade se circunscreve a locais abertos ao público ou a espaços de acesso a pessoas estranhas à empresa, em que exista um razoável risco de ocorrência de delitos contra as pessoas ou contra o património. (…) Esses princípios são aplicáveis às forças de segurança por força do que dispõem os artigos 2º, n.º 3, e 5º, n.º 3, alínea e), da Lei n.º 1/2005, de 10 de Janeiro, no âmbito da sua actividade de prevenção da criminalidade, e por maioria de razão deverão constituir condições de legitimidade de tratamento de dados pessoais por parte de simples sujeitos privados.[98]". Ou seja, a protecção dos bens não é um argumento que se aplique sem mais e para a admissibilidade da invocação desta excepção deve ter-se em conta aspectos como o valor dos bens, o facto de estarem facilmente acessíveis a terceiros por estarem em locais abertos ao público e devem tratar-se de infracções particulares graves e não meros pequenos furtos frequentes por parte dos trabalhadores. Como refere José Luís Goñi Sein[99], admitir a finalidade de protecção da propriedade de forma geral e indiscriminada contra os próprios trabalhadores, equivaleria a admitir entre os fins da videovigilância o controle dos trabalhadores. Também apontam nesse sentido o art.º 8.º,

---

gravação e esse dever de informação era exigido quer pela lei que regula os estabelecimentos de restauração e bebidas (D.L.nº 263/01, de 28/9) quer pelo art. 20.º, n.º 3 do CT.

[96] Disponível in http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/a5ddfc629b87571d80257030004ed166?OpenDocument&Highlight=0,videovigil%C3%A2ncia [Consult. 28 Junho 2009].

[97] Disponível in http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/65e859e4729cc7688025712d00421026?OpenDocument&Highlight=0,videovigil%C3%A2ncia [Consult. 28 Junho 2009].

[98] Nesta decisão é ainda referido que: "A entidade empregadora dispõe de mecanismos legais que lhe permitem reagir contra a actuações ilícitas dos seus trabalhadores, podendo não só exercer o poder disciplinar através do procedimento apropriado, efectuando as adequadas averiguações internas, como também participar criminalmente às entidades de investigação competentes, que poderão determinar as diligências instrutórias que se mostrarem convenientes. (…) Por outras palavras, o empregador, ainda que com base num pretenso interesse público de segurança dos medicamentos, não pode sujeitar os seus trabalhadores a uma permanente medida de polícia, transformando-os indefinidamente em suspeitos de prática de ilícitos criminais, com clara violação dos seus direitos de personalidade."

[99] JOSÉ LUÍS GOÑI SEIN, "*La videovigilancia empresarial y la…",* p.113

n.º 2 da CEDH, que apenas admite a ingerência na vida privada quando se trata de uma situação necessária, e o Grupo do Artigo 29, ao defender no seu Documento de Trabalho sobre o Tratamento de Dados Pessoais mediante videovigilância[100], adoptado a 25 de Novembro de 2002, que um organismo público deve evitar instalar câmaras de vídeo por causa de infracções de importância menor.

Quanto à protecção de pessoas, a videovigilância tem muitas vezes a ver com a prevenção de riscos laborais, quer ao nível da saúde do trabalhador, quer ao nível da sua segurança, como seja na prevenção da violência a que estão sujeitas certas profissões, como é o caso dos condutores de autocarros. Nessas situações, o tratamento de imagens e sons, na medida em que captem imagens e sons do trabalhador, deve ser tratado como "um subproduto não desejado"[101], uma consequência meramente acidental necessária à protecção da segurança e saúde desses trabalhadores.

Quando tenham por finalidade controlar o desempenho profissional do trabalhador as gravações são ilícitas, ainda que tenham o consentimento do trabalhador (cfr. decisão do Ac. do Tribunal da Relação de Lisboa, de 19 de Novembro de 2008[102]**,** Ac. do Tribunal da Relação do Porto, de 26 de Junho de 2008[103] e Ac. do STJ de 22 de Maio de 2007[104], Conselheiro Pinto Hespanhol).

- Princípio da proporcionalidade: A instalação de sistemas de vídeovigilância nos locais de trabalho envolve a restrição do direito de reserva da vida privada pelo que apenas poderá mostrar-se justificada quando for necessária à prossecução de interesses legítimos e dentro dos limites definidos pelo princípio da proporcionalidade (cfr. o Ac. do Supremo Tribunal de Justiça, de 8 de Fevereiro de 2006[105]).

Este princípio da proporcionalidade comporta um triplo juízo prévio: a adequação do meio face à finalidade pretendida; a necessidade ou indispensabilidade do recurso à videovigilância; a proporcionalidade dos direitos sacrificados, priveligiando-se o princípio da intromissão mínima.

Viola o princípio da proporcionalidade uma gravação ininterrupta bem como câmaras de vídeo instaladas no local de trabalho e direccionadas para os trabalhadores

---

[100] Disponível in http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp67_pt.pdf [Consult. 28 Junho 2009]

[101] A. GARILLI y A. BELLAVISTA: "Innovaciones tecnológicas y Estatuto de los Trabajadores: los limites a los poderes del empresário entre la tutlela individual y colectiva (artículos 4-9-13)" Apud JOSÉ LUÍS GOÑI SEIN, "*La videovigilancia empresarial y la…",* p. 116

[102] Disponível in http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/ab2bf2d57c99bd0680257514003a6ea2?OpenDocument&Highlight=0,videovigil%C3%A2ncia [Consult. 28 Junho 2009]

[103] Disponível in http://www.dgsi.pt/jtrp.nsf/c3fb530030ea1c61802568d9005cd5bb/97de01e22a0340178025747b0034ded7?OpenDocument&Highlight=0,videovigil%C3%A2ncia [Consult. 28 Junho 2009]

[104] Disponível in http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/1771be8dfd54aa72802572e40034640f?OpenDocument&Highlight=0,videovigil%C3%A2ncia [Consult. 28 Junho 2009]

[105] Nesse caso julgado pelo Supremo, a recorrida tinha colocado nas suas instalações 82 câmaras de videovigilância, sendo que 69 estavam directamente apontadas para os postos de trabalho. O tribunal considerou que os meios de videovigilância de 69 câmaras visionando e registando a actividade laboral dos trabalhadores, são manifestamente desajustados aos fins pretendidos pela recorrida, sendo excessivos.

(cfr. decisão do Acordão do Supremo Tribunal de Justiça de 8 de Fevereiro de 2006). A videovigilância deverá traduzir-se numa forma de vigilância genérica, destinada a detectar factos, situações ou acontecimentos incidentais, e não numa vigilância directamente dirigida aos postos de trabalho ou ao campo de acção dos trabalhadores, que configuraria uma típica medida de polícia.

Não se levanta a questão, em sede judicial, de saber se é proporcional o facto de a gravação vídeo ser feita também com som mas estamos em crer que essa questão é pertinente e dificilmente conseguimos enquadrar a admissibilidade da gravação vídeo com som no local de trabalho sem violar o princípio da proporcionalidade em sentido estrito. A este propósito, encontramos essa distinção no Workplace Surveillance Act[106], que entende por *camera surveillance* apenas quando são gravadas imagens, sem som.

- **Autorização da CNPD:** tem de haver uma autorização prévia e os termos em que essa autorização é emitida devem ser respeitados (cfr. Acordão do Supremo Tribunal de Justiça, de 8 de Fevereiro de 2006[107]).

Tratamento jurisprudencial da videovigilância oculta em sede laboral:

A videovigilância oculta no local de trabalho realizada pelo empregador não é admitida porque viola o artigo 20.º, n.ºs 1 e 3 do CT bem como o dever de lealdade e boa fé nas relações laborais. As provas obtidas nesses termos são consideradas nulas pelos nossos tribunais para efeitos de julgamento por despedimento com justa causa.

O Tribunal da Relação do Porto, no seu Acordão de 26 de Junho de 2008, parece abordar esta problemática quando, ao julgar o caso do despedimento de um trabalhador que foi filmado nas instalações da empresa-cliente da entidade empregadora, sem ter sido informado de que aí era efectuada videovigilância, a carregar 4 bidons de óleo, que depois não declarou nem entregou à sua entidade empregadora, facto pelo qual veio depois a ser despedido, e o tribunal considera que, naquele caso, não tinha lugar à aplicação do art. 20, n.º 1 do CT porque, mesmo considerando que o cais da empresa-cliente era o seu local de trabalho, visto ser esta empresa a única cliente da ré, não resultou demonstrado que os meios de vigilância desta tivessem como finalidade o desempenho profissional do trabalhador. Este Acórdão vai mais longe e refere que "*Em qualquer das situações não ficou demonstrada nos autos a observância dos supra referidos requisitos legais (autorização, informação e comunicação), para a recolha das imagens, o que, não implicará, contudo, para alguns autores a ilicitude dessa medida de controlo. Com efeito, como refere Júlio Gomes, Direito do Trabalho, Coimbra Editora, pág. 325, em caso de vigilância oculta poderão "ser vigiados os locais da empresa, onde, em princípio, não existe qualquer posto de trabalho e onde os trabalhadores só se desloquem esporadicamente", admitindo ainda a videovigilância quando os trabalhadores forem "filmados a cometer infracção disciplinar não nas*

[106] Ver nota 97, pág. 38.

[107] Nesta decisão é referido o facto de a recorrida não ter sido autorizada pelo CNPD, a colocar as câmaras de vídeovigilância a focalizar os postos de trabalho, mas sim nos corredores, áreas administrativas e outros locais de acesso público.

instalações da empresa, mas nas instalações de um cliente, onde estão a executar a prestação laboral". Cita ainda o mesmo autor, Ob e local cit., sem repudiar a respectiva orientação, a decisão Cour de cassation de 19.04.2005, segundo a qual, é legítima a prova resultante do sistema de videovigilância instalado em armazém ou noutros locais em que os trabalhadores não têm normalmente acesso, bem como "quando tais provas resultam de sistemas de vigilância instaladas por clientes (pense-se em trabalhadores que tipicamente realizam a sua actividade em instalações dos clientes)". Porém, a questão da admissibilidade da prova obtida através de videovigilância oculta não é resolvida porquanto o Tribunal considera que, em todo o caso, os outros meios de prova existentes no processo, prova testemunhal e documental, são suficientes para considerar lícito o despedimento do trabalhador com justa causa.

Não encontrámos no panorama nacional uma decisão jurisprudencial que admita a videovigilância oculta no local de trabalho.

Em França, a Cour de Cassation, na sua decisão de 19 de Abril de 2005, considerou que não existe o dever de informar os trabalhadores acerca da videovigilância quando se trate de instalações em que o acesso por estes esteja vedado, nem as entidades empregadoras têm de informar os trabalhadores dos procedimentos de segurança seguidos pelas suas empresas-clientes quando estas coloquem câmaras de vigilância em locais pelos quais os trabalhadores não devam exercer a sua actividade.

Na Alemanha, considera-se que uma avaliação completa da situação é necessária, em cada caso particular. O BAG, numa decisão datada de 7 de Outubro de 1987, analisou um caso em que uma entidade empregadora alegou que eram necessárias câmaras escondidas na loja porque ocorriam furtos. Segundo o Tribunal Federal do Trabalho, não é suficiente para colocar câmaras ocultas invocar a perda de bens isoladamente. A extensão dos furtos deve ser substancial e a utilização de câmaras ocultas a única alternativa para capturar os ladrões. Neste caso, existia uma alternativa: a colocação de câmaras vísiveis seria uma boa medida preventiva.

No que respeita à jurisprudência espanhola, o STC 186/2000 de 10 de Julho pronunciou-se sobre a instalação clandestina de um circuito de televisão para controlar a zona das caixas registadoras devido à existência de suspeitas sobre o comportamento das trabalhadoras e, utilizando o princípio da proporcionalidade como critério base para determinar a legitimidade de qualquer medida restritiva de direitos fundamentais do trabalhador, chega à conclusão de que a medida era ajustada dado que a gravação serviria de prova e a gravação de imagens limitou-se à zona da caixa e com uma duração temporal limitada, apenas a suficiente para provar a conduta ilícita dos trabalhadores.

Admissibilidade da videovigilância como meio de prova em processo laboral:

O facto de a videovigilância ter como finalidade a protecção de pessoas e bens e não a de controlar o desempenho profissional do trabalhador leva a que a videovigilância não possa ser usada em sede de procedimento disciplinar contra o trabalhador. Neste sentido, o Ac. do STJ de 14 de Maio de 2008[108], e o Ac. da Relação de Lisboa de 3 de Maio de 2006[109] (Relatora Desembargadora Isabel Tapadinhas), decidiram que "A videovigilância não só não pode ser utilizada como forma de controlar o exercício da actividade profissional do trabalhador, como não pode, por maioria de razão, ser utilizada como meio de prova em sede de procedimento disciplinar". Os tribunais também alegam que, "nestas circunstâncias, a divulgação da cassete constitui, uma abusiva intromissão na vida privada e a violação do direito à imagem do trabalhador, - arts. 79º do Cód. Civil e 26º da Constituição da República Portuguesa – criminalmente punível – art. 199º, nº 1, alínea b) do Cód. Penal"[110] referindo que "embora o reconhecimento dos direitos de personalidade do trabalhador no âmbito da relação de trabalho só tenha tido consagração expressa no Código do Trabalho, já anteriormente se entendia que os direitos fundamentais consagrados na Constituição da República Portuguesa - Capítulo I, Título II - e previstos no Código Civil - art. 70 e seguintes - tinham aplicação plena e directa aos trabalhadores no âmbito da execução do contrato de trabalho, uma vez que a celebração deste não implica a privação dos direitos que a Constituição reconhece a qualquer cidadão e o trabalhador não deixa de ser um cidadão como qualquer outro".

Existem decisões que admitiram a utilização de gravações vídeo como meios de prova em processo de despedimento de trabalhador, como foi o caso do Ac. do STJ de 9 de Novembro de 1994[111] que decidiu serem "válidas as gravações vídeo feitas pela dona de casino, na sua propriedade em que explora a indústria de jogo de fortuna e azar, com a finalidade de detecção de eventuais anomalias no acesso a máquinas ou fichas de jogo" acrescentando que "nestes casos, a utilização das gravações como meio de prova contra a actuação dos seus trabalhadores não se pode considerar intromissão ou devassamento da vida privada de outrem". O mesmo ocorreu na decisão da Relação do

---

[108] Disponível in http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/bf086a28e6f63b408025744a003016562?OpenDocument&Highlight=0,videovigil%C3%A2ncia [Consult. 28 Junho 2009]

[109] Disponível in http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/2ee49abdddb133948025717f0042790b?OpenDocument&Highlight=0,videovigil%C3%A2ncia [Consult. 28 Junho 2009]

[110] Na doutrina, e também no sentido de que a videovigilância não só não pode ser utilizada como forma de controlar o exercício da actividade profissional do trabalhador, como não pode, por maioria de razão, ser utilizado como meio de prova em sede de procedimento disciplinar vejam-se Guilherme Dray "Justa causa e esfera privada", "Estudos do Instituto de Direito do Trabalho", vol. II, Almedina, 2001, págs. 81 a 86 e Isabel Alexandre "Provas Ilícitas em Processo Civil", Almedina, 1988, págs. 233 e segs.

[111] Disponível in http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/9ab11724aa7d569b802568fc003ad33b?OpenDocument&Highlight=0,casino [Consult. 28 Junho 2009]

Porto, de 20 de Setembro de 1999[112], onde se sustentou que "A lei do jogo não proíbe que as imagens gravadas nas salas de jogo sejam usadas como meios de prova em acção emergente de contrato de trabalho, quando nela se discutam comportamentos imputados ao trabalhador que exercia funções no Bar de uma sala de jogo."

Porém, as decisões jurisprudenciais posteriores vão no sentido de não admitir essas gravações como meio de prova e, inclusivamente, no Ac. do Tribunal da Relação de Lisboa, de 3 de Maio de 2006[113] (relator Carlos Sousa) o desembargador Mário Morgado votou vencido ao defender a licitude das gravações.[114]

Por outro lado, quando as gravações são consideradas ilícitas para efeitos de utilização em processo disciplinar, daí não resulta a nulidade de todo o processo, antes determinando essa ilicitude que a sobredita recolha de imagens não possa ser considerada na indagação da justa causa de despedimento, é o que resulta do Acordão do Supremo Tribunal de Justiça, de 14 de Maio de 2008 com fundamento no facto de a enumeração do art. 430.º, n.º2 do CT, que prevê os motivos de nulidade do procedimento disciplinar, ser taxativa e não abranger a questão da nulidade do meio probatório. Decisão semelhante foi tomada pelo Tribunal da Relação do Porto, no seu Acordão de 26 de Junho de 2008 que considerou que se o julgador formar a sua convicção com autonomia e plena independência da prova ilícita decorrente de imagens de vídeovigilância, essa convicção é válida.

Quanto ao facto de determinado meio de prova poder ser admissível em sede criminal e não o ser em processo disciplinar, o Ac. do Tribunal da Relação de Lisboa de 19 de Novembro de 2008 decidiu que "não colhe a argumentação de que, sendo admissível no âmbito do processo-crime instaurado contra a trabalhadora, a gravação vídeo também poderá ser utilizada no âmbito do processo de trabalho. A previsão do

---

[112] Disponível in http://www.dgsi.pt/jtrp.nsf/c3fb530030ea1c61802568d9005cd5bb/d9e6398ca6d246c18025686b00673119?OpenDocument&Highlight=0,jogo,despedimento [Consult. 28 Junho 2009]

[113] Disponível in http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/c35d3b6d630e466f80257199003ab4f2?OpenDocument&Highlight=0,videovigil%C3%A2ncia [Consult. 28 Junho 2009]

[114]"Vencido, pelas seguintes razões:
As reproduções fotográficas, cinematográficas, fonográficas ou por meio de processo electrónico e, de um modo geral, quaisquer reproduções só valem como prova dos factos ou coisas reproduzidas se não forem ilícitas, nos termos da lei penal – art. 167º, nº 1, CPP.
Afigura-se-nos que a captação de imagens em causa não integra o crime p. e p. pelo art. 199º, nº 2, a), CP: a captação de imagem dirigida a provar factos ilícitos em locais públicos ou no local de trabalho deve considerar-se desprovida de tipicidade (aquele tipo criminal deve sofrer uma redução da área de tutela de sentido vitimodogmático) ou, pelo menos, de ilicitude (com base, segundo as diferentes posições doutrinárias, em "*quase legítima defesa*", *legítima defesa, direito de necessidade, prossecução de interesses legítimos* ou num *critério geral de interesses*) – cfr. sobre esta problemática Costa Andrade, *Comentário Conimbricense ao Código Penal*, I, 834-840, e *Sobre as proibições de prova em processo penal*, 242-272.
Também não se descortina no caso vertente qualquer violação da integridade física ou moral do arguido ou ofensa da sua dignidade/intimidade – como se sabe, nem toda a lesão de um direito de personalidade viola a dignidade humana.
Lisboa, d. s. *Mário Morgado* "

artº 20º do CT é, quanto à captação de imagens por videovigilância, bem explícita na sua proibição, nos termos expostos, e também importa não olvidar que o ilícito criminal e o ilícito disciplinar podem não ter, e bastas vezes não têm, campos de aplicação coincidentes, podendo determinado facto constituir ilícito criminal e não disciplinar, e vice-versa". Quanto ao facto de estarmos perante ilícitos criminais e não perante uma situação de controlo do desempenho do trabalhador, o mesmo acórdão acrescenta que: "não tem qualquer razão a recorrente quando argumenta que, por estar em causa um eventual ilícito criminal, não estamos perante uma hipótese de controlo do desempenho profissional. Este envolve toda a plenitude da prestação de serviço por parte do trabalhador, inclui todos aos actos que, no desenvolvimento da relação laboral, este venha a praticar no local sujeito a vigilância, mesmo que violadores dos seus deveres contratuais".

Quer isto dizer que, em última análise, podemos ter uma sentença condenatória de um arguido e, simultaneamente contra a mesma pessoa e com base na mesma factualidade, uma acção laboral cujo pedido de despedimento com justa causa da entidade empregadora é declarado improcedente em virtude de a única prova existente – a gravação de videovigilância - não ser admissível?

A intenção do legislador ao não permitir que a videovigilância seja usada para controlo do desempenho do trabalhador é a de proteger a dignidade da pessoa humana e a intimidade da vida privada, direitos constitucionalmente protegidos e que não desaparecem quando o cidadão coloca o pé na porta de entrada do local de trabalho, daí que a proibição do art. 20.º CT deva ser plenamente respeitada em sede de inadmissibilidade de prova em processo laboral. Porém, admitimos que em situações graves do foro criminal e em que é impossível para a entidade empregadora manter a relação de confiança que está na base do contrato de trabalho, situações em que é claramente quebrado esse vínculo e em que a única prova, desde que lícita no âmbito penal, é a videovigilância, nessas situações em que há um claro conflito entre vários direitos constitucionais: a liberdade de prova e o direito de acção, por um lado, e a dignidade da pessoa humana, por outro lado, as gravações devem ser admissíveis sob pena de deixar sem efectiva tutela o direito de acção e os direitos fundamentais serem invocados em claro abuso de direito[115]. Repetimos, são situações excepcionais que devem ser valoradas no caso concreto.

No mesmo sentido parece ir a jurisprudência italiana que, regra geral, considera inadmissível o recurso à videovigilância para despedir o trabalhador[116] mas que

[115] SALAZAR CASANOVA, *Provas Ilícitas em Processo Civil, Sobre a admissibilidade e valoração de meios de prova obtidos por particulares",* Março de 2003, publicação da Biblioteca do TRL, p. 53

[116] Ver a Decisão da Cassazzione de 17/7/2000 que entendeu que: "Il ricorso da parte del datore di lavoro a riprese con telecamera a circuito chiuso, finalizzate a controllare a distanza l'attività dei lavoratori, contrasta (nel caso non siano state seguite le garanzie procedurali per la loro installazione per motivi di sicurezza) con l'articolo 4 L. n. 300/70, la cui violazione è penalmente sanzionata dall'articolo 38 stessa legge, che fa parte di quella normativa diretta a contenere in vario modo le manifestazioni del potere organizzativo e direttivo del datore di lavoro che, per le modalità di attuazione incidenti sulla sfera della persona, si ritengono lesive della dignità e riservatezza della persona. Ne consegue, sul piano processuale,

considerou legal o despedimento por justa causa feito por um empregador que utilizou os elementos de prova reunidos pelo Procurador da República durante uma investigação criminal e que tinha colocado algumas câmaras nas casas de banho e nos corredores da empresa, sem respeito pelo art. 4.º do SL[117].

Decisões da CNPD

Na sua Deliberação n.º 61/2004, a CNPD explicita que a instalação de sistemas de videovigilância deve obedecer ao princípio da proporcionalidade face à finalidade da protecção de pessoas e bens. Para verificar se esse juízo de proporcionalidade se verifica terão de estar cumpridas três condições: idoneidade da medida adoptada para conseguir o objectivo proposto (princípio da idoneidade); necessidade da medida, no sentido de que não existia outra medida capaz de assegurar o objectivo com igual grau de eficácia (princípio da necessidade); a medida adoptada deve ser ponderada e equilibrada ao ponto de através dela, serem atingidos substanciais e superiores benefícios ou vantagens para o interesse geral quando confrontados com outros bens ou valores em conflito (juízo de proporcionalidade em sentido estrito).

As decisões da CNPD têm sempre o cuidado de salvaguardar o disposto no art. 20.º CT, assim, por exemplo, a autorização n.º 806/2009, em que foi pedida a colocação de 4 câmaras num café na zona da caixa, balcão e cozinha, foi dada autorização na medida em que as câmaras colocadas na cozinha não captassem as áreas de trabalho dos empregados e apenas poderiam captar imagens dos cofres e alarmes localizados nesses espaços. Todas as autorizações dadas apresentam sempre a ressalva de que as imagens não podem servir para controlo do desempenho profissional dos trabalhadores nem as câmaras incidir regularmente sobre estes durante a actividade laboral.

Os dados não podem ser transmitidos a terceiros e só podem ser utlizados nos termos da lei processual penal. Uma vez detectada a prática da infracção penal, a entidade responsável pelo respectivo tratamento deve _ com a respectiva participação_ enviar ao órgão de polícia criminal ou à autoridade judiciária competente as respectivas imagens.

Quando não haja infracção penal só se admite a visualização das imagens ao titular dos dados que tenham solicitado o "direito de acesso", nos termos do art. 11.º da Lei 67/98.

---

che nessun valore probatorio può attribuirsi ai fotogrammi così illegittimamente conseguiti (anche se nel caso evidenzianti il reato di furto per sottrazione di denaro in cassa)".

[117] Tribunal de Milão 1/2/2008

Os pedidos de autorização para captação de imagens junto da CNPD têm aumentado exponencialmente[118] por se tratar de um meio barato, e isto apesar de a CNPD alertar para o facto de que se trata de uma medida expcepcional e de que não se deve banalizar o recurso à mesma, devendo as pessoas optar por medidas menos intrusivas da privacidade[119].

[118] Ver notícia de CÉU NEVES, "Pedidos de vigilância duplicam em Portugal" publicada no Diário de Notícias a 14 de Setembro de 2005, in http://dn.sapo.pt/2005/09/14/nacional/pedidos_videovigilancia_duplicam_por.html

[119] VII Encontro Ibérico de Autoridades de Protecção de Dados - Óbidos, 2006, p. 2 in *http://www.cnpd.pt/bin/actividade/Outros/VII_Encontro_Iberico.pdf*, [Consult. 28 Junho 2009]

Identificação por Radiofrequência:

Em que consiste

A identificação por radiofrequência (IDRF) é um sistema automático de identificação que possibilita a transmissão de dados recorrendo a marcas/identificadores (*tags*) portáteis para leitores com a capacidade de processar tais dados.

As marcas são *microchips*, de dimensões muito reduzidas, que muitas vezes não ultrapassam o tamanho de um grão de arroz, que se encontram conectados a uma antena e que possuem a capacidade de transmitir informação de identificação – tipicamente, um código único universal. Os sinais enviados/recebidos pelas marcas de radiofrequência (RF) são, assim, univocamente identificáveis.

Os dados transmitidos pelas marcas de radiofrequência (RF) podem incluir informação sobre a identificação ou a localização, bem como outra relativa às características (propriedades) do produto etiquetado. A transmissão da informação pode ser iniciada/interrompida remotamente sem que o portador da marca disso se aperceba. Normalmente apenas estão activos a curta distância mas alguns podem ser lidos a vários quilómetros de distância.

Os desenvolvimentos verificados na tecnologia emergente de identificação por radiofrequência (IDRF), permitindo a crescente generalização e um alargamento dos respectivos domínios de aplicação, são susceptíveis de abranger a identificação de documentos, notas bancárias, animais e até mesmo pessoas[120].

No local de trabalho, os exemplos mais claros desta utilização são a utilização de *badges*, que tanto poderão consistir num cartão que o trabalhador deve utilizar enquanto está no local de trabalho, numa braçadeira que se coloca na farda ou até, estarem incorporados na própria farda. Há já notícias de pessoas que colocaram essas etiquetas no braço[121] e de empresas que exigem aos empregados o implante de um microchip para poderem aceder a determinadas áreas de trabalho[122].

---

[120] SCOTT GRANNEMAN, "RFID chips are here", The Register (27 Junho 2003) in http://www.theregister.co.uk/2003/06/27/rfid_chips_are_here/ mostra como estão disseminados os chips que utilizam a radiofrequência: desde cães até pneus de carros passando por notas. Também o artigo "RFID and surveillance in the workplace", publicado na Revista da OIT, World of Work, n.º 59, April, 2007, p. 16 mostra como esta tecnologia está presente desde o nascimento _ as pulseiras para identificação dos recém-nascidos_ até à morte _ para localizar corpos enterrados em cemitérios.

[121] OIT, World of Work, n.º 59, April 2007, p. 17, refere o caso de dezoito pessoas no México que trabalham para o Procurador-Geral e aceitaram um implante de um chip no braço para assim poderem aceder a áreas restritas.

[122] JAN LIBBENGA,"Video surveillance outfit chips workers _ RDFID implant scheme", TheRegister (10 de Fevereiro de 2006) in http://www.theregister.co.uk/2006/02/10/employees_chiped/ [Consult. 21 Novembro 2008] relata o caso de uma empresa norte-americana que exige o implante de um chip aos seus trabalhadores para poderem aceder a determinadas áreas do edíficio onde trabalham.

Sabendo a exacta localização de cada trabalhador num dado momento é possível distribuir as tarefas utilizando critérios cada vez mais racionais e economizando tempo. Assim, é possível saber o tempo que um trabalhador se demora a deslocar de um sítio do armazém para outro, estabelecendo tempos médios para a realização da tarefa, distribuir uma tarefa ao trabalhador que esteja mais próximo do local pretendido, colocando o trabalhador numa actividade constante, eliminando ou reduzindo ao mínimo os tempos de não-produtividade que não se inserem nem nas pausas nem nos horários de refeições. Esta maximização da produtividade, facilmente permitida por este sistema, leva a que todos os segundos do trabalhador sejam controlados removendo qualquer margem de decisão que possa caber ao mesmo relativamente ao modo como executa o seu trabalho, retira-lhe o direito que todo o ser humano tem de agir com autonomia e dignidade bem como os traços da individualidade que o permitem distinguir-se dos outros trabalhadores, nomeadamente os traços que fazem dele um bom trabalhador[123].

Os dados recolhidos através desta tecnologia ubíqua permitem-lhes ser utilizados na monitorização dos trabalhadores, desde o controlo do absentismo e da pontualidade até a uma análise detalhada da produtividade. A utilização desta tecnologia para monitorizar a eficiência dos trabalhadores levanta questões a nível da relação de confiança que deve existir entre o trabalhador e o empregador e que, deste modo, pode ser posta em causa.

Apesar desta tecnologia ser amplamente utilizada não existe legislação específica sobre como pode ser utilizada pela entidade empregadora.

Regulamentação existente sobre IDRF

O Código das Boas Práticas da OIT sobre os Dados Pessoais do Trabalhador abrange a IDRF no seu capítulo sobre monitorização no trabalho[124] pelo que os trabalhadores devem ser informados antecipadamente se estão a ser monitorizados, em que horário, que métodos e técnicas são usados e quais os dados recolhidos bem como a monitorização oculta deve ser permitida apenas se a legislação nacional o consentir ou se houver suspeita fundada da prática de actividade criminal e a monitorização contínua apenas deve ser autorizada por questões de saúde ou segurança ou para protecção da propriedade.

Na União Europeia as implicações da IDRF foram analisadas pelo GT 29 e constam de um documento publicado em Janeiro de 2005 com o nome de *Working document on data protection issues related to RFID technology*[125]. O GT 29 concluiu que quando são armazenados dados pessoais nas etiquetas (*tags*) IDRF ou que quando estes são ligados com uma base de dados que contem dados pessoais, bem como quando as *tags*

[123]JEREMY GRUBER, "RFID and workplace privacy", National Workrights Institute, in http://www.workrights.org/issue_electronic/RFIDWorkplacePrivacy.html [Consult. 28 Junho 2009]

[124] "Protection of workers' personal data. ILO code of practice", Geneva, 1997, ponto 6.14 in http://www.ilo.org/public/libdoc/ilo/1997/97B09_118_engl.pdf [Consult. 28 Junho 2009]

[125] Disponível in http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf [Consult. 28 Junho 2009]

colocadas em items individuais possam ser usadas para identificar indivíduos associados a eles, estamos perante um tratamento de dados pessoais que recai nas obrigações previstas na Directiva Europeia 95/46/CE sobre Protecção de Dados Pessoais e, por isso, o tratamento desses dados[126] deve obedecer aos princípios da Directiva.

Assim, determina o GT 29 nesse documento de trabalho que a qualidade dos dados deve obedecer aos seguintes princípios:

_ O princípio da limitação do uso: os dados devem ser usados unicamente para a finalidade para a qual são coligidos, de acordo com o art. 6.º, n.º 1, al. b) da Directiva, sendo finalidades explícitas e legítimas;

_ O princípio da qualidade dos dados: os dados pessoais devem ser adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e quaisquer dados irrelevantes para as finalidades determinadas devem ser eliminados. Os dados também devem exactos e mantidos actualizados.

_ O princípio da conservação dos dados: os dados devem ser mantidos apenas o tempo necessário para a finalidade para que foram recolhidos ou tratados posteriormente.

Quanto à legitimidade do processamento dos dados: é necessário o consentimento da pessoa titular dos dados de forma inequívoca, um consentimento esclarecido e livre de qualquer forma de coacção.

Requisitos da informação disponibilizada ao titular dos dados pessoais pelo responsável pelo tratamento ou seu representante: identidade do responsável pelo tratamento; finalidades do tratamento a que os dados se destinam; outras informações, tais como os destinatários dos dados e a existência do direito de acesso aos dados que lhe digam respeito. No caso dos trabalhadores, isto traduz-se no direito a acederem e corrigirem os dados constantes das suas etiquetas IDRF e a serem informados das finalidades das mesmas de tal forma que percebam os efeitos da aplicação da tecnologia IDRF.

Obrigações de segurança do tratamento: nos termos do art. 17 da Directiva, o responsável pelo tratamento deve pôr em prática medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição acidental ou ilícita, a perda acidental, a alteração, a difusão ou acesso não autorizados.

[126] Exemplos de utilização da tecnologia de IDRF cruzada com a interconexão de dados pessoais: o cruzamento de informações entre mercadorias vendidas, identificadas com recurso a IDRF, e os dados do cartão de crédito do comprador; os passes sociais que contêm esta tecnologia e armazenam simultaneamente os dados do passageiro, permitindo saber onde uma pessoa viaja a todo o tempo (o GT29 alerta para as fragilidades deste sistema IDRF, em termos de segurança, dado que um terceiro pode fazer a leitura dessa tecnologia sem que seja detectado); os cartões de cliente das lojas podem ser equipados com esta tecnologia permitindo saber os hábitos concretos de cada consumidor, permitindo com essa informação fazer assunções sobre o seu estilo de vida, saúde, rendimento, hábitos de compra; certos objectos valiosos, notas de bancos ou medicamentos têm um código IDRF que permitem a qualquer um, desde que equipado com um dispositivo de leitura próprio, detectar informações sobre que objectos pessoais estão na posse de um indivíduo, uma intrusão maior verifca-se se um terceiro não autorizado aceder a informações pessoais que estão por exempo, num passaporte que está equipado com esta tecnologia.

Medidas técnicas ou organizativas susceptíveis de serem aplicadas no local de trabalho quando as entidades empregadoras utilizem tecnologias IDRF em conexão com os dados pessoais dos trabalhadores: visibilidade das etiquetas IDRF e dos leitores IDRF; o uso de tecnologias protectoras de privacidade por parte do empregador, tais como meios de desactivação temporários ou definitivos das etiquetas IDRF.

No plano sindical, a Union Network International, que congrega 20 milhões de associados de 900 sindicatos espalhados pelo mundo inteiro, elaborou em 2006 o *RFID in the workplace: UNI Code of Good Practice*, um projecto sem força jurídica obrigatória mas que serve como linha orientadora dos sindicatos associados da UNI na negociação com as entidades empregadoras e que tem como propósito garantir que a tecnologia IDRF é introduzida no local de trabalho de acordo com as orientações da OIT, incluindo o respectivo Código de Boas Práticas, e de acordo com os melhores princípios de protecção de dados pessoais e em respeito do direito humano fundamental à intimidade privada. Apresenta como orientações: a discussão sobre a introdução das tecnologias IDRF com os representantes dos trabalhadores antes da sua introdução no local de trabalho; a elaboração de um estudo prévio sobre o impacto do uso dessa tecnologia no local de trabalho; a obrigação de a entidade empregadora se comprometer a respeitar a privacidade e dignidade do trabalhador aquando do uso do IDRF; políticas empresariais escritas sobre o uso do IDRF, que indiquem entre outras coisas, qual a sua finalidade, dados recolhidos; utilização feita com o conhecimento dos trabalhadores; não admissão de utilização de IDRF oculta; informação sobre onde estão localizadas as tags, se são activas ou passivas e alcance geográfico das mesmas; dar conhecimento da utlização desta tecnologia logo no processo de recrutamento e selecção; igualdade de tratamento entre os trabalhadores temporários e os trabalhadores da empresa utilizadora da IDRF ao nível da montiorização por esta via; direitos de acesso e de eliminação de dados incorrectos; o uso de localizadores IDRF apenas para controlo do acesso às instalações e, quando utilizado com outras finalidades, a sua utilização deve ser sujeita a negociação com as estruturas representativas dos trabalhadores; proibição de conexão automática entre os dados gerados pelo IDRF e outros dados que deverá ser sujeita a uma negociação prévia com os sindicatos ou comissões de trabalhadores e ter finalidades relevantes e necessárias para o empregador; a monitorização contínua via IDRF não é compatível com a dignidade humana do trabalhador; monitorizações de rotina para detectar a localização geográfica do trabalhador não são por normas permitidas e, caso essas medidas venham a ser tomadas, devem estar sujeitas a negociação prévia pela estrutura representaiva dos trabalhadores e admitidas unicamente com o propósito de facilitar a gestão da organização do trabalho e não para controlar o desempenho profissional do trabalhador; a adopção de medidas técnicas pela entidade empregadora para não permitir a monitorização IDRF durante as refeições, pausas e fora do horário de trabalho ou de férias; os dados recolhidos via IDRF não podem ser utilizados para controlar o desempenho profissional do trabalhador e para o avaliar; os dados obtidos também não podem ser usados com fins disciplinares, excepto em circunstâncias excepcionais em que haja fortes e fundadas suspeitas de que o empregado cometeu um crime ou uma ofensa disciplinar grave e na presença de um

representante do sindicato ou da comissão de trabalhadores; os dados IDRF não podem ser transmitidos a terceiros, excepto em situações em que seja necessário para prevenir uma ameaça séria à vida ou à saúde ou quando seja pedido nos termos da lei penal; conservação dos dados apenas pelo período necessário à realização da finalidade pretendida.

Muito importante neste Código da UNI é a referência ao facto de que os dados recolhidos não devem ser interligados com os dados resultantes de outras tecnologias de monitorização como, por exemplo, o GPS, a monitorização do uso da internet ou a videovigilância).

O Código de Boas Práticas da UNI também chama a atenção para o facto de estas tecnologias não poderem ser utilizadas para dissuadir os trabalhadores de procurar auxílio junto dos seus representantes sindicais ou da comissão de trabalhadores, do mesmo modo que esta tecnologia também não pode ser utilizada para evitar ou dificultar que os representantes dos trabalhadores exerçam as suas funções.

Outro aspecto novo, é a referência às tags colocadas para efeitos de identificação dos uniformes na lavandaria: é proibida a monitorização dos trabalhadores através dos seus uniformes, bem como é proibida a ligação entre os dados dos cartões de pagamento, como por exemplo, os cartões da cantina, e outras tecnologias IDRF utilizadas no local de trabalho.

Este Código opõe-se à implantação de chips no braço, seja em que circunstância for.

As entidades empregadoras devem estar atentas às implicações que esta tecnologia possa ter na saúde e segurança do trabalhador e tomar medidas para evitar que a monitorização via IDRF aumente os níveis de stress no local de trabalho.

A UNI tem estado bastante atenta à utilização da radiofrequência como meio de monitorização do trabalhador e, nesse sentido, enviou uma carta aberta[127] à Comissária da União Europeia responsável pela introdução da tecnologia IDRF na Europa, Vivianne Redding, onde alerta para o facto de ser feito um uso desta tecnologia de um modo que o trabalhador é localizado desnecessariamente, muitas vezes sem o seu conhecimento, e com brechas graves na privacidade deste e, por outro lado, no modo intensivo como é utilizada esta tecnologia que, associado a uma reestruturação da organização do ambiente trabalho, leva a uma desumanização do trabalho.

Jurisprudência

Porque este dispositivo se disseminou silenciosamente e, aparentemente, é inócuo, os trabalhadores, em Portugal, não têm noção da sua utilização e das suas implicações ao nível do tratamento de dados, pelo que inexistem decisões de tribunais nacionais que se pronunciem sobre a utilização da identificação por radiofrequência.

[127]"UNI's letter to EU Commissioner Viviane Reding on RFID technology in Europe", de 26 de Junho de 2006, in -http://www.union-network.org/uniindep.nsf/0/4606CF32F49004EAC1257199002F327B?OpenDocument [Consult. 28 de Junho de 2009]

Em França, a Cour de Cassation, chambre social, no seu arresto de 6 de Abril de 2004 decidiu que o despedimento de um trabalhador que se recusou a usar um *badge* que permitia identificá-lo à entrada e saída do local de trabalho não foi um despedimento com justa causa porquanto o sistema de badges não havia sido notificado à CNIL apesar de ter sido levado ao conhecimento de todos os trabalhadores e constar do regulamento interno.

Decisões da CNPD

Sobre esta matéria a CNPD pronunciou-se especificamente na sua Deliberação n.º 9/2004[128]. Por força desta deliberação ficou bem explícito que a entidade patronal deve notificar o tratamento de dados à CNPD sempre que recorrer à tecnologia IDRF e esta implicar a interconexão com informação de carácter pessoal. Os dados pessoais devem ser recolhidos para finalidades determinadas, explícitas e legítimas. Os dados produzidos via RF e as informações de índole pessoal só podem ser interconectados para as finalidades determinantes da recolha. Os dados recolhidos devem ser adequados, pertinentes, não excessivos e recolhidos de forma transparente, garantindo que o trabalhador é informado da utilização de equipamentos de identificação por RF e do seu direito de oposição.

À semelhança do que se passa com a videovigilância, a entidade empregadora deve colocar avisos nos produtos e nos locais sempre que tal tecnologia é utilizada.

Os trabalhadores devem ser informados sobre a leitura e activação remota das marcas RF, quando tal aconteça, e sobre quando tal vai ocorrer.

Como sucede no tratamento de todos os dados pessoais, estes devem ser eliminados quando a sua manutenção deixar de ser pertinente para o objectivo definido bem como as interconexões entretanto efectuadas devem ser desactivadas.

Hoje em dia, orientações sobre o modo como os dispositivos de identificação por radiofrequência devem ser utilizados são comuns nas comissões de protecção de dados dos países membros da União Europeia[129].

---

[128] Já em 2003, no "IV Encontro Ibérico das Autoridades de Protecção de Dados", op. cit., se havia concluído que a identificação por radiofrequência levantava importantes implicações na matéria da protecção de dados pessoais ficando a constar da Declaração de Jarandilla que a implantação desta tecnologia se deveria fazer com transparência e respeitando os princípios essenciais da protecção de dados pessoais.

[129] No caso da Agência de Dados britânica (ICO) temos o "Data Protection Technical Guidance Radio Frequency Identification", datado de 9 de Agosto de 2006 in http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/radio_frequency_indentification_tech_guidance.pdf [Consult. 28 Junho 2009]. O ICO remete a admissibilidade da utilização da IDRF em termos de monitorização para os mesmos termos em que é feita toda a monitorização no trabalho, isto é, dentro dos termos do Employment Practices Code. Também a CNIL regula a sua utilização no "Guide pour les employers et les salariés", ed. 2008, pp. 33-34, in http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL_GuideTravail.pdf [Consult. 28 Junho 2009]. Em Itália, o Garante per la Protezzione dei Dati Personali fez publicar sobre a IDRF um Provvedimenti a carattere generale, **"**"Etichette intelligenti" *(Rfid)***:** il Garante individua le garanzie per il loro uso - 9 marzo 2005" in http://www.garanteprivacy.it/garante/doc.jsp?ID=1109493 [Consult. 28 Junho 2009]

Geolocalização:

Em que consiste

O Sistema de Posicionamento Global (GPS, do inglês *Global Positioning System*), é um sistema de posicionamento por satélite americano, utilizado para determinação da posição de um receptor na superfície da Terra ou em órbita. O sistema GPS foi criado e é controlado pelo Departamento de Defesa dos Estados Unidos da América, para uso exclusivo militar. Actualmente é aberto para uso civil gratuito, requerendo apenas um receptor capaz de captar o sinal emitido pelos satélites. O sistema está dividido em três partes: espacial, de controlo e utilizador. O segmento do utilizador consiste num receptor que capta os sinais emitidos pelos satélites. Um receptor GPS *(GPSR)* descodifica as transmissões do sinal de código e fase de múltiplos satélites e calcula a sua posição com base nas distâncias em relação a estes. A posição é dada por latitude, longitude e altitude[130].

O baixo custo, disponibilidade e popularidade da tecnologia GPS não pode ser subestimada. Um estudo de 2006, The *C.J. Driscoll & Associates 2005-2006 Mobile Resource Management Systems Market*[131], diz que, no final de 2005, eram utilizados cerca de 1,9 milhões de aparelhos GPS em aplicações de Gestão dos Recursos Humanos nos Estados Unidos da América e previa-se que esse número atingisse os 5.8 milhões de aparelhos em 2009. Por todo o mundo, as vendas GPS aumentaram exponencialmente nos últimos anos e para o seu crescimento contribuíram o número de empregadores que usam GPS para localizar os seus trabalhadores, em pequenas e grandes empresas.

Os telemóveis distribuidos pelos empregadores aos trabalhadores estão, hoje em dia, munidos de um localizador GPS. Se o trabalhador não for informado desse facto e não desligar essa funcionalidade em determinados períodos, ele pode ser localizado mesmo durante o horário das refeições, pausas e fora do horário de trabalho. O empregador pode ficar com o roteiro total sobre onde pára durante todo o dia o trabalhador e, juntando as peças do puzzle, ficar com uma informação completa sobre a sua vida

---

[130] Para uma explicação mais detalhada, ver National Workrights Institute, "On your tracks: GPS tracking in the workplace" August 2005, pp. 4-5 in http://www.workrights.org/issue_electronic/NWI_GPS_Report.pdf [Consult. 28 Junho 2009]

[131] CLEM DRISCALL e MIKE SHELDRICK, "Taking the show on the road: GPS Drives U.S. Mobile Resources Management", InsideGNSS, March 2006, p. 28 in http://www.insidegnss.com/auto/0306%20Taking.pdf [Consult. 28 Junho 2009]

política, social, religiosa, familiar e estado de saúde. Se o trabalhador souber que o empregador detecta todos os seus movimentos, a todos os minutos, poderá sentir-se constrangido na sua liberdade de movimentação, por exemplo, poderá não ir a um congresso de um partido ou poderá não comparecer numa determinada manifestação se souber que o patrão tem uma preferência política ou uma opinião diametralmente oposta à sua. Desta forma, o direito inerente de uma pessoa a passar pelo mundo sem ser detectado é-lhe roubado[132] e rapidamente passamos para uma situação de servidão em que é retirada a dignidade ao trabalhador.

Outra questão que se levanta é que, muitas vezes, são os próprios empregadores que exigem aos trabalhadores que tenham os telemóveis sempre ligados para estarem disponíveis e localizáveis, mesmo fora do horário de trabalho estabelecido. Traçar uma fronteira clara entre o trabalho e a vida privada do trabalhador torna-se muito difícil nos dias de hoje dado que cada vez mais empregadores exigem que os trabalhadores estejam sempre disponíveis[133] e, por outro lado, porque cada vez há mais trabalhadores a exercerem funções fora das instalações da empresa[134].

Os veículos da empresa também já estão hoje em dia equipados com GPS, com benefícios claros para o empregador, em termos de distribuição de tarefas, localização dos veículos e seus conteúdos, por questões de gestão e de segurança. Estão munidos desta tecnologia táxis, reboques, camiões, veículos comerciais ou simplesmente uma viatura que tenha sido atribuída ao trabalhador a tempo inteiro, como forma de retribuição deste. Isto levanta problemas porque, face a tão diferentes tipos de veículos, associados a profissões tão diferentes, bem como a diferentes permissões quanto à sua utlização, ora exclusivamente profissional ora também para uso pessoal, é claro que o seu uso nem sempre aparecerá justificado com base num interesse legítimo do empregador e o uso desta tecnologia poderá invadir a privacidade do trabalhador de uma forma bastante intrusiva.

Os relatórios emitidos por este aparelho, para além de darem a informação sobre a localização da viatura e da velocidade de circulação da mesma, possuem um sistema de sensores ligados a toda a viatura que também fornecem, ou podem fornecer, informações como abertura e fecho das portas, estado dos pneus, ligação do ar condicionado, do rádio. Ou seja, rapidamente passamos da necessidade da localização da viatura por questões de gestão da empresa, de segurança do trabalhador e de protecção da propriedade do empregador para uma monitorização dos passos do trabalhador a todo o momento.

O GPS pode estar colocado na viatura sem que o trabalhador se aperceba disso[135] e a monitorização oculta constitui uma violação da intimidade privada do trabalhador e da

---

[132] "On your tracks: GPS tracking in…", p. 19

[133] Esta disponibilidade fora do local de trabalho é explicitamente regulada no Direito Francês, no artigo L3121-5 a L3121-7 do *Code du Travail*, e denominada de "astreintes".

[134] ADAM GELLER, "Bosses keep sharp eye on mobile workers via GPS", Associated Press (1/03/2005) in http://www.workrights.org/in_the_news/in_the_news_associatedpress.html [Consult. 28 Junho 2009]

[135] Pode ser consultado um exemplo de um aparelho GPS que é vendido com o propósito explícito de monitorizar de forma oculta os empregados em: http://www.brickhousesecurity.com/covert-small-gps-tracking-device.html [Consult. 28 Junho 2009]

sua dignidade bem como coloca em causa a relação de confiança entre trabalhador e empregador.

Outra questão é que, no caso dos veículos equipados com GPS estes poderão estar ligados à ignição do carro[136] pelo que o trabalhador não tem maneira de o desligar, mesmo que esteja autorizado a fazer um uso privado da viatura.

A introdução do GPS permite ao empregador rever todas as decisões do trabalhador, rouba-lhe a autonomia e leva a que este seja tratado como um robot, e repare-se que estamos sobretudo a falar de profissões em que o trabalhador tinha uma maior liberdade de decisão, como era o caso das profissões que são exercidas fora das instalações da empresa. Isto leva a que o trabalhador deixe de se preocupar com a qualidade do seu trabalho e se concentre unicamente nos tempos que têm de ser cumpridos ao segundo. A pressão para aumentar a produtividade, minuciosamente analisada, aumenta o stress sobre o trabalhador com consequências na saúde do mesmo e, consequentemente, no absentismo. O facto de saber que está a ser vigiado todos os dias também pode colocar uma pressão insidiosa sobre o trabalhador, com efeitos adversos na sua saúde.

Jurisprudência

Sobre a utilização do GPS, em sede de contrato de trabalho, pronunciou-se o Supremo Tribunal de Justiça no seu Ac. de 22 de Maio de 2007[137]. O Supremo analisou um recurso por parte da Ré/entidade empregadora de uma decisão judicial que tinha por base um pedido de resolução com justa causa pelo trabalhador, baseado no facto de a entidade empregadora ter colocado na viatura utilizada nas suas deslocações como vendedor um aparelho GPS e com isso ter violado o art. 20.º do Código do Trabalho. Este aparelho só foi colocado na viatura desse trabalhador e não na dos outros vendedores ao serviço da mesma empresa e, por outro lado, o trabalhador não se opôs à colocação do aparelho, embora não tivesse sido solicitada a sua autorização para o efeito. A colocação deste aparelho tinha sido precedida da tentativa, meses antes, de o empregador baixar as remunerações do trabalhador, a que este se opôs. O trabalhador alega, para justificar a justa causa, que se sentiu vexado, que tinha sido violado o princípio da igualdade face aos outros trabalhadores e que foi violado o direito à reserva da sua vida privada com a colocação deste aparelho.

O acórdão recorrido havia decidido que: "*In casu*, cremos que a conduta do empregador, ao colocar aquele mecanismo de controlo exactamente no veículo que o A. utilizava (excluindo todos os outros vendedores), sem se saber qual a finalidade, sem lhe dar qualquer explicação e decorrido algum tempo após a Ré lhe ter tentado baixar as comissões (o que o A. não aceitou, o [que] naturalmente e pela lógica da vida levou à

[136] "On your tracks: GPS tracking in the…", p. 17

[137] Disponível in http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/1771be8dfd54aa72802572e40034640f?OpenDocument&Highlight=0,gps [Consult. 28 Junho 2009]

criação de alguma tensão entre ambos), é de molde a criar no empregado uma falta de confiança na sua entidade patronal, que na óptica do funcionário está já a desconfiar dele.

Este quadro, acaba a nosso ver, por tornar impossível a subsistência da relação laboral, ou melhor dito, por tornar inexigível ao trabalhador, que mantenha o vínculo laboral.

Vale isto dizer e em suma que, em nossa modesta opinião, ocorreu justa causa para que o A. rescindisse o contrato de trabalho, como o fez."

O Supremo Tribunal de Justiça concedeu parcialmente a revista e absolveu a Ré quanto ao pedido de condenação em indemnização por resolução do contrato de trabalho pelo autor com base nos seguintes fundamentos:

1.º - "Embora a formulação literal do n.º 1 do artigo 20.º do Código do Trabalho não permita restringir o âmbito da previsão daquela norma à videovigilância, a verdade é que a expressão adoptada pela lei, «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», por considerações sistemáticas e teleológicas, remete para formas de captação à distância de imagem, som ou imagem e som que permitam identificar pessoas e detectar o que fazem, quando e durante quanto tempo, de forma tendencialmente ininterrupta, que podem afectar direitos fundamentais pessoais, tais como o direito à reserva da vida privada e o direito à imagem."

A nosso ver, independentemente de se considerar o GPS como cabendo ou não na previsão do art. 20.º do Código do Trabalho, aspecto que iremos discutir mais à frente, o facto é que a introdução de quaisquer meios tecnológicos pela entidade patronal destinados a controlar o desempenho profissional do trabalhador e que possam confluir com o direito à reserva da intimidade da vida privada poderão eventualmente constituir fundamento de despedimento por justa causa por parte do trabalhador desde que, ponderados no caso concreto os interesses e valores em presença e ponderados os princípios da necessidade, da adequação e da proporcionalidade se conclua que a utilização do GPS viola esse direito fundamental. Caso se conclua pela violação do direito à reserva da intimidade da vida privada do trabalhador essa justa causa vai existir sempre, mesmo que não houvesse este artigo do Código do Trabalho, e isto por força da aplicabilidade directa dos direitos fundamentais às entidades privadas.

2.º - "Não se pode qualificar o dispositivo de GPS instalado no veículo automóvel atribuído a um técnico de vendas como meio de vigilância a distância no local de trabalho, já que esse sistema não permite captar as circunstâncias, a duração e os resultados das visitas efectuadas aos seus clientes, nem identificar os respectivos intervenientes."

Em nosso entendimento, os meios de vigilância à distância no local de trabalho não têm de captar tudo o que o trabalhador faz para serem considerados como tal, é suficiente que captem uma importante parcela da actividade do trabalhador e, ao mesmo tempo, entrem na reserva da sua intimidade da vida privada. Assim tanto é que uma

câmara de vídeo colocada dentro da viatura, que capte a imagem mas não o som, também não conseguiria "captar as circunstâncias, a duração e os resultados das visitas efectuadas" aos seus clientes, nem identificar os respectivos intervenientes, uma vez que os encontros com os clientes não ocorrem dentro da viatura, e no entanto, ninguém põe em dúvida de que se trata de um meio de vigilância à distância.

Esta decisão, independentemente de se concordar ou não com ela, levanta questões muito importantes:

_ O respeito do princípio da igualdade e da não discriminação é um limite ao poder de organização da actividade laboral pelo empregador e deve ser respeitado aquando da aplicação de meios de vigilância à distância no local de trabalho. Na decisão analisada vemos que a colocação de um GPS na viatura de um trabalhador, com a opção de não se colocar nas outras viaturas, pode traduzir a violação do princípio da igualdade e da não discriminação, por aplicação de condições diferentes de trabalho entre os trabalhadores. O Supremo, no caso julgado, considerou que não foi violado esse princípio porque o aparelho foi colocado a título experimental, pelo que não seria de esperar que fosse posto a funcionar em todas as viaturas comerciais da ré e, por outro lado, o autor/trabalhador não conseguiu provar que as áreas geográficas de actuação dos restantes vendedores da ré correspondiam às características indicadas para efectuar uma experiência conclusiva do equipamento tecnológico em questão.

_ A ausência de uma definição do que sejam "meios de vigilância à distância" cria uma situação de incerteza no sistema jurídico-laboral, com prejuízo para a defesa dos direitos do trabalhador. Neste caso, o Supremo Tribunal de Justiça, com base numa interpretação restritiva veio considerar que a expressão adoptada pela lei, «meios de vigilância a distância no local de trabalho, mediante o emprego de equipamento tecnológico, com a finalidade de controlar o desempenho profissional do trabalhador», por considerações sistemáticas e teleológicas, remete para formas de captação à distância de imagem, som ou imagem e som".

_ A inexistência da consciência da obrigatoriedade da necessidade de um pedido prévio de instalação do GPS à CNPD. Na decisão analisada não foi invocado em momento algum uma situação ao nível da violação da protecção de dados pessoais do trabalhador, e isto apesar de a viatura estar alocada a um trabalhador concreto, o que permitia a sua identificação pelo que, os dados que fossem tratados, seriam dados pessoais. Nenhuma das partes invoca esta situação para alegar a licitude ou ilicitude da instalação o que sugere que nem o trabalhador estava consciente do facto de poder recusar dirigir a viatura com o GPS instalado, nem a entidade empregadora do seu dever de pedir a autorização à CNPD, porque se o tivesse feito certamente o teria alegado para defender que a justa causa era infundada.

- O facto de os nossos tribunais ainda não estarem sensibilizados para as potencialidades desta tecnologia ao nível da intrusão na reserva da vida privada do trabalhador (nem sequer se refere a instalação de um sistema que permita que o GPS seja desligado aquando das pausas ou no horário da refeição do trabalhador) e para o facto de não considerarem a localização de um trabalhador, feita de modo contínuo,

conseguindo a entidade empregadora saber quando pára, onde e durante quanto tempo, ser uma maneira de controlar o seu desempenho profissional.

_ Os nossos tribunais consideram que apenas há um controlo da vida privada do trabalhdor quando a viatura não está "limitada às necessidades do serviço".

Decisões da CNPD

A informação resultante dos dados de localização que estão associados a um determinado equipamento, por sua vez instalado num telefone, computador ou viatura permite identificar ou tornar identificável o utilizador e, por conseguinte, esta informação tem a natureza de informação pessoal nos termos do artigo 3.º da Lei n.º 67/98 (LPDP) e o seu uso deve ser notificado à CNPD.

A CNPD a propósito de um pedido da TMN para um tratamento de dados pessoais com a finalidade de registar o tratamento e análise de reclamações de clientes do Serviço Frotalink (serviço da TMN para localização e gestão das frotas: a TMN instala os equipamentos de geolocalização mas quem insere os dados das viaturas e dos utilizadores é o cliente) e apesar de não estar em causa uma relação laboral mas uma prestação de serviços, na AUTORIZAÇÃO Nº 857 /2005, aproveitou para distinguir que: "As informações captadas por GPS afiguram-se verdadeiros tratamentos de dados pessoais quando se identifica ou torna identificável um titular, pessoa singular.

No caso concreto, a TMN – Telecomunicações Móveis Nacionais, SA proporciona a clientes a instalação e a prossecução deste serviço.

Nestas situações, são os clientes que podem estar a efectuar um tratamento de dados pessoais que deve ser notificado à CNPD .

Se alguém instala no seu veículo este sistema para protecção pessoal não terá que notificar a CNPD. Se uma empresa proceder à mesma instalação, para idêntica finalidade, em relação aos seus funcionários, esta Comissão deve ser notificada.

Nos tratamentos de dados pessoais com esta natureza deve tomar-se em consideração o artigo 20.º do Código do Trabalho."

A propósito da utilização do GPS no local de trabalho, a Commission Nationale de L'Informatique et des Libertés (CNIL) adoptou a 16 de Março de 2006 uma recomendação, o *Guide de la Géolocalisation des Salariés*[138] destinada a informar os empregadores e os trabalhadores sobre as suas obrigações e direitos. Começa por referir que a principal recolha de dados pelos sistemas de geolocalização é relativa ao posicionamento de um veículo e que na medida em que esses dados e outros que lhe são associados podem ser relativos a um empregado identificado (sabemos que é aquele empregado que conduz aquele veículo), esse sistema constitui um tratamento de dados pessoais. Em consequência, uma entidade empregadora que queira utilizar tal sistema

[138]Disponível em http://www.cnil.fr/fileadmin/documents/approfondir/dossier/geolocalisation/Guide-geolocalisation.pdf [Consult. 28 Junho 2009]

deve fazer uma notificação à CNIL e respeitar os princípios relativos à protecção do tratamento de dados pessoais.

O que este guia traz de novo é que faz uma importante distinção entre veículos de função e veículos de sociedade e, consoante as viaturas se insiram numa ou noutra categoria, o seu tratamento é diferente. O veículo de sociedade não pode em princípio ser utilizado por um empregado fora do seu horário de trabalho, estamos a falar de situações em que o veículo constitui ele mesmo objecto do trabalho do empregado, como é o caso de um motorista de pesados ou de passageiros[139]. O veículo de função constitui uma vantagem atribuída ao trabalhador, uma remuneração em espécie. Atendendo a esta distinção, a CNIL recomenda que os dispositivos de geolocalização instalados em veículos de função possam ser desactivados quando o empregado não está a trabalhar de modo a que possa, assim, preservar a sua vida privada. Um procedimento idêntico pode ser adoptado para os veículos de sociedade que sirvam para fins privados como, por exemplo, nos casos em que o empregador tolera que o trabalhador utilize o veículo para voltar para casa no final do dia de trabalho. No caso de veículos de sociedade em que a geolocalização visa captar qual é o veículo mais perto do cliente, a CNIL aconselha que este sistema não esteja permanentemente em funcionamento, sob pena de se tornar uma forma de vigiar o empregado, mas apenas quando há uma chamada de um cliente. Do mesmo modo, este sistema deve ser apenas activado quando a tarefa consiste ela própria na deslocação, como é o caso do táxi.

A CNIL sublinha sempre que os dados recolhidos devem destinar-se unicamente às finalidades declaradas pelo que, se o objectivo é a luta contra o roubo, os dados apenas podem ser acedidos pelas autoridades policiais. O desvio de finalidade, nomeadamente para vigiar os trabalhadores, é punido com uma pena de prisão que pode ir até 5 anos e uma multa que pode ir até 300.000 € (art. 226-21 do *code pénal*).

A CNIL exige que a entidade empregadora indique que medidas tomou para que os empregados fossem informados e que, em aplicação dos disposto no código do trabalho, o *comité d'entreprise* seja informado e consultado previamente, dado que se trata da introdução de novas tecnologias que podem ter consequências no emprego, na qualificação, na remuneração, na formação ou nas condições de trabalho do pessoal. Por outro lado, a não declaração da utilização da geolocalização e do tratamento de dados pessoais associados à CNIL tem como consequência que este dispositivo seja inoponível aos empregados, nomeadamente como causa de despedimento, e isto com base na decisão judicial da Cour de Cassation, chambre social, de 6 de Abril de 2004, que decidiu que o despedimento de um trabalhador que se recusou a usar um *badge* que permitia identificá-lo à entrada e saída do local de trabalho não foi um despedimento com justa causa porquanto o sistema de badges não havia sido notificado à CNIL apesar de ter sido levado ao conhecimento de todos os trabalhadores e constar do regulamento interno.

[139] O critério do veículo como objecto do trabalho ou como acessório do mesmo é explicado por Didier Gasse no 27.e Rapport d'Activité 2006, p. 15 disponível em http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL-27erapport-2006.pdf [Consult. 28 Junho 2009]

A CNIL recomenda que o dispositivo de geolocalização não mencione a velocidade máxima do veículo mas apenas a sua velocidade média dado que é às autoridades judiciárias que compete constatar eventuais infracções ao código da estrada.

Outra recomendação é a de que se o objectivo do aparelho é o da optimização das voltas, o tratamento dos dados deve fazer-se em tempo real. Se o dispositivo for colocado para controlar a actividade dos empregados, a CNIL recomenda que esses dados sejam conservados apenas por um máximo de 2 meses. Se a entidade empregadora tornar os dados recolhidos anónimos, de modo a que seja impossível identificar directa ou indirectamente uma pessoa física, os mesmos podem ser guardados por tempo ilimitado. A questão é que, muitas vezes, o número da matrícula de uma viatura está associado a um empregado que a utiliza e, por isso, é difícil que esses dados sejam considerados anónimos.

No Relatório de Actividades da CNIL de 2006, na referência que fazem a esta recomendação, é sublinhada a importância de se tratar de uma finalidade legítima e que só um imperativo de certeza ou de segurança do empregado ou das mercadorias que os veículos transportam, uma melhor alocação dos meios disponíveis quando os serviços se façam em sítios diferentes, o seguimento e facturação de um serviço ou ainda o seguimento do tempo de trabalho, quando este seguimento não possa ser realizado por outros meios é que justificam a geolocalização. *A contrario*, a geolocalização não é justificada quando o empregado dispõe de liberdade na organização das suas deslocações e, mesmo que assim não seja, não deve conduzir a um controle permanente do trabalhador.

Monitorização telefónica:

Há imensos assuntos que podem ser rapidamente tratados por telefone e, muitas vezes, só é possível fazê-lo durante o horário de expediente. Situações de normalidade social conduzem também a que sejam aceitáveis telefonemas para, por exemplo, saber do estado de saúde de um filho que está doente ou marcar uma consulta médica.

Porém, o telefone é um instrumento de trabalho fornecido pelo empregador e, por isso, é legítimo que este tenha preocupações relacionadas com o controlo de custos e, por outro lado, evitar que seja feito um uso desproporcionado deste que afecte a produtividade do trabalhador. Nesta medida, o controlo das chamadas telefónicas efectuadas, consultando as facturas detalhadas enviadas pelas operadoras é uma maneira de imputar esses custos ao trabalhador bem como de saber quando as chamadas externas têm um tempo ou uma frequência que ultrapassam o razoável.

O trabalhador deve ser informado sobre se pode ou não fazer chamadas e quais as limitações que existem, por exemplo, não poder fazer chamadas internacionais. O meio ideal para o efeito é o regulamento interno mas nem todos os empregadores o fazem, o que leva a uma indeterminação sobre o que é permitido ou não, que pode ser prejudicial para a entidade empregadora ou para o trabalhador e que mais facilmente pode levar a tratamentos discriminatórios, por exemplo, um determinado trabalhador faz as chamadas que quer e quando quer enquanto outro é proibido de fazer telefonemas.

O empregador também quer saber como os trabalhadores executam as suas tarefas, o modo como tratam os clientes, se passam a terceiros informações confidenciais e, por isso, colocam escutas ou fazem gravações telefónicas. O modo como o Direito permite essas escutas variam de país para país e tem sobretudo a ver com o facto de colocarem a tónica no facto de saber se o trabalhador pode ter a legítima expectativa de que as suas conversas não sejam escutadas ou no facto de estar em causa um direito fundamental – o direito à reserva da vida privada que, caso seja violado em sede laboral, põe em causa a própria dignidade humana.

Se varia em cada ordenamento jurídico o facto de as gravações da chamadas serem permitidas ou proibidas, trabalhos há em que a conversa telefónica é o próprio produto do trabalho e, por outro lado, esta é muitas vezes o único meio de prova das declarações negociais, que podem chegar a milhares de euros, como no caso da compra e venda de acções através do serviço de homebanking. Nestas situações as legislações são unânimes em permitir as gravações das chamadas telefónicas, dentro de certas condições[140]. Estamos a falar de Call Centers, espalhados por todo o mundo e Portugal não é excepção. O trabalho de um operador de call center é classificado como trabalho com nível de stress elevado precisamente porque as conversas são constantemente

[140] Veja-se, no caso do Direito Português, o art. 4.º, n.ºs 2 e 3 da Lei n.º 41/2004, de 18 de Agosto, e o art. 9.º, n.º 2 do DL 134/2009, de 2 de Junho.

monitorizadas, são continuamente gravadas, e a autonomia dos trabalhadores é muito reduzida, limitando-se a repetir aos clientes o que está escrito num script, sendo chamados a atenção quando na audição das chamadas se constata que se desviaram das regras de comunicação e parâmetros rigorosamente estabelecidos[141]. Estes trabalhos são precários não só pelo tipo de trabalhadores escolhidos, estudantes na sua maioria, mas também pela pressão que colocam no trabalhador e pelo mal-estar gerado no local de trabalho pelo controlo absoluto de tudo o que este faz e do modo como o faz, desumanizando-o. Este tipo de trabalho, tão ligado ao telefone, deveria merecer por parte do nosso legislador uma especial atenção ao nível da legislação de Higiene e Saúde no Trabalho, como já vem sucedendo noutros países.

Jurisprudência:

Quanto à admissibilidade das escutas telefónicas, a nossa jurisprudência é peremptória e unânime: o princípio da inviolabilidade da correspondência e das telecomunicações, consagrado no art. 34.º, n.º 1 da Constituição, tem carácter absoluto, não admitindo a lei qualquer outra excepção, sendo por isso ilícitas as violações que não tenham sido autorizadas para fins de investigação criminal, nos termos da lei, e quem o fizer sem o consentimento dos visados comete o crime p. e p. pelo art. 194.º, n.º 2, do CP (cfr. Ac. do Tribunal da Relação de Lisboa, de 10 de Dezembro de 1991[142]).

Em situações em que não se pode afastar a reserva da intimidade das comunicações, entende-se inclusivamente que o trabalhador não tem o dever de responder ao empregador sobre se efectuou determinados contactos telefónicos, podendo mentir-lhe sem que isso aporte uma tal carga de desvalor que possa conduzir a um juízo de inviabilidade da relação, e isto mesmo que se entenda que não está em causa uma comunicação de índole pessoal laboral (cfr. Ac. do Supremo Tribunal de Justiça, de 5 de Julho de 2007[143], Relator Bravo Serra). Podemos inferir dessa decisão que caso se provasse que havia uma instrução ao trabalhador de proibição de fazer chamadas que não fossem exclusivamente profissionais, a violação dessa proibição, e nunca o conteúdo da chamada em si, poderia consubstanciar base para um procedimento disciplinar.

O Acordão n.º 241/02 do Tribunal Constitucional, de 29.05.2002, no DR, II, de 23.7.2002, pág. 12825, julgou inconstitucional a norma da al. b) do n.º 3 do art.º 559º do CPC, por infracção ao disposto nos arts. 26º, n.º 1 e 34º, n.ºs 1 e 4 da Constituição, quando interpretada no sentido de que, em processo laboral, podem ser pedidas por despacho judicial, aos operadores de telecomunicações informações relativas aos dados

---

[141] Esta temática encontra-se desenvolvida, numa perspectiva de análise sociológica, na tese de Doutoramento de Selma Borghi Venco, apresentada em Fevereiro de 2006 na Universidade Estadual de Campinas e que tem o título de *Tempos modernissimos nas engrenagens da telemarketing*.

[142] Disponível in http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/09444cce314ceaa88025680300046a2b?OpenDocument&Highlight=0,telefone,trabalho [Consult. 28 Junho 2009]

[143] Disponível in http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/81c458845496995480257325003c8f7f?OpenDocument [Consult. 28 Junho 2009]

de tráfego e à facturação detalhada de linha telefónica instalada na morada de uma parte, sem que enferme de nulidade a prova obtida com a utilização dos documentos que veiculam aquelas informações. E pode ler-se no seu sumário: «I. O sigilo das telecomunicações, garantido nos termos do art. 34º, n.º 1 da Constituição, abrange não só o conteúdo das telecomunicações, mas também o "tráfego" como tal (espécie, hora, duração, intensidade de utilização). (...) VII. A infracção à proibição constitucional de ingerências nas telecomunicações há-de ter nos processos cíveis e em matéria de prova a mesma sanção radical prevista na Constituição em sede de "garantias do processo criminal: a nulidade». Só assim se garante uma efectiva tutela da confidencialidade ou se minimizam os inconvenientes de uma sua violação, mormente se tal violação se repercutir em matérias ligadas a aspectos sancionatórios, como é o caso do processo disciplinar.

Decisões da CNPD

A CNPD em documento aprovado a 29 de Outubro de 2002, na sessão plenária da CNPD, estabeleceu os princípios sobre a privacidade no local de trabalho quanto ao tratamento de dados em centrais telefónicas, o controlo do e-mail e do acesso à internet. Quanto ao tratamento de dados nas centrais telefónicas estabeleceu os seguintes princípios:

a) Obrigatoriedade de definição, *com rigor*, do grau de tolerância quanto à utilização dos telefones e as formas de controlo realizadas;
b) O reconhecimento de que há necessidades do dia a dia do trabalhador que não podem deixar de ser encaminhadas sem que se recorra ao telefone durante o tempo e no local de trabalho.
c) O tratamento dos dados devem limitar-se ao necessário para a realização da finalidade de controlo; o tratamento deve limitar-se à identificação do utilizador, à sua categoria/função, número de telefone chamado, tipo de chamada – local, regional e internacional – duração da chamada e custo da comunicação.
d) Tal como o assinante tem o direito de exigir uma facturação detalhada com supressão dos últimos quatro dígitos (cf. art. 7.º n.º 2 da Lei 69/98), deve ser reconhecida ao trabalhador essa garantia, nomeadamente quando a listagem é acessível a outros trabalhadores.
e) Deve ser estabelecido um prazo limitado de conservação, necessariamente inferior ao prazo legal de pagamento da factura (6 meses);
f) Pode ser equacionada, em função do tipo de empresa e de acordo com os princípios da proporcionalidade, a possibilidade de a empresa assegurar a existência de uma linha não conectada à central telefónica ou o acesso a serviço público de telecomunicações;
g) É proibido o acesso indevido a comunicações, a utilização de qualquer dispositivo de escuta, armazenamento, intercepção e vigilância de comunicações pela entidade empregadora;

h) É possível a gravação de chamadas telefónicas prevista no artigo 5.º n.º 3 da Lei 69/98, isto é, no âmbito de práticas comerciais lícitas e para o efeito de prova de uma transacção comercial ou de qualquer outra comunicação de negócios, desde que o titular dos dados tenha sido disso informado e dado o seu consentimento expresso.

A Comissão mais avançada nesta matéria é a CNIL, que estabelece que as gravações das conversas telefónicas só podem ser realizadas em caso de necessidade reconhecida e devem ser proporcionais aos objectivos prosseguidos sendo que as chamadas privadas devem dispor de linhas próprias, de modo a que as chamadas pessoais não sejam gravadas, ou de uma funcionalidade que permita desactivar a gravação durante a chamada privada. Esta faculdade torna-se ainda mais importante no caso de trabalhadores que são simultaneamente representantes das comissões de trabalhadores ou dos sindicatos.

A CNIL também estabelece que as instâncias representativas dos trabalhadores e os próprios trabalhadores devem ser informados previamente à instalação desses dispositivos das finalidades dos mesmos bem como das consequências individuais que podem acarretar, os destinatários das gravações e das modalidades de exercício do seu direito de acesso.

Não só os trabalhadores mas também os seus interlocutores devem ser informados sobre a gravação da conversa, quer através de uma mensagem no início desta, quer através das condições contratuais que constam do documento relativo ao serviço telefónico.

Em termos de tempo de conservação das gravações, a CNIL distingue entre um período máximo de 6 meses, quando as gravações são efectuadas para fim de formação do pessoal, até um período máximo de 5 anos, quando as gravações são efectuadas para efeitos de prova em matéria bancária, nos termos dos artigos 321-78 e 321-79 do Regulamento Geral da Autoridade dos Mercados Financeiros.

Monitorização do uso da internet e do email :

Até há pouco tempo, quer se tratasse de controlo telefónico, de badges, de geolocalização ou de videovigilância, a vigilância recaía principalmente sobre a presença ou a localização física do indivíduo. Numa palavra, as tecnologias estavam ainda na periferia do processo do trabalho. Com a emergência das novas tecnologias de informação e comunicação (NTIC) e particularmente com a introdução da internet na empresa, verificou-se uma verdadeira migração das tecnologias de controlo da periferia para o coração do processo de trabalho propriamente dito[144].

Para os trabalhadores, a diferença de natureza entre as NTIC e tudo o que as precede reside precisamente na capacidade desta nova tecnologia conservar todos os rastos deixados pelo trabalhador conectado consituindo uma verdadeira "caixa negra" que grava todas as actividades do utilizador.

Como refere Hubert Bouché, no Relatório elaborado para a CNIL sobre a Cibervigilância no local de trabalho, agora tem início a era do "contremaître virtuel"[145], que consegue saber tudo sobre o trabalhador ao ponto de conseguir estabelecer o seu perfil profissional, intelectual e psicológico.

A utilização da internet no local de trabalho veio naturalmente colocar novos problemas em matéria de segurança, uma vez que facilmente se passam para o exterior informações sobre a vida da empresa, os ficheiros de pessoal, os segredos de fabrico e é essencial para o bom funcionamento da empresa que esses aspectos sejam controlados.

Os trabalhadores encontram-se cada vez mais constrangidos pelas políticas da empresa a utilizar o correio electrónico unicamente com fins profissionais sendo que, inclusivamente, certas filiais americanas, estabelecem que todo o correio electrónico enviado pelo empregado se considera como um "registo permanente, escrito, que pode a todo o momento ser controlado e inspeccionado"[146]. Nos E.U.A., a monitorização do uso da internet e do correio electronico é prática comum e legalmente admitida bem como pode ser livremente usada como meio de prova. Como se refere num inquérito conduzido pela AMA em 2007: "Workers' e-mail and other electronically stored information create written business records that are the electronic equivalent of DNA evidence"[147].

A monitorização do uso do computador refere-se não apenas aos sites acedidos e tempo de ligação à internet mas também ao número de vezes que se toca nas teclas (*Keystroke monitoring*), que podem inclusivamente levar a uma pressão para estabelecer metas irrealistas, que levam ao esgotamento do trabalhador. Novamente, a desumanização do trabalhador, encará-lo como uma máquina que deve ter um ritmo

144 "Cybersurveillance sur les lieux de Travail", pp. 2-3
145 Ibid., p. 4
146 Ibid., p. 4
147 2007 Electronic monitoring & Surveillance survey

rápido e constante e, é sabido, que as pessoas não têm sempre o mesmo ritmo, colocar-lhes essa pressão, vistoriar tão detalhadamente o seu trabalho, é tirar os olhos da qualidade e retirar a dignidade ao homem que passa de trabalhador a servo.

O computador é propriedade da empresa e o facto de o acesso a este ser protegido por uma palavra-passe na posse do trabalhador não significa que este tenha o direito de fazer uso privado do mesmo mas sim destina-se a evitar o seu acesso por terceiros. Do mesmo modo, a entidade patronal pode bloquear o acesso a determinados sites e a recepção de determinados anexos identificados como potencialmente maliciosos para o computador. Este controlo e o modo como é feito deve ser levado ao conhecimento dos trabalhadores e deve ser precedido de uma consulta prévia à comissão de trabalhadores por uma questão de lealdade e boa fé no comportamento da entidade patronal perante o trabalhador e porque uma vigilância ilimitada e contínua, ainda que com o conhecimento dos trabalhadores, põe em causa a dignidade do homem, bases de um Estado de Direito.

Jurisprudência:

Correio electrónico

A Jurisprudência portuguesa, entende que o envio de mensagens electrónicas de pessoa a pessoa («e-mail») preenche os pressupostos da correspondência privada (Internet – Serviço de comunicação privada) e que a inviolabilidade do domicílio e da correspondência vincula toda e qualquer pessoa, sendo certo que a protecção da intimidade da vida privada assume dimensão de relevo no âmbito das relações jurídico-laborais (cf. Ac. do Tribunal da Relação de Lisboa, de 5 de Junho de 2008[148]).

Além do mais, os tribunais portugueses, aplicam o artigo 22.º, n.º 1 do CT que garante o direito à reserva e à confidencialidade relativamente a mensagens pessoais e à informação não profissional que o trabalhador receba, consulte ou envie através de correio electrónico, pelo que não admite que o empregador possa aceder ao conteúdo de tais mensagens ou informação, mesmo quando esteja em causa investigar e provar uma eventual infracção disciplinar e, caso o façam, não serão de atender os decorrentes meios de prova juntos ao processo disciplinar (cf. Ac. do Supremo Tribunal de Justiça, de 5 de Julho de 2007[149], relator Mário Pereira e Ac. do Tribunal da Relação de Lisboa, de 5 de Junho de 2008).

O Supremo Tribunal de Justiça, no mesmo acórdão, decidiu que a definição da natureza particular da mensagem obtém-se por contraposição à natureza profissional da comunicação, relevando para tal, antes de mais, a vontade dos intervenientes da comunicação ao postularem, de forma expressa ou implícita, a natureza profissional ou

[148] Disponível in http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/6c195267c4ce32e480257474003464f7?OpenDocument [Consult. 28 Junho 2009]

[149] Disponível in http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/54d3c9f0041a33d58025735900331cc3?OpenDocument [Consult. 28 Junho 2009]

privada das mensagens que trocam. Esta concepção, que vai para além das comunicações relativas à vida familiar, afectiva, sexual, saúde, convicções políticas e religiosas do trabalhador mencionadas no art. 16.º, n.º 2 do CT, entende que não é pela simples circunstância de os intervenientes se referirem a aspectos da empresa que a comunicação assume desde logo natureza profissional, bem como não é o facto de os meios informáticos pertencerem ao empregador que afasta a natureza privada da mensagem e legitima este a aceder ao seu conteúdo, nem o facto de o trabalhador não ter classificado a mensagem expressamente como "pessoal".

O único modo de sancionar o trabalhador seria no caso de a entidade empregadora ter proibido o uso do correio electrónico para fins pessoais, mas aí o que estaria em causa era a desobediência a uma ordem e não o conteúdo da mensagem que a entidade empregadora alegou, no caso julgado pelo Supremo Tribunal, ser difamatória de um superior hierárquico do trabalhador.

A destacar o facto de o Supremo, após ter retirado a consequência lógica ao facto de classificar a mensagem como pessoal, que foi a da nulidade da prova e consequente declaração da ilicitude do despedimento, ter condenado o empregador numa indemnização de € 5.000,00 para compensar a trabalhadora.

Para chegar a esta decisão final, o Supremo fundamentou-se na tutela legal e constitucional da confidencialidade da mensagem pessoal (arts. 34.º, n.º 1, 32.º, n.º 8 e 18.º da CRP, 194.º, n.ºs 2 e 3 do CP e 22.º do CT) e na doutrina, nomeadamente na opinião de Pedro Romano Martinez[150], Júlio Gomes[151], Joana Vasconcelos[152] e Amadeu Guerra[153] que defendem a confidencialidade do correio electrónico não profissional e que o controlo do email deve realizar-se de forma aleatória e não persecutória, tendo como finalidade a promoção da segurança do sistema e da sua performance. Defendem igualmente que a empresa deve ter uma política bem definida, em sede de regulamento interno, da utilização do correio electrónico, prevendo mecanismos para leitura do email em situações de ausência dos trabalhadores.

Páginas de internet consultadas

O Acórdão do Supremo Tribunal de Justiça, de 5 de Julho de 2007, relator Mário Pereira, embora se debruce sobre o carácter pessoal das mensagens de correio electrónico enviadas pelo trabalhador, refere, citando Pedro Romano Martinez, que no mesmo sentido, os sítios da internet que hajam sido consultados pelo trabalhador e as informações por ele recolhidas gozam da protecção do artigo 22.º do CT, pelo que o empregador não deve controlar os sítios da internet que hajam sido consultados pelos trabalhadores. Em regra, o controlo dos acessos à internet deve ser feito de forma não individualizada e global e não persecutória.

[150] "Código do Trabalho Anotado", 4ª Edição, Almedina, Coimbra, 2005, p. 116
[151] "Direito do Trabalho", I, op. cit., pp. 367-384.
[152] *O Contrato de Trabalho. 100 Questões*, Universidade Católica, 2004, pp. 91-93.
[153] *A privacidade no local de trabalho- as novas tecnologias e o controlo dos trabalhadores através de sistemas automatizados- uma abordagem ao código do trabalho*, Almedina, Coimbra, 2004, p. 392

A Jurisprudência francesa segue uma orientação muito semelhante à nossa considerando que o trabalhador tem direito, mesmo no tempo e local de trabalho, ao respeito da sua vida privada, o que implica em particular o segredo da correspondência, pelo que o empregador não pode tomar conhecimento das mensagens de correio electrónico enviadas ou recebidas pelo trabalhador, mesmo que este tenha interdito o uso pessoal do computador, como sucedeu no caso *Nikon*[154]. A Cour de cassation considera que uma mensagem enviada ou recebida num posto de trabalho colocado à disposição pelo empregador tem um carácter profissional, salvo se for identificado como "pessoal", no assunto da mensagem, por exemplo (Cour de cassation, 30 Maio 2007). Neste aspecto particular, difere da jurisprudência portuguesa que admite que mesmo que a mensagem não seja classificada como tal, o que releva é a vontade dos intervenientes da comunicação ao postularem, de forma expressa ou implícita, a natureza profissional ou privada das mensagens que trocam.

Em relação a ficheiros criados pelo trabalhador graças a uma ferramenta informática disponível para a execução do seu trabalho, a Cour de Cassation presume no seu arresto de 18 de Outubro de 2006 que são ficheiros profissionais, salvo se o empregado os identificar como pessoais, pelo que podem ser acedidos sem a presença do empregado (Cour de cassation, 18 octobre 2006).

Nas antípodas desta jurisprudência está a norte-americana porquanto esta distingue entre empregos públicos e privados sendo que apenas os primeiros estão sujeitos à Quarta Emenda e, mesmo nesses casos, os tribunais consideram que o direito de uma pessoa à privacidade apenas é violado quando a pessoa tem uma razoável expectativa de privacidade. A questão aqui é que, como Larry O. Natt Gant[155] refere, a colocação da tónica nas expectativas está mal posicionada porque os empregadores podem manipular as expectativas simplesmente modificando as condições de trabalho.

CNPD

Em documento aprovado a 29 de Outubro de 2002, na sessão plenária da CNPD, foram estabelecidos os princípios sobre a privacidade no local de trabalho quanto ao controlo do e-mail e do acesso à internet. Estabelece, como princípios genéricos, que qualquer tratamento de dados pessoais que recorra a meios total ou parcialmente automatizados, ou utilize ficheiros manuais estruturados, e que tenha como finalidade o controlo de trabalhadores – por mínimo que seja – está submetido às disposições da Lei 67/98, de 26 de Outubro e a entidade empregadora deve – *antes de iniciar qualquer tipo de tratamento* – informar o trabalhador sobre as condições de utilização dos meios da empresa para efeitos particulares ou do grau de tolerância admitido, sobre a existência de tratamento, suas finalidades, existência de controlo (formas e metodologias

[154] Acordão de 2 de Outubro de 2001 da Chambre sociale da Cour de Cassation. Decisões semelhantes e que invocam o caso "Nikon": Cour de Cassation, Chambre sociale, 12 octobre 2004

[155] "An affront to human dignity: electronic mail monitoring in…", op. cit.

adoptadas), sobre os dados tratados e o tempo de conservação, bem como sobre as consequências da má utilização ou utilização indevida dos meios de comunicação colocados à sua disposição. A CNPD também adopta como princípios de orientação que os dados a tratar e os meios utilizados devem ser ajustados à organização da empresa, ao desenvolvimento da actividade produtiva e ser compatíveis com os direitos e obrigações dos trabalhadores consignados na legislação de trabalho, correspondendo a um «interesse empresarial sério» que, utilizando os poderes de direcção e esperando a subordinação do trabalhador, não se revele abusivo e desproporcionado em relação ao grau de protecção da esfera privada do trabalhador.

Devem ser priveligiadas as metodologias genéricas de controlo, evitando a consulta individualizada de dados pessoais. Uma amostragem genérica (vg. quantidade de chamadas feitas por uma extensão, número de *e-mails* enviados, tempo gasto em consultas na *Internet*) pode ser suficiente para satisfazer os objectivos do controlo.

A CNPD também alerta para o facto de o acesso sistemático ao registo das comunicações electrónicas – para além de se poder revelar desproporcionado ao objectivo de controlo e atentar contra a dignidade do trabalhador – pode não se revelar eficaz e necessariamente produtivo, pelo "clima de angústia e tensão" que todos estes métodos podem criar no seio da empresa.

Especificamente, sobre a utilização e controlo do e-mail e Internet, a CNPD entende ser ilógico, irrealista e contraproducente que, no contexto da relação de trabalho, se proíba – de forma absoluta – a utilização do correio electrónico e o acesso à *Internet* para fins que não sejam estritamente profissionais, sendo desejável que esta autorize uma utilização moderada pelos seus trabalhadores, e aconselha a entidade empregadora a analisar todos os factores – a salvaguarda da liberdade de expressão e de informação, a formação, o livre desenvolvimento e iniciativa do trabalhador, a sua sensibilização para acesso às redes públicas, os custos para a empresa, as políticas de segurança, de privacidade e o grau de utilização destes meios, o tipo de actividade e grau de autonomia dos seus funcionários, bem como as suas necessidades concretas e pessoais – para definir regras claras e precisas em relação à utilização do correio electrónico e da *Internet* para fins privados, regras essas que devem assentar nos princípios da adequação, da proporcionalidade, da mútua colaboração e da confiança recíproca.

A CNPD entende que estas regras devem ser submetidas à consideração dos trabalhadores e dos seus órgãos representativos, sendo claramente publicitadas por forma a que seja assegurada uma informação clara sobre o grau de tolerância, o tipo de controlo efectuado e, mesmo, sobre as consequências do incumprimento daquelas determinações

O administrador de sistema está vinculado à obrigação de segredo profissional, não podendo revelar a terceiros os dados privados dos trabalhadores de que tenha tomado conhecimento em consequência das acções de monitorização dos seus postos de trabalho.

É de notar que a notificação à CNPD é dispensada quando a entidade empregadora não faz qualquer tipo de controlo dos trabalhadores em sede de uso da internet, permitindo a utilização do *e-mail* para fins privados e não estabelecendo limitações à utilização da Internet.

Em relação à forma como vão ser exercidos os poderes de controlo sobre o email do trabalhador, a CNPD entende que deve ser levado em conta o grau de autonomia do trabalhador e a natureza da actividade desenvolvida, bem como as razões que levaram à atribuição de um *e-mail* ao trabalhador. Por outro lado, o segredo profissional específico que impende sobre o empregado (*vg.* sigilo médico ou segredo das fontes) deve ser preservado.

Na mesma linha da nossa jurisprudência e doutrina, a CNPD entende que as razões determinantes da entrada na caixa postal dos empregados, com fundamento em ausência prolongada (férias, doença), devem ser claramente explicitadas e do seu conhecimento prévio.

A CNPD adopta como princípios que o controlo dos *e-mails* – a realizar de forma aleatória e não persecutória – deve ter em vista, essencialmente, garantir a segurança do sistema e a sua performance e que a necessidade de detecção de vírus não justifica, só por si, a leitura dos *emails* recebidos.

A CNPD fornece orientações preciosas quanto ao modo como a entidade empregadora deve proceder neste campo e indica que à constatação da utilização desproporcionada do email – que será comparada com a natureza e tipo de actividade desenvolvida – deve seguir-se um aviso do trabalhador e, se possível, o controlo através de outros meios alternativos e menos intrusivos. Eventuais controlos fundamentados na prevenção ou detecção da divulgação de segredos comerciais deve ser direccionado, exclusivamente, para as pessoas que têm acesso a esses segredos e apenas quando existam fundadas suspeitas. O acesso ao *e-mail* deverá ser o último recurso a utilizar pela entidade empregadora, sendo desejável que esse acesso seja feito na presença do trabalhador visado e, de preferência, na presença de um representante da comissão de trabalhadores. O acesso deve *limitar-se à visualização dos endereços dos destinatários, o assunto, a data e hora do envio*, podendo o trabalhador – se for o caso – especificar a existência de alguns *e-mails* de natureza privada e que não pretende que sejam lidos pela entidade empregadora. Perante tal situação a entidade empregadora deve abster-se de consultar o conteúdo do *e-mail*, em face da oposição do trabalhador.

Quanto ao controlo da internet, entende a CNPD que o controlo dos acessos à *Internet* – a ser decidido – deve ser feito de forma não individualizada, e global, em relação a todos os acessos na empresa, com referência ao tempo de conexão na empresa. A realização de estudos estatísticos pode ser suficiente para a entidade empregadora se poder aperceber do grau de utilização da *Internet* no local de trabalho e em que medida o acesso compromete a dedicação às tarefas profissionais ou a produtividade. Perante a verificação de acessos excessivos e desproporcionados deste meio de comunicação deve seguir-se um aviso do trabalhador em relação ao grau de utilização.

O controlo em relação ao tempo de acesso diário e aos sítios consultados por cada trabalhador só deverá ser realizado em circunstâncias excepcionais, nomeadamente

quando, no contexto da sua advertência, o trabalhador duvidar das indicações da empresa e quiser conferir a realização de tais acessos. Em particular, poderá ser necessário verificar as horas de conexão (início e fim) para comprovar que o acesso para fins privados ocorreu fora do horário de trabalho.

Combinações possíveis: a perspectiva global

A nossa lei explica de que modo o empregador pode utilizar os meios de vigilância à distância (art. 21.º CT), e tutela a reserva das comunicações e das telecomunicações privadas (art. 22.º CT) mas sempre numa perspectiva estanque e nunca integrada.

No entanto, se pensarmos bem, a combinação de todas estas tecnologias fazem com que o trabalhador se sinta permanentemente vigiado. No próprio Código de Boas Práticas da UNI, a propósito da IDRF, é referido que os dados recolhidos não devem ser interligados com os dados resultantes de outras tecnologias de monitorização como, por exemplo, o GPS, a monitorização do uso da internet ou a videovigilância.

Longe de as novas tecnologias ajudarem a libertar o potencial humano e a construir uma "sociedade de conhecimento", parece que são usadas para reduzir o potencial para acções e pensamentos independentes no local de trabalho.

E que consequências tem o uso generalizado de todos estes meios tecnológicos de controlo do trabalhador, em simultâneo?

a) Alteração nas relações entre trabalhadores e superiores hierárquicos/empregadores: estes já não precisam de falar e interagir com os trabalhadores para saber como está a correr o trabalho em termos de produtividade, tempos gastos nas tarefas, controle do absentismo, etc. A qualquer momento imprimem um relatório completo com a informação dos trabalhadores que estão presentes, horas de entrada, saídas, intervalos, pausas, refeições, tempos médios na realização da actividade (ex.: tempo médio de uma chamada em actividades de call center). Os empregadores já não conversam com os seus trabalhadores, só os monitorizam. Os trabalhadores sentem-se usados, tratados como números e não como pessoas. A desumanização no local de trabalho é inevitável e este já não é encarado mais como fonte de crescimento e de relacionamento social.

b) Alteração no peso dos critérios de avaliação do trabalhador: dada a facilidade com que se consegue vigiar tudo o que o trabalhador faz, a performance do trabalhador é analisada com base em critérios quantitativos: número e tempo de pausas, número de mails enviados, número de chamadas atendidas, tempo médio de deslocação de um armazém para outro, etc. Por muito que se diga que a qualidade é essencial, a avaliação é feita essencialmente com base na quantidade. Cientes disso, a atenção dos trabalhadores centra-se

precisamente nesses objectivos e não no cliente ou na qualidade do produto. Os escritórios modernos estão a tornar-se "electronic Sweatshops"[156].

c) A linha que separa o poder de controlo da entidade empregadora e a vida privada torna-se mais fluida: o trabalhador é vigiado pela máquina a todo o momento e a vigilância automática não distingue entre o que pode ver, e que respeita à actividade do trabalhador, e os outros aspectos da sua vida privada que não deveriam ficar registados: uma conversa entre colegas numa pausa pode ser escutada ou ficar gravada nas câmaras de vídeo, o empregador pode saber que um trabalhador anda a contactar via email com um sindicato, a consulta das páginas consultadas pelo trabalhador permitem saber quem faz parte da sua rede de amigos, etc. Mesmo quando sai do trabalho, leva consigo o cartão de identificação com o dispositivo IDRF, o portátil da empresa ou o telemóvel com o localizador GPS ou conduz a viatura da entidade empregadora que tem instalado um geolocalizador.

d) Grupos de trabalhadores específicos são mais sujeitos à "pervasive surveillance", isto é, a uma vigilância em que tudo o que o trabalhador faz é analisado e verificado[157]. Como a OIT apontou no seu relatório sobre monitorização no trabalho, há trabalhadores mais afectados: mulheres, imigrantes, estudantes e trabalhadores com baixos salários.

e) Efeitos na saúde física e mental dos trabalhadores: há boas razões para acreditar que uma monitorização sem limites seja contraproducente. Um possível impacto negativo na saúde física e mental dos trabalhadores pode contrariar os supostos benefícios do aumento da eficiência como resultado da monitorização. Os efeitos psicológicos incluem ansiedade, depressão, agressividade, irritabilidade com consequências inevitáveis no desempenho do trabalho e levando a um maior absentismo. Foi conduzido um estudo conjunto entre a Universidade do Wisconsin e a Communications Workers of America sobre monitorização electrónica e stress no trabalho que confirmou que a primeira introduz um factor de stress importante no local de trabalho e que está ligado, em parte, à sensação de impotência que os trabalhadores sentem. O stress também foi identificado como uma fonte importante de preocupação nos call centers[158].

Outras preocupações apontadas têm a ver com os efeitos ainda desconhecidos da radiações electro-magnéticas dos telemóveis bem como os riscos potenciais do uso de implantes IDRF, sendo que esta última

---

[156] GANTT, Larry O. Natt, "An affront to human dignity: electronic mail monitoring in…", op. cit., p. 345, nota 5.

[157] GMB, "GMB Congress Demands End To Electronic Tagging Of Workers "Battery Farm" Workplaces", GMB@work (6 Junho 2005) in http://www.gmb.org.uk/Templates/PressItems.asp?NodeID=91861 [Consult. 28 Junho 2009]

[158] SELMA VENCO, *Tempos moderníssimos nas engrenagens…, op. cit*., pp. 169-176 e 209-220

preocupação não se coloca em Portugal porquanto os implantes não são permitidos.

f) Enfraquecimento da representação colectiva dos trabalhadores: os sindicatos crêem que a vigilância no local de trabalho e a monitorização podem ser usados para desencorajar uma efectiva representação colectiva; por outro lado, quanto mais controlado for o dia de trabalho, menores hipóteses há de serem estabelecidas ligações informais entre o trabalhador e os seus representantes.

g) Colocação em causa da dignidade do trabalhador: tal como é referido no relatório elaborado pelo GT 29 sobre a vigilância das comunicações electrónicas no local de trabalho: "Os trabalhadores não abandonam o seu direito à privacidade e à protecção dos dados pessoais todas a manhãs ao entrarem no local de trabalho". De facto, a privacidade tornou-se cada vez mais importante dado que se têm esbatido as fronteiras entre tempo de trabalho e tempo pessoal, dado o desenvolvimento do teletrabalho e das modalidades de contratos de trabalho com horários flexíveis.

A recolha de dados sobre os trabalhadores através dos meios de vigilância à distância não é uma mera questão técnica ligada à protecção de dados. O que aqui está em causa são questões de direitos humanos fundamentais. No fundo, o que estamos a tratar é da dignidade humana.

O art. 20.º do Código do Trabalho

Qual o âmbito de aplicação deste artigo?

O Artigo 20.º, com a epígrafe "Meios de vigilância a distância" dispõe no seu n.º 1 que "O empregador não pode utilizar meios de vigilância a distância no local de trabalho, mediante o emprego de equipamento tecnológico, com a finalidade de controlar o desempenho profissional do trabalhador."

Dentro do âmbito de aplicação deste artigo está, desde logo, a videovigilância, quer seja unicamente com captação de imagem, quer captando imagem e som, como se retira claramente da letra do art. 20.º, n.º 3 do CT.

Fora do âmbito do art 20.º CT ficam desde logo a monitorização do conteúdo do email bem como as escutas telefónicas porque o princípio constitucional da inviolabilidade da correspondência e telecomunicações tem carácter absoluto e as únicas excepções prendem-se com exigências de investigação criminal (art. 34.º, n.º 1 e 4 da CRP). Por outro lado, o próprio art. 22.º do CT vem especificamente regular essas situações esclarecendo que o empregador não pode consultar as comunicações pessoais do trabalhador, embora possa estabelecer regras de utilização dos meios de comunicação na empresa, nomeadamente do correio electrónico.

Com esta primeira delimitação do âmbito do art. 20.º CT podemos desde já concluir que existem meios tecnológicos que não podem ser utilizados para vigilância pela entidade empregadora por força da própria Constituição. O uso que a entidade empregadora pode fazer da monitorização do uso do email e da internet bem como o controlo do uso do telefone estão reduzidos a níveis tais que, embora pudessem tecnicamente ser utilizados como meios de vigilância à distância no local de trabalho, a nossa Constituição não o permite sequer. Questão diferente é a necessidade de se passarem, para o plano legislativo comum, estas restrições ao poder de controlo da entidade empregadora que, neste momento, apenas estão a ser delineadas pelo labor da CNPD mas cujas orientações não são vinculativas para a entidade empregadora e, embora tenham o seu peso argumentativo quando invocadas nos tribunais, não são um escudo defensor do trabalhador no seu dia-a-dia. A Constituição protege o trabalhador, os direitos fundamentais podem ser invocados no local de trabalho mas a segurança jurídica também é um valor muito importante e, sem saber no plano concreto "as linhas com que se cose", o trabalhador facilmente se calará e deixará que o atropelem na sua

dignidade. Como refere Carlos Aurélio Mota de Souza[159] "*a Segurança objetiva das leis dá ao cidadão a Certeza subjetiva das ações justas, segundo o Direito".*

A geolocalização e a radiofrequência podem integrar o âmbito de aplicação do art. 20.º do CT?

O STJ, na decisão de 22 de Maio de 2007, entendeu que a remissão do n.º 3 do art 20.º do CT para o art. 29.º da LECT que estabelecia que "Nos casos previstos no número anterior o empregador informa o trabalhador sobre a existência e finalidade dos meios de vigilância utilizados, devendo nomeadamente afixar nos locais sujeitos os seguintes dizeres, consoante os casos: «Este local encontra-se sob vigilância de um circuito fechado de televisão» ou «Este local encontra-se sob vigilância de um circuito fechado de televisão, procedendo -se à gravação de imagem e som», seguido de símbolo identificativo" aponta no sentido de que a proibição de utilização de meios de vigilância a distância para controlo do desempenho profissional do trabalhador refere-se aos meios tecnológicos de vigilância com capacidade para procederem à gravação de imagem ou de imagem e som. O argumento do elemento sistemático, utilizado pelo STJ, quer queiramos quer não, saiu reforçado na nova redacção do Código do Trabalho dado que agora é o próprio n.º 3 do art. 20.º do CT que estipula essa norma.

O outro argumento do Supremo é baseado no elemento teleológico da interpretação dado que "o artigo 20.º do Código do Trabalho proíbe o emprego de meios de vigilância a distância no local de trabalho, «com a finalidade de controlar o desempenho profissional do trabalhador» (*elemento teleológico*), isto é, aqueles que «podem alcançar o que se faz, quando e durante quanto tempo» (na feliz expressão de REGINA REDINHA, «Os Direitos de Personalidade no Código do Trabalho: Actualidade e Oportunidade da sua Inclusão», em *A Reforma do Código do Trabalho*, Coimbra Editora, Coimbra, 2004, p. 166)."

Sobre isto oferece-se-nos dizer o seguinte:

_ A forma de vigilância de pessoas e bens que existe na lei consiste na contratação de vigilantes e/ou na colocação de sistemas de vídeo com gravação de imagem ou som e imagem. Assim o previa o Decreto-Lei n.º 231/98, de 22 de Julho, que regulava o exercício da actividade de segurança privada[160] e o Decreto-Lei n.º

[159] Apud MAURO NICOLAU JUNIOR, "Segurança Jurídica e Certeza do Direito: realidade ou utopia num Estado Democrático de Direito*",* Universo Jurídico in http://www.universojuridico.com.br/publicacoes/doutrinas/1868/SEGURANCA_JURIDICA_E_CERTEZA_DO_DIREITO_REALIDADE_OU_UTOPIA_NUM_ESTADO_DEMOCRATICO_DE_DIREITO [Consult. 28 Junho 2009]

[160] Este diploma permitia a adopção de *sistemas de videovigilância* no âmbito do exercício da actividade de segurança privada, os quais podiam estar a cargo de empresas privadas (art. 1.º n.º 3 al. a) ou de serviços de «autoprotecção com vista à protecção de pessoas e bens, bem como à prevenção da prática de crimes» (art. 1.º n.º 3 al. b). Este diploma determinou a obrigatoriedade de adopção destes sistemas para o Banco de Portugal, instituições de crédito e sociedades financeiras (art. 5.º n.º 1), bem como, nomeadamente, para os estabelecimentos de restauração e bebidas que disponham de salas destinadas a dança (cf. n.º 1 da Portaria n.º 26/99, de 16 de Janeiro). As disposições específicas de segurança para as

168/97, de 4 de Julho, e, subsequentemente, o DL n.º 35/2004, de 21 de Fevereiro, aplicável à utilização destes meios por parte das empresas que exercem *actividade no âmbito da segurança privada*. Outras leis existem que obrigam à colocação de sistemas de videovigilância: a Lei 38/98, de 4 de Agosto, obrigou os organizadores de competições desportivas a dotarem os seus recintos de sistemas de videovigilância; o DL 139/2002, de 17 de Maio, obriga os estabelecimentos de fabrico e armazenagem de produtos explosivos a "estarem protegidos por um sistema de vigilância permanente que assegure a detecção de intrusos", admitindo que uma das opções de controlo possa passar pela adopção de um "sistema de videovigilância instalado nos termos da lei geral" (artigo 22.º n.º 2 e 3 alínea b).

A partir daqui podemos ver que a legislação que funcionou como inspiradora do art. 20.º do CT adopta a videovigilância como meio essencial na protecção de pessoas e bens sendo que, inclusivamente, os dizeres que são colocados ao abrigo do n.º 3 do art. 20.º do CT são os que já constavam do art. 12.º n.º 3 do DL 231/98. Ou seja, estamos em crer que este enquadramento "sistemático" tem a ver mais com uma justificação de carácter histórico, com base nas leis a que este artigo foi buscar as suas raízes, e que são as leis que já regiam matéria semelhante e que também elas pretendem proteger "pessoas e bens".

_ Actualmente já se começa a regulamentar o recurso à geolocalização e, particularmente, à radiofrequência pelas entidades públicas e, nessa sede, estes meios electrónicos são encarados como meios de vigilância à distância ou meios que encerram esse perigo. Basta pensarmos na "pulseira electrónica"[161] que não é mais do que um sistema baseado na radiofrequência e que visa a monitorização telemática posicional do arguido, isto é, a vigilância de determinada pessoa em local previamente definido. Este meio de vigilância electrónica à distância permite controlar se o arguido sai ou entra na habitação e apenas é colocado com o consentimento do arguido e dos que coabitam com ele. Também o "chip na matricula" recorre à tecnologia da radiofrequência[162] e, embora o objectivo não seja a vigilância à distância dos cidadãos e do local onde se encontram, existe esse perigo. Como refere o Presidente da CNPD, Luís Silveira[163]: «Não se pode usar tecnologia que permita a qualquer momento que essas tais entidades passem a conhecer em que ponto do país se encontram todos os veículos. Seria uma medida

instituições de crédito constavam do Decreto-Lei n.º 298/79, de 17 de Agosto, entretanto revogado pelo DL 35/2004, de 21 de Fevereiro.

[161] Esta é a designação que comummente se dá à vigilância electrónica e que não é mais do que um conjunto de meios de controlo e fiscalização à distância que desde 2002 está ao dispor da justiça portuguesa para fiscalizar a medida de coacção de Obrigação de Permanência na Habitação, regulada pela Lei 122/99, de 20 de Agosto.

[162]A este propósito leia-se a notícia da autoria de FILIPE CAETANO, "Chips nas matrículas: dúvidas e petição na internet", IOL Diário (29/08/2008) in http://diario.iol.pt/tecnologia/matriculas-chip-rfid-e-matricula-dados/986132-4069.html [Consult. 28 Junho 2009] que diz: "Com a autorização legislativa surgiu uma outra dúvida sobre a natureza do chip, se seria de monitorização por satélite ou local. O Governo explicou que seria local, colocando de parte o GPS e abrindo portas ao RFID (Radio-Frequency IDentification)."

163 Entrevista dada pelo Presidente da CNPD à TSF no dia 16 de Julho de 2008 "Proposta de lei sobre instalação de chips electrónicos nas matrículas dos veículos debatida no Parlamento" in http://tsf.sapo.pt/PaginaInicial/Portugal/Interior.aspx?content_id=968536 [Consult. 28 Junho 2009]

desproporcionada». A CNPD pronunciou-se sobre esta matéria e sublinha que a «detecção e identificação electrónica dos veículos não pode transformar-se numa forma sofisticada de vigilância física, que cai fora dos fins permitidos pela lei e contraria o direito à privacidade dos condutores dos veículos»[164]. Ou seja, a radiofrequência e a geolocalização são tratados pela legislação mais recente como meios de vigilância à distância e que encerram perigos de violação da privacidade do cidadão pelo "simples" facto de se poder saber onde este está num dado momento do tempo.

_ O elemento teleológico da norma é a proibição do emprego de meios de vigilância a distância no local de trabalho, «com a finalidade de controlar o desempenho profissional do trabalhador» sob pena de se violar o direito à reserva da vida privada do trabalhador. Não se trata apenas do direito à imagem, que justificaria que o âmbito da norma ficasse restrito à videovigilância, mas de proteger a própria dignidade do trabalhador dado que o poder legítimo de controlo do empregador não justifica uma vigilância permanente e contínua sobre toda a actividade do trabalhador.

_ A geolocalização e a radiofrequência levantam questões relacionadas com a reserva da intimidade da vida privada do trabalhador porque também podem alcançar o que se faz, quando e durante quanto tempo. Basta pensarmos no caso de um trabalhador que está autorizado a utilizar a viatura de serviço para fins pessoais e que, se mantiver sempre o localizador GPS ligado, o empregador pode traçar o percurso completo deste e locais de paragem. Ora, o direito à reserva da intimidade da vida privada inclui o "direito a passar desapercebido por este mundo" e afecta a própria liberdade de deslocação do trabalhador que, ao saber-se vigiado, pode sentir-se condicionado nas suas deslocações pessoais. Estes meios de vigilância à distância no local de trabalho permitem o mesmo tipo de controlo que a videovigilância, podendo inclusivamente ser mais intrusivos na privacidade do trabalhador.

_ Também a geolocalização e a radiofrequência podem ser utilizadas com o objectivo da "protecção de pessoas e bens" e nunca para controlar o desempenho profissional do trabalhador porquanto também a sua utilização nesses termos comprime o direito à reserva da vida privada do trabalhador.

_ No local de trabalho, a geolocalização e a radiofrequência são sistemas eficazes de protecção de pessoas e bens, basta pensarmos no uso de identificadores de radiofrequência em trabalhadores das minas ou nos badges que condicionam o acesso a áreas do local de trabalho bem como nos GPS localizados nas viaturas que permitem identificar a localização das mesmas, nomeadamente em caso de roubo.

_ A CNPD na sua Autorização N.º 857/2005 refere, a propósito da instalação por uma empresa de um sistema de geolocalização na viatura do funcionário para protecção pessoal que: "As informações captadas por GPS afiguram-se verdadeiros tratamentos de dados pessoais quando se identifica ou torna identificável um titular, pessoa singular.

[164] Cit. da notícia "Chips nas matrículas não garantem privacidade dos condutores" publicada na edição de 27 de Novembro de 2008 do IOL Diário http://diario.iol.pt/sociedade/chips-matriculas-privacidade-proteccao-de-dados-parecer-automoveis/1018072-4071.html [Consult. 28 Junho 2009]

(…) Nos tratamentos de dados pessoais com esta natureza deve tomar-se em consideração o artigo 20.º do Código do Trabalho."

_ A CNPD, a propósito da radiofrequência, emitiu a Deliberação n.º 9/2004 onde determina que sempre que o recurso à tecnologia de IDRF implica a interconexão com informação de carácter pessoal se está em presença de um tratamento de dados pessoais (nos termos da alínea b) do artigo 3.º da Lei 67/98 de 26 de Outubro).

_ Tendo em conta as novas tecnologias que estão constantemente a aparecer e as potencialidades das mesmas, tem de ser feita uma interpretação actualista deste artigo 20.º CT de modo a que este abranja todos os meios de vigilância à distância no local de trabalho que recorram a equipamento tecnológico quando esses meios entram em conflito com a reserva da vida privada do trabalhador e, em última instância com a sua dignidade.

Uma última nota, a geolocalização e a radiofrequência são instrumentos tecnológicos que podem ser utilizados como meios de vigilância à distância no local de trabalho. Quero com isto dizer que apenas recaem no âmbito de protecção do art. 20.º CT quando existe um tratamento de dados pessoais associado porque só essa combinação dá azo a que possa haver uma violação da reserva da intimidade da vida privada do trabalhador e, por outro lado, a possibilidade de se controlar o seu desempenho profissional, proibida pelo artigo 20.º CT. Aliás, é precisamente esse tratamento de dados pessoais que justifica que, nos termos do art. 21.º, n.º 1 do CT, seja solicitada a autorização da instalação desses meios à CNPD.

Perspectivas de evolução: uma análise crítica do art. 20.º Código do Trabalho

Todos os meios de vigilância à distância no local de trabalho têm de ser necessariamente regulados por lei. Não são os trabalhadores que vão ditar os limites da sua subordinação ou o empregador os limites do seu poder de controlo num campo em que, por um lado, nem os trabalhadores estão conscientes do poder de intrusão destas tecnologias e por outro lado, os empregadores consideram-se plenamente legitimados a controlar a actividade do trabalhador pela posse que têm sobre os instrumentos de trabalho.

O art. 20.º fica aquém do que seria desejável nessa regulação dos meios de vigilância à distância no local de trabalho. Por um lado, porque é interpretado comummente como limitando apenas a videovigilância exercida pela entidade patronal e, por uma questão de segurança jurídica, deveria referir expressamente que é aplicável, com as necessárias adaptações, a todos os meios electrónicos que se possam revelar susceptíveis de realizar uma vigilância à distância no local de trabalho. É necessária maior clareza e rigor na redacção e interpretação deste artigo sob pena de ficar ao critério do empregador, salvo nas situações de videovigilância que estão expressamente previstas, o que se entende por meios de vigilância à distância no local de trabalho. Na prática, a indefinição leva à auto-compressão dos direitos fundamentais do trabalhador e não à auto-limitação do poder de controlo da entidade empregadora.

Além do mais, o art. 20.º, ainda que referisse a geolocalização e a radiofrequência, ou ainda que se considere aplicável a estas tecnologias quando são utilizadas no local de trabalho sempre que exista um tratamento de dados pessoais associado, deveria apresentar outros parâmetros legais para admitir a introdução dos meios de vigilância à distância no local de trabalho. Estamos a falar de adicionar, na análise do critério da proporcionalidade, nomeadamente na sua vertente de necessidade, o facto de terem de ser obrigatoriamente ponderados e declarados o número de meios de vigilância à distância já existentes no estabelecimento ou em relação aos trabalhadores que fossem afectados pela medida. Outra medida importante, seria a de proibir a interligação entre os dados produzidos pelos vários meios de vigilância à distância que fossem utilizados no local de trabalho.

Outra medida legislativa a incluir seria a de se enviar à CNPD, juntamente com o pedido de autorização, para além do parecer da comissão de trabalhadores sobre a instalação em concreto daquele meio de vigilância à distância como já é feito, enviar também a cópia do projecto do regulamento interno. O regulamento interno enviado deveria conter: a explicitação sobre os termos em que vão ser instalados esses meios; os fins para os quais podem ser utilizados; a explicação do modo pode através do qual pode ser exercido o direito de acesso aos dados pelos trabalhadores bem como informando que estes têm o direito de exigir a rectificação dos dados; uma clausula a referir que "não podem ser utilizados para controlo do desempenho profissional do trabalhador". Desse projecto de regulamento seria também dado conhecimento prévio aos trabalhadores, juntamente como a informação de que se pretende instalar determinado meio de vigilância à distância e de que vai seguir pedido de autorização para a CNPD sendo que estes se poderiam pronunciar sobre o que achassem pertinente junto da entidade empregadora e/ou da CNPD. Estamos em crer, inclusivamente, que a obrigatoriedade de enviar cópia do projecto do regulamento interno para a CNPD deveria existir em todas as situações de tratamento de dados pessoais dos trabalhadores porque isso iria obrigar a entidade empregadora a definir os termos em que poderia tratar esses dados bem como a deixar claras as situações das quais poderia resultar um procedimento disciplinar para o trabalhador. A clarificação destas situações é muito importante, sobretudo ao nível do uso da internet e do email pelo trabalhador. Os níveis de permissão do uso ficariam ao critério da entidade empregadora permitindo assim uma variação de critérios, consoante a estrutura organizativa da empresa e as suas políticas. Ou seja, não estamos a sugerir uma interferência no poder de controlo da entidade empregadora mas apenas uma clarificação dos termos em que esse poder pode ser exercido. O legislador comum não retiraria poder à entidade empregadora mas iria obrigá-la a traçar as fronteiras que entendesse, desde que dentro dos limites constitucionais estabelecidos.

Obviamente que, dado o volume de pedidos de autorização de tratamentos de dados pessoais que entram todos anos na CNPD, isso iria obrigá-la a ampliar o seu quadro organizativo, e de pessoal especializado na área laboral, mas essa questão não nos compete aqui analisar.

Esta sugestão prende-se com o facto de reconhecermos que o importante não é o consentimento do trabalhador, que está sempre numa posição de facto débil, mas sim assegurar que a informação chega até ele. Essa informação vai para além de um autocolante a indicar que estão a ser recolhidas imagens e compreende o conhecer os meios de controlo do empregador e quais os limites do seu poder disciplinar e das suas ordens, o que tem por reverso, saber quais as fronteiras da subordinação jurídica do trabalhador.

Não vai existir aqui uma duplicação, por um lado porque o trabalhador vai ter a oportunidade de se pronunciar e vai fazê-lo muito numa óptica individual, ao passo que a comissão de trabalhadores o faz também (ou deveria fazer) numa óptica de efeito da introdução do meio de vigilância à distância no ambiente laboral, na organização da empresa e questões relacionadas com a eventual necessidade de formação adequada. Por outro lado, sem desvalorizar o papel das comissões de trabalhadores, esse papel é importante quando existe e, como sabemos, não existem muitas empresas com uma estrutura de representação dos trabalhadores[165] pelo que o pedido de autorização é, na esmagadora maioria das vezes, acompanhado de uma simples declaração de inexistência da Comissão de Trabalhadores. O facto de se dar um conhecimento prévio aos trabalhadores através de um projecto de regulamento interno tem um efeito triplo: consciencializar a entidade empregadora de que estes meios podem afectar os direitos dos trabalhadores obrigando-a a definir fronteiras que, numa perspectiva de lealdade e boa fé no cumprimento do contrato, vão proteger ambas as partes, e tranquilizar os trabalhadores de que os seus direitos estão acautelados, e de que eles os podem defender, sem necessidade de entrar numa postura de resistência e ludismo, por último, suprir parcialmente a falta de um parecer da comissão de trabalhadores.

Todavia, reconhecemos que os níveis de intrusão na vida privada do trabalhador são diferentes consoante se trate de uma videovigilância, em que está em causa também o próprio direito à imagem do trabalhador, ou da instalação de um sistema de geolocalização ou de radiofrequência. Queremos com isto dizer que estes outros meios deveriam ter regulamentação própria dado que, hoje em dia, é perfeitamente legítimo e importante em termos de melhoria da competitividade empresarial que se possam utilizar meios de geolocalização ou de radiofrequência por questões organizativas, que não estão ligadas a motivos de protecção de pessoas e bens. Pensemos, por exemplo, numa empresa de reboques que tenha instalados esses dispositivos de localização permitindo assim destacar para um determinado acidente, o reboque que estiver localizado mais perto do local em causa. Sobre a questão da geolocalização seguimos de perto as orientações da CNIL sobre esta matéria[166] e pensamos que já é tempo de a legislação laboral esclarecer os termos da sua utilização sob pena de o trabalhador se sentir permanentemente vigiado.

[165] Conforme podemos ver pelos dados constantes do Livro Branco das Relações Laborais, p. 74, Quadro 29.
[166] "Guide de laGéolocalisation des…", op. cit.

É impossível pensarmos no artigo 20.º CT sem pensarmos no conflito entre o direito à reserva da intimidade da vida privada do trabalhador, o poder de controlo do empregador, o direito à autodeterminação informacional e à protecção dos dados pessoais dos trabalhadores. Mais do que isso, é impossível pensarmos nos meios de vigilância à distância no local de trabalho sem acreditarmos que eles existem na medida em que nos seja possível garantir a protecção da dignidade humana. Porque é ao homem que cabe escolher os limites dos tentáculos do "Big Brother" e pô-lo a funcionar na medida em que respeite os direitos de todos.

Os tribunais e o intérprete devem estar atentos às mudanças no mundo, em particular às mudanças recentes que ocorreram no seio da organização laboral com a introdução de novas tecnologias e as suas implicações nos direitos dos trabalhadores[167]. As novas tecnologias agudizam antigos conflitos e a leitura que se faz da lei deve acompanhar esses avanços, procurando resolver os conflitos de interesses latentes e tendo em conta, por um lado, que o direito não deve impedir a competição entre as empresas, competição essa que é feita com empresas que estão sedeadas noutros países, mas também deve assegurar os direitos dos trabalhadores perante a possibilidade de um controlo sem limites e violador da dignidade humana.

Duas últimas notas de reflexão, em tom de desafio, para temas em relação aos quais o conteúdo do artigo 20.º CT é importante.

Em primeiro lugar, para os prestadores de serviços. Quando o prestador utiliza instrumentos fornecidos pela entidade a quem presta serviços, ou quando presta os serviços nas instalações desta, pode a entidade a quem é prestado o serviço monitorizar o uso que este faz do computador, do telefone? E obrigá-lo a utilizar dispositivos de geolocalização na viatura ou dispositivos com radiofrequência associado a um tratamento de dados pessoais? Sabendo que em relação à videovigilância existe legislação própria, que vai determinar os termos em que esta pode ser instalada, quanto às restantes situações não existe legislação específica e o enquadramento é feito com base na LPDP. O desafio que aqui deixamos é para a necessidade de se pensar também esta problemática no âmbito dos chamados "falsos recibos verdes". Estes "trabalhadores de facto" estão mais desprotegidos que o comum dos trabalhadores. O tratamento ilegal de dados pessoais nestes casos poderia ser travado com uma legislação penal semelhante à francesa[168], que possibilita a responsabilização penal das pessoas colectivas que violem os direitos resultantes dos tratamentos de dados pessoais e que aplicam, entre outras sanções, o fecho do estabelecimento da empresa nos quais foram praticados os factos constitutivos do crime e a divulgação pública da decisão judicial.

Em segundo lugar, os voluntários que trabalham numa organização não governamental. Como tratar a questão dos meios de vigilância à distância no local onde se exerce o voluntariado? A aplicação do artigo 20.º do Código do Trabalho a estas situações não nos pareceria despropositada sendo que, inclusivamente, na legislação

[167] ANDREA STANCHI, "L'utilizzo della Radio Frequency Identification (Rfid) e le implicazioni...",
[168] Vide nossa página 23

australiana, no Workplace Surveillance Act 2005[169], prevê-se precisamente que as regras aí constantes sejam também aplicadas às pessoas que desempenhem trabalho voluntário.

Conclusões

1- A protecção da liberdade individual deve fazer-se, quer nas relações privadas, quer perante o Estado. A personalidade é um valor indivisível e a sua tutela é um dever que resulta da nossa Constituição dado que na sua base está o princípio da dignidade humana. "Proteger a dignidade do ser humano é possivelmente a mais nobre função do Direito"[170].

A eficácia horizontal dos direitos fundamentais ao nível da relação laboral aparece como uma exigência natural, em virtude de estarmos perante relações em que uma das partes tem um poder económico ou social de facto, o que faz com que a outra parte seja um contraente débil.

Para os defensores da teoria da eficácia directa os direitos fundamentais aplicam-se sem necessidade de interposição legislativa ao passo que para os defensores da eficácia indirecta os direitos fundamentais funcionam como princípios influenciadores da interpretação das cláusulas gerais de direito privado.

Na prática, acabam por não haver grandes diferenças entre estas teorias acabando todas por aplicar as regras dos conflitos de direitos, nomeadamente, os princípios da necessidade, da adequação e da proporcionalidade para delimitar a eficácia dos direitos fundamentais em cada caso concreto.

2- O direito à reserva da intimidade da vida privada é um dos direitos mais importantes do homem. O conceito de vida privada é um conceito aberto onde estão em causa aspectos que se prendem com as experiências, lutas e paixões pessoais de cada um e que não devem, enquanto tal, ser objecto da curiosidade do público.

Também no local de trabalho o trabalhador mantém os seus direitos de cidadão e, embora veja a sua esfera privada limitada, esta não fica confinada às casas de banho e cacifos abrangendo aspectos como as conversas pessoais com os seus companheiros de trabalho, a actividade sindical destes, o rendimento auferido, o seu estado de saúde.

---

[169] Disponível in http://www.austlii.edu.au/au/legis/nsw/consol_act/wsa2005245/ [Consult. 28 Junho 2009]

[170] Frase de MAURO NICOLAU JUNIOR, "Segurança Jurídica e Certeza do Direito: …", *op. cit.*

Com os novos desenvolvimentos tecnológicos, sobretudo ao nível da informática, surge também um novo direito fundamental: o direito à autodeterminação informacional. Este direito é mais abrangente que o direito à intimidade, é o direito a dispor de todas as informações sobre a sua pessoa e o bem protegido não é apenas o espaço defendido da curiosidade alheia mas também o direito em geral de personalidade, a identidade, o património moral da pessoa, que dá a possibilidade de exercer um controlo sobre a totalidade da pessoa.

3- O poder de controlo também tem também raízes constitucionais, dado que é instrumental para a realização da liberdade de empresa, livre iniciativa e organização empresarial. Para poder gerir a empresa e conformar a prestação laboral, o empregador tem o poder directivo para poder fixar os termos em que deve ser prestado o trabalho e o poder de fiscalizar a actividade do trabalhador.

A alteração do espaço em que as empresas trabalham, que é agora em grande parte um espaço cibernético, também alterou o lugar e a forma como se exerce o poder de controlo do empregador. A cibervigilância passa a ser uma necessidade porque é nesse espaço que se desenrola a actividade da empresa.

Um dos perigos da actual capacidade informática de recolha de dados é a de que se consiga saber tudo sobre o trabalhador, passando este a ser um *"trabalhador de vidro".*

As novas tecnologias permitem potenciar a criatividade e estimular a proactividade e autonomia do trabalhador ou podem conduzir à alienação do trabalhador, provocando a queda da sua produtividade.

A utilização de meios de vigilância à distância no local de trabalho pode levar à desumanização do trabalho, servindo-se o empregador das novas tecnologias para controlar todos os aspectos da actividade do trabalhador e todos os segundos do seu trabalho, não deixando qualquer margem para a sua autonomia.

4- Ao nível do Direito Internacional, é reconhecido o direito à vida privada, família, domicílio e correspondência, quer ao nível da Declaração Universal dos Direitos do Homem, que tem um importante significado simbólico-político no nosso Direito Constitucional, quer ao nível do Pacto Internacional sobre Direitos Civis e Políticos, bem como ao nível da Convenção Europeia dos Direitos do Homem, tendo o próprio Tribunal Europeu dos Direitos do Homem decidido que o respeito pela vida privada deve também englobar o direito de cada pessoa desenvolver relações com os seus semelhantes e por isso não vê razão para não ser aplicado também às actividades comerciais e laborais.

Notámos que as disposições de Direito Internacional específicas sobre a monitorização e vigilância no local de trabalho provêem de normas que não têm força obrigatória como é o caso da *Recolha de Directivas Práticas sobre a Protecção de*

Dados Pessoais dos trabalhadores, OIT, 7/10/96 e *da Recomendação R (89)2 do Comité de Ministros do Conselho da Europa.* É impossível unificar esta matéria mas os princípios gerais pelos quais se devem reger os vários países deveriam ser vinculativos. De destacar, em ambos os normativos, a recomendação do dever de informação e consulta prévia dos trabalhadores antes da introdução ou adaptação de sistemas automatizados de recolha de dados pessoais dos trabalhadores. Este princípio também se aplica à introdução ou adaptação de tecnologias destinadas a monitorizar os movimentos ou a produtividade dos empregados. No âmbito das recomendações da OIT, e em relação à monitorização oculta, estabelece-se que esta apenas deve ser permitida se estiver em conformidade com a legislação nacional ou se houver suspeitas fundadas de actividade criminosa ou outros delitos graves. Quanto à monitorização contínua, deve ser permitida somente se for necessária por questões de saúde, segurança ou de protecção da propriedade.

Sobre protecção de dados pessoais temos disposições específicas de Direito comunitário, como é a Carta de Direitos Fundamentais da União Europeia, que consagra o direito à protecção dos dados de carácter pessoal como um direito fundamental, e a Directiva n.º 95/46/CE, de 24 de Outubro relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, e que veio a ser determinante na elaboração das várias leis nacionais de protecção de dados pessoais. Princípios específicos em relação ao tratamento de dados pessoais dos trabalhadores não são estabelecidos e, seria importante deixar de lado neste campo a exigência do consentimento do titular dos dados pessoais e substituí-la explicitamente pelo conceito de dever de informação prévia e consulta aos trabalhadores.

Ao nível do direito comparado podemos distinguir, desde logo, três metodologias adoptadas para lidar com os meios de vigilância à distância no local de trabalho:

_ Proibição expressa da utilização de meios de vigilância à distância no local de trabalho, como é feita pelo artigo 20.º do CT e pelo artigo 4.º do SL.

_ Proibição da utilização de meios de vigilância à distância no local de trabalho resultante da interpretação que é feita pelos tribunais das disposições constitucionais, conjugadas com as normas de direito civil, laboral e de protecção de dados pessoais. Como sucede no caso do Direito Alemão, Espanhol e Francês.

_ Autorização para a introdução de meios de vigilância à distância no local de trabalho. Como acontece no direito anglo-saxónico. No Reino Unido, sem prejuízo de se respeitar a Directiva relativa à Protecção de Dados Pessoais, transposta através do *Data Protection Act 1998*, o empregador introduz com a amplitude que pretende os meios de vigilância no local de trabalho, sendo comummente aceites práticas como abertura do email do trabalhador, registo das chamadas telefónicas efectuadas e *keystroke monitoring*, desde que este leve a cabo previamente um adequado *impact assessment*. O mesmo sucede no Direito norte-americano, e até de modo mais ostensivo porque a única limitação à aplicação desses meios é a expectativa de privacidade dos trabalhadores e não o seu direito a essa privacidade. Desde que as empresas tenham uma

política clara quanto à utilização dos meios de vigilância à distância no local de trabalho, tudo lhes é permitido.

As normas constitucionais portuguesas tutelam a reserva da intimidade da vida privada, o sigilo das comunicações, determinam a nulidade das provas obtida com violação desse segredo e prescrevem o direito à autodeterminação informacional. As normas penais e que tutelam os dados pessoais têm âmbitos específicos, pelo que uma norma que viola o modo como devem ser tratados os dados pessoais, não configura necessariamente um ilícito penal. Do mesmo modo, a Lei de Protecção de Dados Pessoais não dá resposta às questões concretas que se colocam no âmbito laboral mas porque também não é esse o seu objectivo. Nenhuma LPDP, nem a própria Directiva que esteve na sua base, tutela a especial problemática dos trabalhadores, nomeadamente ao nível do papel das comissões de trabalhadores ou protegendo o trabalhador na questão do consentimento, requisito que deveria ser expressamente substituído por outros mais rigorosos que garantissem o efectivo conhecimento do trabalhador acerca das circunstâncias em que os seus dados pessoais são recolhidos. Caso não existisse o art. 20.º CT estamos convencidos que as orientações jurisprudenciais relativamente aos meios de vigilância à distância no local de trabalho poderiam ser muito semelhantes às da vizinha Espanha, o que teria as consequências apontadas por Goñi Sein, isto é, provocaria uma grande insegurança jurídica porquanto deixaria totalmente na mão dos empresários a decisão de adopção dos meios de vigilância à distância no local de trabalho e que teria como único limite o respeito da dignidade humana, conceito com um grande grau de indeterminação e que por isso não é garantia suficiente para evitar arbitrariedades. E isto apesar de existir no Direito Laboral português normas laborais genéricas nas quais podemos fundamentar o dever de informação prévia ao trabalhador (art. 106.º CT), o facto de o poder de direcção estar limitado pelo contrato e pelas normas que o regem (art 97.º CT) e a importância do dever de lealdade do trabalhador ou a obrigação de ambas as partes procederem de boa fé na execução do contrato.

O artigo 20.º CT está enquadrado na Subsecção II relativa aos Direitos de Personalidade do Trabalhador, depois de o legislador definir o que entende por contrato de trabalho e antes de entrar na regulação do poder de direcção e dos poderes e deveres da entidade empregadora e do trabalhador. Só na Subsecção IX é que o legislador passa para "O trabalhador e a empresa" começando logo, à cabeça, com a referência ao poder de direcção. Esta sistemática, quanto a nós, valoriza o homem, o cidadão, antes do trabalhador e do seu dever de subordinação jurídica podendo, e devendo, ser entendida como estabelecida com o intuito de passar uma mensagem de limitação ao poder de direcção do empregador e que transmite como ideia essencial que estes meios não podem ser utilizados para controlar o desempenho profissional do trabalhador.

O artigo 21.º do CT especifica as obrigações que resultam por parte da entidade patronal perante a CNPD, mas o único aspecto inovador refere-se à obrigatoriedade de juntar o parecer da comissão de trabalhadores aquando do pedido de autorização para a instalação de meios de vigilância à distância no local de trabalho, e isto sem prejuízo de defendermos que sempre que existe a introdução de novas tecnologias de vigilância no

local de trabalho, estas estão sujeitas a parecer da comissão de trabalhadores por força da Constituição e do que entendemos que deve fazer parte do regulamento interno, também ele sujeito a parecer da comissão de trabalhadores (art. 99.º, n.º 2 do CT). O parecer da comissão de trabalhadores, quando exista comissão de trabalhadores na empresa, é importante porque poderá alertar para alguma situação concreta que influencie os termos em que a autorização vai ser concedida pela CNPD, ou até recusada, e, se repararmos bem, é a única altura em que os trabalhadores têm acesso, através da informação que é enviada à comissão pela entidade empregadora, dos termos em que vão ser instalados os meios de vigilância à distância, prevenindo assim uma oposição "a posteriori" destes, muito mais complicada porque teria de seguir a via judicial.

5- Vigilância e monitorização são termos utilizados indistintamente e não encontramos uma clara distinção entre estes termos ao nível do Direito Comparado. Ou falamos em "monitorização e vigilância" ou só em "vigilância" mas as expressões significam o mesmo. A diferenciação legal ao nível do tratamento que lhes é dado está muitas vezes relacionada com os meios que são utilizados e o modo como estes permitem controlar o trabalhador: pela sua localização (tracking devices), como é o caso do gps e da identificação por radiofrequência, pela escuta dos telefonemas e conversas (tapping), pela visualização da imagem dos trabalhadores (camera surveillance) e pela informação sobre o que fazem no computador (computer surveillance).

No Direito Laboral português não encontramos qualquer referência à monitorização. Os termos em que pode ser efectuada a utilização dos meios de vigilância à distância é um limite ao poder de controlo do empregador, dado que este não pode utilizar estes meios para controlar o desempenho profissional do trabalhador (art. 20.º, n.º 1 CT) mas apenas por questões de protecção de pessoas e bens ou quando particulares exigências inerentes à actividade o justifiquem (art. 20.º, n.º 2 CT). Esta limitação ao poder de controlo encontra, por sua vez, justificação no princípio do respeito da reserva da intimidade da vida privada e, sobretudo, no respeito pela dignidade humana.

Entendemos como susceptíveis de se enquadrarem no conceito de meios de vigilância à distância no local de trabalho com recurso a equipamentos tecnológico: toda a vigilância, com recurso a equipamento tecnológico, que possibilita a observação de algum aspecto da vida do trabalhador no local de trabalho mediante um tratamento de dados pessoais e sendo tecnicamente possível utilizar esses meios de forma contínua ou oculta.

6- Para a videovigilância ser lícita, nos termos do art. 20.º do CT, a jurisprudência portuguesa analisa se estão preenchidos os seguintes requisitos:

- Informação ao trabalhador: a videovigilância só é admitida em circunstâncias excepcionais mas, quando o seja, ainda assim tem de ser cumprido o dever de informar o trabalhador e é necessário que sejam afixados nos locais sujeitos a vigilância os dizeres prescritos no n.º 3 do art. 20.º CT. Este dever de informação é essencial por uma questão de lealdade e boa fé nas relações laborais.

- Finalidade legítima: A licitude da videovigilância afere-se pela sua conformidade ao fim que a autorizou. Os tribunais analisam a questão da videovigilância sob a perspectiva da finalidade de protecção de pessoas e bens sendo que essa possibilidade se circunscreve a locais abertos ao público ou a espaços de acesso a pessoas estranhas à empresa, em que exista um razoável risco de ocorrência de delitos contra as pessoas ou contra o património e, mesmo nesses casos, têm de estar em causa bens de valor razoável, facilmente acessíveis a terceiros e em que exista o risco de cometimento de infracções graves. Quando tenham por finalidade controlar o desempenho profissional do trabalhador as gravações são ilícitas, ainda que tenham o consentimento do trabalhador.

- Proporcionalidade: A instalação de sistemas de videovigilância nos locais de trabalho envolve a restrição do direito de reserva da vida privada pelo que apenas poderá mostrar-se justificada quando for necessária à prossecução de interesses legítimos e dentro dos limites definidos pelo princípio da proporcionalidade. Este princípio da proporcionalidade comporta um triplo juízo prévio: a adequação do meio face à finalidade pretendida; a necessidade ou indispensabilidade do recurso à videovigilância; a proporcionalidade dos direitos sacrificados, privilegiando-se o princípio da intromissão mínima. Viola o princípio da proporcionalidade uma gravação ininterrupta bem como câmaras de vídeo instaladas no local de trabalho e direccionadas para os trabalhadores. A videovigilância deverá traduzir-se numa forma de vigilância genérica, destinada a detectar factos, situações ou acontecimentos incidentais, e não numa vigilância directamente dirigida aos postos de trabalho ou ao campo de acção dos trabalhadores, que configuraria uma típica medida de polícia.

Não se levanta a questão, em sede judicial, de saber se é proporcional o facto de a gravação vídeo ser feita também com som mas estamos em crer que essa questão é pertinente e dificilmente conseguimos enquadrar a admissibilidade da gravação vídeo com som no local de trabalho sem violar o princípio da proporcionalidade em sentido estrito.

- Autorização da CNPD: tem de haver uma autorização prévia e os termos em que essa autorização é emitida devem ser respeitados.

A videovigilância oculta no local de trabalho realizada pelo empregador não é admitida porque viola o artigo 20.º, n.ºs 1 e 3 do CT bem como o dever de lealdade e boa fé nas relações laborais. As provas obtidas nesses termos são consideradas nulas pelos nossos tribunais para efeitos de julgamento por despedimento com justa causa.

A nossa jurisprudência parece deixar alguma abertura para admitir situações de videovigilância oculta quando se trate de locais da empresa onde, em princípio, não existe qualquer posto de trabalho e onde os trabalhadores só se desloquem esporadicamente. Não existe nenhuma decisão em Portugal nesse sentido mas em França, a Cour de Cassation, já considerou que não existe o dever de informar os trabalhadores acerca da videovigilância quando se trate de instalações em que o acesso por estes esteja vedado, nem as entidades empregadoras têm de informar os trabalhadores dos procedimentos de segurança seguidos pelas suas empresas-clientes quando estas coloquem câmaras de vigilância em locais pelos quais os trabalhadores não devam exercer a sua actividade.

O facto de a videovigilância ter como finalidade a protecção de pessoas e bens, e não a de controlar o desempenho profissional do trabalhador, leva a que a videovigilância não possa ser usada em sede de procedimento disciplinar contra o trabalhador, mas sem que isso invalide todo o processado porque poderão existir outros meios de prova válidos. É essa a actual tendência de julgamento dos tribunais em sede laboral e com a qual concordamos. Admitimos que em situações graves do foro criminal e em que é impossível para a entidade empregadora manter a relação de confiança que está na base do contrato de trabalho, situações em que é claramente quebrado esse vínculo e em que a única prova, desde que lícita no âmbito penal, é a videovigilância, nessas situações em que há um claro conflito entre vários direitos constitucionais: a liberdade de prova e o direito de acção, por um lado, e a dignidade da pessoa humana, por outro lado, as gravações devem ser admissíveis sob pena de deixar sem efectiva tutela o direito de acção e os direitos fundamentais serem invocados em claro abuso de direito.

7- A identificação por radiofrequência (IDRF) é um sistema automático de identificação que possibilita a transmissão de dados recorrendo a marcas/identificadores (*tags*) portáteis para leitores com a capacidade de processar tais dados. No local de trabalho, os exemplos mais claros desta utilização são a utilização de *badges*, que tanto poderão consistir num cartão que o trabalhador deve utilizar enquanto está no local de trabalho, numa braçadeira que se coloca na farda ou até, estarem incorporados na própria farda. Este sistema, muito utilizado em armazéns, permite determinar a localização do trabalhador, saber quanto tempo demora de um local para o outro e distribuir rapidamente tarefas, levando a que todos os segundos do trabalhador sejam controlados removendo qualquer margem de decisão que lhe possa caber relativamente ao modo como executa o seu trabalho, retirando-lhe o direito que todo o ser humano tem de agir com autonomia e dignidade, bem como os traços da individualidade que o permitem distinguir-se dos outros trabalhadores, nomeadamente os traços que fazem dele um bom trabalhador.

Não existem normas laborais nem decisões judiciais que mencionem a identificação por radiofrequência. Esta temática é abordada no Código das Boas Práticas da OIT sobre os Dados Pessoais do Trabalhador, no seu capítulo sobre monitorização no trabalho, e que refere que os trabalhadores devem ser informados antecipadamente se estão a ser monitorizados, em que horário, que métodos e técnicas são usados e quais os dados recolhidos bem como a monitorização oculta deve ser permitida apenas se a legislação nacional o consentir ou se houver suspeita fundada da prática de actividade criminal e a monitorização contínua apenas deve ser autorizada por questões de saúde ou segurança ou para protecção da propriedade.

Na União Europeia as implicações da IDRF foram analisadas pelo GT 29 e constam de um documento publicado em Janeiro de 2005 com o nome de *Working document on data protection issues related to RFID technology*. O GT 29 concluiu que quando são armazenados dados pessoais nas etiquetas (*tags*) IDRF ou que quando estes são ligados com uma base de dados que contem dados pessoais, bem como quando as *tags* colocadas em items individuais possam ser usadas para identificar indivíduos

associados a eles, estamos perante um tratamento de dados pessoais que recai nas obrigações previstas na Directiva Europeia 95/46/CE sobre Protecção de Dados Pessoais e, por isso, o tratamento desses dados deve obedecer aos princípios da Directiva.

No plano sindical, a Union Network International, que congrega 20 milhões de associados de 900 sindicatos espalhados pelo mundo inteiro, elaborou em 2006 o *RFID in the workplace: UNI Code of Good Practice*, um projecto sem força jurídica obrigatória mas que serve como linha orientadora dos sindicatos associados da UNI na negociação com as entidades empregadoras e que tem como propósito garantir que a tecnologia IDRF é introduzida no local de trabalho de acordo com as orientações da OIT, incluindo o respectivo Código de Boas Práticas, e de acordo com os melhores princípios de protecção de dados pessoais e em respeito do direito humano fundamental à reserva da intimidade da vida privada.

8- Através da geolocalização conseguimos saber o exacto posicionamento de uma pessoa, a velocidade a que se desloca, onde pára e durante quanto tempo. Estes sistemas podem ser usados pelo trabalhador, colocados numa viatura ou estarem inseridos num telemóvel. O seu uso espalha-se rapidamente por todo o mundo sendo facilmente utilizado de forma oculta e muitas vezes, de forma contínua. A introdução do GPS permite ao empregador rever todas as decisões do trabalhador, rouba-lhe a autonomia e leva a que este seja tratado como um robot, e repare-se que estamos sobretudo a falar de profissões em que o trabalhador tinha uma maior liberdade de decisão, como era o caso das profissões que são exercidas fora das instalações da empresa. Isto leva a que o trabalhador deixe de se preocupar com a qualidade do seu trabalho e se concentre unicamente nos tempos que têm de ser cumpridos ao segundo. A pressão para aumentar a produtividade, minuciosamente analisada, aumenta o stress sobre o trabalhador com consequências na saúde do mesmo e, consequentemente, no absentismo. O facto de saber que está a ser vigiado todos os dias também pode colocar uma pressão insidiosa sobre o trabalhador, com efeitos adversos na sua saúde.

Segundo o nosso Supremo Tribunal de Justiça: "Não se pode qualificar o dispositivo de GPS instalado no veículo automóvel atribuído a um técnico de vendas como meio de vigilância a distância no local de trabalho, já que esse sistema não permite captar as circunstâncias, a duração e os resultados das visitas efectuadas aos seus clientes, nem identificar os respectivos intervenientes."A nosso ver, os meios de vigilância à distância no local de trabalho não têm de captar tudo o que o trabalhador faz para serem considerados como tal, é suficiente que captem uma importante parcela da actividade do trabalhador e, ao mesmo tempo, entrem na reserva da intimidade da sua vida privada. Assim tanto é que, uma câmara de vídeo colocada dentro da viatura, que capte a imagem mas não o som, também não conseguiria "captar as circunstâncias, a duração e os resultados das visitas efectuadas" aos seus clientes, nem identificar os respectivos intervenientes, uma vez que os encontros com os clientes não ocorrem dentro da viatura, e, no entanto, ninguém põe em dúvida de que se trata de um meio de vigilância à distância.

Posição diferente da do Supremo é a da CNPD, que considera que, quando uma empresa instala num veículo de um seu funcionário este sistema para protecção pessoal, a CNPD deve ser notificada referindo expressamente na sua Autorização N.º 857/2005 que: "As informações captadas por GPS afiguram-se verdadeiros tratamentos de dados pessoais quando se identifica ou torna identificável um titular, pessoa singular. (…) Nos tratamentos de dados pessoais com esta natureza deve tomar-se em consideração o artigo 20.º do Código do Trabalho."

Contributos importantes para o aperfeiçoamento legislativo nesta matéria são dados pela CNIL que distingue entre veículos de função e veículos de sociedade e, consoante as viaturas se insiram numa ou noutra categoria, o seu tratamento é diferente. O veículo de sociedade não pode em princípio ser utilizado por um empregado fora do seu horário de trabalho, estamos a falar de situações em que o veículo constitui ele mesmo objecto do trabalho do empregado, como é o caso de um motorista de pesados ou de passageiros. O veículo de função constitui uma vantagem atribuída ao trabalhador, uma remuneração em espécie. Atendendo a esta distinção, a CNIL recomenda que os dispositivos de geolocalização instalados em veículos de função possam ser desactivados quando o empregado não está a trabalhar de modo a que possa, assim, preservar a sua vida privada.

A cláusula do n.º1 do art. 20.º CT, que admite a utilização de meios de vigilância à distância quando particulares exigências inerentes à actividade o justifiquem, poderia ser aplicada com proveito a situações em que a utilização da geolocalização consubstancia um tratamento de dados pessoais e não é utilizada por razões de protecção de pessoas e bens. É o caso do empregador que recorre à geolocalização para uma melhor alocação dos meios disponíveis quando os serviços se façam em sítios diferentes, para fazer o seguimento e facturação de um serviço ou ainda o seguimento do tempo de trabalho, quando este seguimento não possa ser realizado por outros meios. Partilhamos da opinião da CNIL, isto é, a geolocalização não é justificada quando o empregado dispõe de liberdade na organização das suas deslocações e, mesmo que assim não seja, não deve conduzir a um controle permanente do trabalhador.

9- Quanto à admissibilidade das escutas telefónicas, a nossa jurisprudência é peremptória e unânime: o princípio da inviolabilidade da correspondência e das telecomunicações, consagrado no art. 34.º, n.º 1 da Constituição, tem carácter absoluto, não admitindo a lei qualquer outra excepção, sendo por isso ilícitas as violações que não tenham sido autorizadas para fins de investigação criminal, nos termos da lei. A este respeito, o Tribunal Constitucional considerou que o sigilo das telecomunicações abrange não só o conteúdo das telecomunicações, mas também o "tráfego" como tal (espécie, hora, duração, intensidade de utilização). A infracção à proibição constitucional de ingerências nas telecomunicações tem nos processos cíveis e em matéria de prova a mesma sanção radical prevista na Constituição em sede de garantias do processo criminal: a nulidade. Só assim se garante uma efectiva tutela da confidencialidade ou se minimizam os inconvenientes de uma sua violação, mormente se tal violação se repercutir em matérias ligadas a aspectos sancionatórios, como é o caso do processo disciplinar.

Quando as gravações telefónicas são autorizadas, nos termos da lei, seria importante obrigar a entidade empregadora a disponibilizar aos seus empregados linhas próprias para chamadas privadas ou que os telefones fossem munidos de uma funcionalidade que permitisse desactivar a gravação durante a chamada privada. Esta faculdade torna-se ainda mais importante no caso de trabalhadores que são simultaneamente representantes das comissões de trabalhadores ou dos sindicatos. A permissão para a gravação de chamadas não torna legal a gravação ininterrupta, isto é, a continuação da gravação mesmo quando o operador não está a receber nenhuma chamada, ficando gravadas as conversas com os colegas de trabalho.

10- Com a emergência das novas tecnologias de informação e comunicação (NTIC) e particularmente com a introdução da internet na empresa, verificou-se uma verdadeira migração das tecnologias de controlo da periferia para o coração do processo de trabalho propriamente dito. Para os trabalhadores, a diferença de natureza entre as NTIC e tudo o que as precede reside precisamente na capacidade desta nova tecnologia conservar todos os rastos deixados pelo trabalhador conectado constituindo uma verdadeira "caixa negra" que grava todas as actividades do utilizador. Como refere Hubert Bouché, no Relatório elaborado para a CNIL sobre a Cibervigilância no local de trabalho, agora tem início a era do "contremaître virtuel", que consegue saber tudo sobre o trabalhador ao ponto de conseguir estabelecer o seu perfil profissional, intelectual e psicológico.

A Jurisprudência portuguesa, entende que o envio de mensagens electrónicas de pessoa a pessoa («e-mail») preenche os pressupostos da correspondência privada (Internet – Serviço de comunicação privada) e que a inviolabilidade do domicílio e da correspondência vincula toda e qualquer pessoa, sendo certo que a protecção da intimidade da vida privada assume dimensão de relevo no âmbito das relações jurídico-laborais. Além do mais, os tribunais portugueses, aplicam o artigo 22.º, n.º 1 do CT que garante o direito à reserva e à confidencialidade relativamente a mensagens pessoais e à informação não profissional que o trabalhador receba, consulte ou envie através de correio electrónico, pelo que não admite que o empregador possa aceder ao conteúdo de tais mensagens ou informação, mesmo quando esteja em causa investigar e provar uma eventual infracção disciplinar e, caso o façam, não serão de atender os decorrentes meios de prova juntos ao processo disciplinar.

O Supremo Tribunal de Justiça, no mesmo acórdão, decidiu que a definição da natureza particular da mensagem obtém-se por contraposição à natureza profissional da comunicação, relevando para tal, antes de mais, a vontade dos intervenientes da comunicação ao postularem, de forma expressa ou implícita, a natureza profissional ou privada das mensagens que trocam.

No mesmo sentido, os sítios da internet que hajam sido consultados pelo trabalhador e as informações por ele recolhidas gozam da protecção do artigo 22.º do CT, pelo que o empregador não deve controlar os sítios da internet que hajam sido consultados pelos trabalhadores. Em regra, o controlo dos acessos à internet deve ser feito de forma não individualizada e global e não persecutória.

11- A combinação de todas estas tecnologias fazem com que o trabalhador se sinta permanentemente vigiado. No próprio Código de Boas Práticas da UNI, a propósito da IDRF, é referido que os dados recolhidos não devem ser interligados com os dados resultantes de outras tecnologias de monitorização como, por exemplo, o GPS, a monitorização do uso da internet ou a videovigilância.

O uso generalizado de todos estes meios tecnológicos de controlo do trabalhador, em simultâneo, acarreta consequências:

- Alteração nas relações entre trabalhadores e superiores hierárquicos/empregadores: estes já não precisam de falar e interagir com os trabalhadores para saber como está a correr o trabalho em termos de produtividade, tempos gastos nas tarefas, controle do absentismo, etc. Os empregadores já não conversam com os seus trabalhadores, só os monitorizam. Os trabalhadores sentem-se usados, tratados como números e não como pessoas. A desumanização no local de trabalho é inevitável e este já não é encarado mais como fonte de crescimento e de relacionamento social.

- Alteração no peso dos critérios de avaliação do trabalhador, passando-se a centrar, sobretudo, em critérios quantitativos. Cientes disso, a atenção dos trabalhadores centra-se precisamente nesses objectivos e não no cliente ou na qualidade do produto. Os escritórios modernos estão a tornar-se "electronic Sweatshops".

- A linha que separa o poder de controlo da entidade empregadora e a vida privada torna-se mais fluida: o trabalhador é vigiado pela máquina a todo o momento e a vigilância automática não distingue entre o que pode ver, e que respeita à actividade do trabalhador, e os outros aspectos da sua vida privada que não deveriam ficar registados.

- Grupos de trabalhadores específicos, como mulheres, imigrantes, estudantes e trabalhadores com baixos salários são mais sujeitos à "pervasive surveillance", isto é, a uma vigilância em que tudo o que o trabalhador faz é analisado e verificado.

- Efeitos na saúde física e mental dos trabalhadores: um possível impacto negativo na saúde física e mental dos trabalhadores pode contrariar os supostos benefícios do aumento da eficiência como resultado da monitorização. Os efeitos psicológicos incluem ansiedade, depressão, agressividade, irritabilidade com consequências inevitáveis no desempenho do trabalho e levando a um maior absentismo.

- Enfraquecimento da representação colectiva dos trabalhadores: os sindicatos crêem que a vigilância no local de trabalho e a monitorização podem ser usados para desencorajar uma efectiva representação colectiva; por outro lado, quanto mais controlado for o dia de trabalho, menores hipóteses há de serem estabelecidas ligações informais entre o trabalhador e os seus representantes.

- Colocação em causa da dignidade do trabalhador. Tal como é referido no relatório elaborado pelo GT 29 sobre a vigilância das comunicações electrónicas

no local de trabalho: "Os trabalhadores não abandonam o seu direito à privacidade e à protecção dos dados pessoais todas a manhãs ao entrarem no local de trabalho". A privacidade tornou-se cada vez mais importante dado que se têm esbatido as fronteiras entre tempo de trabalho e tempo pessoal, dado o desenvolvimento do teletrabalho e das modalidades de contratos de trabalho com horários flexíveis.

12- Em relação ao âmbito de aplicação do artigo 20.º do CT, este abrange, desde logo, a videovigilância, quer seja unicamente com captação de imagem, quer captando imagem e som, como se retira claramente da letra do art. 20.º, n.º 3 do CT.

Fora do âmbito do art 20.º CT ficam a monitorização do conteúdo do email bem como as escutas telefónicas porque o princípio constitucional da inviolabilidade da correspondência e telecomunicações tem carácter absoluto e as únicas excepções prendem-se com exigências de investigação criminal (art. 34.º, n.º 1 e 4 da CRP). Por outro lado, o próprio art. 22.º do CT vem especificamente regular essas situações esclarecendo que o empregador não pode consultar as comunicações pessoais do trabalhador, embora possa estabelecer regras de utilização dos meios de comunicação na empresa, nomeadamente do correio electrónico.

Questão diferente é a necessidade de se passarem, para o plano legislativo comum, estas restrições ao poder de controlo da entidade empregadora que, neste momento, apenas estão a ser delineadas pelo labor da CNPD mas cujas orientações, embora tenham o seu peso quando invocadas nos tribunais, não são um escudo defensor do trabalhador no seu dia-a-dia. A Constituição protege o trabalhador, os direitos fundamentais podem ser invocados no local de trabalho mas a segurança jurídica e a certeza do direito são também valores muito importantes, sobretudo num plano pautado por uma desigualdade natural, como o são as relações laborais.

O STJ, na decisão de 22 de Maio de 2007, entendeu que a remissão do n.º 3 do art 20.º do CT para o art. 29.º da LECT que estabelecia que "Nos casos previstos no número anterior o empregador informa o trabalhador sobre a existência e finalidade dos meios de vigilância utilizados, devendo nomeadamente afixar nos locais sujeitos os seguintes dizeres, consoante os casos: «Este local encontra-se sob vigilância de um circuito fechado de televisão» ou «Este local encontra-se sob vigilância de um circuito fechado de televisão, procedendo-se à gravação de imagem e som», seguido de símbolo identificativo" aponta no sentido de que a proibição de utilização de meios de vigilância a distância para controlo do desempenho profissional do trabalhador refere-se aos meios tecnológicos de vigilância com capacidade para procederem à gravação de imagem ou de imagem e som. O argumento do elemento sistemático, utilizado pelo STJ, quer queiramos quer não, saiu reforçado na nova redacção do Código do Trabalho dado que agora é o próprio n.º 3 do art. 20.º do CT que estipula essa norma. O outro argumento do Supremo é baseado no elemento teleológico da interpretação dado que "o artigo 20.º do Código do Trabalho proíbe o emprego de meios de vigilância a distância no local de trabalho, «com a finalidade de controlar o desempenho profissional do trabalhador»

(*elemento teleológico*), isto é, aqueles que «podem alcançar o que se faz, quando e durante quanto tempo».

Em nosso entender, a legislação que funcionou como inspiradora do art. 20.º do CT adoptava a videovigilância como meio essencial na protecção de pessoas e bens sendo que, inclusivamente, os dizeres que são colocados ao abrigo do n.º 3 do art. 20.º do CT são os que já constavam do art. 12.º n.º 3 do DL 231/98. Ou seja, estamos em crer que este enquadramento "sistemático" tem mais a ver com uma justificação de carácter histórico, com base nas leis a que este artigo foi buscar as suas raízes, e que são as leis que já regiam matéria semelhante e que também elas pretendem proteger "pessoas e bens".

Actualmente, já se começa a regulamentar o recurso à geolocalização e, particularmente, à radiofrequência pelas entidades públicas e, nessa sede, estes meios electrónicos são encarados como meios de vigilância à distância ou meios que encerram esse perigo. Basta pensarmos na "pulseira electrónica" que não é mais do que um sistema baseado na radiofrequência e que visa a monitorização telemática posicional do arguido, isto é, a vigilância de determinada pessoa em local previamente definido. Também o "chip na matrícula" recorre à tecnologia da radiofrequência e, embora o objectivo não seja a vigilância à distância dos cidadãos e do local onde se encontram, existe esse perigo. A CNPD pronunciou-se sobre esta matéria e sublinha que a «detecção e identificação electrónica dos veículos não pode transformar-se numa forma sofisticada de vigilância física, que cai fora dos fins permitidos pela lei e contraria o direito à privacidade dos condutores dos veículos». Ou seja, a radiofrequência e a geolocalização são tratados pela legislação mais recente como meios de vigilância à distância e que encerram perigos de violação da privacidade do cidadão pelo "simples" facto de se poder saber onde este está num dado momento do tempo.

O elemento teleológico da norma é a proibição do emprego de meios de vigilância a distância no local de trabalho, «com a finalidade de controlar o desempenho profissional do trabalhador» sob pena de se violar o direito à reserva da vida privada do trabalhador. Não se trata apenas do direito à imagem, que justificaria que o âmbito da norma ficasse restrito à videovigilância, mas de proteger a própria dignidade do trabalhador dado que o poder legítimo de controlo do empregador não justifica uma vigilância permanente e contínua sobre toda a actividade do trabalhador.

A geolocalização e a radiofrequência levantam questões relacionadas com a reserva da intimidade da vida privada do trabalhador porque também podem alcançar o que se faz, quando e durante quanto tempo. Basta pensarmos no caso de um trabalhador que está autorizado a utilizar a viatura de serviço para fins pessoais e que, se mantiver sempre o localizador GPS ligado, o empregador pode traçar o percurso completo deste e locais de paragem. Ora, o direito à reserva da intimidade da vida privada inclui o "direito a passar desapercebido por este mundo" e afecta a própria liberdade de deslocação do trabalhador que, ao saber-se vigiado, pode sentir-se condicionado nas suas deslocações pessoais.

Também a geolocalização e a radiofrequência podem ser utilizadas eficazmente com o objectivo da "protecção de pessoas e bens" mas nunca para controlar o

desempenho profissional do trabalhador porquanto a sua utilização com essa finalidade comprime o direito à reserva da vida privada do trabalhador.

A própria CNPD na sua Autorização N.º 857/2005 refere, a propósito da instalação por uma empresa de um sistema de geolocalização na viatura do funcionário para protecção pessoal que: "As informações captadas por GPS afiguram-se verdadeiros tratamentos de dados pessoais quando se identifica ou torna identificável um titular, pessoa singular. (…) Nos tratamentos de dados pessoais com esta natureza deve tomar-se em consideração o artigo 20.º do Código do Trabalho."

A CNPD, a propósito da radiofrequência, emitiu a Deliberação n.º 9/2004 onde determina que sempre que o recurso à tecnologia de IDRF implica a interconexão com informação de carácter pessoal se está em presença de um tratamento de dados pessoais (nos termos da alínea b) do artigo 3.º da Lei 67/98 de 26 de Outubro). O perigo da identificação por radiofrequência está, muitas vezes, associado ao facto de esses dados poderem ser cruzados com os dados pessoais e com outros dados produzidos pelos outros meios de vigilância à distância no local de trabalho.

Tendo em conta as novas tecnologias que estão constantemente a aparecer e as potencialidades das mesmas, tem de ser feita uma interpretação actualista deste artigo 20.º CT de modo a que este abranja todos os meios de vigilância à distância no local de trabalho que recorram a equipamento tecnológico quando esses meios entram em conflito com a reserva da vida privada do trabalhador e, em última instância, com a sua dignidade.

Uma última nota, a geolocalização e a radiofrequência são instrumentos tecnológicos que podem ser utilizados como meios de vigilância à distância no local de trabalho. Quero com isto dizer que estes meios apenas recaem no âmbito de protecção do art. 20.º CT quando existe um tratamento de dados pessoais associado porque só essa combinação dá azo a que possa haver uma violação da reserva da intimidade da vida privada do trabalhador e, por outro lado, a possibilidade de se controlar o seu desempenho profissional, proibida pelo artigo 20.º CT. Aliás, é precisamente esse tratamento de dados pessoais que justifica que, nos termos do art. 21.º, n.º 1 do CT, seja solicitada a autorização da instalação desses meios à CNPD.

13- Todos os meios de vigilância à distância no local de trabalho têm de ser necessariamente regulados por lei. Não são os trabalhadores que vão ditar os limites da sua subordinação ou o empregador os limites do seu poder de controlo num campo em que, por um lado, nem os trabalhadores estão conscientes do poder de intrusão destas tecnologias e por outro lado, os empregadores consideram-se plenamente legitimados a controlar a actividade do trabalhador pela posse que têm sobre os instrumentos de trabalho.

O art. 20.º fica aquém do que seria desejável nessa regulação dos meios de vigilância à distância no local de trabalho. Por um lado, porque é interpretado comummente como limitando apenas a videovigilância exercida pela entidade patronal e, por uma questão de segurança jurídica, deveria referir expressamente que é aplicável, com as necessárias adaptações, a todos os meios electrónicos que se possam revelar susceptíveis de realizar uma vigilância à distância no local de trabalho. É necessária

maior clareza e rigor na redacção e interpretação deste artigo sob pena de ficar ao critério do empregador, salvo nas situações de videovigilância que estão expressamente previstas, o que se entende por meios de vigilância à distância no local de trabalho. Na prática, a indefinição leva à auto-compressão dos direitos fundamentais do trabalhador e não à auto-limitação do poder de controlo da entidade empregadora.

Os tribunais e o intérprete devem estar atentos às mudanças no mundo, em particular às mudanças no seio da organização laboral e as suas implicações nos direitos dos trabalhadores. As novas tecnologias agudizam antigos conflitos e a leitura que se faz da lei deve acompanhar a realidade. Da realidade não faz actualmente apenas parte um mundo físico mas também um mundo virtual mas que não é por isso que deixa de afectar, tanto ou mais, as pessoas na sua dignidade e liberdades fundamentais.

BIBLIOGRAFIA

ABRANTES, José João – "O novo Código do Trabalho e os direitos de personalidade do trabalhador", in *Estudos sobre o Código de Trabalho,* Coimbra Editora, pp. 145-167

- *Contrato de trabalho e direitos fundamentais,* Coimbra Editora, Coimbra, 2005

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS – "Videovigilancia en el lugar de trabajo - Año 2001", in https://www.agpd.es/portalweb/canaldocumentacion/informes_juridicos/videovigilancia/common/pdfs/2001-0000_Videovigilancia-en-el-lugar-de-trabajo.pdf [Consult. 28 Junho 2009]

ALEXANDRE, Isabel - "Provas Ilícitas em Processo Civil", Almedina, 1988

ALSEVER, JENNIFER – "Monitoring the staff pays off: installing online cameras helped one restaurant owner boost profits by 40%"", CNNMoney.com (3 Outubro 2008) in http://money.cnn.com/2008/10/03/smallbusiness/surveillance.fsb/index.htm [Consult. 28 Junho 2009]

A.M.A. - American Association Management - 2007 Electronic monitoring & Surveillance survey

ANDRADE, José Carlos Vieira de – *Os Direitos Fundamentais na Constituição Portuguesa de 1976,* 3.ª edição, Almedina, Coimbra, 2004

BOUCHET, Hubert - "La Cybersurveillance sur les lieux de travail", mars 2004, in http://www.cnil.fr/fileadmin/documents/approfondir/rapports/Rcybersurveillance-2004-VD.pdf [Consult. 28 Junho 2009]

CAETANO, Filipe – "Chips nas matrículas: dúvidas e petição na internet", *IOL Diário* (29/08/2008) in http://diario.iol.pt/tecnologia/matriculas-chip-rfid-e-matricula-dados/986132-4069.html [Consult. 28 Junho 2009]

CANOTILHO, J.J. Gomes; MOREIRA, Vital – *Constituição da República Anotada,* 4ª ed. revista, Coimbra Editora, Coimbra, 2007, pp. 293-325, 379-396, 458-474 e 512-526

CASANOVA, Salazar - *Provas Ilícitas em Processo Civil, Sobre a admissibilidade e valoração de meios de prova obtidos por particulares",* Março de 2003, publicação da Biblioteca do TRL

CASTRO, Catarina Sarmento e - "A protecção de dados pessoais dos trabalhadores", in *Questões Laborais,* 19, Ano IX, 2002, pp. 27-60

CAUPERS, João - *Os direitos fundamentais dos trabalhadores e a Constituição,* Almedina, Coimbra, 1985

"Chips nas matrículas não garantem privacidade dos condutores", IOL Diário (27/11/2008 in http://diario.iol.pt/sociedade/chips-matriculas-privacidade-proteccao-de-dados-parecer-automoveis/1018072-4071.html [Consult. 28 Junho 2009]

C.N.I.L., Commission Nationale de l'Informatique et dês Libertés – "Guide de la

Géolocalisation des Salariés", in http://www.cnil.fr/fileadmin/documents/approfondir/dossier/geolocalisation/Guide-geolocalisation.pdf [Consult. 28 Junho 2009]
- 27.e Rapport d'Activité 2006, Paris, 2007, in http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL-27erapport-2006.pdf [Consult. 28 Junho 2009]
- "Guide pour les employers et les salariés", ed. 2008, in http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL_GuideTravail.pdf [Consult. 28 Junho 2009]

C.N.P.D., Comissão Nacional de Protecção de Dados – "VII Encontro Ibérico de Autoridades de Protecção de Dados – Óbidos, 2006", p. 2 in *http://www.cnpd.pt/bin/actividade/Outros/VII_Encontro_Iberico.pdf* [Consult. 28 Junho 2009]

DRAY, Guilherme – *O princípio da igualdade no Direito do Trabalho: sua aplicabilidade no domínio específico da formação de contratos individuais de trabalho*, Almedina, Coimbra, 1999
- "Justa causa e esfera privada", "Estudos do Instituto de Direito do Trabalho", vol. II, Almedina, Coimbra, 2001

DRISCALL, Clem; SHELDRICK, Mike - "Taking the show on the road: GPS Drives U.S. Mobile Resources Management", InsideGNSS, March 2006, pp. 28-32 in http://www.insidegnss.com/auto/0306%20Taking.pdf [Consult. 28 Junho 2009]

FESTAS, David de Oliveira - "O direito à reserva da intimidade da vida privada do trabalhador no Código do Trabalho", in *R.O.A.*, Ano 64, vol I/II, Novembro 2004

GANTT, Larry O. Natt - "An affront to human dignity: electronic mail monitoring in the private sector workplace" in *Harvard Journal of Law and Technology*, vol 8, number 2, spring 1995, pp. 345-413

GELLER, Adam - "Bosses keep sharp eye on mobile workers via GPS", Associated Press (1/03/2005) in http://www.workrights.org/in_the_news/in_the_news_associatedpress.html [Consult. 28 Junho 2009]

GMB - "GMB Congress Demands End To Electronic Tagging Of Workers "Battery Farm" Workplaces", GMB@work (6 Junho 2005) in http://www.gmb.org.uk/Templates/PressItems.asp?NodeID=91861 [Consult. 28 Junho 2009]

GOMES, Júlio Manuel Vieira - *Direito do Trabalho,*Vol. I, Coimbra Editora, Coimbra, 2007

GOÑI SEIN, José Luís - *La videovigilancia empresarial y la protección de datos personales*, Civitas / Colección Estudios de protección de datos, 2007.

GOUVEIA, Jorge Bacelar – "A Declaração Universal dos Direitos do Homem e a Constituição da República Portuguesa", *Perspectivas do Direito,*Vol. IV, n.º 6, Julho 1999, pp. 23-60

G.P.D.P., Garante per la Protezzione dei Dati Personali - ""Etichette intelligenti" *(Rfid)***:** il Garante individua le garanzie per il loro uso - 9 marzo 2005" in http://www.garanteprivacy.it/garante/doc.jsp?ID=1109493 [Consult. 28 Junho 2009]

GRANDE DICIONÁRIO DA LÍNGUA PORTUGUESA, Porto Editora, Porto, 2004, p. 391, 1043 e 1588

GRANNEMAN, Scott - "RFID chips are here", The Register (27 Junho 2003) in

http://www.theregister.co.uk/2003/06/27/rfid_chips_are_here/ [Consult. 28 Junho 2009]

GRUBER, Jeremy - "RFID and workplace privacy", National Workrights Institute, in http://www.workrights.org/issue_electronic/RFIDWorkplacePrivacy.html [Consult. 28 Junho 2009]

GT29, Grupo de Trabalho do Artigo 29 - *Working document on data protection issues related to RFID technology*, Janeiro 2005, in http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf [Consult. 28 Junho 2009]

GUERRA, Amadeu – *A privacidade no local de trabalho- as novas tecnologias e o controlo dos trabalhadores através de sistemas automatizados- uma abordagem ao código do trabalho*, Almedina, Coimbra, 2004

HENDRICKX, Frank – "Protection of worker's personal data in the European Union" -"Innovation technologique et droit du travail", estudo preparado para a Comissão Europeia, Julho 2002

HÖRSTER, Heinrich Ewald - *A parte geral do Código Civil português – Teoria Geral do Direito Civil*, Almedina, Coimbra, 1992.

I.C.O., Information Commissioner's Office - "Data Protection Technical Guidance Radio Frequency Identification" (9 de Agosto de 2006) in http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/radio_frequency_indentification_tech_guidance.pdf [Consult. 28 Junho 2009]

JOHNSON, Phil - "A new policy for internet use in the workplace", (16 Março 2009) in http://adage.com/smallagency/post?article_id=135266 [Consult. 28 Junho 2009]

LIBBENGA, JAN"Video surveillance outfit chips workers _ RDFID implant scheme", TheRegister (10 de Fevereiro de 2006) in http://www.theregister.co.uk/2006/02/10/employees_chiped/ [Consult. 21 Novembro 2008]

MENEZES CORDEIRO, António - *Manual de Direito do Trabalho*, Almedina, Coimbra, 1991

- "O respeito pela esfera privada do trabalhador", in *I Congresso Nacional de Direito do Trabalho _Memórias* (coord. António Moreira), Almedina, Coimbra, 1998, pp. 17-37

MIRANDA, Jorge - *Manual de Direito Constitucional*, Tomo IV, *Direitos Fundamentais*, 3.ª edição, Coimbra Editora, 2000

MONTEIRO FERNANDES, António - *Direito do Trabalho*, 13.ª edição, Almedina, 2007

MOREIRA, Teresa Alexandra Coelho – "Da esfera privada do trabalhador e o controlo do empregador", in *Studia Iuridica*, n.º 78, Coimbra Editora, Coimbra, 2004

MOREIRA, Vital – v. CANOTILHO, J.J. Gomes

NATIONAL WORKRIGHTS INSTITUTE, "On your tracks: GPS tracking in the workplace", August 2005, in http://www.workrights.org/issue_electronic/NWI_GPS_Report.pdf [Consult. 28 Junho 2009]

NEVES, Céu - "Pedidos de vigilância duplicam em Portugal", Diário de Notícias (14 de Setembro de 2005), in http://dn.sapo.pt/2005/09/14/nacional/pedidos_videovigilancia_duplicam_por.html [Consult. 28 Junho 2009]

NICOLAU JUNIOR, Mauro – "Segurança Jurídica e Certeza do Direito: realidade ou

utopia num Estado Democrático de Direito", *Universo Jurídico* in http://www.universojuridico.com.br/publicacoes/doutrinas/1868/SEGURANCA_JURIDICA_E_CERTEZA_DO_DIREITO_REALIDADE_OU_UTOPIA_NUM_ESTADO_DEMOCRATICO_DE_DIREITO [Consult. 28 Junho 2009]

OIT- "Workers' privacy: Part II: Monitoring and surveillance in the workplace", *Conditions of Work Digest*, Vol. 12, No. 1, 1993

- "Protection of workers' personal data. ILO code of practice", Geneva, 1997, in http://www.ilo.org/public/libdoc/ilo/1997/97B09_118_engl.pdf [Consult. 28 Junho 2009]

-"RFID and surveillance in the workplace", World of Work, n.º 59, April 2007, pp. 16-19

PEREIRA DA SILVA, VASCO – "A vinculação das entidades privadas pelos direitos, liberdades e garantias", in *R.D.E.S.* 1987, n.º 2, pp. 259 ss

PINTO, Paulo Mota - "A protecção da vida privada e a Constituição", *in B.F.D.U.C.*, n.º 76, 2000, pp. 153-204

PORTUGAL. Ministério do Trabalho e da Solidariedade Social. Comissão do Livro Branco das Relações Laborais - Livro Branco das Relações Laborais, 20 Dezembro 2007

PRATA, Ana – *A tutela constitucional da autonomia privada*, Livraria Almedina, Coimbra, 1982

PRIVACY INTERNATIONAL - **"**Privacy and Human Rights – An International Survey of Privacy Laws and Practice" in http://gilc.org/privacy/survey/intro.html [Consult. 28 Junho 2009]

"Proposta de lei sobre instalação de chips electrónicos nas matrículas dos veículos debatida no Parlamento", TSF (16/07/2008) in http://tsf.sapo.pt/PaginaInicial/Portugal/Interior.aspx?content_id=968536 [Consult. 28 Junho 2009]

ROMANO MARTINEZ, Pedro – "Código do Trabalho Anotado", 4ª Edição, Almedina, Coimbra, 2005

- *Direito do Trabalho*, 4ª ed., Almedina, Coimbra, 2007

SHELDRICK, Mike – v. DRISCALL, Clem

SOUSA, Rabindrananath Valentino Aleixo Capelo de - *Direito Geral de Personalidade*, Coimbra Editora, 1995

SPECHT, Michael - "Internet usage at work makes you more productive" in http://specht.com.au/michael/2009/04/03/internet-usage-at-work-makes-you-productive/ [Consult. 28 Junho 2009]

STANCHI, Andrea "L'utilizzo della Radio Frequency Identification (Rfid) e le implicazioni giuslavoristiche." in http://www.dielle.it/consultazione/approfondimenti_4/radio_frequency_identification_790/view/790/ [Consult. 28 Junho 2009]

VASCONCELOS, Joana - *O Contrato de Trabalho. 100 Questões*, Universidade Católica, 2004

VENCO, Selma Borghi - *Tempos moderníssimos nas engrenagens da telemarketing*, tese de doutoramento apresentada em Fevereiro de 2006 na Universidade Estadual de Campinas

"Vigilancia electrónica total a los trabajadores británicos de la distribución". Elmundo.es (8 Junho 2005) in http://www.elmundo.es/navegante/2005/06/08/esociedad/1118217101.html [Consult. 28 Junho 2009]

UNI Global Union – "UNI's letter to EU Commissioner Viviane Reding on RFID

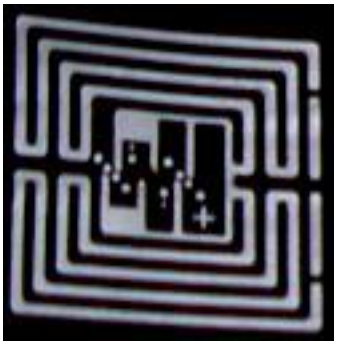
technology in Europe", de 26 de Junho de 2006, in -http://www.union-network.org/uniindep.nsf/0/4606CF32F49004EAC1257199002F327B?OpenDocument [Consult. 28 de Junho de 2009]
- "You're being followed: Electronic Monitoring and surveillance in the Workplace", in http://www.uniglobalunion.org/Apps/UNIPub.nsf/vwLkpById/3A8CFDE3607D5CC5C125754C004FB7F9/$FILE/E-ELECTRONIC%20MONITORING.PDF [Consult. 28 Junho 2009]

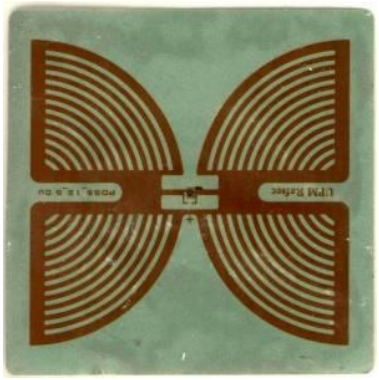
Páginas da internet consultadas:

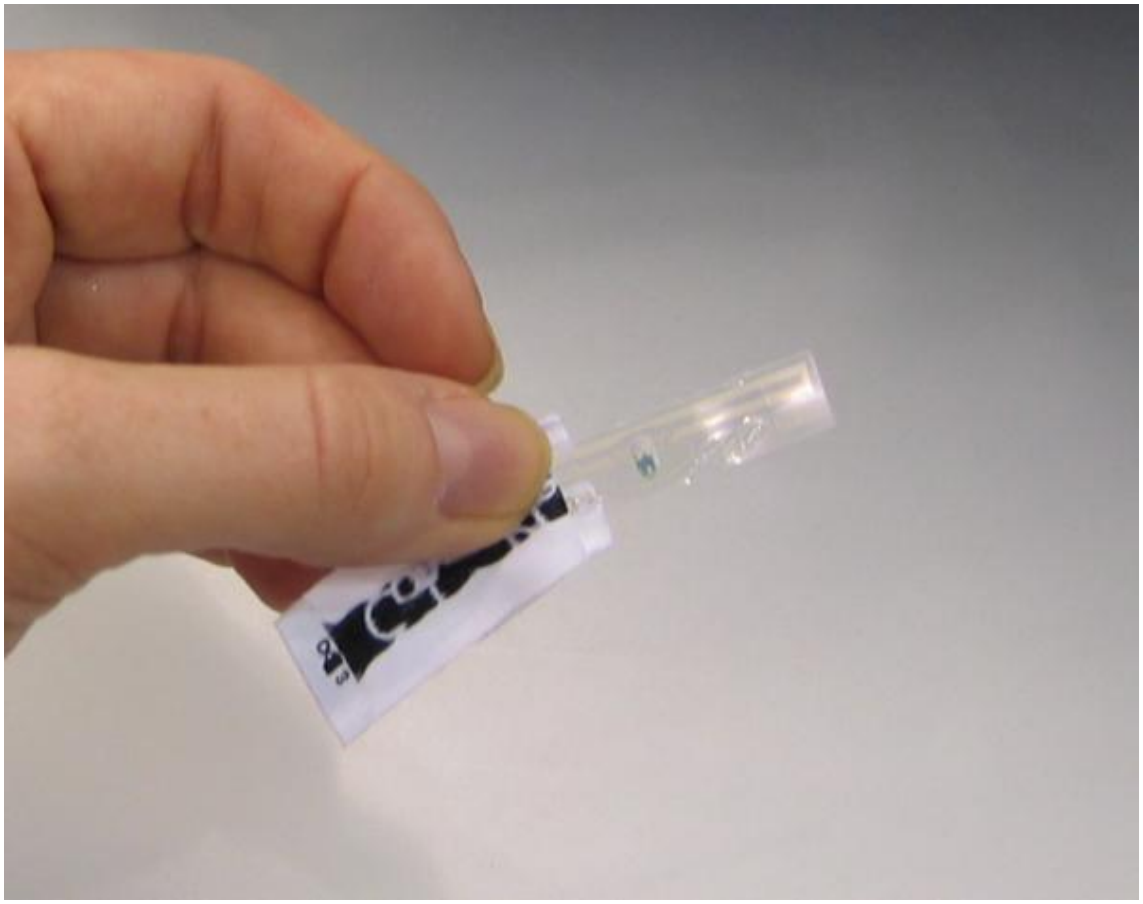
www.agpd.es/portalweb/index-ides-idphp.php
www.amanet.org/
www.austlii.edu.au/
www.brickhousesecurity.com/
www.cnil.fr/
www.cnpd.pt
www.courdecassation.fr/
www.dgsi.pt
http://ec.europa.eu/index_pt.htm
www.foruminternet.org
www.garanteprivacy.it/garante/navig/jsp/index.jsp
www.ico.gov.uk
www.legifrance.gouv.fr/

ANEXO I

Exemplos de Etiquetas IDRF








VariChip

Índice