PREVENCIÓN DEL DELITO EN LA EMPRESA

Límites ético–jurídicos en la implementación de sistemas de videovigilancia

José R. Agustina Sanllehí [1]
Profesor de Criminología y Derecho Penal
Universitat Internacional de Catalunya

AGUSTINA SANLLEHÍ, José R. Prevención del delito en la empresa: Límites ético-jurídicos en la implementación de sistemas de video-vigilancia. *Revista Electrónica de Ciencia Penal y Criminología* (en línea). 2009, núm. 11-10, p. 10:1-10:48. Disponible en Internet:
http://criminet.ugr.es/recpc/11/recpc11-10.pdf
ISSN 1695-0194 [RECPC 11-10 (2009), 13 oct]

RESUMEN: En el marco de la criminalidad en el interior de la empresa, se originan ciertos deberes de vigilancia y control del empresario respecto de aquellos delitos que llegan a cometerse en su esfera de organización, en virtud de los cuales, puede llegar a imputarse a quien ostenta una posición de garante distintos grados de responsabilidad por el hecho ajeno. Junto a ello, se erigen también determinados límites que derivan del debido respeto a la privacidad del trabajador. Así, en base a tales límites, la implementación de estrategias de prevención y control debe realizarse conforme a ciertos principios que logren un equilibrio entre los intereses contrapuestos, sin que puedan desarrollarse medidas de injerencia de forma ilimitada. En el presente artículo se abordan los fundamentos ético–jurídicos que subyacen en este ámbito, aportando desde un enfoque interdisciplinar algunos principios materiales que orienten la práctica empresarial.

PALABRAS CLAVE: video-vigilancia; estrategias de prevención del delito en la empresa; delitos de los trabajadores. Privacidad versus prevención: límites ético-jurídicos.

Fecha de publicación: 13 octubre 2009

[1] Se recogen en este artículo algunas de las reflexiones y propuestas derivadas de la tesis doctoral defendida por el autor en la Universitat Pompeu Fabra, bajo la dirección de los profesores Jesús-M. Silva Sánchez (UPF) y Joan Fontrodona Felip (IESE), y que lleva por título: "Estrategias de prevención y deberes de control en la criminalidad intra-empresarial. Especial referencia al delito de descubrimiento y revelación de secretos en su aplicación al control del correo electrónico del trabajador" (2008).

I. **INTRODUCCIÓN**

Es un hecho ciertamente constatable que vivimos en tiempos difíciles para la privacidad. En los últimos años, nos hemos adentrado de forma aparentemente inexorable en la era de la videovigilancia. El fenómeno, sobradamente conocido en el entorno cultural y jurídico de los países anglosajones, comienza paulatinamente a irrumpir con fuerza en el paisaje cultural y jurídico de los países de tradición continental, a rebufo de los nuevos paradigmas en materia de prevención y seguridad.

En este sentido, la Agencia Española de Protección de Datos (AEPD) ha denunciado un incremento vertiginoso en 2008 respecto de la instalación de cámaras de videovigilancia en una inmensa variedad de espacios privados, públicos y semipúblicos: cámaras en los vestíbulos de los hoteles, a lo largo de los pasillos de los hospitales, en las escaleras de fincas privadas, a las puertas de los garajes o tras la nuca de los clientes de bancos y entidades financieras[2].

Ante tal situación, la AEPD ha difundido una Guía de Videovigilancia, documento en el que se ofrecen indicaciones y criterios prácticos que permitan el adecuado cumplimiento de la legislación vigente en todos los casos[3]. Por su parte, la Agencia Catalana de Protección de Datos (APDCAT) ha aprobado recientemente una Instrucción sobre el tratamiento de datos de carácter personal mediante cámaras con fines de videovigilancia[4].

[2] Véase noticia publicada en *La Vanguardia*, "Vigilar al videovigilante", de 16 de abril de 2009, donde se afirma que la cifra de denuncias se ha disparado en el último año y medio: sólo en 2008, las reclamaciones de ciudadanos que creyeron vulnerados su derecho a la intimidad aumentaron en más de un 45%.

[3] Disponible en: https://www.agpd.es/portalweb/canaldocumentacion/publicaciones/common/pdfs/guia_videovigilancia.pdf

[4] Instrucción 1/2009, de 10 de febrero, sobre el tratamiento de datos de carácter personal mediante cámaras con fines de videovigilancia (documento íntegramente disponible en Internet en la dirección: http://legal4.ecija.com/documentos/Legislacion/090219_instruccion_ag_catalana_prot-datos_videovigilancia.pdf).

Al margen de la concreta regulación legal vigente en los distintos países, en el presente artículo se propone revisar, desde sus fundamentos ético-jurídicos, algunos aspectos de orden axiológico que subyacen en los conflictos entre la privacidad de los trabajadores y las necesidades de prevención del delito en la empresa.

II. **EL ADVENIMIENTO DE UNA NUEVA CULTURA DEL CONTROL: NUEVOS PARADIGMAS EN PREVENCIÓN Y SEGURIDAD, NUEVOS DESAFÍOS PARA LA PRIVACIDAD**

Para encuadrar adecuadamente el objeto de nuestras reflexiones en las actuales circunstancias históricas, culturales y sociológicas conviene referirse –aunque sea someramente– a la estrecha relación en el tiempo y en el espacio, en sus concretas formas de desarrollo, entre lo que viene denominándose la "cultura del control" (Garland, 2001) y la llamada revolución tecnológica. Sin aludir a ambas tendencias y a sus manifestaciones actuales en la sociedad contemporánea, sería difícil describir con acierto el estado actual de los problemas que se suscitan en las estrategias de prevención del delito y los sistemas de video-vigilancia en contextos organizacionales. Partimos así de la propia realidad social y empresarial de nuestro tiempo, con el fin de tratar de comprender la génesis del fenómeno relativo a la implementación creciente de estrategias de prevención en múltiples ámbitos y, por lo que aquí interesa, en el interior de la empresa. Desde esta perspectiva, la evolución reciente del Derecho penal contemporáneo no puede dejar de circunscribirse en las coordenadas que, desde la sociología política, social y laboral, vienen caracterizadas por la cultura del control, la irrupción de las nuevas tecnologías y el énfasis en la prevención a que conduce una «sociedad de riesgos» (Beck, 1993).

Existen numerosas y conocidas aproximaciones doctrinales que tratan de describir las distintas implicaciones que, en materia de privacidad y políticas públicas y privadas, ha supuesto la revolución de las tecnologías de la información[5]. Sin embargo, desde un punto de vista propiamente sociológico, deben citarse los análisis efectuados por Castells (1997), Lyon and Zureik (1996) y, en relación a un enfoque más criminológico, Garland (2001).

Como resultado de la evolución social descrita, en el ámbito penal, el centro de la atención «ya no es la penalidad –o al menos no es sólo la penalidad–, sino un campo más amplio que abarca las prácticas de actores estatales y no estatales y formas de control del delito que son tanto preventivas como penales». Las profundas transformaciones históricas, sociológicas y culturales han modificado el modo de concebir la realidad criminológica y de actuar sobre el delito, operándose un giro desde la «aplicación de la ley» al «management de la seguridad»[6]. Estamos asistiendo, en este sentido,

[5] *Vid.* al respecto, WALTERS, G.J., *Privacy and Security: An Ethical Analysis*, Computers and Society, June 2001, donde cita, entre otros, los trabajos de *Cavoukian and Tapscott* (1995), *Bennett* (1992), *Burnham* (1983), *Flaherty* (1989). El análisis de *Walters*, en cambio, pretende trazar una línea desde una perspectiva ética entre prácticas de vigilancia y seguridad positiva y negativa de acuerdo con los principios de derechos humanos.

[6] La fórmula consolidada del modelo de justicia penal moderna concebía el control del delito como una tarea especializada y profesional de «aplicación de la ley». Desde esa concepción, se imponía *ab initio* la separación

a los inicios de una transición desde un sistema diferenciado de control del delito monopolizado por el Estado a un sistema des–diferenciado que involucra asociaciones entre actores estatales y no estatales[7].

La implementación de una vigilancia intensificada como mecanismo generalizado para el control de la delincuencia y la desviación social plantea diferentes conflictos en los distintos ámbitos de actuación de la persona[8]. La aproximación a una nueva concepción de la vigilancia y el control social responde a un mayor convencimiento de la necesidad y conveniencia de nuevos métodos como parte integrante del arte del buen gobierno. En este sentido, asistimos a una reorientación de las políticas de control social de forma que éstas sean capaces de «hacer visible todo», mediante una «vigilancia permanente, exhaustiva y omnipresente»[9].

Sin duda, la irrupción y sofisticación de las nuevas tecnologías tiene una enorme incidencia en los modos de convivencia, relación, desarrollo y trabajo de los individuos, en la complejidad de interacciones e interrelaciones que se producen en una sociedad progresivamente cada vez más globalizada, en las nuevas formas de criminalidad. Y, consecuentemente, en las nuevas formas de control de esa misma criminalidad. El avance de las nuevas tecnologías plantea nuevos desafíos en la privacidad de los individuos. No obstante, el binomio nuevas tecnologías y privacidad no sólo afecta a las relaciones entre el Estado y los ciudadanos. Una de las características de esta nueva era de las tecnologías es la generación de mayores facilidades y nuevas oportunidades para acceder a la esfera íntima o de mera privacidad de la persona: la capacidad intrusiva que aporta la tecnología no depende tanto de facto del previo consentimiento o cesión de datos del sujeto, o del empleo de fuerza física o habilidad subrepticia.

Las esferas que pueden llegar a ser objeto de vigilancia como consecuencia de una tal concepción de los medios de control social son extensas en el espacio e intensas en los medios. Los sujetos que ejercen tales medidas, como actores de esta nueva cultura del control, pueden ser enormemente variados: las instituciones del Estado, el empresario, la familia, la escuela y el sistema educativo en su conjunto, el ámbito municipal y vecinal, entre otros muchos.

Sin embargo, la pretendida necesidad y conveniencia de una mayor injerencia en la esfera de actuación de la persona exige como contrapeso, una revisión del título de legitimación que, en cada caso, justifique una determinada intervención. El afán de control no es más que uno de los campos en los que se libra la batalla entre el Estado

entre la acción de los poderes públicos y la acción de los distintos agentes y de todas aquellas instituciones privadas que ejercen controles sociales en sus ámbitos respectivos (familia, escuela, vecindario, lugar de trabajo, asociaciones). Se entendía que los problemas sociales eran mejor gestionados por *burocracias especializadas*, en lo que sería una versión criminológica de lo que James C. SCOTT ha llamado *alto modernismo* (*vid.* GARLAND, D., *La cultura del control*, 2005, p. 81; SCOTT, JAMES C., *Seeing Like a State*, New Haven, 1998).

[7] GARLAND, D., *La cultura del control*, 2005, p. 20–21.

[8] Así, en Gran Bretaña, tras los atentados del 7 de julio de 2005 en el metro de Londres, el gobierno comenzó a poner en práctica medidas especiales de vigilancia (*vid.* ACEPRENSA, *Demasiada vigilancia genera inseguridad en Gran Bretaña*, 18/08, febrero de 2008).

social, con su lógica de la prevención y la seguridad como línea predominante, y el Estado liberal, donde priman las garantías y libertades del ciudadano. Tanto en el plano teórico como en el práctico, se aprecia de forma evidente el vínculo indisociable que une la libertad –en sus múltiples manifestaciones– y la privacidad e intimidad de los individuos y de los grupos en que se integran. Piénsese en términos psico–sociales, cómo el aumento generalizado del control –independientemente de que éste sea transparente u oculto– afecta a la vivencia cotidiana de la libertad y a la espontaneidad de actuación de los individuos.

Para preservar la privacidad, uno debería abstenerse de firmar ningún papel, comprobante o cheque, ni hacer ninguna llamada. Sería imprudente entablar conversaciones con otras personas o pasear, incluso aunque sea en una propiedad privada, por fuera de la propia casa. Si se desea tener una barbacoa o simplemente leer en el patio trasero, hágase sólo si se está rodeado por una valla o muro más alto que un autocar de dos pisos y mientras se esté sentado bajo un toldo opaco. El individuo prudente podría también considerar comprarse una protección antiaérea para no ser espiado, si puede. En el momento de retirarse al interior de la casa, asegúrese de dejar las persianas en vertical, bien juntas. Cuando trate de deshacerse de cartas u otros materiales delicados, hágalo sólo después de haber triturado los documentos; lo ideal sería tomar la basura personalmente y llevarla al lugar previsto para su depósito y ocultarla bien adentro, en profundidad. Finalmente, cuando compre cualquier clase de objetos, inspecciónelos cuidadosamente, no sea que llevaran incorporados algún sistema de rastreo electrónico[10].

Debemos analizar, por tanto, el equilibrio entre derechos y libertades que oponen al Estado y a otras instancias de control frente al individuo y su privacidad: ¿bajo qué condiciones morales, legales y sociales debe ceder el derecho a la privacidad? Cuando una sociedad no permite bajo ningún concepto que el derecho a la privacidad sea limitado, ¿qué perjuicios específicos y relevantes nos acontecen?[11].

1. **La cultura de control en la empresa**

Por lo que respecta al ámbito específico del control de los trabajadores en la empresa, se viene planteando en los últimos años un conjunto creciente y continuamente renovado de conflictos ético–jurídicos. A partir de la línea de pensamiento que permitió justificar en la década de los ochenta una cruzada nacional frente la importante crisis social relativa a la generalización del consumo de drogas ilegales (War on Drugs), John Gilliom describe con agudeza el nacimiento en el seno de las políticas de control social de un nuevo paradigma de vigilancia absoluta y de total prevención de la delincuencia[12].

Una estrategia clave en la «guerra contra las drogas» consistió en solicitar a los trabajadores norteamericanos que probaran su abstinencia –de drogas ilegales– mediante el análisis de la orina depositada en una pequeña botella de plástico. Este procedimiento vino a denominarse employee drug

[9] FOUCAULT, M., *Discipline and Punish*, New York, 1979, p. 234 (*vid.* en español, *Vigilar y castigar*, trad. de Aurelio GARZÓN DEL CAMINO, Madrid, 1979, primera edición).

[10] *Cfr.* SUNDBY, S.E., *Everyman's Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?* Columbia Law Review 94 (1994): 1789–1790.

[11] ETZIONI, A., *The limits of privacy*, 1999, p. 3.

[12] *Vid.* GILLIOM, J., *Surveillance, Privacy, and the Law*, 1994, 1–4.

testing –control de drogas al trabajador–. Como técnica de vigilancia, el empleo regular de controles de droga permite la observación y dirección del comportamiento de individuos en cualquier lugar y en cualquier momento. Las nuevas técnicas de análisis de las propiedades moleculares de la orina transforman el cuerpo humano y sus fluidos en un verdadero registro de las sustancias que una persona ha comido, respirado o esnifado, se ha inyectado o ha fumado. El resultado es que el gobierno y los directivos en la empresa no necesitan durante más tiempo descubrir el comportamiento desviado de sus trabajadores mediante el testimonio verbal o una simple observación casual, porque pueden acabar con la capacidad humana de albergar un secreto, engañar, o negarse a declarar, tan sólo mirando en el interior de su cuerpo y viendo de esta forma lo que el individuo ha estado haciendo[13].

Los sorprendentes niveles de vigilancia empresarial que se han alcanzado con los nuevos instrumentos tecnológicos plantean así importantes problemas ético–jurídicos en un vasto espectro de facetas y ámbitos del trabajador, llegando hasta extremos de vigilancia total en algunos casos. La literatura en la materia es extensa y describe la situación del trabajador con crudeza y realismo: «the visible employee» (Stanton and Stand)[14] o «the naked employee» (Lane III)[15]. La información disponible sobre un candidato a un puesto de trabajo –por mencionar un ámbito de injerencia de la tecnología al servicio del empresario: applying for a Job in a Digital and Wired World–, puede, en la práctica, llegar a extenderse a datos personales de muy distinta naturaleza:[16]

De forma descriptiva se puede afirmar que la obtención y recopilación de datos será una tarea cada vez más asequible y, tal vez, en el contexto del debate entre libertad y seguridad, más susceptible de legitimación (employment screening «will be the equivalent of what drug testing was in the 1980's»)[17]. Así, se utilizan en la práctica desde informes procedentes de detectives privados, certificados de antecedentes penales y huellas dactilares[18], historial de multas de tráfico, informes médicos, informes de las compañías de tarjetas de crédito y de empresas privadas dedicadas a informes del perfil financiero de los posibles trabajadores o clientes, registros judiciales, test de personalidad, hasta la mencionada prueba del polígrafo[19].

La paradoja es que la misma tecnología que convierte a los trabajadores en agentes potencialmente peligrosos permite al empresario invadir la privacidad de un modo anteriormente inimaginable[20]. A pesar de la lejanía en el tiempo, la célebre sentencia del caso Arroyo v. Rattan Specialties (1986)[21] nos viene a ilustrar de forma gráfica en

[13] GILLIOM, J., *Ibid.*, 1994, 1.

[14] STANTON, J.M., STAM, K.R., *The Visible Employee*, New Jersey, 2006.

[15] *Vid.* LANE III, F.S., *The naked Employee*, 2003.

[16] LANE III, F.S., *The naked Employee*, 2003, pp. 27–48.

[17] EDGECLIFF–JONSON, A., «Corporate Security: Industry Comes Out of the Dark Shadows», *The Financial Times* (April 10, 2001).

[18] Así, en Estados Unidos, muchos Estados requieren huellas dactilares y certificado de antecedentes penales para presentarse a un puesto de trabajo que implique tratar con menores o ancianos (*vid.* LANE III, F.S., *The naked Employee*, 2003, p. 33).

[19] Si bien la cooperación entre los empresarios y las fuerzas de seguridad es actualmente un terreno por explorar, y visto que se justifica la obtención de huellas dactilares (*vid.* pie de página anterior), parece un salto menor extender esa justificación en determinados usos del CODIS (*Combined* DNA *Index System*) en procesos de selección de trabajadores (LANE III, F.S., *The naked Employee*, 2003, p. 179).

[20] LANE III, F.S., *The naked Employee*, 2003, p. 213.

[21] *Vid. Arroyo v. Rattan Specialties*, 117 D.P.R. 35 (1986), Sentencia del Tribunal Superior, Puerto Rico, 5 de marzo de 1986: 86 JTS 20.

sus líneas fundamentales la tensión existente en el seno de la empresa entre prevención e intimidad que va recorrer de forma constante todas y cada una de las reflexiones del presente trabajo.

2. **El caso *Arroyo v. Rattan Specialties***

En Arroyo v. Rattan Specialties (1986), se plantea la legalidad y constitucionalidad de la regla 41 del Reglamento de la empresa Rattan Specialties, en la que se establecía que la negativa a disponerse a la prueba del polígrafo por un trabajador –se tratara ésta de una prueba periódica o específica– era motivo justificado para aplicar suspensión de empleo y sueldo. Además, en segunda instancia, si el empleado continuaba negándose a someterse a la prueba, el empresario tenía causa justificada para imponer la separación definitiva del trabajador (despido procedente).

Interesa citar para la comprensión del caso la definición de polígrafo que recoge la sentencia. Así, se define como un «instrumento que mide reacciones del sistema nervioso de una persona bajo situaciones controladas. Dicho instrumento registra cambios en la presión sanguínea, respiración, pulso y la reacción galvánica cutánea. La prueba del polígrafo comienza con una entrevista entre el técnico del polígrafo y la persona que va a ser sometida a la prueba. Los propósitos de esta entrevista son obtener la información sobre la persona que será examinada, y convencerla de que la prueba del polígrafo será fiable. De esta forma se trata de lograr su más completa cooperación y evitar que mienta. La información obtenida en la entrevista será utilizada más tarde por el técnico durante el examen para formular preguntas irrelevantes y de control que miden la reacción fisiológica de la persona cuando ésta miente y cuando es veraz»[22].

Ya por aquellos años había tomado cuerpo en Estados Unidos la práctica de condicionar la obtención o retención de un empleo a que la persona se sometiera a pruebas de polígrafo, tanto en las empresas privadas como en la esfera gubernamental[23]. Mediante la prueba del polígrafo se pretendía auscultar el pensamiento de la persona y supuestamente verificar de forma objetiva la veracidad de la información o predecir su conducta futura. Al margen de la escasa fiabilidad de la prueba, el Tribunal trajo a su consideración la diferencia esencial entre la prueba de polígrafo y un interrogatorio común: la persona sometida a la prueba de polígrafo no puede decidir qué preguntas contesta y qué preguntas se niega a contestar, debido a que el polígrafo registra las reacciones fisiológicas de la persona, aunque ésta rehúse o se niegue a contestar.

Así, frente a medios de prevención y control de alcance general, la prueba del polígrafo se inserta entre aquella clase de medidas de alcance individualizado. Ante la limitada capacidad de rendimiento que se atribuye en ocasiones a las estrategias globales de prevención y la constatación de que un uso excesivo de las mismas es contraproducente, las empresas, en lugar de adoptar medidas de control genérico sobre

[22] *Arroyo v. Rattan Specialties*, 117 D.P.R. 35 (1986): Congress of the United States, Office of Technology Assessment, Scientific Validity of Polygraph Testing, A Research Review and Evaluation, U.S. Government Printing Office, noviembre de 1983; R. Lowe, Regulation of Polygraph Testing in the Employment Context: Suggested Statutory Control on Test Use and Examiner Competence, 15 U.C.D.L. Rev. 113, 124-126 (1981), apartado II de la sentencia.

[23] No obstante, en la actualidad sólo se permite la prueba de polígrafo con carácter general en las empresas propiedad del Estado, salvo algunas excepciones: *vid. infra.*

la organización empresarial, acuden a mecanismos rigurosos para la selección del personal. Una de las estrategias que se vienen implementando consiste en realizar exámenes dirigidos a averiguar la integridad u honradez de una persona (Integrity Tests), los cuales pretenden descubrir qué riesgos de desviación presenta el candidato a un cargo en la empresa. De esta forma se obtiene un diagnóstico ex ante sobre el perfil criminológico del aspirante, ya sea con anterioridad a su contratación o antes de decidir otorgarle mayores o especiales responsabilidades. Sin embargo, se ha argumentado que este mecanismo es de poca utilidad en el caso de los perfiles criminológicos del personal directivo, porque los delincuentes económicos, a diferencia de otras clases de delincuentes, son socialmente discretos y, sobre todo, porque el perfil que se busca en el buen directivo –capacidad de decisión, falta de aversión al riesgo, carácter extrovertido, etc.– coincide de hecho, en buena parte, con el perfil de delincuente empresarial[24].

La regulación federal norteamericana vigente en la materia, la Employee Polygraph Protection Act (1988), establece una prohibición genérica del uso del polígrafo y otros detectores fisiológicos de mentiras en la empresa privada[25]. Sin embargo, se contemplan tres principales áreas de excepción. En primer lugar, (1) pueden emplearse tales medios en el curso de una investigación en marcha sobre incidentes que comporten pérdidas para el empresario, si bien debe existir una sospecha razonable acerca de la implicación del trabajador en tal incidente. En segundo lugar, (2) quedan excluidos de la prohibición general los trabajadores dependientes de ciertas empresas o instituciones: así, pueden someterse a la prueba del polígrafo u otros «physiological lie–detecting» los empleados del gobierno, o de empresas relacionadas con la seguridad nacional, la defensa o el contra–espionaje; o trabajadores que lleven a cabo servicios de seguridad privada, entre otros. Y finalmente, en tercer lugar, (3) la legislación federal no impide que a nivel estatal o local se establezca una regulación propia, superponiéndose en tales supuestos a la legislación federal. Así, al menos 39 Estados han establecido normativas específicas sobre el uso del polígrafo y los detectores de mentiras. El alcance de tales leyes varía desde, por ejemplo, la normativa del Estado de Virginia, que permite la prueba del polígrafo pero requiriendo a los empresarios proveer a los trabajadores la grabación de todo el procedimiento, hasta la normativa vigente en Minnesota, que prohíbe incluso pedir a los empleados someterse a pruebas de detectores de mentiras[26].

En Arroyo v. Rattan Specialties (1986), que –conviene resaltarlo– precede en el tiempo a la Employee Polygraph Protection Act (1988), se anticipa de algún modo en

[24] BUSSMANN, K.–D. (2003), "Business Ethics und Wirtschaftsstrafrecht. Zu einer Kriminologie des Managements", *MschrKrim*, 86, pp. 95 y ss. y BUSSMANN, Kai-D. (2004) "Kriminalprävention durch Business Ethics. Ursachen von Wirtschaftskriminalität und die besondere Bedeutung von Werten", *Zfwu* 5/1, p. 40. En efecto, puede que una persona apocada y conformista no tenga el perfil de delincuente económico, pero entonces tampoco tendrá el perfil de un buen directivo.

[25] SCHWARTZ, P.M., SOLOVE, D.J., *Information Privacy. Statutes and Regulations 2008–2009*, New York, 2008, p. 544.

[26] *Vid.* PHILLIPS, D.J., *Privacy and Data protection in the workplace: the US case*, published in NOUWT, S., DE VRIES, BEREND R., PRINS, CORIEN, Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy, The Netherlands, 2005, p. 45-47.

el ámbito de la empresa el dilema fundamental que va a atravesar todo el ámbito de la prevención y la seguridad en su conjunto: ¿dónde queremos vivir, en una sociedad sin delitos o en una sociedad sin libertades? Es interesante subrayar que a mediados de los ochenta todavía no se había precipitado el ritmo de avance de las nuevas tecnologías y su irrupción en la empresa que tendrá lugar en los noventa.

Una de las cuestiones que se plantean en Arroyo v. Rattan Specialties es si estamos ante una cuestión novedosa[27]. Es decir, ¿los canales que las nuevas tecnologías ofrecen a los sujetos activos alteran de forma esencial, cualitativamente, las conductas delictivas?[28]. Una respuesta positiva o negativa no impide sostener que las nuevas formas de criminalidad asociadas a las nuevas tecnologías multipliquen los efectos negativos del delito o promuevan y acerquen las ocasiones delictivas, al menos en algunos casos. En este sentido, la sentencia del Tribunal Superior de Puerto Rico realiza una serie de consideraciones en torno al derecho a la intimidad y a la naturaleza y extensión con que se empleaba ya en aquella fecha la prueba del polígrafo, que nos pueden servir de marco orientador.

El Tribunal sostiene que nos encontramos frente a «una de las áreas de la intimidad más preciadas para el ser humano: su mente, sus pensamientos». En este sentido, de forma manifiestamente desproporcionada, se le está exigiendo a una persona –argumenta el Tribunal– que para que pueda acceder a trabajar en un oficio corriente como el de ebanista –profesión sin aparentes indicios de peligrosidad–, deba permitir la intrusión del empresario en sus pensamientos. La razón genérica que esgrime la empresa para la utilización del polígrafo –tratarse de un «mecanismo económico y efectivo para proteger la propiedad»– no es motivo suficiente y proporcional que pueda justificar un recorte de esta naturaleza en la dignidad humana. El empresario no ha demostrado «circunstancias especiales de amenaza real a la seguridad nacional, o a un grave peligro para el orden social, o cualquier otro interés apremiante del Estado»[29].

Aunque el Tribunal alegue que no existen circunstancias especiales, en realidad parece realizar una ponderación de distintos derechos e intereses en colisión, sin considerar el derecho de propiedad del empresario en sí mismo como una justificación válida en detrimento de la intimidad del trabajador. A juicio del Tribunal, no es lo mismo

[27] Como resalta el juez asociado HERNÁNDEZ DENTON en su opinión particular –concurrente en el fondo, disidente en la forma–, refiriéndose al análisis de la prueba del polígrafo en sí misma: «el resultado sería el mismo aun si el interrogatorio no se hubiese realizado mediante un detector de mentiras». Es decir, según su argumentación, el ataque a la dignidad de la persona no se produce en razón del medio empleado. A su juicio, no violaría el derecho a la intimidad una prueba del detector de mentiras cuando sólo se pregunte aquello que normalmente se pregunta en cualquier entrevista de empleo (*vid. Arroyo v. Rattan Specialties*, 117 D.P.R. 35 (1986), opinión particular del juez asociado HERNÁNDEZ DENTON, apartado II.

[28] En relación a las discusiones en torno a si los delitos de la era virtual alteran o no los conceptos fundamentales de las teorías tradicionales, *vid.* YAR, M., *The Novelty of 'Cybercrime'. An Assessment in Light of Routine Activity Theory*, European Journal of Criminology, Volume 2 (4), 2005, p. 408, donde se analizan las distintas perspectivas desde las que se intenta relacionar la *novedad* del uso de nuevas herramientas y técnicas –en este caso, en relación al *'cybercrime'*– con las tradicionales formas de criminalidad, y la *'routine activity theory'*.

[29] *Arroyo v. Rattan Specialties*, 117 D.P.R. 35 (1986), V. En los comentarios a este apartado al final del texto (*escolios*), recordando que el derecho a la intimidad no tiene carácter absoluto, el Tribual cita dos ejemplos que supondrían *circunstancias apremiantes de mayor peso* que podrían justificar, *en ausencia de otras alternativas efectivas*, un recorte en la intimidad: las agencias de seguridad pública y las industrias farmacéuticas que producen sustancias objeto de control. La necesidad de proteger tales intereses sociales estaría por encima del derecho a la intimidad de los empleados.

sopesar intimidad versus propiedad, que intimidad versus intereses de seguridad nacional.

No obstante, si las circunstancias atentatorias contra el derecho de propiedad de los empresarios supusieran un agravamiento progresivo del contexto empresarial que llegara a poner en peligro la economía nacional ¿se consideraría en ese caso que no existe solución de continuidad entre la propiedad privada y los intereses generales de la economía nacional? Si bien tradicionalmente se recoge en numerosas Constituciones y leyes estatales que la propiedad privada viene delimitada por los intereses generales –es decir, que debe cumplir cierta «función social»[30]–, no es menos cierto y necesario que, al mismo tiempo, deba ser protegida en virtud de esos mismos intereses generales. En definitiva, no puede dejar de considerarse que la empresa también cumple una función social indiscutible, al ser *condicio sine qua non* para la existencia de puestos de trabajo y la generación de riqueza y que, por lo tanto, defender la propiedad de la empresa no es sólo defender al empresario: el daño en su patrimonio repercute a corto, medio o largo plazo, en el conjunto de los trabajadores y en la sociedad entera.

Es importante distinguir el principio general que proscribe un excesivo e injustificado afán de prevención de la criminalidad intra–empresarial en aras de una defensa ilimitada de la propiedad de la empresa, del caso concreto, de los supuestos de hecho en los que existe un patrón de riesgo objetivo, una amenaza real. Cuando en la sentencia se proclama que «el demandante, un ebanista, en su búsqueda legítima del sustento diario, no debe tener que abdicar [de] su derecho a la intimidad permitiendo que el empresario invada su mente y ausculte sus pensamientos», parece en este sentido una declaración rotunda. Sin embargo, que el trabajador no debe renunciar a su derecho a la intimidad –como veremos con detalle– no implica que no queden condicionados los contornos que delimitan ordinariamente la intimidad de las personas. Con ello, la proyección hacia el exterior de las manifestaciones de la personalidad que protege el derecho a la intimidad sufre –no podría ser de otro modo– serias modulaciones en virtud de la entrada del trabajador en la esfera de dominio del empresario.

La tensión inherente a la relación entre privacidad y la seguridad en el contexto laboral ha sido sintetizada de forma magistral en el Documento de trabajo relativo a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo, aprobado el 29 de mayo de 2002 por el Grupo de Trabajo sobre Protección de datos Artículo 29:

«Los trabajadores no dejan su derecho a la vida privada y a la protección de datos cada mañana a la puerta de su lugar de trabajo. Esperan legítimamente encontrar allí un grado de privacidad, ya que en él desarrollan una parte importante de sus relaciones con los demás. Este derecho debe, no obstante, conciliarse con otros derechos e intereses legítimos del empleador, en particular, su derecho a administrar con cierta eficacia la empresa, y sobre todo, su derecho a protegerse de la responsabilidad o el perjuicio que pudiera derivarse de las acciones de los trabajadores. Estos derechos e intereses constituyen motivos legítimos que pueden justificar la adopción de medidas adecuadas destinadas a limitar el derecho a la vida privada de los trabajadores. Los casos en que el empleador es víctima de un delito imputable a un trabajador constituyen el ejemplo más claro»[31].

[30] El artículo 33 de la CE establece: (1) Se reconoce el derecho a la propiedad privada y a la herencia. (2) La función social de estos derechos delimitará su contenido, de acuerdo con las Leyes. (3) Nadie podrá ser privado de sus bienes y derechos sino por causa justificada de utilidad pública o interés social, mediante la correspondiente indemnización y de conformidad con lo dispuesto por las Leyes.

[31] *Vid.* Introducción al *Documento de trabajo relativo a la vigilancia de las comunicaciones electrónicas en el*

Pues bien, del análisis de legitimidad de la prueba del polígrafo corresponde concluir que existen distintas reglas de valoración respecto de la proporcionalidad en el control empresarial. Responden a lógicas distintas y, por tanto, conviene distinguir el control ordinario del empresario sobre la prestación laboral, de aquellas medidas de control que tienen su origen en una respuesta preventiva o reactiva a un patrón de riesgo objetivo[32].

Sin embargo, si bien la lucha contra la delincuencia puede justificar limitaciones en la privacidad debidamente fundamentadas, no puede servir como «patente de corso» que pueda tratar de legitimar medidas limitadoras de la libertad de conciencia del sospechoso e incluso de quien se ha declarado culpable. Una antigua sentencia del Bundesgerichtshof alemán, en el contexto de un caso criminal, ya resolvió que las pruebas de polígrafo violaban la libertad del individuo para tomar sus propias decisiones y actuar de conformidad con su voluntad. De acuerdo con tal razonamiento, esas pruebas eran inadmisibles en tanto que suponían un atentado contra la condición ética del acusado como «persona moral independiente».

El tribunal se expresó en los siguientes términos: «Estos principios de derecho constitucional y de procedimiento criminal están cimentados en el hecho de que, al enfrentarse a la comunidad, aun un sospechoso o uno que merezca ser castigado se considera una persona moral independiente; al establecerse su culpa, éste puede y debe expiarla bajo la ley que ha sido violada; sin embargo, más allá de tales restricciones estatutarias, no debe sacrificarse su personalidad al propósito público de combatir el crimen, aunque esto es sin duda muy importante».[33]

III. CUESTIONES ÉTICO-JURÍDICAS EN TORNO A LA VIDEO-VIGILANCIA EN LA EMPRESA

Desde una aproximación antropológica a la cultura del trabajo, con el fin de organizar de forma adecuada una empresa se requiere un mínimo de confianza y un mínimo de control. La suma de esfuerzos individuales necesita al mismo tiempo ciertas pautas de coordinación, dirección y control para proporcionar unidad de sentido al trabajo individual en el marco del fin corporativo. A tal propósito, confianza y control no dejan de ser dos elementos igualmente necesarios e interdependientes. Así, se puede afirmar que la dignidad humana es merecedora de expectativas basadas en la confianza, sin perjuicio de que deba realizarse complementariamente cierta actividad de control. Si existe tal actividad de control es porque, en realidad, se ha generado previamente una expectativa basada en la confianza. No son por tanto actitudes contradictorias, sino de

lugar de trabajo, aprobado el 29 de mayo de 2002 por el GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS ARTÍCULO 29, en la introducción. El Grupo de Trabajo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Se trata del órgano consultivo independiente de la UE sobre protección de los datos y la vida privada. Sus tareas se definen en el artículo 30 de la Directiva 95/46/CE y en el artículo 14 de la Directiva 97/66/CE.

[32] Tampoco puede dejar de apreciarse que entre una *respuesta preventiva* y una *respuesta reactiva* hay diferencias sustanciales. En realidad, la expresión *respuesta preventiva* no deja de ser una *contradictio in terminis*.

[33] Sentencia del Bundesgerichtshof (I. Strafsenat), 16 de febrero de 1954, 5 Entscheidungen des Bundesgerichtshofes in Strafsachen 332, 334, citado en H. SILVING, *Testing of the Unconscious in Criminal Cases*, 69 Harv. L. Rev. 683, 688, 689 (1956), –énfasis suplido y traducción de la sentencia en *Arroyo v. Rattan Specialties*, 117 D.P.R. 35 (1986), *vid.* nota al final del texto n. 15–.

algún modo complementarias, en tanto que se trata de un fiel reflejo de aquellas raíces antropológicas en las que se basan tanto la dinámica de la confianza como la lógica del control en el ámbito de la empresa.

En tal sentido, «no existe alternativa funcional a la confianza»[34], aunque ésta sea un elemento constitutivo que deba armonizarse con el contrapeso del necesario control. La empresa no surge como un nexo de contratos, ni como una coincidencia de curvas de preferencia, sino como una asociación de personas comprometidas entre sí en una tarea común, a la que contribuyen con sus propios talentos. El necesario equilibrio entre confianza y control describe así las posibilidades y límites de la libertad humana en sus relaciones interpersonales. Tanto el liderazgo del empresario como la lealtad del trabajador deben de este modo inspirarse en la armonía entre confianza y control. Por tanto, el mantenimiento de una razón comunitaria junto a la implementación de políticas razonables de control empresarial debe servir de fundamento ético y jurídico a unas relaciones laborales equitativas.

El Derecho debería reflejar esa búsqueda de equilibrio armónico. En este sentido, es improbable que algún Estado respalde en la actualidad una legislación que prohíba de forma absoluta cualquier manifestación de vigilancia electrónica en el lugar de trabajo, incluso en aquellos países en los que está arraigada una fuerte cultura de protección de la intimidad en el ámbito laboral. Por el contrario, se han aprobado leyes sobre la vigilancia electrónica en el lugar de trabajo en un contexto en el que se reconoce –en líneas generales– la validez de las razones de la empresa para tal vigilancia, al mismo tiempo que se toman en consideración los intereses de los trabajadores en proteger su privacidad en el ámbito laboral[35].

Nuestro punto de partida se define así por la búsqueda de un punto de equilibrio en la adecuada vigilancia del empresario respecto de los trabajadores y del entorno empresarial. En virtud de tal «poder de vigilancia y control» del empresario[36], éste puede instalar cámaras de video–vigilancia mediante las que se pueden captar y acceder a imágenes en las que aparezcan trabajadores o terceras personas. Sin embargo, antes de abordar desde un punto de vista ético–legal con qué finalidad y alcance se pueden permitir tales prácticas, conviene subrayar un hecho relevante, que podría parecer obvio. Una vez en funcionamiento, la actividad de las cámaras van a registrar indistintamente tanto la posible comisión de un delito o el incumplimiento laboral de un trabajador, como algunas manifestaciones inherentes a su intimidad –o a la posible expectativa a no ser observado–.

Así se recoge, por ejemplo, en una de las alegaciones presentadas por el recurrente en la STC 186/2000, al afirmar que «la instalación por parte de la empresa en la que prestaba servicios de un circuito cerrado de televisión enfocando su puesto de trabajo lesiona su derecho a la intimidad, porque aunque esta clase de instalaciones tengan como fin controlar el trabajo, también registran el resto de

[34] *Vid.* BRISEBOIS, R., *Sobre la confianza*, Cuadernos Empresa y Humanismo, Vol. 65, Pamplona 1997, p. 16–19, donde describe la dinámica de la confianza en cuatro fases: el período del compromiso, el período de la expectativa, la actuación del fiduciario, y la reaparición de la confianza.

[35] LASPROGATA, G., KING, N.J., PILLAY, S., Regulation of electronic employee monitoring: identifying fundamental principles of employee privacy through a comparative study of data privacy legislation in the European Union, United States and Canada, 2004 Stanford Technology Law Review 4, p. 27.

[36] Por remisión del artículo 2.2 LO 1?1982, el legislador considera una *intromisión legítima* aquélla que se realiza en virtud de la potestad de vigilancia empresarial, respetando los límites del artículo 20.3 ET.

actos del trabajador pertenecientes a su intimidad, toda vez que este tipo de control no es selectivo en cuanto a las imágenes que capta».

La reflexión entorno a las prácticas de video–vigilancia en el marco de las posibles medidas de control empresarial debe abarcar en realidad muy distintas formas de vigilancia. La variedad en extensión, intensidad y tipología de los distintos medios de video–vigilancia nos lleva a tener que analizar casos prácticos también muy distintos, permitiendo ampliar el campo de discusión e interpretar a través de la analogía aquel conjunto de situaciones que tienen lugar en lo que se viene denominando «electronic monitoring». No obstante, conviene adelantar una importante salvedad: mientras que el control electrónico suele aplicarse sobre herramientas de trabajo –el ordenador, el teléfono, el GPS del vehículo de la empresa–, la video–vigilancia se proyecta sobre una realidad mucho más compleja que viene a situarse en la «periferia del proceso de trabajo»[37].

Así pues, en función de las prestaciones del sistema de cámaras –por ejemplo, si llevan incorporados sistemas de audio–, se pueden registrar con mayor o menor detalle los muy distintos tipos de actividad de los trabajadores. La variedad de situaciones y conflictos de intereses en torno a la privacidad en la empresa es ciertamente extensa: por tal motivo, desde el punto de vista de las necesidades de vigilancia y control, conviene distinguir las actividades peligrosas que pueden amenazar bienes jurídicos relevantes, de aquellas otras actividades inocuas que pueden ser objeto de conocimiento y que merecen ser protegidas.

(A) Un trabajador decide confiar un secreto personal a un compañero en el transcurso de un desplazamiento necesario dentro del propio centro de trabajo. Una trabajadora redacta unas notas íntimas en una libreta personal, durante el descanso de apenas quince minutos que permite el convenio colectivo. Dos trabajadores mantienen una relación afectiva y, una o dos veces durante la jornada, se besan de forma no prolongada, sin interrumpir apenas su labor. Dos trabajadoras discuten sobre sus opiniones políticas mientras realizan una ocupación manual, plenamente compatible con mantener una conversación entre compañeros.

(B) Un trabajador aprovecha la cercanía de su puesto de trabajo respecto de la fotocopiadora de la empresa para realizar sin autorización copias no relacionadas con su trabajo. Un directivo intenta acosar a una secretaria en una zona común, sin la presencia de testigos. Un trabajador comparte pequeñas dosis de droga para autoconsumo dentro del recinto de la empresa. Un directivo pasa largos ratos de su jornada laboral delante de la pantalla del ordenador conectado a páginas de ocio en Internet.

(C) Las cámaras de vigilancia de un centro comercial fueron instaladas con fines de seguridad general y no para vigilar a los empleados. Posteriormente, las cámaras detectan a un trabajador bebiendo un zumo de una estantería. La grabación fue presentada como prueba para despedir al trabajador. ¿Deben los Tribunales admitir la prueba como válida?[38] El hecho de hallarse las cámaras en un lugar visible ¿tiene relevancia a efectos de vulnerar la expectativa de intimidad del trabajador? La finalidad para la que fue instalada la cámara ¿condiciona la admisibilidad de la prueba? Una empleada del hogar es acusada de cometer un hurto en la casa en la que trabajaba. El Tribunal no

[37] LASPROGATA, G., KING, N.J., PILLAY, S., *Ibid*., §17.
[38] Con frecuencia, la discusión jurídica se circunscribe a la admisibilidad o no de la prueba.

aceptó como prueba la grabación mediante cámara oculta que presentó el empleador, porque se vulneró el derecho a la intimidad de la empleada.

A la vista de los ejemplos anteriores, debe tenerse en cuenta que la vigilancia en la empresa puede encaminarse tanto a fines de seguridad y prevención del delito como a controlar la prestación laboral, sin que, como es lógico, se pueda pretender o perseguir el conocimiento de aspectos de la esfera personal no relacionados con la prestación laboral. Sin embargo, no es posible separar con nitidez, ni en el plano teórico ni en el práctico, ciertos aspectos íntimos de la persona, de aquellas conductas que –por tener lugar en el contexto laboral– son susceptibles de control. En tanto que tales manifestaciones personales del trabajador son frecuentemente indisociables respecto del desarrollo de la prestación laboral, se requiere algún tipo de protección jurídica frente a la vigilancia empresarial. Además, aunque las imágenes no afectaran a la esfera íntima de la persona del trabajador, no dejarían de ser consideradas «datos de carácter personal» y, por tanto, protegidas como tales[39].

Nuestra perspectiva de análisis no parte del derecho positivo, aunque se realicen puntuales referencias a distintas normativas que regulan este ámbito[40]. Los intentos de cualquier legislador por regular esta materia –o las regulaciones que puedan derivarse de un contexto «inter partes»– siempre serán aproximaciones al problema que, a pesar de sus pretensiones por abarcar toda la casuística, no podrán llegar a resolver algunos casos más complejos o más humanos[41]. En cuanto al sujeto responsable que realiza un control mediante video–vigilancia, éste puede ser tanto el Estado como un particular (en este caso, el empresario)[42]. Sin embargo, ¿pueden existir diferencias sustanciales en función del sujeto que realiza el control? Por de pronto, conviene resaltar que la vigilancia estatal en espacios públicos sólo se orienta a la seguridad y prevención de la delincuencia. A este respecto, en el derecho positivo español la Ley Orgánica 4/1997, de 4 de agosto[43], norma básica en la materia, regula la utilización de videocámaras por las fuerzas y cuerpos de seguridad en lugares públicos.

[39] *Vid.* por ejemplo, las definiciones legales de *datos de carácter personal* y *fichero* contenidas en el artículo 3, a) y b) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

[40] Nuestras reflexiones no se fundamentan, por tanto, directamente en el derecho positivo existente, tal como se regula la materia en la actualidad, ni en las actuales corrientes doctrinales en materia de derechos constitucionales, aunque se citen normativas y algunas sentencias del Tribunal Constitucional como pauta o instrumento de análisis. Se pretende aportar desde una concepción ética coherente algunas herramientas ético–jurídicas que permitan analizar la vigilancia mediante CCTV y sus límites.

[41] En este sentido, afirma un sector de la doctrina que la jurisprudencia tiene, en materia de colisiones entre derechos fundamentales, una *función creativa* como en ningún otro ámbito del derecho positivo.

[42] La vigilancia ejercida en la empresa deberá respetar la regulación establecida por la Ley 23/1992 sobre seguridad privada y su Reglamento de desarrollo, en cuanto a los requisitos que deben cumplir las empresas de seguridad. El control deberá realizarse mediante la contratación de una empresa de seguridad privada: el empresario no podrá en ningún caso tener un servicio de vigilancia propio, realizado por parte de la plantilla de la empresa, debiendo acudir siempre a la subcontratación. *Vid.* también la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

[43] El artículo 3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal establece que «se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales: […] e) Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia».

Esta ley establece en su artículo primero que viene a «regula[r] la utilización por las Fuerzas y Cuerpos de Seguridad de videocámaras para grabar imágenes y sonidos en lugares públicos, abiertos o cerrados, y su posterior tratamiento, a fin de contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública. Asimismo, esta norma establece específicamente el régimen de garantías de los derechos fundamentales y libertades públicas de los ciudadanos que habrá de respetarse ineludiblemente»[44].

1. **Video-vigilancia y prevención situacional del delito en el lugar de trabajo**

A. *La prevención situacional del delito como estrategia de prevención*

En su conocido artículo «Situational Crime Prevention» (1995), Ronald Clarke describe las estrategias de vigilancia como un importante instrumento en el marco de la prevención situacional del delito[45]. Si en términos generales la prevención del delito se encamina a reducir los riesgos de que se puedan cometer hechos de naturaleza delictiva –o al menos disminuir su gravedad mediante la intervención sobre sus causas–, la prevención situacional de la delincuencia se encamina de modo específico a incidir en aquellas causas que el delincuente encuentra o busca en las inmediatas circunstancias del hecho delictivo[46].

El enfoque particular que caracteriza a la prevención situacional del delito se refiere, descrita a grandes rasgos, a aquellas estrategias preventivas encaminadas a reducir las oportunidades de cometer delitos dentro de un entorno físico determinado. Esta perspectiva tiene por objeto principal de análisis, por tanto, el entorno delictivo, sin prestar apenas atención a la persona del delincuente[47]. Así, un lugar determinado –en cuanto posible objetivo para potenciales delincuentes–, se protege frente a la comisión de posibles delitos mediante la introducción de mayores dificultades para la perpetración de los mismos, o haciendo menos rentable su realización en ese preciso lugar –por el elevado riesgo de ser descubierto–. Por contraposición a los medios de naturaleza normativa, desde este enfoque criminológico se trata de introducir aquellos medios cognitivos[48] que pueden influir en la voluntad de delinquir, bien haciéndola estéril al imposibilitar la consumación del hecho delictivo –mediante

[44] En su desarrollo reglamentario, son interesantes las distinciones ético–jurídicas que subyacen a los diferentes presupuestos y límites que justifican la utilización de *dispositivos fijos* y *equipos móviles* (establecidos por los artículos 2.2 y 2.3 del Decreto 134/1999, de 18 de mayo, de regulación de la *video–vigilancia* por parte de la policía de la Generalitat de Catalunya y de las policías locales).

[45] CLARKE, R.V. (1995) 'Situational Crime Prevention', in M. Tonry and D. Farrington, (eds.), *Building a Safer Society. Strategic Approaches to Crime Prevention. Crime and Justice: A Review of Research* 19: 91–150, Chicago: University of Chicago Press, pp. 113–114.

[46] MCLAUGHLIN, E., MUNCIE, J., *The Sage Dictionary of Criminology*, 2007, p. 383. La primera formulación de la teoría de la prevención situacional del delito se explicita en CLARKE, R., *Situational Crime Prevention: Its Theoretical Basis and Practical Scope*, Crime and Justice: An Annual Review of Research, vol. 4, Chicago, 1983.

[47] El cambio de enfoque metodológico para la prevención del delito –no atender a las características *personales* del delincuente– puede manifestar un cierto *pesimismo antropológico*. Así, el *desencanto posmoderno* de la Criminología ante el *fracaso resocializador*, llevaría a abandonar la ingenuidad por la que se pretendía incidir sobre la *persona* del delincuente –por tratarse de una quimera de tiempos anteriores– para focalizarse en el *entorno*, en cuanto elemento sobre el que sí se puede incidir. En ese sentido, las variables ambientales sí que pueden ser objeto de *rigurosos* estudios empíricos, al posibilitar su reducción a datos cuantitativos.

[48] Para una mayor profundización en la distinción entre medios *cognitivos* y *normativos* puede consultarse *in genere* JAKOBS, G., *Sociedad, Norma y Persona en una Teoría de un Derecho Penal Funcional*, 1996 (trad. M. CANCIO MELIÁ), especialmente la introducción.

barreras o impedimentos absolutos para acceder al objeto–, bien desincentivando el intento de cometer el delito por la alta probabilidad de su detección[49].

En el contexto de las tesis que sustentan la «teoría de la prevención situacional», la implementación de las estrategias de video–vigilancia persigue una doble finalidad en la lucha eficaz contra el delito. Así, ésta se encamina indistintamente a prevenir y a responder frente a la comisión de un delito, pretendiendo por tanto (1) disuadir ex ante a potenciales delincuentes por el sólo conocimiento de que sus acciones van a ser visibles; y (2) posibilitar o facilitar ex post facto la detección de hechos delictivos y la identificación de los delincuentes. A este respecto, aunque conviene señalar que la instalación de cámaras de seguridad es tan sólo uno entre distintos posibles métodos de vigilancia, este tipo de medidas –y en sentido amplio la vigilancia electrónica– son de enorme eficacia disuasoria y están siendo utilizadas de forma generalizada en el ámbito de las relaciones laborales –desde hace ya tiempo–, en ocasiones de forma intensa, especialmente en los países del ámbito anglosajón.

Ya en la década de los noventa, el uso de diversos mecanismos de vigilancia electrónica sobre los trabajadores en el sector privado comenzó a tratarse como objeto de particular estudio y debate. En 1996, la American Civil Liberties Union National Task Force on Civil Liberties in the Workplace llegó a estimar que alrededor de cuarenta millones de trabajadores estaban siendo sujetos a algún tipo de vigilancia electrónica. En 1997, estudios de la American Management Association indicaron que al menos dos terceras partes de sus miembros utilizaban algún tipo de vigilancia electrónica hacia sus empleados[50]. En 2001, los datos de otra encuesta realizada de nuevo por la American Management Association elevaron al 77.7% el número de encuestados que grababa y revisaba las comunicaciones de los trabajadores u otras actividades, ya fuera mediante la monitorización de llamadas telefónicas o mensajes de voz, la videovigilancia sobre el modo de realizar la prestación laboral o el registro del correo electrónico o de archivos de ordenador[51].

Tal vez por este motivo, el debate ético–jurídico en torno a los límites y las garantías que debe respetar la vigilancia mediante circuitos cerrados de televisión (CCTV[52]) está cobrando una importancia creciente en nuestros días. Y, en este contexto, el conflicto latente entre libertad y seguridad necesita resolverse mediante una sólida argumentación, a fin de analizar los distintos casos en que pueda justificarse un uso legítimo de tales medios de vigilancia.

[49] Sobre la teoría de la prevención situacional del delito *vid.:* CLARKE, R.V. (1995) 'Situational Crime Prevention', in M. TONRY, D. FARRINGTON, (eds.), Building a Safer Society. Strategic Approaches to Crime Prevention. Crime and Justice: A Review of Research 19: 91–150, Chicago: University of Chicago Press, pp. 91–150; MEDINA ARIZA, J.J., *El control social del delito a través de la prevención situacional*, Revista de Derecho Penal y Criminología, núm. 2 (1998), p. 281–323.

[50] *Vid.* Sentencia del Tibunal Supremo de Puerto Rico, Caso *Héctor Vega Rodríguez v. Telefónica de Puerto Rico*, 2002 TSPR 50, 156 DPR, apartado IV *in principio*). Para acceder a la evolución de los datos y el crecimiento del mercado de CCTV y su masiva expansión en los noventa, tanto en espacios públicos como en el lugar de trabajo: *vid.* MCCAHILL, M., NORRIS, C., *Watching the workers: Crime, CCTV and the Workplace*, in DAVIS, P., FRANCIS, P., JUPP, V., *Invisible Crimes. Their Victims and their Regulation*, London, 1999, pp. 208-209.

[51] FINKIN, M.W., Information Technology and workers' privacy: the United States Law, in JEFFERY, M., Information Technology and workers´ privacy: a comparative study, Comparative Labor Law & Policy Journal, volume 23, number 2, 2002, p. 474.

[52] En el ámbito anglosajón se emplea la expresión *closed circuit television cameras* (CCTV) para hacer referencia a las cámaras de vigilancia o seguridad.

Conviene realizar, a este respecto, una consideración preliminar. Si la instalación de un sistema de CCTV se utiliza como instrumento de prevención situacional del delito, no tendría sentido que las cámaras cubrieran sin una particular necesidad toda la superficie del recinto empresarial, a no ser que los objetivos delictivos estén presentes por todo el espacio físico que comprende la empresa y no sea posible acudir a otros medios de control menos restrictivos. Es decir, si la finalidad es prevenir situaciones criminógenas, habrá que justificar que en el radio de acción de las cámaras se generan con mayor probabilidad situaciones u ocasiones propicias para cometerse un hecho delictivo.

B. *Análisis de la irrupción de sistemas de CCTV en el lugar de trabajo*

Algunas investigaciones empíricas en el lugar de trabajo –uno de los contextos que Foucault pensó que podría beneficiarse de las tesis del Panopticum– indican que incluso en el entorno laboral la vigilancia tiene en parte efectos negativos. Según tales estudios, los trabajadores que son objeto de monitorización tienen más probabilidades de sentirse con menor confianza, menor motivación, menores sentimientos de lealtad y con mayor stress que aquellos trabajadores que no están sometidos a vigilancia [53].

Según Slobogin, la mejor investigación a este respecto procede de Botan. En un estudio realizado sobre la base de las respuestas de 465 trabajadores –en el sector de la communications industry–, se descubrió que los trabajadores que son vigilados experimentan distintos «efectos panópticos», incluyendo entre ellos un sentido reducido de la privacidad, una incertidumbre creciente –inseguridad en el trabajo– y una comunicación menor[54].

En un segundo estudio basado en los resultados de la misma encuesta, dirigido por Vorvoreanu, se aprecian algunos otros efectos seriamente perjudiciales. El meta–mensaje insoportable [overwhelming meta–message] que la misma vigilancia parece enviar a los trabajadores es que no se confía en ellos. En una interpretación muy próxima, muchos trabajadores ven la vigilancia como si se tendiera una trampa a alguien –quizá se trate de ellos mismos– para poder practicar un despido o en su caso adoptar medidas disciplinarias. Muchos también perciben la vigilancia como si implicase que la dirección de la empresa considera que merecen ser tratados como de un modo infantil. Los trabajadores intensamente vigilados manifiestan tener una menor motivación para sobrellevar una mayor carga de trabajo o para desempeñar trabajos de mayor calidad. Finalmente, los trabajadores intensamente vigilados manifiestan una lealtad menor a la organización, un stress creciente en el trabajo y un menor entusiasmo incluso para ir a trabajar, todo ello apoyado en comentarios personales –métodos cualitativos–[55].

Los distintos efectos positivos y negativos examinados deben pues contextualizarse. El contexto de nuestro análisis ético–jurídico toma como punto de referencia esencial la valoración del justo equilibrio entre confianza y control en las relaciones laborales como criterio de justicia y de utilidad. Pretendemos afirmar que mediante la búsqueda de soluciones que armonicen ambos extremos y reduzcan la tensión natural que tiende

[53] SLOBOGIN, C., *Privacy at Risk*, Chicago, 2007, p. 95 y nota núm. 129.

[54] BOTAN, C., "Communication Work and Electronic Surveillance: a Model for Predicting Panoptic Effects", 63 *Communications Monographs* 293, 308–9 (1996).

[55] BOTAN, C., VORVOREANU, M., *What are you really saying to me?*, Electronic Surveillance in the Workplace (June 2000) (unpublished manuscript, on file with author), citado en SLOBOGIN, C., *Privacy at Risk. The New Government Surveillance and the Fourth Amendment*, Chicago, 2007, nota núm. 129.

a enfrentarlos, se multiplicarán las consecuencias positivas, a pesar de su difícil verificación empírica. Ciertamente, cualquier trabajador manifestará que preferiría no estar sometido a vigilancia, siendo así que de tal opción preferencial no pueden extraerse conclusiones fiables, ni tampoco puede derivarse que, por este motivo, esté predispuesto a cometer irregularidades. Simplemente, pertenece a la propia naturaleza humana el deseo de no ser objeto de control por nadie.

La implementación de sistemas de CCTV puede ser evaluada así desde muy distintas perspectivas. Se pueden proponer consideraciones éticas o principios filosófico–jurídicos, verificar los efectos psicológicos u organizacionales o valorar las medidas en términos de rentabilidad económica. A grandes rasgos, cabría señalar dos ámbitos de análisis: (1) aquél que trata de aportar consideraciones valorativas en base a principios normativos, o construir teorías explicativas que describan cómo opera el sistema en función de las alternativas (perspectiva ex ante); y (2) aquél otro que se dirige a verificar los efectos o consecuencias en función de las posiciones adoptadas (perspectiva ex post). Sin embargo, las dificultades de verificación de principios y postulados en el campo de las ciencias sociales reducen las posibilidades de poder extraer conclusiones generales o establecer vínculos causales, tal y como se acaba de apuntar en líneas precedentes.

Así, desde un punto de vista valorativo o normativo, los principios éticos que limitan la actividad de vigilancia empresarial deberían tener en cuenta el objeto de la acción, el fin que persigue y las circunstancias concomitantes[56]. A los efectos que aquí interesan, la bondad o maldad intrínseca del objeto moral –su conveniencia ética–, podría atenuarse o agravarse en base al fin y a las circunstancias. Sin embargo, desde concepciones consecuencialistas de la ética, se intentaría cualificar la acción en función únicamente de las consecuencias que trae consigo[57]. Es decir, el sacrificio de unos pocos podría justificarse por los mayores beneficios individuales o sociales que comporta. De este modo, en el balance global, teniendo en cuenta el conjunto de consecuencias de una determinada política empresarial, se podrían relativizar los efectos negativos de una determinada acción.

Sin embargo, entre el conjunto de instrumentos de dirección empresarial, la actividad de vigilancia de los trabajadores, en sí misma considerada, debe ser valorada de forma neutral. El objeto de la acción no condiciona a tales efectos el juicio de valor o de desvalor de forma intrínseca[58]. Tal como sostiene Alder, la complejidad del debate en torno a la monitorización electrónica de los trabajadores –pudiéndose extrapolar a toda forma de vigilancia empresarial– no debe por este motivo resolverse de forma

[56] *Vid.* al respecto, *in genere*, MELÉ, D., *Ethics in decisión–making*, IESE Technical note (TDN–118–E), 1998.

[57] Desde la *ética teleológica*, «an act is right if and only if it or the rule under which it falls produces or is intended to produce at least as great a balance of good over evil as any available alternative, an act is wrong if and only if it does not do so» (FRANKENNA, W., *Ethics*, 2nd ed., 1973, p. 14). El matiz que se añade desde concepciones utilitaristas es que la acción no sólo es *conveniente* sino *obligatoria* (*vid.* ALDER, G.S., *Ethical Issues in Electronic Performance Monitoring*, 1998, p. 730, al referirse al *utilitarismo* como una específica *teoría teleológica o consecuencialista*.

[58] ALDER, G.S., *Ibid.*, 1998, p. 741, argumentando que la discusión no debe girar en torno a si la monitorización electrónica en el ámbito empresarial es en sí misma ética o no lo es, sino que debe centrarse en cómo se lleva a cabo y en qué condiciones se realizará éticamente.

simplista (win–lose approach), como si el objeto de la acción fuera, en términos absolutos, intrínsecamente bueno o malo.

Así, en el balance de argumentos y consideraciones al respecto deben aportarse conjuntamente (1) argumentaciones en términos teleológicos que resalten los efectos positivos de la vigilancia en base a que la monitorización beneficia a las organizaciones, a los clientes y a la sociedad en general; y (2) argumentaciones en términos deontológicos por los que se establezcan límites, en tanto que la monitorización viene a deshumanizar a los trabajadores, invade la privacidad de las personas, aumenta los niveles de stress y perjudica la salud, y disminuye la calidad de vida en el trabajo. Como parece lógico, la mayoría de argumentos en favor de la monitorización electrónica de los trabajadores tiene un trasfondo basado en las tesis utilitaristas.

Desde la perspectiva teleológica, se tiene presente en tal análisis que las prácticas organizacionales –entre las que se encuentra la vigilancia electrónica– se evalúan en función de la maximización de beneficios (the greatest balance of good over evil). De este modo, cualesquiera consecuencias negativas se someten a una ponderación final. En este sentido, la capacidad para evaluar la efectividad y competitividad a través de los datos proporcionados por la vigilancia electrónica deviene esencial para competir en un mercado global. Se ha demostrado repetidamente a este respecto que una efectiva monitorización conduce a un incremento de la productividad, a una mejora de la calidad del servicio y a una reducción de costes. Las compañías que han instalado un sistema de control de las llamadas pueden esperar como mínimo una reducción del 10% en la facturación telefónica y simultáneamente un aumento de la productividad. Por otra parte, escuchar las llamadas telefónicas supone un instrumento eficaz en la formación de los operadores y asegura la calidad del servicio. Por todo lo cual, finalmente se concluye que aunque es difícil –sino imposible– valorar empíricamente los resultados generales que la monitorización electrónica tiene en el conjunto de la sociedad, las prácticas que benefician a las empresas deben beneficiar también –indirectamente– al conjunto de la sociedad. La defensa de los resultados satisfactorios se basa en un importante número de casos estudiados y evidencias empíricas[59].

No obstante, desde perspectivas deontológicas se argumenta que el enfoque utilitarista no tiene en consideración el proceso a través del cual se llega a tales resultados y si existe, en este sentido, un deber de actuar de una determinada manera sin que se deba tener en cuenta las consecuencias (positivas) que puede conllevar[60]. Las posturas deontológicas se fundamentan –al menos algunas de ellas– en el imperativo categórico kantiano (el hombre es un fin en sí mismo y nunca puede ser tratado como un medio), aplicándolo al ámbito de la vigilancia empresarial, de forma que no tendría justificación ningún acto que lesione a otra persona reduciendo su libertad, aunque pueda beneficiar a otros[61].

El argumento principal de una concepción deontológica reside por tanto en el hecho de que el proceso implica una invasión en la privacidad de los trabajadores. Se argu-

[59] ALDER, G.S., *Ibid.*, 1998, pp. 730–732.
[60] FRANKENNA, W., *Ethics*, 2nd ed., 1973, (*cfr.* ALDER, G.S., *Ibid.*, 1998, p. 732).
[61] WERHANE, P., Persons, Rights, and Corporations, 1985.

menta al respecto que la dignidad del trabajador requiere una protección de la privacidad de la persona. Sin embargo, la cuestión relevante es si la dignidad de la persona del trabajador, en términos de privacidad, debe ser protegida de forma homogénea sin atender al contexto en que se produce la invasión en la privacidad o sin atender al contexto que genera las reglas de delimitación misma de la privacidad.

Es ilustrativa en este punto la declaración del senador Simon, en la fase de presentación de un proyecto de ley norteamericano relativo a la privacidad de consumidores y trabajadores: «Como Nación, hemos dado respaldo a leyes que protegen nuestra privacidad y evitan que podamos ser espiados por nuestros conciudadanos y nuestro gobierno, en cualquier sitio excepto en el lugar de trabajo. Estados Unidos permanece solo junto a Sudáfrica en omitir la protección de los derechos de los trabajadores en este punto […] en realidad es una triste ironía que mientras el FBI debe solicitar por exigencia de la ley autorización judicial para intervenir una conversación telefónica, incluso en casos de seguridad nacional, a los empresarios les está permitido espiar libremente a sus trabajadores y al público»[62].

Aunque de forma limitada, también se ha tratado de argumentar desde posturas deontológicas que la vigilancia electrónica en último término viene a perjudicar la productividad de la organización, la calidad del proceso productivo y del propio trabajo de los empleados[63]. Podría objetarse *prima facie* que carece de coherencia interna una tal argumentación de corte consecuencialista desde una postura que se dice deontológica. Sin embargo, deberían realizarse las siguientes consideraciones. En primer lugar (1) podría admitirse como un mero intento de rebatir el pretendido criterio de la maximización de beneficios que comporta la vigilancia electrónica. Además, (2) desde una postura deontológica, las consecuencias no debieran estar per se excluidas de su ámbito de análisis, sin que por ello constituyan el centro de referencia para la calificación ética de la acción. En este sentido, pueden y deben influir en el juicio, especialmente en aquellas acciones que de suyo son éticamente neutrales. En tercer lugar, (3) el fraccionamiento del análisis, especialmente en el terreno ético–moral, no conduce generalmente a respuestas plenamente satisfactorias. Finalmente se aduce que (4) en realidad, el hecho de perjudicar en líneas generales la productividad de la empresa sería un simple signo perceptible en ese caso de la falta de idoneidad o comunicación de la política de vigilancia empresarial.

En este sentido, en referencia a la última de las consideraciones apuntadas, las estrategias comunicativas del diseño e implementación de sistemas de monitorización debería poder resolver el dilema ético planteado y aportar soluciones que armonicen las posturas deontológicas y teleológicas[64]. En realidad, la idoneidad del sistema de delimitación de la privacidad en el trabajo se identifica en gran medida con una adecuada comunicación. Así, el elemento ético–comunicativo en las políticas de control

[62] *Vid.* U.S. Senate, Statements on introduced bills and joint resolutions, 1993, citado en ALDER, G.S., *Ethical Issues in Electronic Performance Monitoring*, 1998, p. 733.

[63] NUSSBAUM, K., DU RIVAGE, V., *Computer Monitoring: Mismanagement by Remote Control*, Business and Society Review 56, 1986, pp. 16–20.

[64] En la misma línea ALDER, G.S., *Ibid.*, 1998, p. 737, al referirse al «communicative–ethical approach to Electronic Performance Monitoring» como elemento diferenciador de un planteamiento ético de la política empresarial.

deviene un factor esencial en la calificación ética de una determinada práctica empresarial. Sólo una política manifiestamente abusiva, aunque fuera debidamente comunicada, sería no–ética. Y, en este sentido, el carácter abusivo y las circunstancias de cada empresa nos remiten a formas y soluciones distintas, adaptadas al caso concreto (made–to–measure).

Tal como apunta Alder, el diseño e implementación del sistema por parte de la empresa debería cumplir los siguientes requisitos: (1) los trabajadores sujetos a monitorización deberían poder participar y comunicar sus preferencias y sugerencias en el diseño del sistema; (2) la empresa debería comunicar toda práctica relativa a la monitorización e informar a los trabajadores cuando ésta se esté llevando a cabo; (3) la empresa debe complementar la información proporcionada por el sistema de monitorización con la información suministrada mediante un contacto humano personalizado con los trabajadores; y finalmente, (4) se deberían dar pasos que aseguren que tal feedback no tiene efectos punitivos [65].

Este punto de vista es compatible con regulaciones jurídicas flexibles que garanticen debidamente los criterios de proporcionalidad. El Derecho debe establecer, en este sentido, aquellos límites más allá de los cuales sería absolutamente intolerable que se afectara la privacidad de los trabajadores. La norma jurídica debe pues tratar de fijar, mediante una serie de principios y pautas objetivas, una «línea roja infranqueable». Pero al mismo tiempo, debe dejar a la autonomía del empresario la política de control y privacidad que mejor se adapte a las necesidades de la empresa y a las particularidades de los trabajadores. En última instancia, es el propio empresario el que debería auto–limitarse, ya que en función del modo de enfocar la tensión entre privacidad y control depende la productividad de la empresa.

C. *El impacto de la video–vigilancia en la delincuencia intra–empresarial*

Tras el análisis preliminar en torno a la irrupción de sistemas de CCTV y vigilancia electrónica en el lugar de trabajo, conviene centrarse a continuación en la valoración de los efectos que tales medidas pueden tener en las irregularidades y delitos que se cometen en el entorno empresarial. Sin embargo, como se señaló *supra*, la realidad del «employee crime» presenta unos contornos difusos.

Tal y como he analizado detenidamente en otro lugar [66], aquellos delitos que se cometen contra la empresa adolecen, en numerosas ocasiones, de un carácter difuso que los convierten en «delitos invisibles», sin víctima aparente y de realización continuada en el tiempo. Así, su carácter imperceptible impide tazar una línea divisoria entre delito e irregularidad, al menos en los efectos y repercusión que comportan en la economía de la empresa. Ello no es óbice para que la suma continuada de pequeñas irregularidades pueda generar de hecho un efecto devastador, irreparable y a veces definitivo. El desarrollo del fenómeno ha sido descrito acertadamente por Laureen Snider como «theft of time», en cuanto que se trata de un *continuum* que viene a surgir de la malversación del tiempo y las propiedades del empresario por los trabajadores, fenómeno que tiene sus raíces históricas en el ambiente laboral y el discurso taylorista del siglo XIX [67].

[65] ALDER, G.S., *Ibid.*, 1998, p. 737.
[66] AGUSTINA SANLLEHÍ, J.R., *El delito en la empresa*, Barcelona, 2009.
[67] SNIDER, L., *Crimes against capital: Discovering theft of time*, Social Justice, vol. 28, no. 3, 2001, pp. 105–

Sin embargo, para comprender adecuadamente el impacto de la implementación de sistemas de CCTV en el lugar de trabajo, McCahill y Norris consideran necesario atender al significado global y a las enormes consecuencias que la irrupción de CCTV tiene en la estructura organizacional de la empresa, y en la economía en general. En primer lugar, la introducción de CCTV implica un incremento de la visibilidad respecto de todo un conjunto de prácticas y asunciones tácitas que se generan en torno a las «recompensas ocultas» en el lugar de trabajo (hidden rewards)[68]. Así, una tal mayor visibilidad crea incomodidad en sistemas de cierta complicidad colectiva: ante la evidencia de las cámaras es ciertamente más problemático permitir tales prácticas como si nadie las conociera (turning a blind eye). Ante el cambio de situación, las construcciones del lenguaje y los subterfugios morales para hacer referencia a ciertas prácticas como «fiddles» –trapicheos, pequeñas trampas– y «perks» –ventajas o beneficios adicionales– se encuentran con que esa ambigüedad es difícil de mantener cuando la prueba de que los compañeros de trabajo se ayudan entre sí queda registrado por las cámaras[69].

Entre las implicaciones en el sistema, McCahill y Norris señalan las siguientes: (1) el trastorno que supone en la economía informal relativa a aquellas compensaciones subterráneas en el lugar de trabajo viene a tener consecuencias en la economía formal. Es decir, se produce un «trasvase de recompensas», de modo que el trabajador, ante tal tesitura, buscará compensar por otros medios el lucro cesante del que ha dejado de beneficiarse o aumentará su irritabilidad laboral. Como consecuencia, puede tener un efecto en el nivel de beligerancia en las relaciones laborales o en la afluencia de demandas más o menos justificadas de aumentos salariales[70]; (2) tiene lugar una extensión de las posibilidades de utilización del sistema de video–vigilancia con fines de control empresarial del trabajador, convirtiéndose en realidad en un instrumento disciplinario.

La tergiversación del fin inicialmente previsto –por ejemplo, la prevención de los hurtos por parte de clientes y trabajadores en centros comerciales– influye en la percepción de los trabajadores y en el nivel de confianza de éstos en el empresario. Si los sistemas de CCTV se utilizan principalmente como instrumento disciplinario, y especialmente si se emplean medios encubiertos, se genera una percepción en los empleados de ausencia de rectitud ética, engaño y ruptura de la confianza. La deslegitimación de la vigilancia empresarial –ya sea por una vigilancia transparente aunque abusiva o por un control clandestino–, puede llegar a tener así un efecto contraproducente, siendo

120.

[68] MARS, G., NICOD, M., «Hidden rewards at work: the Implications from a Study of British Hotels», in S. HENRY (ed.), *Can I have it in Cash?*, London, 1981.

[69] *Vid.* al respecto, MCCAHILL, M., NORRIS, C., «Watching the workers: Crime, CCTV and the Workplace», in DAVIS, P., FRANCIS, P., JUPP, V., *Invisible Crimes. Their Victims and their Regulation*, 1999, pp. 227–228.

[70] Uno de los motivos por los que no es tan simple la relación entre la implementación entre CCTV y la erradicación de la desviación en el contexto laboral es la posible complicidad de los mismos agentes que realizan la vigilancia, difícilmente identificados con los intereses de la dirección de la empresa (*vid.* MCCAHILL, M., NORRIS, C., *Ibid.*, 1999, p. 228).

así que el control carente de ética mediante CCTV sea un factor causal respecto de los delitos de los trabajadores, perdiendo su función como efectivo remedio[71].

La importancia del contexto, de las particulares características organizacionales de una empresa, debe influir –según se ha señalado con anterioridad– en el diseño de la política de control, en su implementación y en el mismo proceso constructivo–comunicativo. Y una parte fundamental del contexto viene configurada también por la realidad criminológica. Así, si en una empresa determinada la zona de las taquillas personales de los trabajadores –o los mismos lavabos– devienen un lugar propicio para el delito donde, de forma recurrente, se cometen hurtos, u otros delitos violentos, es posible que los mismos trabajadores toleren, e incluso deseen, la monitorización en tales zonas[72]. Del mismo modo, si en la red interna de la empresa se realizan con cierta periodicidad conductas de acoso más o menos persistentes a trabajadoras. Por tanto, el contexto criminológico presente en una determinada empresa puede justificar la adopción de medidas intrusivas en beneficio de los propios trabajadores que, de otro modo, serían probablemente desproporcionadas. En tales situaciones, el sacrificio en la privacidad de la persona del trabajador (1) debe limitarse a ciertos espacios físicos o virtuales –o ciertas circunstancias[73]–; (2) tendría que fundamentarse en una causa relacionada con la seguridad y prevención de la delincuencia –no bastaría en principio un interés por controlar la prestación laboral, a fin de optimizar el tiempo de trabajo–; y (3) la medida debería adoptarse en favor de los propios trabajadores. Una última consideración: (4) en el caso de que la medida no beneficie directamente a los trabajadores, el empresario debería aportar una causa legítima u objetivar un patrón de riesgo precedente que justifique una medida de carácter excepcional.

La participación del trabajador en el proceso de diseño e implementación de los sistemas de seguridad viene a reforzar –como se apuntó *supra*– la misma legitimidad y transparencia de las medidas de invasión en la privacidad. De este modo, la participación de los trabajadores puede ser activa –mediante el consentimiento libre– o meramente pasiva –mediante el conocimiento–. Desde un punto de vista ético, la mera puesta en conocimiento basta para evitar que la vigilancia empresarial sea subrepticia. Sin embargo, podrían plantearse dos tipos distintos de vigilancia no transparente de carácter extraordinario: (1) supuestos de vigilancia oculta en beneficio de los trabajadores; (2) aquellos casos en los que se pretenda justificar una vigilancia oculta de la que no se beneficien directamente los trabajadores, sino que vienen legitimados por la defensa del patrimonio de la empresa o el cumplimiento de un deber de garante que obliga gravemente al empresario[74].

[71] MCCAHILL, M., NORRIS, C., *Ibid.*, 1999, p. 228.

[72] Tal posibilidad reactiva de los trabajadores fue verificada empíricamente en dos centros de trabajo (*vid.* MCCAHILL, M., NORRIS, C., *Ibid*., 1999, p. 229).

[73] Piénsese, por ejemplo, en que en una empresa determinada tuviera lugar el primer lunes de cada mes un delito contra las personas en los despachos individuales. Aunque el ejemplo es irreal, las amenazas cíclicas que pueden verificarse en determinadas empresas podrían justificar especiales medidas de seguridad.

[74] La exigencia legal que pesa sobre el empresario para que mantenga a salvo el lugar de trabajo, libre de comportamientos de acoso y de la circulación de droga, a menudo requiere algún tipo de monitorización: *vid.* EVERET, A.M., WONG, Y., PAYNTER, J., *Balancing employee and employer rights: an international comparison of e-mail privacy in the workplace*, J. Individual Emplo yment Rights, Vol. 11(4) 291–310, 2004–2005 (2006), p.

La vigilancia oculta o no transparente se analizará con detenimiento más adelante. Basta por el momento señalar que el hecho de fundamentarse una medida de control sin el debido conocimiento de los trabajadores –aunque en beneficio de ellos mismos– requerirá *prima facie* una menor exigencia de justificación empresarial. Piénsese así, por ejemplo, en la instalación de cámaras ocultas para frenar una escalada de pequeños hurtos en dependencias de la empresa. Si el objeto de sustracción pertenece a los trabajadores, será en beneficio de su propia protección y, a efectos de garantizar una mayor eficacia, podría justificarse el carácter encubierto de la medida, con el fin de no prevenir al trabajador que está cometiendo repetidamente tales hurtos. Sin embargo, si se acepta la legitimidad de un control oculto en este caso, es difícil interponer serias objeciones cuando la propiedad amenazada por la serie de hurtos antecedentes sea la propia del empresario, a pesar de que no beneficie directamente a los trabajadores. Como es lógico, en uno y otro caso, la legitimidad del carácter no transparente de la vigilancia se justifica restrictivamente: una vez se haya identificado al trabajador, se debería –en caso de seguir siendo necesaria la presencia de cámaras de seguridad– efectuar una comunicación a los trabajadores. En tal caso, la finalidad sería claramente preventiva, y no reactiva (en el sentido de que no pretender resolver un caso ya acaecido).

2. **Finalidad genérica de la captación de imágenes: ¿control de la prestación laboral o prevención del delito?**

A. *Alcance objetivo de la observación mediante sistemas de CCTV*

En este contexto, el análisis sobre las cuestiones éticas en torno a la vigilancia en espacios públicos mediante sistemas de CCTV que realiza Andrew von Hirsch[75], parte de una aporía difícil de superar: las cámaras no pueden discriminar entre ciudadanos corrientes que acatan la legalidad y potenciales delincuentes, debiendo a priori tratar a todos por igual. Tras considerar los inconvenientes éticos que presenta la video–vigilancia[76], en cuanto que infringe las expectativas y convenciones sobre el anonimato –en algunos casos afectando a la intimidad– , von Hirsch trata de limitar una excesiva justificación de la video–vigilancia como instrumento utilizado en la prevención e investigación del delito.

A lo largo de las presentes reflexiones, con frecuencia se acude a datos, argumentos, comparaciones y paralelismos entre la video–vigilancia en un entorno laboral y en los espacios públicos en general. Aunque se traten de señalar las diferencias relevantes en cada caso, conviene resaltar algunos factores generales distintivos, a pesar de la dificultad para realizar un balance global o verificar sus consecuencias prácticas. En

295.

[75] *Vid.* VON HIRSCH, A., *Cuestiones éticas en torno a la vigilancia en espacios públicos mediante cámaras de televisión* (trad. de José R. AGUSTINA SANLLEHÍ), en VON HIRSCH, A., GARLAND, D., WAKEFIELD, A. (eds), *Ethical and Social Perspectives on Situational Crime Prevention*, London: Hart, 2000, (publicado en InDret 4/2007).

[76] En términos kantianos, podría argumentarse en su contra que se viene a instrumentalizar o sacrificar la expectativa de anonimato –e incluso de intimidad– de aquellos ciudadanos obedientes en favor de los objetivos de seguridad.

cierto modo, tales factores influirán en la motivación individual para delinquir (nivel psicológico–preventivo). En este sentido, (1) suele haber grandes diferencias entre el modo de advertir al trabajador y al ciudadano respecto del funcionamiento de un sistema de CCTV, y por tanto la eficacia preventiva del mismo sistema de vigilancia será distinta[77]; (2) el trabajador tiene un mayor riesgo en ser descubierto, al disponer el empresario de una mayor información y accesibilidad sobre su persona y sus pertenencias; (3) existe por parte del trabajador el riesgo de poder perder el puesto de trabajo como consecuencia de ser descubierto; por último, (4) la exposición diaria del trabajador a situaciones propicias para cometer delitos determina que las tentaciones situacionales sean también mayores –especialmente, si se descuidan mecanismos de control: el trabajador tiene un conocimiento privilegiado del entorno–.

Sin embargo, en el contexto laboral ¿se puede seguir oponiendo en los mismos términos una expectativa de anonimato en favor de los trabajadores? Aunque las circunstancias del entorno son relevantes, trataré de argumentar la vigencia de algunos paralelismos entre ambos espacios en los que operan sistemas de video–vigilancia. Así, se puede entender que las diferencias operan sobre todo en el nivel psicológico–preventivo y no tanto en los principios éticos generales. Ciertamente, el contexto puede modular algunas exigencias éticas, pero a pesar de las diferencias permanece un denominador común, la dignidad de la persona humana.

Como se ha mencionado con anterioridad, el empresario ostenta un poder de vigilancia y control sobre los trabajadores, en orden a supervisar su actividad profesional –ex art. 20 ET–. Aunque será inevitable realizar puntuales referencias, la video–vigilancia en el ámbito laboral con la finalidad exclusiva de controlar a los trabajadores en el modo de desempeñar la prestación laboral no se traerá a consideración en estas líneas. Piénsese en este sentido que el empresario fácilmente, bajo el pretexto de una vigilancia encaminada a prevenir el delito, también podría tener acceso a un control permanente sobre la conducta del trabajador, contraviniendo la finalidad inicialmente prevista[78].

Pues bien, una de las primeras objeciones in genere que presentan las medidas de vigilancia mediante CCTV (como apunta von Hirsch) se refiere al «extenso ámbito de observación» que abarcan tales sistemas en su radio de acción. Como se ha apuntado, las cámaras no pueden llegar a discriminar la actividad que registran sino que necesariamente afectan a cualquier persona realizando cualquier acción, estando presente –aunque tan sólo sea por unos instantes– en el espacio físico que es objeto de vigilancia[79].

[77] Normalmente, el trabajador conocerá la existencia de sistemas de CCTV por la política informativa del empresario, siempre más personalizada.

[78] Así por ejemplo, entre los principios generales que establece la OIT en su Repertorio de recomendaciones (1997), el artículo 5.4 establece: «Los datos personales reunidos en función de disposiciones técnicas o de organización que tengan por objeto garantizar la seguridad y el buen funcionamiento de los sistemas automatizados de información no deberían servir para controlar el comportamiento de los trabajadores».

[79] VON HIRSCH, A., *Ibid.*, 2007. Esta *obligatoria generalización* del campo de visión provoca que se vea afectado un número elevado de personas, incluyéndose entre ellas mayoritariamente personas sin ninguna intención de cometer un delito. Nadie puede evitar ser objeto de captación y grabación por el hecho de respetar y acatar el ordenamiento jurídico.

En cuanto al número de personas que previsiblemente pueden resultar afectadas por la video–vigilancia en un entorno laboral, éste puede variar ostensiblemente. Algunas zonas pueden así gozar de mayores restricciones al acceso del público en general, limitando la entrada a personal de plantilla, aunque, en realidad, puede ser difícil que no existan en la práctica eventuales afectaciones a terceros –clientes, proveedores, servicios de mantenimiento externo a la empresa, etc.–. A este respecto, ¿puede considerarse irrelevante el impacto en la privacidad de tales terceros? Por terceros se entiende aquellas personas que no son el objeto o la causa de la medida de vigilancia. Se podría equiparar, a estos efectos, a un efecto imprevisto, no deseado, que produce un daño colateral. En este sentido, aun siendo un efecto no deseado, se trata de una consecuencia en muchos casos inevitable y, por tanto, también previsible –pudiéndose advertir adecuadamente, mediante un rótulo visible–. De algún modo, atendiendo al elemento cognoscitivo de la acción de vigilar, se estaría ante un *dolus directus*, en tanto que es extremadamente probable que se afecte a la intimidad de las personas[80].

Es necesario también distinguir y aplicar distintas reglas de vigilancia sobre las personas en función del lugar, tiempo y colectivo al que pertenecen, a fin de no incurrir en una discriminación injustificada[81]. En este sentido, «la igualdad no es una realidad objetiva o empírica anterior al Derecho, que éste sólo tenga que percibir», sino que toda constatación jurídica de la igualdad –o de desigualdad– implica siempre un juicio de valor que depende de la elección de las propiedades o los rasgos que son considerados relevantes y que constituyen el objeto de comparación[82].

Veamos pues las tres coordenadas que se acaban de señalar. En cuanto a (1) las condiciones de lugar, conviene distinguir si el espacio físico objeto de control pertenece al ámbito estrictamente interno de la empresa, o se trata de una zona semipública, en el sentido de que es un lugar destinado o abierto al público en general. Así, la previsibilidad objetiva de afectación al público en general debería llevar a extremar las garantías. Respecto de (2) las condiciones de tiempo, en tanto que el trabajador no somete todo su ser y su obrar al empresario, convendrá limitar en el tiempo la actividad que pueda ser objeto de control –tenga lugar dentro o fuera del recinto físico de la empresa[83]–. Finalmente, (3) en cuanto al colectivo afectado, ¿se debe tener en consideración si se pretende prevenir la criminalidad intra–empresarial o por el contrario se dirige

[80] JESCHECK, H., WEIGEND T., *Tratado de Derecho Penal*, 2002, p. 320.

[81] Por ejemplo, no podría admitirse que los trabajadores *negros* de una empresa tuvieran que someterse, por la *peligrosidad estadística* asociada a la raza a la que pertenecen, a pruebas de polígrafo o a una video–vigilancia más intensa. Para profundizar en las bases ético–jurídicas que estructuran el principio jurídico–positivo de no discriminación en el ambito de la Unión Europea puede consultarse el comentario –aunque trate de un problema completamente distinto– al conocido caso *Kalanke* (Judgment of the Court of 17 October 1995. *Eckhard Kalanke v. Freie Hansestadt Bremen*. Case C-450/93, European Court reports 1995, p. I–03051) en REY MARTÍNEZ, F., *La discriminación positiva de mujeres*, Revista Española de Derecho Constitucional, 1996 mayo–agosto, pp. 309–332.

[82] De ahí que el «concepto» de la igualdad tenga –como señala LUHMANN–, un sentido de distribución desigual de la carga de las argumentaciones de las decisiones jurídicas. El esquema «igual/desigual» no ofrece respuesta inmediata a los problemas, sino que tan sólo abre un margen para el argumentar racional (*vid.* REY MARTÍNEZ, F., *La discriminación positiva de mujeres*, 1996. p. 318).

[83] Los avances tecnológicos han dado lugar a nuevas formas de control–remoto y tele–trabajo que pueden suponer con mayor facilidad, a estos efectos, invasiones en la esfera privada del trabajador.

sólo a potenciales delincuentes ajenos a la empresa? En realidad, ambas finalidades no son excluyentes, sin perjuicio de que pueda prevalecer una sobre la otra en la mente del empresario. No obstante, conviene analizar la medida en sí misma. Es decir, cualitativamente, no puede tener la misma intensidad el control preventivo sobre un trabajador que sobre clientes o terceras personas ajenas a la empresa. Al margen de la posible idéntica peligrosidad que pueda presentar un trabajador–delincuente y un cliente–delincuente, el trabajador pertenece a la empresa, con todo lo que ello significa. Piénsese, por ejemplo, que el trabajador puede haber firmado un anexo al contrato de trabajo conforme aceptaba la política de seguridad y control de la empresa[84].

Es importante resaltar, a estos efectos, la relación contractual como factor distintivo. El trabajador se ha incorporado a la esfera de organización del empresario, siendo en cierto modo un alter ego del empresario y un representante de la compañía para la que trabaja. Ha sido objeto de una confianza que se manifiesta en una mayor accesibilidad a los bienes de la empresa. Es decir, en igualdad de predisposiciones o inclinaciones personales al delito, la vulnerabilidad delictiva del empresario frente a un trabajador es notoriamente mayor en comparación con las facilidades delictivas que pueda tener un tercero ajeno. Todo ello justifica la adopción de medidas de control más intensas o intrusivas[85]. De este modo, la pregunta que se plantea von Hirsch al inicio de su artículo ¿hasta qué punto existen legítimas expectativas de privacidad o de anonimato en espacios públicos?, como es lógico, no puede responderse del mismo modo en el ámbito de la criminalidad intra–empresarial. El recurso a la analogía no puede omitir las diferencias cualitativas que se acaban de exponer.

Además de la posible y conveniente exteriorización de reglas de control derivadas del vínculo contractual, conviene resaltar la importancia del contrato, en cuanto que de sus precisiones se deducen el espacio y el tiempo en cuanto variables para distinguir un control laboral de una vigilancia genérica. Ambos elementos constituyen las coordenadas espacio–temporales ya mencionadas, a las que debe circunscribirse –no sin dificultades– la relación laboral. Mediante el elemento temporal el trabajador se ha obligado a entregar un tiempo de trabajo y, en ese sentido, su actividad no le pertenece dentro de esos límites –de los límites del contrato–. O al menos, no le pertenece con carácter exclusivo, sino que debe dar cuenta del empleo de ese tiempo y permitir por tanto un control razonable sobre el mismo –siendo así que la medida de lo razonable puede venir definida, en gran parte, por el contrato–. No obstante, no siempre se puede encorsetar la prestación laboral en un horario laboral predeterminado, y habrá por tanto que atender en última instancia a un criterio material (la prestación laboral en cuanto producto o resultado, al margen de cuándo y dónde se haya realizado).

B. *Finalidad de la video–vigilancia*

[84] Parece razonable sostener que se deben tener en cuenta los tres factores. Así, es tan relevante el criterio subjetivo que motivó la instalación de las cámaras, como el criterio objetivo: el número previsible de personas afectadas por el sistema de vigilancia –tengan o no relación contractual con la empresa–.

[85] No obstante, podría objetarse que el empresario ha podido elegir *libremente* a sus trabajadores, libertad de la que no siempre goza frente a clientes o terceros –a pesar ciertamente de la *tendencia expansiva* que el derecho de admisión pueda experimentar en relación a *listas negras* (*'blacklists'*) de personas *peligrosas*: *vid.* VON HIRSCH, A., *Ibid.*, 2007, p. 20 y nota 16, sobre la puesta en práctica de un conjunto de *estrategias de exclusión*, con el fin de mantener al margen de los lugares públicos a aquellas personas que se consideren socialmente indeseables, o que se piense que representan riesgos de cometer delitos en el futuro–. Sin embargo, la *libertad* del empresario respecto a la elección de sus trabajadores no radica tanto en razón de las personas (*intuitu personae*) sino que se concretiza en las medidas de control a las que se somete el trabajador desde su *ingreso* en la empresa.

En el momento de implementar una medida de video–vigilancia debemos plantearnos por tanto la finalidad y los medios que se pretenden emplear. En primer lugar, la finalidad debe ser legítima, es decir, debe realizarse en virtud de un fin lícito que justifique el recorte en la privacidad de las personas. En línea de principios, el control de la prestación laboral y la prevención del delito pueden ser justificaciones legítimas. No obstante, las reglas y los límites que se aplican a uno y otro tipo de control responden a lógicas distintas. Sin entrar en razones de conveniencia[86], los problemas fundamentales que afectan al control de la prestación laboral se centran en justificar que la medida responde a una política genérica –no discriminatoria–, que debe precisar ex ante la finalidad específica que se persigue con tal medida. Mientras que en las medidas de seguridad y prevención de la delincuencia, el principio que tendrá mayor peso no debiera ser la transparencia ex ante, sino que se limite el acceso al contenido de las cintas sin una causa justa o con una finalidad distinta a la que inicialmente se previó –utilización ex post–.

En cierto sentido, a los efectos de la detección y persecución ex post facto de la delincuencia, la característica del entorno es en parte irrelevante. Es decir, ya se trate del ámbito intra–empresarial o de un espacio público –o semipúblico–, en términos de impacto respecto a la expectativa de anonimato, lo más relevante no será la operación de las cámaras en sí misma, sino la utilización que se dé a las cintas resultantes. El trabajador que se mueve por las dependencias de la empresa –como todo ciudadano que transita por espacios públicos– tiene la expectativa de que las imágenes captadas por motivos de seguridad no van a ser examinadas a posteriori en detalle sin un motivo justificado.

Como señala von Hirsch, en el momento de realizar los sucesivos visionados y revisiones de las cintas es cuando se puede enfocar y someter a un prolongado y repetido escrutinio la actividad de una persona en particular. Lo que le lleva a preguntarse: ¿en qué medida entonces deberían tener acceso a las cintas las fuerzas de seguridad de acuerdo con sus fines? La pregunta se puede trasladar al empresario que, ante la comisión de un delito en las dependencias de su empresa, acude a la grabación de las cámaras. A la cuestión planteada responde von Hirsch apuntando tres posibles opciones, en función de una mayor o menor permisividad: (1) las cintas podrían ser revisadas sólo para ayudar en el descubrimiento o investigación de delitos; (2) las cintas podrían ser utilizadas también para identificar posibles infracciones en determinados entornos restringidos en los que los riesgos de cometerse delitos sean más elevados que en las zonas inmediatamente circundantes, y la posibilidad de que sean observadas detenidamente terceras personas no involucradas sea reducida; (3) las cintas podrían ser generalmente utilizadas, sin las limitaciones antes mencionadas[87].

Mutatis mutandis, se puede tratar de aplicar las restricciones que señala von Hirsch en el ámbito de la investigación policial al control de la delincuencia intra–empresarial. Así, advierte que uno de los problemas que presenta actualmente la vigilancia mediante CCTV es su utilización –y posterior acceso al contenido de las grabaciones por las fuerzas de seguridad–, en cualquier lugar del espacio público y sin necesidad de

[86] Según las consideraciones realizadas *supra*, existen posibles consecuencias negativas que pueden generarse en el clima laboral de la empresa, siendo así que las medidas de control pueden tener efectos contraproducentes, provocando la desafección del trabajador leal a la compañía.

[87] VON HIRSCH, A., *Ibid*., 2007, p. 16.

determinar ulteriores motivos de sospecha. En este punto, von Hirsch es partidario de imponer algunas restricciones análogas a lo que se conoce en los sistemas jurídicos anglosajones como «probable cause», con el propósito de limitar el alcance de la revisión de las cintas a lugares y tiempos en los que efectivamente existan razones para la sospecha de que se ha cometido un delito[88]. Parecen no existir razones para que no debiera aplicarse el mismo razonamiento a la revisión de las cintas por parte del empresario. De esta forma, sería legítimo que por motivos de seguridad se ampliara el área de video–vigilancia a zonas que no afecten per se a la intimidad de los trabajadores –por ejemplo, los lavabos–, abarcando una gran parte de las dependencias empresariales. Sin embargo, debería poder garantizarse que, en contrapartida, el empresario sólo podrá acceder y revisar el contenido de las grabaciones ante un motivo justificado suficientemente. En ese sentido, sólo le sería permitido para revisar las cintas relativas a aquellos lugares y ocasiones en las cuales haya habido un daño en el patrimonio de la empresa, un conflicto laboral con incidentes graves o ante la advertencia de otros hechos que pudieran ser constitutivos de delito[89]. En definitiva, si el empresario ha instalado unas cámaras por motivos de seguridad no puede emplearlas para verificar el cumplimiento de la prestación laboral, ni revisar las cintas en una búsqueda generalizada de infracciones sancionables sin causa previa.

En este sentido, como argumenta von Hirsch, tal limitación impediría llevar a cabo seguimientos al azar ['fishing expeditions'], echando una ojeada a través de las cintas a lo largo de un extenso periodo de tiempo y una amplia área, con la expectativa de encontrar a alguien cometiendo un delito. Así, se vendrían a reducir de esta forma, significativamente, el número de intrusiones en los intereses de anonimato. Los trabajadores podrían trabajar y moverse por las dependencias de la empresa, sin miedo a que vayan a seguirse con detalle sus movimientos sin un motivo que lo justifique. Sólo podría suceder si el trabajador se hallaba presente en el lugar y momento precisos en que se ha denunciado la comisión de un delito. Cuando esto ocurra, sus actividades serían sometidas a examen, aunque sólo se tratara de un inocente espectador; no obstante, las limitaciones espaciales y temporales restringen mucho el alcance de lo que se examina[90].

Sin embargo, como apunta Martín Morales acertadamente a través de los medios de video–vigilancia se pueden obtener dos tipos de imágenes: (1) las inicialmente previstas –abarcadas por la intención que motivó su instalación– y (2) las casualmente aparecidas (imágenes casuales). Sin perjuicio de la gran variedad de la casuística en la materia, las videocámaras de una entidad bancaria, por ejemplo, pueden grabar, aparte de las imágenes de un robo en la misma (captación tipo), el acoso sexual de su director a una empleada (captación casual del interior) o el robo de un automóvil en la

[88] *Cfr.* al respecto, VON HIRSCH, A., *Ibid.*, 2007, p. 16, en donde argumenta a favor de la primera opción y, en algunos casos, de la segunda.

[89] *Vid.* el Código de Prácticas del *Cambridge City Council* (1998): «Las cámaras no serán utilizadas para realizar un seguimiento del progreso de los individuos en el curso ordinario de sus asuntos legítimos…»; «los individuos solo serán objeto de seguimiento particularizado si media causa razonable para sospechar que se ha cometido un delito» (parágrafo 1.2). La policía tiene por tanto la obligación de especificar *la hora y el lugar de un incidente en particular* y debe pedir a las autoridades municipales autorización para ver las oportunas grabaciones (VON HIRSCH, A., *Ibid.*, 2007, p. 16).

[90] VON HIRSCH, A., *Ibid.*, 2007, p. 17, refiriéndose a la actuación de las fuerzas de seguridad.

calle (captación casual del exterior). Siempre que la instalación de esos dispositivos ópticos no sea ilícita –en el sentido de tratarse de una actividad lesiva de derechos constitucionales–, las grabaciones casualmente obtenidas podrán ser utilizadas procesalmente, lo que viene refrendado por la utilización que hace el Tribunal Supremo [vid., *ad exemplum*, STS de 08–03–1994] del criterio de la flagrancia, que debe entenderse tanto más aplicable cuando no hay por medio resolución judicial: «si aparecen objetos constitutivos de un cuerpo de posible delito distinto a aquel para cuya investigación se extendió el mandamiento habilitante, tal descubrimiento se instala en la nota de flagrancia»[91].

3. **El principio de proporcionalidad en la actividad de control**

A. *Legitimidad de los medios: adecuación a la finalidad*

Una vez examinado de modo genérico el principio de finalidad, en el análisis del caso concreto debe tenerse en cuenta que los medios deben adecuarse al fin inicialmente previsto y respetar el principio de proporcionalidad. En este sentido, la existencia de un fin (legítimo) justifica la adopción de unos medios (legítimos). Es decir, la relación justificante fin–medios significa que (1) sin causa final legítima no está justificado ningún medio, y que (2) sólo algunos medios son legítimos, aquéllos que guarden la debida proporción al fin señalado. Por tanto, el alcance y la intensidad de la vigilancia deben adaptarse al fin perseguido, buscando entre las diferentes técnicas disponibles aquéllas que limiten al mínimo imprescindible la afectación en la privacidad.

Sin embargo, para realizar el «juicio de adecuación» se debe concretar la finalidad genérica en las circunstancias del caso concreto. Es decir, en función del examen de la situación de hecho y del nivel de las amenazas y la peligrosidad del concreto entorno empresarial será justificable la intensidad y extensión de las medidas de vigilancia que se adopten. Sólo la finalidad específica aquí y ahora que motiva la instalación de las cámaras, en las circunstancias del caso concreto, se erige en criterio rector para emitir adecuadamente el juicio de proporcionalidad de las medidas que se vayan a adoptar.

En este sentido, el Tribunal Constitucional reconoce que si bien la esfera de la inviolabilidad de la persona frente a injerencias externas sólo en ocasiones tiene proyección hacia el exterior, por lo que no comprende, en principio, los hechos referidos a las relaciones sociales y profesionales en que se desarrolla la actividad laboral, que están más allá del ámbito del espacio de intimidad personal y familiar sustraído a intromisiones extrañas por formar parte del ámbito de la vida privada (SSTC 170/1987, de 30 de octubre [RTC 1987, 170], F. 4; 142/1993, de 22 de abril [RTC 1993, 142], F. 7, y 202/1999, de 8 de noviembre, F. 2), no por ello el empresario, sin límite alguno, queda apoderado para llevar a cabo, so pretexto de las facultades de vigilancia y control que le confiere el artículo 20.3 ET, intromisiones ilegítimas en la intimidad de sus empleados en los centros de trabajo.

Es decir, la intimidad cede ante el interés legítimo del empresario de acuerdo con ciertas pautas determinadas por el principio de proporcionalidad y que, ya en repetidas ocasiones[92], ha expuesto el propio Tribunal Constitucional, al afirmar la necesidad de que las resoluciones judiciales preserven «el necesario equilibrio entre las obligaciones dimanantes del contrato para el trabajador y el ámbito -modulado por el contrato, pero en todo caso subsistente- de su libertad constitucional» (STC 6/1998,

[91] *Cfr.* MARTÍN MORALES, R., «El derecho a la intimidad: grabaciones con videocámaras y microfonía oculta», *La Ley*, Año XXV, núm. 6079, 06–09–2004, donde señala que la aplicación de este último criterio es discutible en el caso de los delitos de «efectos permanentes».

[92] Entre otras, *vid.* SSTC 66/1995, de 8 de mayo [RTC 1995, 66], F. 5; 55/1996, de 28 de marzo [RTC 1996, 55], F. 6, 7, 8 y 9; 207/1996, de 16 de diciembre, F. 4 e), y 37/1998, de 17 de febrero [RTC 1998, 37], F. 8.

de 13 de enero (RTC 1998, 6). Pues bien, dada la posición preeminente de los derechos fundamentales en nuestro ordenamiento, esa modulación sólo deberá producirse en la medida estrictamente imprescindible para el correcto y ordenado respeto de los derechos fundamentales del trabajador y, muy especialmente, del derecho a la intimidad personal que protege el artículo 18.1 CE, teniendo siempre presente el principio de proporcionalidad (STC 186/2000).

En efecto, de conformidad con la consolidada doctrina del Tribunal Constitucional español, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del «principio de proporcionalidad» (vid. al respecto, por todas, STC 186?2000, FJ 6). Así, para comprobar si una medida restrictiva de un derecho fundamental supera el principio de proporcionalidad, es necesario constatar que aquellos instrumentos instalados por el empresario –ya sean cámaras de seguridad u otros sistemas de control, por ejemplo sobre el correo electrónico– cumplen los tres requisitos o condiciones siguientes: (1) la medida debe ser idónea, susceptible de conseguir el objetivo propuesto (juicio de idoneidad); (2) debe ser necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); (3) finalmente, debe ser ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)[93].

B. *Intensidad y alcance de los medios*

De lo anterior se desprende que la intensidad y capacidad intrusiva de las cámaras de seguridad no son en absoluto aspectos irrelevantes. En función del tipo y prestaciones de las cámaras empleadas, del modo de registrar la actividad, del tiempo y lugar de la grabación, podrá considerarse legítima o ilegítima la injerencia en la privacidad o intimidad de las personas.

Al hilo de las distintas capacidades de algunos tipos de cámaras que describe Von Hirsch, se pueden realizar algunas consideraciones en torno a la legitimidad de las prácticas de video–vigilancia en orden a establecer una adecuada relación entre medios y fines en el caso concreto.

Cámaras de filmación continua [Filmed Camera Sweeps]

Mediante tal tipo de cámaras automáticas se realiza un barrido continuo de un área determinada, grabándose imágenes de todo lo que acontece en su radio de alcance –ya sean cámaras estáticas o de recorrido programado–. La cinta resultante contiene por tanto una grabación permanente de todas aquellas personas y sus acciones que hayan tenido lugar en ese espacio determinado. Veamos las limitaciones que conviene establecer (1) en el espacio y (2) en el tiempo de una medida de vigilancia de tales características.

[93] Para analizar la aplicación jurisprudencial del principio de proporcionalidad a distintas medidas de video–vigilancia en función del supuesto de hecho, *vid.* SEMPERE NAVARRO, A.V., SAN MARTÍN MAZZUCCONI, C., *Nuevas Tecnologías y Relaciones Laborales*, 2002, pp. 141–144.

(1) En cuanto a la limitación temporal de la filmación conviene resaltar las objeciones éticas y las consecuencias psicológicas que comporta una vigilancia permanente sobre los trabajadores. A este respecto, es ilustrativo el contenido de la disposición 6.14 del Repertorio de recomendaciones prácticas de la OIT (1997)[94]:

> Como norma general, no se prohíbe la vigilancia de los trabajadores, pero se fijan límites muy claros. El repertorio señala muy claramente que los empleadores no tienen la libertad de elegir el método y los medios de vigilancia que ellos consideren como los mejor adaptados a sus objetivos. Por el contrario, deben dar preferencia a los medios que tengan los menores efectos sobre la intimidad de los trabajadores y velar por las consecuencias que se puedan derivar de la implementación de las medidas de vigilancia. En este sentido, el repertorio adopta un enfoque decididamente más restrictivo que limite la «vigilancia secreta o permanente». Entre las consecuencias que una vigilancia de tal naturaleza tiene en los trabajadores, se ha probado que una vigilancia permanente es causa de una ansiedad constante, que a su vez puede originar enfermedades físicas o perturbaciones psicológicas. Por tanto, se debe limitar a los casos en donde la vigilancia sea realmente necesaria para hacer frente a problemas específicos relacionados con la salud y la seguridad o la protección de los bienes.

No obstante, las diferencias de principio –en su justificación– entre la cámara que se instala para proteger la seguridad de un edificio (protección de bienes), de aquélla que se dirige a vigilar a los trabajadores, en la práctica, pueden ser difíciles de establecer: ¿cómo deben tratarse las zonas grises? Puede suceder así que el trabajador lleve a cabo la prestación laboral de forma ininterrumpida junto a un punto estratégico de la seguridad de la empresa y, por tanto, esté sometido de forma indirecta a un sistema de vigilancia permanente. En estos casos, se deberá contrarrestar la permanente exposición del trabajador al control de las cámaras mediante alguna medida correctora que aminore el impacto en la intimidad de la persona[95].

(2) En cuanto a la limitación espacial del objetivo de las cámaras, la mencionada STC 186?2000 aplica a un caso concreto los criterios de necesidad y proporcionalidad en sentido estricto. En el supuesto que se analizaba, el Tribunal llegó a verificar que el empresario adoptó la medida de vigilancia «de modo que las cámaras únicamente grabaran el ámbito físico estrictamente imprescindible (las cajas registradoras y la zona del mostrador de paso de las mercancías más próxima a los cajeros)»[96].

¿Sería legítimo como norma habitual el seguimiento particularizado de los trabajadores en lugares de alto riesgo? Piénsese en lugares en los que las tentaciones del trabajador puedan ser mayores y los daños al patrimonio empresarial especialmente sensibles. Por ejemplo, el tipo de control que podría diseñarse para trabajadores que tuvieran que entrar en contacto con información confidencial, o con secretos tecnológicos. También podría utilizarse este tipo de seguimiento particularizado de un lugar bien determinado para reducir costes de personal. Por ejemplo, si para reducir puestos de trabajo se permite –previa instalación de cámaras de seguridad– el acceso a la caja a todos los trabajadores del área económica: de tal forma, se evitaría que hubiera un responsable a quien se le exigiera la asunción de responsabilidad ante un descuadre contable.

[94] *Vid.* Repertorio de recomendaciones prácticas que en materia de Protección de los Datos Personales de los Trabajadores efectuó la Oficina Internacional del Trabajo (OIT, Ginebra) en 1997, citado en el DGT Artículo 29.

[95] Como los criterios que se especificarán a continuación *infra* sobre los *hot-spots* en la empresa.

[96] *Vid.* Fundamento jurídico sexto de la STC 186?2000.

En esta cuestión se pueden traer a consideración las reflexiones de von Hirsch sobre la «restricción geográfica del lugar afectado» por la video–vigilancia. En la tarea de establecer límites al acceso a la revisión del contenido de las cintas por las fuerzas y cuerpos de seguridad, entiende que sería razonable permitir un control continuado de aquellos lugares de especial peligrosidad –como los cajeros automáticos–, a la vista de que son mayores los riesgos de cometerse un delito en tales emplazamientos.

Sin embargo, el riesgo no es el único factor relevante en estos casos, sino que, a juicio de von Hirsch, otros dos factores parecen importantes. En primer lugar, (1) la «restricción geográfica del lugar afectado». Es decir, si determinados puntos o emplazamientos, circunscritos lo más estrechamente posible [cajeros automáticos], están sujetos a una vigilancia más intensa, siendo objeto de revisiones continuadas, las personas conservan la oportunidad para moverse sin perder el anonimato en otros lugares. Sin embargo, (2) en la misma medida en que las personas deben soportar el control de las cámaras, se benefician de la misma protección que les dispensan. Ordinariamente, las personas que están sometidas al control de las cámaras en los cajeros automáticos son aquellas que están retirando dinero, es decir, no se trata de meros espectadores; siendo esas mismas personas las que corren especialmente el riesgo de que les roben el dinero que han retirado[97].

Regresando al estricto ámbito intra–empresarial, se debería, análogamente, autorizar una monitorización continua por motivos de seguridad sólo en aquellos lugares de la empresa en los que se verifiquen los tres factores señalados por von Hirsch: (1) existencia de un riesgo más elevado de cometerse un delito; (2) máxima restricción geográfica del espacio físico sujeto al control de las cámaras; (3) la medida debe también, de algún modo, beneficiar al trabajador, ya sea en tanto que puede ser una posible víctima del delito o, al menos, como un medio efectivo para descartar –en beneficio propio– su participación delictiva ante la comisión de un delito en la empresa.

Así por ejemplo, (1) algunos supermercados no dejan al acceso del público determinados productos que, por sus dimensiones y accesibilidad, sean de fácil sustracción (riesgo más elevado), guardándose en el almacén al que sólo tiene acceso el personal, y en el que las medidas de seguridad son mayores. En segundo lugar, (2) el hecho de que la revisión continua de las cintas se limite a las que registran la actividad en torno a los almacenes u otros puntos calientes (hot–spots), permite que el trabajador trabaje con la sensación de menor control, en tanto que es consciente que su conducta sólo será grabada y revisada de forma continua en esas zonas limitadas. Por último, (3) el hecho de que haya cámaras de seguridad en los almacenes de un centro comercial beneficia a los trabajadores que, ante la desaparición de material fungible, no pueden ser imputados, ni se puede desconfiar de ellos ante la evidencia incriminatoria de la prueba que se derive del acceso a las cintas. También evita otro tipo de medidas de control para descubrir al trabajador que cometió el hurto, tales como registros personales o en las taquillas de los trabajadores o interrogatorios, e incluso –en los países en que está autorizada– la prueba del polígrafo.

Cámaras con posibilidades de enfoque personalizado [Filmed Surveillance with Focusing Capabilities]

[97] *Vid.* al respecto, VON HIRSCH, A., *Ibid.*, 2007, pp. 17–18.

En cuanto al segundo tipo de cámaras, encontramos aquéllas que están dirigidas desde una cabina de control centralizado y que permiten enfocar de forma precisa sobre una persona determinada, siguiendo y grabando sus movimientos[98]. También es posible obtener una imagen mas detallada mediante la utilización del correspondiente zoom.

Al margen de la demostración empírica de vínculos causales entre el uso de CCTV y una correlativa eficacia preventiva, la utilidad y eficacia que puede suponer el aprovechamiento de sistemas de CCTV ya instalados, puede medirse por el recurso a la revisión de las grabaciones para resolver un caso determinado[99]. Sin embargo, el acceso al contenido de las cintas como un instrumento auxiliar que coadyuve en la identificación o corroboración de algún dato referido a un sospechoso determinado puede ir más allá en ocasiones de la específica finalidad prevista ex ante que motivó la instalación de la cámara[100]. Su utilización en tales casos excede la estrategia relacionada con la concreta prevención situacional del delito que se pretendía.

No obstante, el empresario que instala un sistema de CCTV pretende, ciertamente, no sólo prevenir ex ante la comisión de delitos sino que también persigue identificar a los culpables ex post facto, una vez ya se ha consumado el injusto. El problema radica en que, en algunas ocasiones, la finalidad que originó la instalación de CCTV no guarda ninguna relación con la finalidad en su utilización, bien porque (1) el empresario quiera utilizar las cintas con una finalidad distinta y por tanto ilegítima[101]; o (2) porque se produzca una cesión a terceros. Así sucede, por ejemplo, cuando en el marco de una investigación policial o judicial se revisan las cintas grabadas de propiedad privada en las inmediaciones al lugar del delito, para descartar o confirmar la presencia de sospechosos.

A este respecto, se deberían establecer límites a la utilización del material grabado. Piénsese que incluso se podría seguir la pista a sospechosos a lo largo de una amplia zona geográfica. La tecnología actualmente existente permite seguir a alguien allá donde vaya, de una parte a otra, a través de un sistema de cámaras de televisión interconectadas, que estén diseñadas para responder a determinadas imágenes o patrones. Como señala Von Hirsch, tales técnicas, al tiempo que conllevan en sí mismas serios problemas éticos, no se emplearían en ese caso en aras de la prevención situacional del delito

[98] Como apunta VON HIRSCH, esta técnica es utilizada en muchas áreas de centros urbanos y centros comerciales.

[99] Existen evidencias de que el uso de sistemas de CCTV, en ciertos escenarios y para determinados tipos de delitos, viene acompañado por el descenso de los índices delictivos o por el aumento del índice de esclarecimiento de casos. Sin embargo, a juicio de VON HIRSCH el grado de tales asociaciones, no obstante, es bastante variable; los vínculos causales están lejos de ser claros; y también viene a dificultar su valoración el grado en que el delito ha sido desplazado hacia otras zonas (para una revisión de las evidencias puede consultarse SKINNS, 1999; PHILLIPS, 1999, citado en VON HIRSCH, A., *Ibid*., 11–12).

[100] Bastaría con realizar una simple comprobación en la estadística judicial para percibir su eficacia y utilidad en innumerables casos. La revisión policial o judicial de cintas de grabación con imágenes captadas por cámaras de seguridad, tanto de empresas privadas como de entidades públicas, puede abarcar muy distintos tipos de establecimientos: cajeros automáticos, estaciones de metro, cámaras exteriores de seguridad de edificios públicos y privados, tiendas y grandes almacenes. Piénsese en la capacidad de seguimiento de sospechosos que puede realizarse con los próximos y no tan próximos avances tecnológicos, por ejemplo vía satélite.

[101] El problema de la finalidad de la instalación de las cámaras de seguridad y su eventual aprovechamiento ante un *hallazgo casual*: por ejemplo, si revisando las cintas que se grabaron para velar por la seguridad del edificio se constata el repetido incumplimiento contractual de un trabajador.

stricto sensu: su propósito en tal caso sería el seguimiento de sospechosos y no tanto la protección de un concreto espacio físico frente a la comisión de delitos.

Con todo, las concretas amenazas a la privacidad también pueden proceder de un uso inadecuado de datos personales de los consumidores. Así, las cintas grabadas con motivo de la seguridad de centros comerciales, ¿pueden utilizarse para estudiar los hábitos de conducta de los consumidores? El empresario podría estar interesado en realizar estudios sobre el perfil de sus clientes habituales. En este sentido, podría ser un aporte valioso la inmediatez de la fuente visual para conocer las tendencias, proporcionada por las imágenes captadas[102]. El problema podría agravarse, además, ante el riesgo de comercialización de los datos y estudios extraídos cediéndolos a empresas del sector. Como apunta Etzioni, es un hecho ciertamente paradójico que la psicosis generalizada en torno a las amenazas contra la privacidad se centra en las posibles invasiones por parte del Estado, sin prestar la misma atención al potencial lesivo de las corporaciones privadas. La ingente recolección de datos personales acerca de la vida de millones de individuos es comparable a los excesos totalitarios del pasado, y que de ser perpetrados en la actualidad por el Estado conllevaría la condena sin paliativos de un tal régimen político[103].

Registro del sonido [Audio Capability]

Finalmente, algunos tipos de video–vigilancia pueden incluir la escucha y grabación de conversaciones entre personas en los espacios objeto de control. La indudable capacidad intrusiva en la intimidad que posee el registro de conversaciones exige que la necesidad de la medida se acredite mediante una justificación verdaderamente excepcional.

A este respecto, se ha pronunciado la jurisprudencia constitucional (STC 98/2000, ponente Garrido Falla), poniendo de manifiesto las dificultades para justificar un control de esta naturaleza, en base a la doctrina ya mencionada relativa al principio de proporcionalidad.

La empresa «Casino de La Toja, SA», para conseguir un adecuado control de la actividad laboral que se desarrollaba en las instalaciones dedicadas al juego de azar y, en concreto, en las dependencias de caja y en donde se hallaba ubicada la ruleta francesa, decidió completar uno de los sistemas de seguridad de que disponía, consistente en un circuito cerrado de televisión –existente desde la apertura del casino–, con la instalación de micrófonos que permitieran recoger y grabar las conversaciones que pudieran producirse en las indicadas secciones del casino. Dichos micrófonos, colocados junto a las cámaras de televisión, aunque podían pasar inadvertidos, no eran ocultos: su instalación se había puesto en conocimiento de los trabajadores desde el primer momento. Su instalación también pretendía utilizar las grabaciones como prueba audible en caso de reclamación de algún cliente. El

[102] En términos muy parecidos se plantea el problema relativo a la privacidad en Internet. Como describe Manuel CASTELLS, las nuevas tecnologías de la identificación aplicadas a los usos de navegación mediante el uso de contraseñas, *cookies* y procesos de autentificación ha abierto un campo extenso y muy valorado para la realización de investigaciones de mercado, bases de datos interconectadas y perfiles agregados. Piénsese en la reducción a la *libertad de navegación* o la intromisión en la privacidad de la persona: una vez se ha insertado la *cokie* en un ordenador, todos los movimientos *on line* realizados desde dicho ordenador son grabados automáticamente por el servidor del sitio *web* que la colocó (*vid.* CASTELLS, M., *La Galaxia Internet*, 2003, pp. 220–221).

[103] *Vid.* ETZIONI, A., *The limits of privacy*, 1999, p. 10.

Comité de Empresa impugnó la instalación de los micrófonos[104], dando lugar en última instancia a la STC 98/2000.

Así, se viene a plantear en este caso si la instalación de micrófonos que permiten grabar las conversaciones de trabajadores y clientes en determinadas zonas del casino se ajusta a las exigencias indispensables del respeto del derecho a la intimidad. Es indiscutible, a juicio del Tribunal, que la instalación de aparatos de captación y grabación del sonido en dos zonas concretas del casino –como son la caja y la ruleta francesa– no carece de utilidad para la organización empresarial, sobre todo si se tiene en cuenta que se trata de dos zonas en las que se producen transacciones económicas de cierta importancia. Ahora bien, la mera utilidad o conveniencia para la empresa no legitima sin más la instalación de los aparatos de audición y grabación, habida cuenta de que la empresa ya disponía de otros sistemas de seguridad que el sistema de audición pretende complementar.

Concluye el Tribunal Constitucional, por tanto, que la finalidad que se persigue –dar un plus de seguridad, especialmente ante eventuales reclamaciones de los clientes– resulta desproporcionada para el sacrificio que implica en el derecho a la intimidad de los trabajadores, e incluso de los clientes del casino. Tal sistema permitía captar comentarios privados, tanto de los clientes como de los trabajadores del casino, comentarios que eran ajenos por completo al interés empresarial y, por tanto, irrelevantes desde la perspectiva de control de las obligaciones laborales, pudiendo, sin embargo, tener consecuencias negativas para los trabajadores que, en todo caso, se van a sentir constreñidos de realizar cualquier tipo de comentario personal ante el convencimiento de que van a ser escuchados y grabados por la empresa[105].

4. **El control oculto de los trabajadores a la luz de la STC 186?2000**

Sin embargo, para analizar las condiciones y límites a partir de los cuales, desde un punto de vista ético–jurídico, sería admisible una vigilancia no transparente de los trabajadores, partiremos de la importante STC 186?2000 (ponente Garrido Falla). La relevancia de esta sentencia en la materia, a modo de precedente jurisprudencial, estriba en que se trata de la primera resolución judicial que, desarrollando la doctrina constitucional relativa al principio de proporcionalidad, justifica un control oculto de los trabajadores, al estimar que se realizó conforme a un adecuado equilibrio de los derechos e intereses fundamentales en conflicto.

Sucintamente, los hechos en los que se basa la sentencia son los siguientes:

Como consecuencia de un descuadre llamativo en los rendimientos de la sección de textil y calzado del economato y de alguna advertencia previa sobre el irregular proceder de los cajeros, la dirección de la compañía contrató con una empresa de seguridad privada la instalación de un circuito cerrado de televisión. El sistema de cámaras de vigilancia instalado enfocaba desde el techo única-

[104] Obsérvese sin embargo que –a diferencia de la STC 186/2000–, en este caso no hubo impugnación de prueba ilícita. Es decir, es razonable pensar que el Tribunal hubiera argumentado de forma distinta ante un supuesto de hecho que presentara algún serio precedente. Por ejemplo, la sospecha motivada de delitos por parte de los trabajadores en los que la audición de la conversación fuera un elemento esencial de prueba.

[105] *Vid.* STC 98/2000, de 10 de julio, Antecedente n. 1 y FJ 9.

mente a las tres cajas registradoras y al mostrador de paso de las mercancías, en el radio de acción aproximado que alcanzaba el cajero con sus manos. Como resultado de la vigilancia realizada, se verificaron y corroboraron las fundadas sospechas que habían motivado la adopción de un sistema de control oculto, y se determinó la adopción de medidas disciplinarias contra los tres trabajadores, aportando como prueba las grabaciones videográficas.

La doctrina que el Tribunal Constitucional español establece, a través de la resolución de este caso, debería poder extenderse a cualesquiera otros medios de vigilancia y control, en la medida en que lo permitan las reglas generales relativas a la *analogia iuris*. En este sentido, el análisis de la adecuación constitucional de los sistemas de video–vigilancia puede establecerse como paradigma en las estrategias generales de prevención de la criminalidad intra–empresarial.

A. *El problema del «observador inobservable»*

El principio general desde el que se debe partir es que la vigilancia a través de CCTV puede vulnerar el derecho a la intimidad cuando ésta tiene lugar mediante una «observación oculta». Ciertamente, el derecho a la intimidad en el entorno laboral debe sufrir restricciones y modulaciones en razón de la particularidad del contexto. El trabajador debe así adaptar su conducta a las legítimas limitaciones impuestas por el empresario. Sin embargo, aunque es cierto que la proyección expansiva de la intimidad de la persona debe restringirse según la naturaleza y las reglas del entorno concreto (en tanto que no es lo mismo el domicilio, el espacio público o el lugar de trabajo), se debe reconocer un principio general de transparencia en la actividad de control. Es decir, la expectativa de visibilidad de las personas que rodean el espacio que se ocupa debe permitir a la persona disfrutar legítimamente de un reducido ámbito mínimo de intimidad, aún en el contexto de un espacio público o semipúblico.

Cuando un trabajador está pasando por una zona de la empresa sometida al control de las cámaras, debería al menos ser capaz de saber que está siendo observado, para poder así adecuar legítimamente su conducta ante la observación de terceros. Como señala von Hirsch, la «observabilidad del observador» permite a la persona –en la medida en que le afecte lo que puedan pensar los demás– ajustar su comportamiento cuando sabe que le están observando terceras personas[106]. Un trabajador que tuviera la costumbre de hablar en voz alta de cosas íntimas con su esposa difunta mientras realiza un trabajo manual, si deseara no dar la impresión a los demás de que está loco, dejaría de hacerlo en el momento en que pasaran cerca de él otras personas. No se trata de que la conducta sea inocua, lícita o legal, o de que tenga una justificación. En ese momento, ese espacio constituye una prolongación de la esfera íntima, únicamente porque se da la expectativa de hallarse uno a solas. No es tan relevante el contexto, sino que basta la expectativa de hallarse a solas, unido a la expectativa de que el observador será observable.

A juicio de von Hirsch, la «observación oculta» presenta problemas de legitimidad por dos razones. En primer lugar, (1) en tanto que se registra la conducta de la persona estando ésta desprevenida, pudiendo razonablemente pensar para sí misma que está libre de observación por parte de terceros, cuando en realidad no es así. Además, (2) en segundo lugar, porque puede producir un efecto intimidatorio en las personas («chilling effect»), en tanto que una vez se es consciente de que se están llevando a cabo contro-

[106] VON HIRSCH, A., *Ibid*., 2007, p. 15.

les de forma encubierta, se puede generar un sensación general de control cuando se está circulando por espacios públicos[107]. Si se permitiera con carácter general una vigilancia encubierta, no sólo la privacidad de las personas quedaría seriamente comprometida, sino que afectaría a todo el régimen de libertades y derechos fundamentales. Desde este punto de vista, la libertad en sentido amplio está íntimamente vinculada al «dominio personal del conocimiento sobre mi persona que libremente deseo comunicar a los demás», ya sea en mi esfera de amistades más cercana o en mi proyección personal en las relaciones sociales en general[108].

En relación a las consecuencias que una injerencia desmedida en la esfera individual puede tener en la libertad de actuación del individuo, Schoeman describe la profunda relación intrínseca entre privacidad y libertad[109]. La privacidad es así garantía de libertad, en tanto que la orientación y especificación del «libre albedrío en lo social» queda protegida frente al conocimiento de terceros[110], o frente a aquellas posibles consecuencias negativas que pudieran derivarse de ese conocimiento[111]. Sin embargo, en las relaciones laborales tiene lugar una contradicción irreconciliable, en tanto que en el ámbito del trabajo la persona se inserta y participa como en ningún otro ámbito de la existencia humana en las relaciones sociales, estando su libertad de pensamiento y actuación en buena medida condicionados.

«Understanding how privacy works in the social context is more complicated than understanding how privacy works in the governmental context […]. Although the political and legal approaches to privacy have been illuminating and important, they have omitted an especially important dimension of privacy: the form and function of privacy in promoting social freedom […]. John Stuart Mill wrote his great essay On Liberty to change public consciousness in ways that would better protect people from social overreaching. He was concerned that we are more vulnerable to the insidious control of other citizens than we are to the tyrannical impulses of government. Yet present–day uses of the essay focus on the relatively brief discussion Mill devotes to governments and leave unexplored what Mill took to be most important […]. It follows that when we act because of social pressures, or because we want to conform to what we see around us, we are less than free, less than rational, less than autonomous»[112].

[107] *Vid.* VON HIRSCH, A., *Ibid.*, 2007, p. 15, donde concluye que argumentar que los potenciales delincuentes deben sentirse constreñidos si van a cometer delitos en espacios públicos no es respuesta a esas objeciones, en tanto que la vigilancia se extiende más allá de los delincuentes sospechosos, alcanzando a cualquiera que esté bajo el radio de acción de las cámaras.

[108] Lo que subyace bajo el derecho a la intimidad no es sino la libertad humana, configurada como «fundamento del orden político y de la paz social» (*vid.* CABEZUELO ARENAS, A.L., *Derecho a la intimidad*, 1998, p. 19 y art. 10 CE).

[109] SCHOEMAN, F.D., *Privacy and social freedom*, 1992.

[110] Dentro del la vida social de la persona y en relación a su propio entorno laboral, las intromisiones o revelaciones que pueden razonablemente exigirse deberían estar relacionadas con aspectos específicos estrictamente necesarios: el empresario tiene derecho a conocer cuándo el trabajador desea tomarse las vacaciones y durante cuánto tiempo, pero no a puede pretender conocer las actividades tiene previsto realizar o el lugar de descanso elegido –ejemplo tomado en parte de VON HIRSCH, A., *Ibid*., 2007, p. 9–.

[111] Aunque el empresario conozca de forma fortuita la orientación religiosa del trabajador o su extravagante conducta los fines de semana, no podrá derivar consecuencias, a menos que guarde estricta relación con la prestación laboral. El empresario accede en todo caso de forma casual a la información, o por voluntad gratuita del trabajador. Se podría decir que se trata de un *conocimiento especial*, en tanto excede del derecho del empresario y del rol asociado a su posición.

[112] SCHOEMAN, F.D., *Privacy and social freedom*, 1992, pp. 1–3. Para profundizar en la relación entre *privacy*

En cuanto a las condiciones en que el control deja de ser oculto, la advertencia de la presencia de las cámaras puede realizarse de formas diversas, teniendo distintos efectos en los trabajadores. Así, las personas objeto de vigilancia pueden tener conciencia efectiva (advertencia psicológica) o simplemente haber sido receptores de una genérica advertencia formal conforme a la norma (advertencia normativa). Es decir, el hecho de que se haya cumplido normativamente con el deber general de indicar la existencia de un sistema de vigilancia en funcionamiento, no impide que las cámaras pasen desapercibidas al trabajador, especialmente si están integradas entre otros accidentes en el entorno físico circundante. El objetivo de la norma es limitar en cierto grado el carácter absolutamente imprevisible y arbitrario de la actividad de vigilancia empresarial. En este sentido, las políticas de advertencia empresarial podrían variar, desde una mínima formalidad –aunque sea genérica y no especifique el lugar y el tiempo de la vigilancia– hasta un férreo sistema que obligue a una comunicación diaria de las cámaras y sistemas de vigilancia en funcionamiento. Sin embargo, la justificación de un seguimiento encubierto de personas o lugares por la existencia de un patrón de riesgo objetivo no puede considerarse imprevisible –el empresario debe poder defenderse de alguna forma– o arbitrario –la excepción al principio general se puede ajustar a una argumentación jurídica–.

Pueden darse, por tanto, muy distintas formas de advertencia previa que convendrá analizar. En ocasiones, puede consistir en un anuncio genérico e indeterminado. La ley puede fijar, a este respecto, los concretos requisitos formales con que debe instalarse un sistema de CCTV. Las garantías relativas al procedimiento también pueden variar, entendiendo que cuando sean formalmente válidas, la inadvertencia del trabajador no sería imputable al empresario. Sin embargo, por encima del requisito formal específico parece razonable exigir, con carácter general al menos, un principio de control transparente –no oculto– acorde con la dignidad humana de los trabajadores.

Una vez se ha fijado un rígido sistema de comunicación o advertencia previa, el defecto de forma puede plantear serios problemas desde un punto de vista ético–jurídico, especialmente por lo que respecta a qué consecuencias deben seguirse de un cumplimiento similar o una advertencia mínima. Así por ejemplo, en la referida anteriormente STC 186/2000 no se realizó la comunicación preceptiva al Comité de Empresa, considerándose éste un mero defecto de forma.

Efectivamente, los trabajadores alegaron que la implantación del sistema de seguridad «no se puso en conocimiento del Comité de empresa, como prescribe el art. 64.1.3 d) ET. Este tipo de control –afirma el recurrente– debe hacerse con publicidad, no con procedimientos ocultos, y en este caso ni el Comité de empresa ni los trabajadores lo conocían» (FJ 6, STC 186/2000).

Sin embargo, a juicio del Tribunal, el hecho de que la instalación del circuito cerrado de televisión no fuera previamente puesta en conocimiento del Comité de empresa y de los trabajadores afectados –sin duda por el justificado temor de la empresa de que el conocimiento de la existencia del sistema de filmación frustraría la finalidad perseguida– «carece de trascendencia desde la perspectiva constitucional», pues, fuese o no exigible el informe previo del Comité de empresa a la luz del art. 64.1.3 d) ET, estaríamos en todo caso ante «una cuestión de mera legalidad ordinaria, ajena por

y *autonomy vid.* pp. 20–22.

completo al objeto del recurso de amparo». Todo ello sin perjuicio de dejar constancia de que los órganos judiciales han dado una respuesta negativa a esta cuestión, respuesta que no cabe tildar de arbitraria o irrazonable, lo que veda en cualquier caso su revisión en esta sede (FJ 7, STC 186/2000). Es relevante destacar que, aunque el Tribunal no necesita pronunciarse sobre el fondo, la interpretación *obiter dicta* que realiza pone de manifiesto que el requisito de forma está al servicio de la finalidad legítima y proporcional que origina la vigilancia oculta.

Entendemos en este sentido que no se puede confundir procedimiento formal con una objetiva vulneración del espíritu de la ley. Es decir, el defecto de forma debería ser subsanable en determinados casos, de modo que el procedimiento generalmente previsto debería poder sufrir alteraciones en función de una causa justa, a tenor de las circunstancias concomitantes. En este sentido, como afirma Martín Morales, un garantismo llevado a los extremos confunde lo justo con lo injusto y provoca una reacción social que termina erosionando el propio derecho que se pretendía proteger[113].

B. *Patrón de riesgo objetivo y legítima defensa*

El concreto motivo justificante del carácter no transparente de la vigilancia va a resultar así el elemento determinante de la legitimidad de un control oculto a los trabajadores. De esta forma, si el patrón de riesgo guarda un sólido fundamento –en el caso de la STC 186/2000, la existencia de un delito precedente y continuado–, bastará aplicar a las circunstancias del supuesto de hecho las medidas convenientes según el principio de proporcionalidad anteriormente mencionado.

En este sentido es especialmente elocuente el Fundamento Jurídico séptimo de la STC 186/2000, en el que se contiene el nervio del razonamiento del Tribunal y la concreta aplicación del principio de proporcionalidad al caso objeto de recurso, concluyéndose que los derechos a la intimidad personal y a la propia imagen no han resultado en efecto vulnerados:

«Pues bien, del razonamiento contenido en las Sentencias recurridas se desprende que, en el caso que nos ocupa, la medida de instalación de un circuito cerrado de televisión que controlaba la zona donde el demandante de amparo desempeñaba su actividad laboral era una medida justificada (ya que existían razonables sospechas de la comisión por parte del recurrente de graves irregularidades en su puesto de trabajo); idónea para la finalidad pretendida por la empresa (verificar si el trabajador cometía efectivamente las irregularidades sospechadas y en tal caso adoptar las medidas disciplinarias correspondientes); necesaria (ya que la grabación serviría de prueba de tales irregularidades); y equilibrada (pues la grabación de imágenes se limitó a la zona de la caja y a una duración temporal limitada, la suficiente para comprobar que no se trataba de un hecho aislado o de una confusión, sino de una conducta ilícita reiterada), por lo que debe descartarse que se haya producido lesión alguna del derecho a la intimidad personal consagrado en el art. 18.1 CE.

En efecto, la intimidad del recurrente no resulta agredida por el mero hecho de filmar cómo desempeñaba las tareas encomendadas en su puesto de trabajo, pues esa medida no resulta arbitraria ni caprichosa, ni se pretendía con la misma divulgar su conducta, sino que se trataba de obtener un conocimiento de cuál era su comportamiento laboral, pretensión justificada por la circunstancia de haberse detectado irregularidades en la actuación profesional del trabajador, constitutivas de trasgresión a la buena fe contractual. Se trataba, en suma, de verificar las fundadas sospechas de la empresa sobre la torticera conducta del trabajador, sospechas que efectivamente resultaron corroboradas por

[113] MARTÍN MORALES, R., *El régimen constitucional del secreto de las comunicaciones*, 1995, p. 68.

las grabaciones videográficas, y de tener una prueba fehaciente de la comisión de tales hechos, para el caso de que el trabajador impugnase, como así lo hizo, la sanción de despido disciplinario que la empresa le impuso por tales hechos.

Pero es más, como ya quedó advertido, en el caso presente la medida no obedeció al propósito de vigilar y controlar genéricamente el cumplimiento por los trabajadores de las obligaciones que les incumben, a diferencia del caso resuelto en nuestra reciente STC 98/2000, en el que la empresa, existiendo un sistema de grabación de imágenes no discutido, amén de otros sistemas de control, pretendía añadir un sistema de grabación de sonido para mayor seguridad, sin quedar acreditado que este nuevo sistema se instalase como consecuencia de la detección de una quiebra en los sistemas de seguridad ya existentes y sin que resultase acreditado que el nuevo sistema, que permitiría la audición continuada e indiscriminada de todo tipo de conversaciones, resultase indispensable para la seguridad y buen funcionamiento del casino. Por el contrario, en el presente caso ocurre que previamente se habían advertido irregularidades en el comportamiento de los cajeros en determinada sección del economato y un acusado descuadre contable. Y se adoptó la medida de vigilancia de modo que las cámaras únicamente grabaran el ámbito físico estrictamente imprescindible (las cajas registradoras y la zona del mostrador de paso de las mercancías más próxima a los cajeros). En definitiva, el principio de proporcionalidad fue respetado».

IV. **CONSIDERACIONES FINALES**

A modo de conclusión, puede afirmarse que la justificación de las concretas medidas empresariales de control o injerencia debe analizarse desde una perspectiva sui generis respecto de los medios de legítima defensa. Con ello, no se pretende llegar a dar cobertura a intromisiones en casos denominados de «legítima defensa preventiva», ya que en ellos no se puede afirmar, propiamente, que la agresión ya se ha iniciado y no ha concluido enteramente.

Así, una vez iniciada la agresión, ante la más que probable prolongación en el tiempo de los actos parciales en que se divide la conducta delictiva del trabajador, la única forma de defenderse por parte del empresario podría pasar por identificar al agresor. En tal contexto, por razón de la necesaria confianza a la que se ve forzado el empresario en el normal desarrollo de la actividad en la empresa (puesto que algún trabajador deberá tener acceso a la caja registradora), no le queda más remedio que instalar un sistema oculto de control de los trabajadores sospechosos[114].

La trascendencia de la legitimación de una actividad de control de esta naturaleza por parte del Tribunal Constitucional todavía debe ser valorada con prudencia. Sin embargo, la *ratio decidendi* del fallo sienta un precedente que puede proporcionar mayor seguridad jurídica, y adelantar en qué circunstancias podrá el empresario realizar un control oculto de los trabajadores ante patrones de riesgo ya manifestado.

[114] Para un análisis en profundidad de la eventual tipicidad y antijuricidad de la conducta de *control oculto* del empresario, puede verse AGUSTINA SANLLEHÍ, J.R., *El delito de descubrimiento y revelación de secretos en su aplicación al control del correo electrónico del trabajador*, 2009. En ese trabajo he analizado con detenimiento las exigentes condiciones en que se podría tratar de justificar una causa de justificación en defensa del empresario.

BIBLIOGRAFÍA

AGUSTINA SANLLEHÍ, J.R. (2009), El delito de descubrimiento y revelación de secretos en su aplicación al control del correo electrónico del trabajador, Colección Temas La Ley, Editorial La Ley, Madrid.

AGUSTINA SANLLEHÍ, J.R. (2009), "Límites en las estrategias de prevención del delito en la empresa. A propósito del control del correo electrónico del trabajador como posible violación de la intimidad", Revista InDret 2/2009, Barcelona, http://www.indret.com

AGUSTINA SANLLEHÍ, J.R. (2009), Privacidad del trabajador versus deberes de prevención del delito en la empresa, BdeF, Buenos Aires-Montevideo-Madrid, 2009.

AGUSTINA SANLLEHÍ, J.R. (2009), El delito en la empresa. Prevención de la criminalidad intraempresarial y deberes de control del empresario, Atelier, Barcelona.

AGUSTINA SANLLEHÍ, J.R. (2009), "La arquitectura digital de Internet como factor criminógeno: Estrategias de prevención frente a la delincuencia virtual", International e-Journal of Criminal Science, Artículo 4, Número 3 (2009), ISSN: 1988-7949, http://www.ehu.es/inecs

AGUSTINA SANLLEHÍ, J.R. (2007), "Cuestiones Éticas en torno a la vigilancia en espacios públicos mediante cámaras de televisión", InDret 4/2007, octubre. Traducción del texto de VON HIRSCH, A. "The Ethics of Public Television Surveillance", publicado en VON HIRSCH, A., GARLAND, D. AND WAKEFIELD, A. (eds). Ethical and Social Perspectives on Situational Crime Prevention, London: Hart, 2000, http://www.indret.com

ALDER, G.S. (1998), Ethical Issues in Electronic Performance Monitoring: A Consideration of Deontological and Teleological Perspectives, Journal of Business Ethics 17: 729–743.

BARNES, P., LAMBELL, J. (2002), Organisational Susceptability to Fraud: Does Fraud Strike Randomly or Are There Organisational Factors Affecting its Likelihood and Size?, Working Paper, Nottingham Business School.

BECK, U. (1993), De la sociedad industrial a la sociedad del riesgo (trad. DEL RÍO HERRMANN), en «Revista de Occidente», núm. 150, noviembre 1993.

BIRKS, P. (ed.) (1997), Privacy and Loyalty, Clarendon Press, Oxford.

BLANPAIN, R. (ed.) (2000), On–line Rights for Employees in the Information Society. Use and Monitoring of E–mail and Internet at Work, Brussels 13–14 November 2000. Proceedings of the Conference by the Royal Flemish Academy of Belgium for Science and the Arts, Union Network International, UNI–Europa, The Euro–Japan Institute for Law and Business, Bulletin of Comparative Labour Relations 40–2002.

BLOSS, W.P. (1998), Warrantless search in law enforcement workplace: court interpretation of employer practices & employee privacy rights under Ortega doctrine, Police Quarterly, vol. 1, no. 2, pp. 51–69.

BLOUNT, E.C. (2003), Occupational Crime. Deterrence, Investigation, and Reporting in Compliance with Federal Guidelines, Florida.

BOLOGNA, J., SHAW, P. (1997), Corporate Crime Investigation, Washington.

BOOKMAN, Z.F. (2007), Convergences and Omissions in the Reporting of Corporate and White Collar Crime, Yale Law School Student Scholarship Series, paper 43. Disponible en http://lsr.nellco.org/yale/student/papers/43

BRAITHWAITE, J. (1984), Corporate Crime in the Pharmaceutical Industry, London.

BROWN, W.S. (1996). Technology, workplace privacy, and personhood, Journal of Business Ethics, 15, 1237–1248.

BRISEBOIS, R. (1997), Sobre la confianza, Cuadernos Empresa y Humanismo, Vol. 65, Pamplona.

BRUCE, A., FORMISAND, R. (2003), Building a high–morale workplace, New York.

BURGOS, J.M. (2003), El personalismo, Madrid.

BUSSMANN, K.–D. (2003), Causes of Economic Crime and the Impact of Values: Business Ethics as a Crime Prevention Measure, paper presented at the Swiss Conference on Coping with Economic Crime. Risks and Strategies, Zurich.

BUSSMANN, K.–D., WERLE, M.M. (2006), Addressing Crime in Companies. First Findings from a Global Survey of Economic Crime, British Journal of Criminology, 46, 1128–1144.

BYRNE, J.M., REBOVICH, D.J. (2007), The new technology of crime, law and social control, Monsey, NY: Criminal Justice Press.

CABEZUELO ARENAS, A.L. (1998), Derecho a la intimidad, Valencia.

CASEY, E. (2004), Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet, First edition 2000, London.

CASTELLS, M. (1997), La era de la información. Volumen 1: La sociedad red. Madrid.

CASTELLS, M. (2003), La Galaxia Internet, Barcelona.

CLAES, E., DUFF, A., GUTWIRTH, S. (2006), Privacy and the Criminal Law, Oxford.

CLARKE, R.V. (1992), Situational Crime Prevention: Successful Case Studies, New York.

CLARKE, R.V. (1995), Situational Crime Prevention, Crime and Justice, 91.

CLARKE, R.V. (1984), Opportunity–based Crime Rates, British Journal of Criminology, 24:74–83.

COFFEE, J.C., JR (2006), Gatekeepers: The Professions and Corporate Governance, Oxford.

COHEN, L.E., FELSON, M. (1979) ´Social change and crime rate tends: a routine activities approach´, American Sociological Review, 44, pp. 588–608.

CRUZ CRUZ, J. (1995), Valores éticos, Cuadernos Empresa y Humanismo, Vol. 50, Pamplona.

DAVIS, P., FRANCIS, P., JUPP, V. (1999), Crime–Work Connections: Exploring the 'Invisibility' of Workplace Crime, in DAVIS, P., FRANCIS, P., JUPP, V., Invisible Crimes. Their Victims and their Regulation, London, pp. 54–74.

DICKENS, W.T., KATZ, L.F., LANG, K., SUMMERS, L.H. (1989), Employee crime and the monitoring puzzle, Journal of Labour Economics, 7, pp. 331–347.

DODD N.J. (2004), 'Troublemaker' and 'Nothing to Lose' Employee Offenders Identified from a Corporate Crime Data Sample, Crime Prevention and Community Safety: An International Journal, 6 (3), 23–32.

DUFF, R.A. (2007), Answering for Crime. Responsability and Liability in the Criminal Law, Oxford.

ECK, J.E. (1997), «Do premises liability suits promote business crime prevention?» in FELSON, M., CLARKE, R.V. (ed.), Business and Crime Prevention, New York, pp. 125–150.

ETZIONI, A. (1999), The limits of privacy, New York.

EVERETT, A.M., WONG, Y.–Y., PAYNTER, J. (2006), Balancing employee and employer rights: an international comparison of e–mail privacy in the workplace, Journal of Individual Employment Rights, Vol. 11(4) 291–310, 2004–2005.

FALGUERA BARÓ, M.A. (2004), Trabajadores, empresas y nuevas tecnologías, artículo publicado en Cuadernos y Estudios de Derecho Judicial, pp. 187–221.

FELSON, M. (1994), Crime and Everyday life. Insights and Implications for Society, California (second edition).

FELSON, M., CLARKE, R.V. (ed.) (1997), Business and Crime Prevention, New York.

FENNELLY, L.J. (2004), Handbook of loss prevention and crime prevention, Burlington, MA: Elsevier Butterworth–Heinemann.

FERNÁNDEZ VILLAZÓN, L.A. (2003), La facultades empresariales de control de la actividad laboral, Navarra.

FINKIN, M.W. (2005), Employee Privacy and the "Theory of the Firm", Journal of Labor Research, Volume XXVI, Number 4, Fall, pp. 711–723.

FINKIN, M.W. (2002), "Information Technology and workers' privacy: the United States Law", in JEFFERY, M., Information Technology and workers´ privacy: a comparative study, Comparative Labor Law & Policy Journal, volume 23, number 2.

FISHMAN, C.S., MCKENNA, A.T. (2007), Wiretapping & Eavesdropping: Surveillance in the Internet Age, 3rd ed.

FLETCHER, G.P. (1993), Loyalty. An Essay on the Morality of Relationships, Oxford.

FONTRODONA FELIP, J., GUILLÉN PARRA, M, RODRÍGUEZ SEDANO, A. (1998), La ética que necesita la empresa, Madrid.

FONTRODONA FELIP, J. y GARCÍA CASTRO, R. (2002), Estudio sobre políticas, hábitos de uso y control de Internet y correo electrónico en las principales empresas españolas, disponible en http://www.iese.edu/es/files/5_6604.pdf

FORD, M. (2002), Two Conceptions of Worker Privacy, Industrial Law Journal, Vol. 31, No. 2, June, pp. 135–155.

FOUCAULT, M. (1979), Discipline and Punish, New York.

FRANKEL, T. (2006), Trust and Honesty. America's Business Culture at a Crossroad, Oxford.

FRIEDRICHS, D.O. (2002), Occupational crime, occupational deviance, and workplace crime: Sorting out the difference, Criminal Justice, Vol. 2, No. 3, 243–256.

GARCÍA GONZÁLEZ, J. (2006), "Intervenciones de terceros en el correo electrónico. Especial referencia al ámbito laboral y policial", en El cibercrimen: nuevos retos jurídico–penales, nuevas respuestas político–criminales, ROMEO CASANOVA, C.M. (coord.), Granada, pp. 297–323.

GARCÍA RUIZ, P. (1994), La lógica del directivo: el control necesario y la confianza imposible, Cuadernos Empresa y Humanismo, Vol. 47, Pamplona.

GARLAND, D. (2005), La cultura del control (trad. de M. SOZZO), Barcelona.

GILL, M. (1994), Crime at Work: Studies in Security and Crime Prevention, Leicester, UK.

GOOLD, BENJAMIN J. (2002), Privacy rights and public spaces: CCTV and the problem of the unobservable observer, Criminal Justice Ethics, vol. 21, no. 1, pp. 21–27.

GREEN, G.S. (1997), Occupational Crime, Second Edition, Chicago.

GREEN, S.P. (2006), Lying, Cheating, and Stealing. A Moral Theory of White-Collar Crime, Oxford University Press.

GUERIN, L. (2004), Workplace Investigations: a step by step guide.

GUILLÉN, M. (1996), La Ética empresarial: una aproximación al fenómeno, Cuadernos Empresa y Humanismo, Vol. 58, Pamplona.

HAGGERTY, K.D., ERICSON, R.V. (2006), The New Politics of Surveillance and Visibility, University of Toronto Press.

HAYES, R. (2008), Strategies to detect and prevent workplace dishonesty, Connecting Research in Security to Practice (CRISP).

HENDRICKX, F. (2002), Employment Privacy Law in the European Union: Surveillance and Monitoring, Antwerp–Oxford–New York.

HOME OFFICE RESEARCH (2005), Public attitudes towards CCTV: Results from the pre-intervention public attitude survey carried out in areas implementing CCTV, Development and Statistics Directorate, London, United Kingdom.

HUNTER, R. (2002), World Without Secrets: Business, Crime and Privacy in the Age of Ubiquitous Computing, John Wiley and Sons.

JEFFERY, M. (2002), Information Technology and workers´ privacy: a comparative study, Comparative Labor Law & Policy Journal, volume 23, number 2.

JEFFERY, M. (2001), ¿Carta Blanca para espiar a los trabajadores? Perspectivas inglesas sobre poder informático e intimidad. Ponencia presentada el 30 de marzo de 2001 en el Seminario "Poder informático e intimidad: límites jurídico–laborales y penales al control empresarial", organizado por los Estudios de Derecho y Ciencias Políticas de la UOC.

JUPP, V.R., DAVIS, P., FRANCIS, P. (1999), ´The features of Invisible Crimes´ in DAVIS, P., FRANCIS, P. AND JUPP, V.R., Invisible Crimes. Their Victims and their Regulation, London.

KATYAL, N.K. (2002), Digital Architecture as Crime Control, 111 Yale Law Journal 1039.

KUPRITZ, F.J., et al. (1998), Privacy in the workplace: the impact of building design, Journal of Environmental Psychology, 18, pp. 341–356.

LANE III, F.S. (2003), The naked Employee. How technology is compromising workplace privacy, New York.

LASPROGATA, G., KING, N.J., PILLAY, S. (2004), Regulation of electronic employee monitoring: identifying fundamental principles of employee privacy through a comparative study of data privacy legislation in the European Union, United States and Canada, Stanford Technology Law Review 4.

LORENTE, J. (2007), El uso laboral y sindical del correo electrónico e Internet en la empresa. Aspectos constitucionales, penales y laborales, Valencia.

LUHMANN, N. (2005), Confianza, (trad. Amada FLORES), Santiago de Chile.

LYON, D. (2003), Surveillance as Social Sorting. Privacy, risk, and digital discrimination, London.

MANSELL, R., COLLINS, B.S. (2005), Trust and crime in information societies, Cheltenham: Edward Elgar.

MARCHENA GÓMEZ, M. (2006), «Dimensión jurídico–penal del correo electrónico», Diario La Ley, n. 6475, 4 de mayo, ref. D–114.

MARÍN ALONSO, I. (2005), El poder de control empresarial sobre el uso del correo electrónico en la empresa, Valencia.

MARS, G. (1982), Cheats at Work. An Anthropology of Workplace Crime, London.

MAZA MARTÍN, J.M. (2001), La intervención judicial de las comunicaciones a través de Internet, en Internet y Derecho Penal, Cuadernos de Derecho Judicial 10, pp. 633–643.

MCCAHILL, M., NORRIS, C. (1999), Watching the workers: Crime, CCTV and the Workplace, in DAVIS, P., FRANCIS, P., JUPP, V., Invisible Crimes. Their Victims and their Regulation, London, pp. 208–231.

MCCAHILL, M. (2002), The Surveillance Web. The rise of visual surveillance in an English city, USA–Canada.

MELÉ, D. (2007), La empresa como comunidad de personas frente a otras visiones de la empresa, en J. M. Burgos (Ed.), La filosofía personalista de Karol Wojtyla, Madrid, pp. 315–328.

MONTERDE FERRE, F. (2006), Especial consideración de los atentados por medios informáticos contra la intimidad y la privacidad, en Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?, Cuaderno de Derecho Judicial, Madrid, pp. 191–262.

MORALES GARCÍA, O. (2001), La tutela penal de las comunicaciones laborales. A propósito de la estructura típica del artículo 197.1 CP. Ponencia presentada el 30 de marzo de 2001 en el Seminario "Poder informático e intimidad: límites jurídico–laborales y penales al control empresarial", organizado por los Estudios de Derecho y Ciencias Políticas de la UOC.

MORRIS, G.S. (2001), Fundamental Rights: Exclusion by Agreement?, Industrial Law Journal, Vol. 30, No. 1, March, pp. 49–71.

MUÑOZ CONDE, F. (2004), Valoración de las grabaciones audiovisuales en el proceso penal, Ed. Hammurabi.

NAGIN, D.S., PATERNOSTER, R., REBITZER, J.B., SANDERS, S., TAYLOR, L.J. (2002), Monitoring, motivation, and management: the determinants of opportunistic behaviour in a field experiment, American Economic Review, 92, 850–873.

NOUWT, S., DE VRIES, B.R., PRINS, C. (2005), Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy, The Netherlands.

OZ, E., GLASS, R., BEHLING, R. (1999), Electronic workplace monitoring: what employees think, Omega, The International Journal of Management Science, 27 167–177.

PÉREZ LÓPEZ, J.A. (2002), Fundamentos de la Dirección de Empresas, quinta edición, Madrid.

PORTER II, W.G., GRIFFATON, M.C. (2003), Between the Devil and the Deep Blue Sea: Monitoring the Electronic Workplace. Employers should have Detailed, Understandable and Fair Computer, E-Mail and Internet Usage Policies Impartially Administered, Defense Counsel Journal, January.

RATCLIFFE, J. (2006), Video Surveillance of Public Places, U.S. Department of Justice, Office of Community Oriented Policing Services, Problem-Oriented Guides for Police Response Guides, Series Guide No. 4.

RAY, D.E., SHARPE, C.W., STRASSFELD, R.N. (1999), Understanding Labor Law, New York.

RICKMAN, N., WITT, R. (2007), The Determinants of Employee Crime in the UK, Economica 74, 161–175.

SCOTT, J.C. (1998), Seeing Like a State, New Haven.

SILVA SÁNCHEZ, J.M. (2001), La expansión del Derecho penal. Aspectos de la política criminal en las sociedades postindustriales, Madrid.

SIMONS, R. (1991), Strategic orientation and top management attention to control systems, Strategic Management Journal, 12 (1), pp. 49–62.

SIMPSON, S.S. (2002), Corporate Crime, Law, and Social Control, Cambridge.

SIPIOR, J.C. (1998), Ethical management of employee e–mail privacy, Information Systems Management, 15, pp. 41–47.

SLOBOGIN, C. (2007), Privacy at Risk. The New Government Surveillance and the Fourth Amendment, Chicago.

SNIDER, L. (1990), Cooperative Models and Corporate Crime: Panacea or Cop–Out?, Crime and Delinquency 36.

SNIDER, L. (2001), Crimes against capital: Discovering theft of time, Social Justice, vol. 28, no. 3, pp. 105–120.

SOLOVE, D.J. (2008), Understanding Privacy, London.

SPEED, M. (2003), Reducing Employee Dishonesty: In Search of the Right Strategy, in Managing Security. Crime at Work (Volume III), Leicester, Chapter 10, pp157-179.

STANTON, J.M., STAM, K.R. (2006), The Visible Employee. Using workplace monitoring and surveillance to protect information assets without compromising employee privacy or trust, New Jersey.

TAYLOR, N. (2002), State Surveillance and the Right to Privacy, Surveillance & Society 1 (1): 66–85.

TRAUB, S.H. (1996), Battling Employee Crime: A Review of Corporate Strategies and Programs, Crime & Delinquency, Vol. 42 No. 2, April 244–256.

UGARTE, J.L. (2000), El derecho a la intimidad y la relación laboral, Doctrina, Estudios y comentarios en el Boletín Oficial de la Dirección del Trabajo, núm. 139.

VON HIRSCH, A. (2000), Cuestiones éticas en torno a la vigilancia en espacios públicos mediante cámaras de televisión (trad. de J.R. AGUSTINA SANLLEHÍ), en VON HIRSCH, A., GARLAND, D., WAKEFIELD, A. (eds), Ethical and Social Perspectives on Situational Crime Prevention, London: Hart (publicado en InDret 4/2007).

WALTERS, G.J. (2001), Privacy and Security: An Ethical Analysis, Computers and Society, June 2001. Excerpted from Chapter 5 of Human Rights in an Information Age: A Philosophical Analysis, University of Toronto Press.

WATSON, G. (2002), E–mail surveillance in the UK workplace – a management consulting case study, Aslib Proceedings, Volume 54, Number 1, pp. 23–40.

WECKERT , J. (2005), Electronic monitoring in the workplace: controversies and solutions, UK-US.

WEN, H.J., GERSHUNY, P. (2005), Computer–based monitoring in the American workplace: Surveillance technologies and legal challenges, Human Systems Management 24 165–173, IOS Press.

WHITAKER, R. (1999), El fin de la privacidad (The End of Privacy), Barcelona.

WIKSTRÖM, P.–O.H., SAMPSON, R.J. (2006), The Explanation of Crime. Context, Mechanisms and Development, published in New York by Cambridge University Press.

WILDING, E. (2006), Information risk and security: preventing and investigating workplace computer crime, UK-US

WILLISON, R. (2006), Understanding the perpetration of employee computer crime in the organizational context, Information and Organization 16 304–324.

YAR, M. (2005), The Novelty of 'Cybercrime'. An Assessment in Light of Routine Activity Theory, European Journal of Criminology, Volume 2 (4), p. 407–427.

ZUREIK, E. (2003), Theorizing surveillance. The case of the workplace, in LYON, D., Surveillance as Social Sorting. Privacy, risk, and digital discrimination, London.