IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

www.uoc.edu/idp

ARTÍCULO

¿Cómo prevenir conductas abusivas y delitos tecnológicos en la empresa?

Estudio interdisciplinar sobre políticas de uso de las TIC, prevención y gestión de «conflictos» en una muestra de empresas españolas[1]

Jose R. Agustina
Profesor contratado doctor de la Universitat Internacional de Catalunya

Fecha de presentación: abril de 2013
Fecha de aceptación: junio de 2013
Fecha de publicación: junio 2013

Resumen

El estudio de las conductas desviadas de los trabajadores en el empleo de los recursos informáticos que la empresa pone a su disposición (el ordenador, el correo electrónico, el teléfono móvil, las PDA...) constituye un área de investigación de creciente interés, en buena medida por su impacto económico, directo e indirecto, en los beneficios empresariales. En este artículo se analizan las estrategias de prevención y control del uso de las nuevas tecnologías por parte de los trabajadores en una muestra de empresas españolas.

El gobierno y la dirección de personas y la prevención de conductas abusivas, cuando menos, requiere la búsqueda de fórmulas de gestión que tengan en consideración los distintos aspectos éticos, motivacionales y jurídicos implicados, de forma que el necesario control no menoscabe la generación y el mantenimiento de un indispensable clima de confianza en el seno de las organizaciones.

El presente estudio pretende aportar mayor conocimiento de la realidad acerca de cómo se están implementando distintos mecanismos de control, en sintonía con investigaciones similares, si bien pone el énfasis en la propia actividad de control y en la reacción de la empresa, más que en los actos desleales o abusivos de los trabajadores. A modo de conclusión, se sugieren algunas orientaciones prácticas dirigidas a las empresas a la hora de abordar el control de la actividad de los trabajadores en el uso de las TIC.

1. Los resultados completos del presente estudio fueron publicados previamente en: José R. Agustina, Ana Alós Ramos y Javier Sánchez Marquiegui (2012). Informe *Estrategias de control de las nuevas tecnologías en la empresa. Estudio sobre la gestión de personas y recursos tecnológicos para prevenir conductas abusivas y delictivas en la empresa*. Universidad-Empresa Control de las TIC en el entorno laboral. Barcelona: Ribas y asociados. ISBN 9788461611799.

Palabras clave
delito en la empresa, política de uso de las TIC, control de los trabajadores y privacidad, delito informático, ética empresarial, gestión de recursos humanos.

Tema
delitos tecnológicos en la empresa

How to prevent abusive behaviour and technological crime at companies?

An interdisciplinary study of the ICT use policies, and prevention and management of "conflicts" in a sample of Spanish companies

Abstract
The study of improper behaviour of employees in the use of the computer resources that a company provides them (PC, email, mobile telephone, PDA, etc.) represents an area of research of growing interest, in great part due to the financial impact, both direct and indirect, it can have on profits. This article analyses the strategies for prevention and control of the use of new technologies by employees in a sample of Spanish companies.

Governance and direction of people and the prevention of abusive behaviour requires, at the very least, management formulas that take into account the different ethical, motivational and legal aspects involved so that the necessary control does not impinge on the creation and maintenance of the climate of trust required at organizations.

This study aims to contribute more knowledge on the reality of how different control mechanisms are introduced, in line with similar studies, though it focuses on the control activity itself and the company's reaction, rather than the disloyal or abusive acts of employees. In conclusion, certain practical guidelines for companies are suggested with regard to controlling the activities of employees when using ICTs.

Keywords
corporate crime, ICT use policy, control of employees and privacy, computer crime, business ethics, human resources management

Subject
corporate technological crime

1. Introducción

> *A workplace in which people can be, and are, trusted, has much more potential to be efficient and productive than one in which tasks are accomplished only through constant supervision [...] While there is a need to create and maintain a climate for trust, there is also a need to minimize opportunities for workplace crime and corruption.*
> Weckert (2002)

En el presente estudio, hemos partido de la observación de la realidad de la empresa en cuanto entorno de convivencia y trabajo entre personas. En el ámbito de la empresa, junto a los comportamientos esperados conforme a las reglas de funcionamiento interno, surgen de modo natural acciones o actitudes desviadas, abusivas o meramente improductivas que pueden llegar a tener, en ocasiones, relevancia jurídico-penal. Ese conjunto de conductas desviadas, tengan o no implicaciones jurídicas, responden a una lógica y a unos patrones que, en parte, son comunes. En su variedad, tales conductas se distinguen entre ellas tan solo por su intensidad, si se analizan desde la perspectiva del carácter abusivo o del grado de deslealtad del empleado en la utilización de los recursos que el empleador pone a su disposición *para el trabajo*. Por tanto, cuanto se refiera a continuación a conductas delictivas del trabajador se puede aplicar, de forma gradual, a otros comportamientos desviados de menor gravedad.

Dentro del amplio abanico de posibles conductas abusivas de los trabajadores, conviene tener presente que estas revisten, en numerosas ocasiones, un carácter difuso que, en caso de constituir delito, las convierte en «delitos invisibles», sin víctima aparente y de realización continuada en el tiempo. Respecto a la primera característica, su carácter imperceptible impide trazar una línea divisoria entre *delito* e *irregularidad*, distinción que podría ser poco relevante, al menos, en relación con los efectos y la repercusión que comportan en la economía de la empresa. Es decir, en ocasiones poco importa si la conducta abusiva es propiamente delictiva, en tanto que la suma continuada de pequeñas irregularidades puede generar, en la práctica, un efecto devastador, irreparable y, a veces, definitivo. Piénsese en las consecuencias económicas del, en ocasiones, imperceptible absentismo laboral. El estudio 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 de las propiedades del empresario por parte de los trabajadores, fenómeno que tiene ya sus raíces históricas en el ambiente laboral y en el discurso *taylorista* del siglo XIX.[2]

Dicho lo anterior, las interacciones humanas que tienen lugar en ese *mundo en común particular* que constituye toda empresa generan, por sus propias motivaciones y particularidades, una delincuencia con unas características específicas, que de algún modo guarda relación con ese mundo en común particular.[3] Tal delincuencia, surgida y desarrollada *en* la empresa y *desde* la empresa, refleja en su *modus operandi* (aunque pueda objetarse que lo hace de forma limitada) la lógica del mundo empresarial y los códigos de conducta que el *modo de ser de la empresa* imprime en quienes en ella se relacionan.

En tal sentido, un factor significativo en el modo de interactuar *entorno* y *persona* en el ámbito empresarial es el que se refiere a la *dimensión organizacional de la empresa*. Así, por ejemplo, el hecho de tratarse de una corporación en la que trabaja un número importante de personas, frente a la pequeña y mediana empresa, tiene consecuencias directas en las oportunidades delictivas que se generan y en los mecanismos de control que (según los recursos financieros de cada compañía) se implementan en la vigilancia de los trabajadores, y estructura su espacio de actuación. La ausencia de controles y la *atmósfera de anonimato* (*a priori* más acentuada en la pequeña y mediana empresa) son elementos criminógenos relevantes que están relacionados directamente con el entorno inmediato del trabajador.[4]

Evidentemente, dentro del contexto de la delincuencia empresarial también influyen otros factores individuales y sociológicos (las características individuales de las personas, su nivel económico, la formación recibida o su adaptación

2. Snider (2001, págs. 105-120)
3. *Operari sequitur esse*: el obrar sigue al ser. Sin entrar en el análisis de la aplicabilidad de este principio tomista al ámbito empresarial, sin duda la descripción general del *modo de ser* de la empresa proporciona claves de explicación del *modo de obrar*, y del delito, que tiene lugar en su interior. Véase, al respecto, J. R. Agustina (2009a).
4. De acuerdo con datos estadísticos de la U. S. Small Business Administration, la pequeña empresa representa el 99,7% del número de empresas en el mercado; tiene contratado alrededor del 50% de los trabajadores del sector privado; genera el 51% del producto interior bruto del sector privado; y en la última década ha contribuido con la creación de entre el 60 y el 80% de los nuevos puestos de trabajo.

social, entre otros). En este sentido, los tipos de delito (o las conductas abusivas y desleales)[5] guardan una relación significativa con el *estatus económico* de la persona y, sobre todo, con la posición u ocupación desde la que opera. La posición que una persona ocupa en la estructura organizacional y económica (en la empresa y en la sociedad en general) determina de modo decisivo las oportunidades, facilidades y posibilidades para cometer delitos específicos.[6] Así las cosas, se afirma que una persona de bajo nivel económico no puede ordinariamente cometer *delitos de cuello blanco* porque no tiene oportunidad para ello.[7]

A nuestro entender, el enfoque adecuado para prevenir que tales *oportunidades-para-la-desviación* (derivadas de la posición) cristalicen en actos concretos requiere profundizar en cómo configurar los espacios de autonomía responsable y en cómo establecer una relación armónica entre *confianza* y *control*.[8] Toda posición en la empresa se configura con base en unas *expectativas de confianza* y, concretamente, en el valor de la *lealtad*. Dicha relación de confianza, no obstante, no es en absoluto unidireccional, sino que debe ser recíproca, si se desea que la organización del trabajo y la producción funcionen adecuadamente. Así, en el quebrantamiento de los vínculos de lealtad mutua, las partes rompen, cada una desde su posición, esa relación necesaria, ya sea por medio del delito del trabajador, ya sea a través del delito del empresario (por ejemplo, violando la intimidad de los trabajadores por llevar a cabo un control desorbitado).

Desde un punto de vista criminógeno, la ausencia de vínculos de integración social del trabajador respecto de la empresa, su falta de identificación con la compañía o la carencia de motivaciones positivas desde el punto de vista psicológico o emocional pueden considerarse una causa de su comportamiento delictivo. La empresa no deja de ser una comunidad de personas, «una sociedad dentro de una sociedad», en la que a escala menor se aplican las teorías de los vínculos sociales (*social bond theories*). La importancia de los lazos personales e institucionales explica, de acuerdo con tales teorías, por qué algunos individuos cometen delitos mientras que la mayoría no lo hace.[9]

A este respecto, una característica relevante en la descripción de las relaciones laborales entre los miembros de la *comunidad empresarial* es la estructuración jerarquizada y el desequilibrio entre las distintas posiciones, en tanto se fundamentan en una *manifiesta desigualdad entre las partes*. Así, la posición de subordinación del trabajador respecto del empresario responde a una situación estructural de naturaleza económica, que tiene lugar en ese *microcosmos* particular que es la empresa. En este sentido, es pacíficamente admitido que la existencia de comportamientos ilegales en el seno de la empresa se debe no tanto a la eventual *predisposición personal* de cada individuo, sino a *factores estructurales* como la división del trabajo, las relaciones jerárquicas o el sistema normativo interno.[10] Es decir, para explicar el delito en el ámbito empresarial es ciertamente relevante la *posición* que ocupa el individuo, el rol determinado que cumple dentro de la estructura organizacional.

Sin pretender simplificar en exceso la explicación del delito en la empresa (no se puede interpretar lo anteriormente expuesto como si la presión que ejerce la estructura empresarial fuera determinante en términos absolutos), tampoco se puede ignorar la *proclividad criminal* que comportan determinados requerimientos de la producción, o el hecho de concentrar en la persona del directivo facultades de decisión y disposición sobre los intereses de la empresa, terreno abonado para los abusos[11] Así, el trabajador goza necesariamente de ciertos *espacios de confianza* (por la propia imposibilidad de implementar un *control omnicomprensivo*), que pueden inducir a la deslealtad, al abuso de la confianza otorgada. Como concluye Solivetti, no puede hablarse de sistema de coerción al crimen, mas no puede negarse la existencia de condiciones internas favorables a la génesis de actos ilícitos.[12]

5. Sobre la relación entre tipos de puestos de trabajo o trabajador y tipos de delito, véase José R. Agustina, (2010, págs. 352-409).
6. *Vid.* E. H. Sutherland (1939, pág. 177).
7. En la actualidad, ha ganado terreno entre los criminólogos la denominación de este tipo de delincuencia como «delitos ocupacionales», en detrimento de la clásica denominación como «delitos de cuello blanco». Véase, entre otros: G. S. Green, E. C. Blount (2003). D. O. Friedrichs (2002).
8 Véase: José R. Agustina (2009d, págs. 13-60).
9. K. D. Bussmann (2003, pág. 10).
10. A. Baylos Grau, J. Terradillos Basoco (1997, pág. 40). Sin embargo, junto a tales factores estructurales se debería agregar siempre un factor personal adicional, como, por ejemplo, la sensación *subjetiva* de impunidad (independientemente de que esa percepción se apoye en una base real *objetiva*).
11. M. Sánchez Álvarez (1996, pág. 34).

Del mismo modo, factores organizacionales que inciden en la motivación y la psicología del trabajador pueden tener gran relevancia y ser un factor criminógeno contrastado. Así, por ejemplo, una de las conclusiones de las investigaciones psicológicas sobre la delincuencia en la empresa revela la correlación entre una insuficiente justificación de recortes salariales y el incremento de sustracciones en la empresa.[13]

Pues bien, y como se verá, en el presente estudio se ponen de manifiesto algunas de las singularidades de los delitos y otras conductas abusivas en la empresa, y ello a la luz de los problemas que plantea una adecuada estrategia de prevención, detección y control de los actos desleales de los trabajadores con ocasión del uso de las TIC; las nuevas tecnologías son una importante fuente de conflicto y, al mismo tiempo, una herramienta de indudable eficacia en el control y prueba. Por ello se necesitan límites éticos y jurídicos.

2. Objetivos del estudio

El presente proyecto de investigación nació con el objetivo de conocer las distintas estrategias y sistemas de prevención y control que las empresas españolas, a partir de un determinado umbral de facturación, estaban llevando a cabo respecto de las nuevas tecnologías en el ámbito laboral.

En dicho contexto, el estudio de las conductas de los empleados y de los directivos a la hora de utilizar los recursos informáticos que la empresa pone a su disposición (ordenador, e-mail, teléfono móvil, PDA, etc.) constituye en la actualidad un área de investigación de creciente interés por sus repercusiones directas en el rendimiento en la actividad laboral y en los beneficios empresariales. Haciendo especial referencia al correo electrónico e Internet, se pretendía confeccionar un cuestionario que estuviera llamado a suscitar un proceso de reflexión en cada empresa, de modo que, como resultado, se gestionara de una forma ética, legal y, al mismo tiempo, práctica el necesario control de las personas, sin menoscabar, al mismo tiempo, la generación del indispensable clima de confianza necesario en el seno de las organizaciones. Para ello, se incluirían en el cuestionario preguntas relativas a las estrategias en la gestión de conflictos internos a partir del control de las nuevas tecnologías, para tratar de dimensionar la incidencia numérica de conflictos, su tipología y su repercusión económica.

Partiendo de que la «lógica del control» y la «lógica de la confianza», junto con una adecuada formación técnica, se hallaban en la misma base de toda estrategia empresarial, se pretendía avanzar, de este modo, en propuestas orientadas a lograr un equilibrio razonable entre los intereses en conflicto, respetando en todo caso la dignidad de la persona. En este sentido, el presente proyecto se enmarcaba en una línea de investigación interdisciplinar encaminada a la creación de un entorno de control adecuado en la empresa que inspire y promueva, al mismo tiempo, la necesaria confianza y el cuidado del factor humano, entendiendo que este no está reñido con la implementación (efectiva) de ciertas políticas de control proporcionadas.

3. Metodología y muestra del estudio, fases de ejecución y limitaciones

En una primera fase del proyecto, se diseñó un cuestionario, elaborado por un equipo de trabajo multidisciplinar, con la finalidad de enviarlo a mil empresas con sede en España, que se seleccionaron a partir de un umbral mínimo de facturación de cincuenta millones de euros anuales y de al menos quinientos empleados. La búsqueda se realizó utilizando la base de datos SABI. Se obtuvo una muestra de 1065 empresas.

El equipo de trabajo multidisciplinar que diseñó el cuestionario y estableció los criterios de selección de la muestra objeto de estudio estuvo formado por cinco profesionales: una abogado laboralista, un abogado asesor de empresas especializado en derecho de las nuevas tecnologías, un ingeniero informático especializado en seguridad informática y prueba electrónica, un profesor investigador en el área de *business ethics* y un profesor investigador en criminología y magistrado en la jurisdicción penal.

Tras la discusión sobre las numerosas preguntas relevantes que debían incluirse en el cuestionario, finalmente se decidió limitar su número a treinta y cinco cuestiones de respuesta

12. L. M. Solivetti, (1987).
13. Bussmann, K. D. (2003, pág. 10).

múltiple, y añadir una segunda encuesta-simulacro (*Validación funcional de procedimientos operativos existentes*) de diecisiete preguntas.

A partir de la base de datos inicial, se hizo una primera criba de empresas, para tratar de evitar reduplicaciones mediante la identificación de las sedes principales de los grupos empresariales, de manera que no se enviara el cuestionario a la misma empresa en distintas sedes.

Se redactó la carta explicativa del proyecto en formato papel y electrónico, para enviar el cuestionario a las empresas. Hubo que ponerse en contacto con Informa, empresa proveedora de los datos a SABI, para poder hacer uso de la información seleccionada e incluir en el envío el origen de los datos.

> Se cruzaron los datos de las empresas obtenidas con la base de datos del IESE para incluir solo las empresas coincidentes. Tras dicho proceso, finalmente, la muestra quedó reducida a 967 registros.
>
> Paralelamente, se diseñó e implementó la página web del proyecto. Para este cometido, hubo una puesta en común en una reunión inicial del equipo de trabajo donde se discutió el modo en que debía llevarse a cabo.

Para garantizar la confidencialidad de las compañías, no se revelaría la identidad de las empresas participantes a los componentes del equipo. A esta información únicamente tendría acceso el responsable del fichero.

En junio de 2010 se dio de alta definitivamente la página web del proyecto y se llevó a cabo el primer envío de cartas a las empresas seleccionadas. Tras un primer envío, del que se obtuvieron pocas respuestas, se decidió realizar un segundo envío en septiembre de 2010.

Al ser, de nuevo, insuficiente el número de respuestas obtenidas, se contactó telefónicamente con las empresas para animarlas a colaborar en el proyecto. Se constató la enorme dificultad para obtener respuestas.

Finalmente se obtuvieron un total de cuarenta y dos. En solo veintiséis casos se respondió íntegramente a todas las preguntas. El resto contestó mayoritariamente al primer bloque de preguntas.

4. Comparativa con estudios anteriores

Para el diseño del cuestionario se tuvieron en cuenta los estudios precedentes en el ámbito del control de las nuevas tecnologías en la empresa, si bien ninguno de ellos se planteó con el principal objetivo de obtener información sobre los instrumentos técnicos utilizados a tal fin. En el presente estudio se han tratado, por tanto, de abordar aquellos aspectos menos analizados en los precedentes, para dar un paso más y poner especial énfasis en las estrategias reactivas y no solo en las preventivas en el ámbito de estudio.

4.1. Estudio precedente de 2002

En el anterior estudio, llevado a cabo por el **e-Business Center PwC&IESE** y publicado con el título *Estudio sobre políticas, hábitos de uso y control de Internet y correo electrónico en las principales empresas españolas* (Fontrodona Felip y García Castro, 2002) se partía de que, al ser en la actualidad el correo electrónico y el acceso a Internet herramientas de trabajo tan universales como el teléfono, y al constatarse los diferentes enfoques para su correcto uso en las empresas entre los países de nuestro entorno, debía responderse a la pregunta recurrente que se realizaban los directivos en la organización y control de su empresa: «¿Debo adoptar una actitud de *laissez-faire* o tengo que establecer unos límites permitidos de uso de estas herramientas?».

Ya entonces se constataba en el contexto laboral la existencia de una tendencia evidente hacia la fuerza del trabajo en línea; dicha cuestión se revelaba como de suma importancia. En dicho estudio se constataba también que los directivos habían empezado a implementar políticas y mecanismos de control para gestionar este problema, esgrimiendo razones de productividad, seguridad y de carácter legal. En el estudio, se mostraba en cifras la situación de estas políticas y de los mecanismos de control en España, para conocer cómo se estaban produciendo los cambios en nuestro país.

En España, el uso de Internet y del correo electrónico entre las mil mayores empresas se encontraba ya entonces bastante extendido, como refleja el hecho de que el 98% de las compañías de la muestra seleccionada contestasen que sus empleados tenían acceso a Internet y al correo electrónico en el puesto de trabajo.

Estas son las principales conclusiones a partir de los resultados obtenidos en el estudio de 2002:

- El número de políticas escritas entre las mayores empresas españolas era, por entonces, todavía bajo. Muchas empresas confiaban en las políticas no escritas para gestionar el acceso a Internet y al correo electrónico de sus empleados. También existía **un importante porcentaje de empresas que no poseían políticas de ningún tipo**.
- Esas políticas regulaban los contenidos permitidos, los usos aceptables o la custodia de datos personales de los trabajadores, pero en general **se prestaba poca atención a aspectos clave como la supervisión y la política de sanciones**.
- Un porcentaje significativo de empresas españolas ya restringía en sus políticas el uso de Internet y del correo electrónico con «fines exclusivamente profesionales» (38%). El uso totalmente libre de estos medios se daba en una minoría de empresas españolas (12-14%).
- Se constataba en España una falta de madurez respecto a la privacidad en línea. En caso de no adoptar políticas, el problema no era el presupuesto, sino la falta de conciencia de la dirección de la empresa. De hecho, las empresas dedicaban una media de 0,24 millones de euros a ese capítulo. De los datos parecía desprenderse una falta de conocimiento acerca de los riesgos legales que conlleva una violación de la intimidad de los empleados.
- En cuanto a los sistemas de supervisión, se apreciaba una clara diferencia entre la supervisión del acceso a Internet (45%) y la del correo electrónico (24%). Se creyó que, fundamentalmente, se explicaba por cuestiones legales.
- La mayoría de las empresas afirmaban que existía una «causa justificada» para llevar a cabo actuaciones inspectoras. Sin embargo, la práctica totalidad de estas empresas no cumplían con los requisitos legales para la supervisión, o bien los desconocían.
- El 20% de los directores generales accedían, según la encuesta realizada, a los datos obtenidos a través de la supervisión.
- Algo menos del 3% de las empresas habían despedido a algún trabajador por el uso incorrecto de sus telecomunicaciones, y casi un 10% de las empresas habían sancionado a algún trabajador por tales razones.
- Tan solo una de cada cuatro empresas de la muestra poseía estadísticas respecto a los hábitos de uso de Internet y del correo electrónico de sus empleados.
- En Internet, los empleados de las mayores empresas frecuentaban los servicios de noticias, los servicios financieros en línea y la búsqueda de software o hardware. La pornografía o la música en línea no figuraban entre lo más citados.
- Lejos de adoptar un enfoque uniforme, las empresas españolas presentaban diferencias entre las políticas, la supervisión y la disponibilidad de estadísticas. En el análisis bivariante se pusieron de manifiesto las diferencias existentes por tamaño y facturación entre las mayores empresas españolas.

4.2. Exploring Emerging Risks (2009)

En un estudio realizado en 2009 por PriceWaterHouseCoopers y titulado *Exploring Emerging Risks*, ya se hizo referencia a la aplicación de estrategias de gestión de riesgos en el seno de las empresas (*extending enterprise risk management* [ERM]).

Siguiendo dicho estudio, se debían evaluar las dimensiones de los riesgos, su interconexión con otros riesgos asociados y las implicaciones en la marcha de la empresa.

Para evaluar de modo efectivo los riesgos emergentes se requería considerar el significado que estos tienen en la empresa y en los accionistas (tanto internos como externos), analizando el impacto de los riesgos, la probabilidad de que sucedan y las correlaciones con otros riesgos (interconectividad entre riesgos) en relación con las estrategias y los objetivos de la empresa.

Según dicho estudio, los recursos debían dirigirse (o redirigirse) a tratar de identificar y realizar un seguimiento de los indicadores de riesgos emergentes y a desarrollar la agilidad organizacional de la empresa para enfrentarse a ellos. En consideración a la naturaleza, las dimensiones y la interconectividad de tales riesgos y a las alternativas disponibles para mitigar los riesgos dentro de las organizaciones, tales recursos debían poder permitir una gestión de riesgos dinámica que lograra encaminarse hacia los objetivos estratégicos de las empresas; se podía realizar un seguimiento y un control de los riesgos emergentes a través de métodos cualitativos y cuantitativos. Una adecuada comprensión de las circunstancias que rodean los posibles riesgos emergentes constituía el punto de partida a partir del cual se podían controlar los síntomas de los riesgos que están empezando a desarrollarse, síntomas que se podrían precisar mejor en la medida en que se recabara más información, la cual determinaría la necesidad de respuestas alternativas a estos riesgos emergentes.

4.3. Human Factors Working Group (2007)

De modo parecido, en el estudio publicado bajo el título *Human Vulnerabilities in Security Systems* por el Human Factors Working Group (2007), se abordaban cuestiones que, sin duda, guardan relación con el presente estudio. No obstante, además de no aportar datos empíricos de base, se centraba en la interacción entre el factor confianza y la lógica del control aplicadas a los medios técnicos de control, pero sin que se analizara en concreto qué medios se utilizan y de qué modo, ni tampoco las estrategias de reacción de la empresa a partir de la emergencia de un incidente interno.[14]

5. Análisis y valoración de los datos obtenidos

5.1. Evolución comparativa entre 2002 y 2010

En relación con el estudio realizado en 2002 se aprecian las siguientes comparaciones significativas:

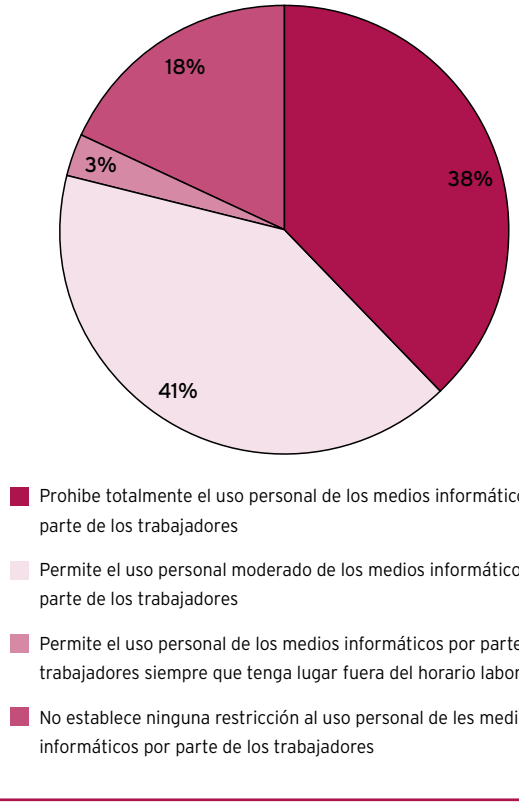
(i) En cuanto al porcentaje de políticas de uso de las nuevas tecnologías que prohíben totalmente su uso privado, es significativo que no haya variado, y que se sitúe de nuevo en un 38%.

Este dato sorprende en la medida en que en el año 2007 el Tribunal Supremo (**sentencia de 26 de septiembre de 2007**)[15] ya declaró que uno de los elementos esenciales para que el empresario pueda desarrollar una actividad de supervisión y control de los medios informáticos es la existencia de una política empresarial clara, que debe proporcionarse a los trabajadores para que la conozcan. A este respecto, el Tribunal Supremo entendió, en dicha sentencia, que con este tipo de medidas el trabajador no puede alegar la existencia de una «expectativa razonable de intimidad» y, por tanto, que se haya producido lesión alguna en sus derechos fundamentales. Con ello se puso fin a un largo periodo en el que se sucedieron sentencias contradictorias respecto a la capacidad de control del empresario y los medios para llevarlo a cabo.[16]

Por ello, se podía esperar que tras la sentencia se desarrollara un gran número de políticas en las empresas, presunción que no parece ser acertada a la luz de los datos obtenidos.

(ii) Sin embargo, sí se aprecia un aumento de las empresas que permiten un uso moderado (para fines particulares): un 41% en 2010 frente a un 29-32% en 2002.

Gráfico 1. Políticas de uso de las TIC y utilización con fines personales



Como ocurrió con el uso del teléfono, la generalización de este tipo de medios no solo en el ámbito profesional, sino también en el privado, ha generado una mayor tolerancia por parte del empresario. A ello se suma el hecho de que los horarios laborales tienden a flexibilizarse, y cuando ello ocurre con frecuencia no es posible ejercer un control

14. Véase también el estudio de PwC's 4th biennial Global Economic Crime Survey (2007).
15. Véase al respecto: J. R. Agustina (2009c).
16. Aunque no pudo tener impacto en el momento de la recogida de datos para este estudio, es importante destacar que la posición del Tribunal Supremo en este punto se ha consolidado con posterioridad por medio de la **Sentencia de 6 de octubre de 2011**, en la que reconocía la validez de una política de uso que incluía una prohibición absoluta de utilización de los medios de la empresa para fines propios, tanto dentro como fuera del horario de trabajo, y entendía que «lleva implícita la advertencia sobre la posible instalación de sistemas de control del uso del ordenador», por lo que se exonera *de facto* a la empresa de informar expresamente de la instalación de este tipo de dispositivos.

basado en el horario laboral. Además, se puede percibir como injustificado prohibir el uso de unas herramientas que facilitan una mejor conciliación de la vida personal y laboral cuando el trabajador ha incrementado sustancialmente su disponibilidad a través precisamente de dispositivos móviles o accesos remotos a la red de empresa.

5.2. Modo de implementación de políticas de uso, prevención y control de las TIC en la empresa. Capacidad técnica real en la detección e identificación de la infracción

(i) **Identificación del usuario**. En un 98% de las empresas encuestadas se requiere identificación y autenticación del usuario para acceder a los sistemas informáticos. Sin duda, esta es una medida necesaria, no solo a efectos de proteger la privacidad del trabajador, sino como medio para identificar al usuario de una terminal en un momento dado.

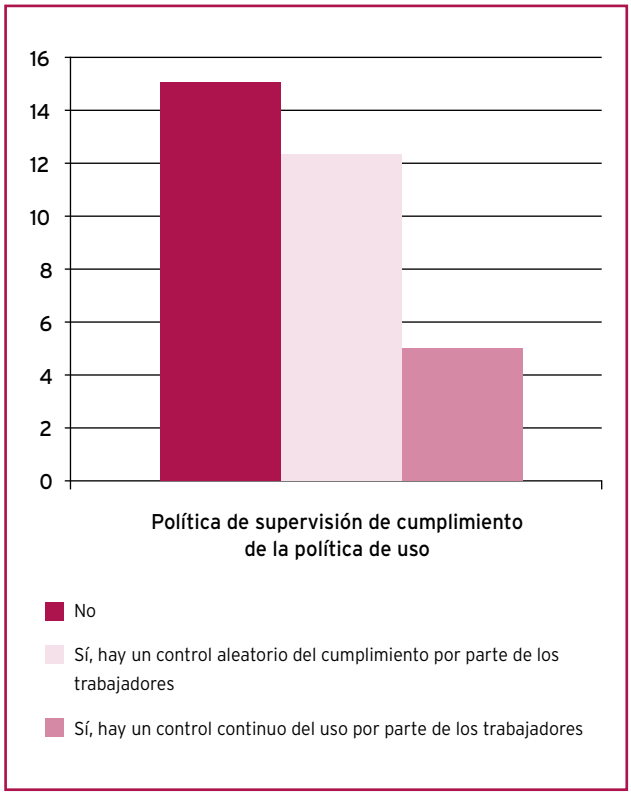
Sin embargo, a partir de los resultados de la encuesta-simulacro (*Validación funcional de procedimientos operativos existentes*), se revelan unas carencias significativas en la capacidad técnica para detectar e identificar al infractor (*cfr.* apartado (v) *infra*).

En relación con lo anterior, es significativo que ninguno de los encuestados reconozca que tiene dudas sobre la fiabilidad de los sistemas de identificación y autenticación, cuando compartir contraseñas con los compañeros es una mala práctica generalizada más que constatada. En todo caso, es conveniente señalar que el Tribunal Supremo, en la citada sentencia de 26 de septiembre de 2007, señala que el hecho de que no exista clave de acceso no supone un obstáculo para la protección de la intimidad. Es decir, el trabajador debe ver su derecho a la intimidad tutelado exista contraseña o no en el ordenador. Sin embargo, desde el punto de vista de la determinación y la prueba de la autoría de los incumplimientos que se detecten, la existencia de una clave de acceso es una herramienta útil.

(ii) **Revisión periódica y supervisión del cumplimiento de las políticas de uso**. La mayoría de las empresas encuestadas llevan a cabo una revisión periódica de las políticas de uso aprobadas (un 89,9%), si bien solo un 45% lo hace de forma regular (periodicidad fija).

En cuanto a si la empresa había implementado alguna estrategia de supervisión del cumplimiento de las políticas de uso de las TIC, un 46,9% respondió negativamente, frente a un 37,5%, que afirmó realizar un control aleatorio, y un 15,6%, que realizaba un control continuo.

Gráfico 2. Políticas de supervisión del cumplimiento de la política de uso



Es importante señalar que, si las empresas definen y comunican una política de uso de las TIC pero no realizan control alguno de su cumplimiento, se genera una situación de tolerancia empresarial que dificultará la implementación de medidas disciplinarias en caso de que se detecte un incumplimiento. Por otro lado, el control y las medidas disciplinarias deben ser aplicadas bajo los principios de igualdad, proporcionalidad y progresividad. Sin embargo, en muchas ocasiones la práctica empresarial es distinta, ya que: (i) se evita sancionar los incumplimientos menores, pues ello genera una conflictividad que se prefiere evitar, (ii) no se aplica con el mismo rigor el régimen disciplinario, o (iii) la investigación sobre el cumplimiento de las políticas TIC se realiza como un medio para justificar una decisión disciplinaria preexistente y dirigida contra un trabajador.

Ante la pregunta de si dichas políticas de supervisión incluyen un protocolo de actuación en determinadas situaciones de especial riesgo: en un 16% de los casos la respuesta fue

negativa; un 21% disponía de un protocolo específico para el caso de trabajadores que han preavisado de su marcha de la empresa, y un 30% para los que se ha decidido despedir. Es de destacar que solo un 10% de las empresas prevean políticas de supervisión especial por razón de las remarcables responsabilidades del trabajador en función del departamento o por razón del rango del trabajador u otros miembros de la empresa. También es escaso (13%) el número de empresas que prevén una supervisión especial para trabajadores que han incurrido en conductas específicamente tipificadas (por ejemplo, por exceso en el volumen de correos electrónicos).

En la práctica, reforzar los mecanismos de control en algunos colectivos especialmente sensibles, como los directivos de la empresa, es complejo, ya que: (i) son los mismos órganos de dirección quienes deben adoptar la decisión de reforzar su fiscalización, (ii) el control suele llevarse a cabo internamente y, en consecuencia, la mayoría de las veces por personas jerárquicamente subordinadas, (iii) preservar la confidencialidad en determinados niveles resulta esencial.

(iii) **Control de fugas de información**. Un 26% de las empresas encuestadas no dispone mecanismos técnicos para evitar almacenar información corporativa en soportes extraíbles (mediante *pen drive* o CD); un 35% no tiene ninguna política limitativa al respecto; mientras que un 27% requiere el consentimiento de un responsable y limita el volumen de lo extraído, y un 12%, pese a no tener una política sobre dicha posibilidad, manifiesta disponer de mecanismos que impiden almacenar la información en soportes extraíbles.

En cuanto a otros mecanismos de detección y prevención de fugas de información corporativa, un 24% de las empresas manifestó disponer de distintas tecnologías que conjuntamente persiguen dicho objetivo; solo un 9% de las empresas dispone de una solución específica a tal efecto (por ej., mediante un sistema de *Data Leakage Prevention*).[17] Un 67% declaró no contar con mecanismo alguno.

Debe tenerse en cuenta que en aquellas empresas en la que además de proteger la información generada por estas se tenga un deber de custodia respecto a información o documentación entregada por un tercero, este tipo de medidas son esenciales.

(iv) **Control de la navegación por Internet**. La mayoría de las empresas (52%) establecen mecanismos que impiden el acceso a determinados sitios por su contenido pornográfico o inmoral; frente a un 24% que no establece límite alguno. Tan solo un 3% impide el acceso a sistemas de correo electrónico personal, y un 3% a determinados sitios web por su contenido claramente no profesional. Un 9% impide el acceso a redes sociales.

Sin embargo, respecto a este último punto, la tendencia incipiente de aquellas empresas con amplia presencia en la Red (como las dedicadas al gran consumo) es distinta. A la selectiva limitación del acceso a las redes, se une un interés empresarial en regular o promover determinadas prácticas «conscientes» de sus trabajadores en su uso privado de las redes sociales. Sin duda, los mensajes, escritos o gráficos, que los trabajadores de una empresa insertan en la Red, y en especial de todos aquellos que ostentan un cargo de responsabilidad, pueden repercutir en la propia compañía positiva o negativamente. Ello con independencia de que dicha actividad se realice fuera del horario laboral o sin hacer un uso indebido de los medios empresariales.

(v) **Capacidad técnica en la detección e identificación de la infracción**. Ante la pregunta de si la empresa está capacitada para recuperar los *logs* de asignación de IP dinámicas de hace tres meses, para detectar desde qué ordenador se realizó un posible ataque informático, solo un 37% afirmó tener acceso a dichos *logs*; un 22,2% manifestó que el periodo de conservación de estos es inferior a tres meses. La mayoría de las empresas, un 40,7%, respondieron que no almacenan dicha información.

Además, de las empresas que sí conservan por algún tiempo dicha información (un 59,2% del total), una inmensa mayoría limita dicho acceso a los *logs* a menos de seis meses (un 65,4%).

En cuanto a los protocolos de notificación previa al trabajador antes de proceder a examinar el ordenador, el 27% de las empresas disponen de un protocolo informático que permite investigar el incidente sin notificación previa al trabajador; un 15% también dispone de un protocolo para dichos escenarios, pero en todo caso se notificaría siempre

17. Los sistemas DLP (*Data Leakage Prevention* o *Data Loss Prevention*) responden a un concepto que se ha vuelto fundamental dentro del mundo empresarial. Abarca todas las políticas, las herramientas y los medios de seguridad que implementa una compañía, con el fin de que sus sistemas informáticos no sean violados y los datos no se pierdan o sean robados. Es decir, se refiere a todo lo relativo a políticas de uso de Internet e instalación de antivirus, *firewalls* y filtros web en los equipos de una organización.

antes al trabajador; un 19% carece de protocolo alguno, pero también se lo notificaría previamente al trabajador. Finalmente, un significativo 39% ni dispone de protocolo alguno ni advertiría al trabajador.

Debe tenerse en cuenta que, en la actualidad, está cada vez más generalizado el trabajo en red y, por tanto, con conexión a un ordenador central. Por tanto, y sin perjuicio de los archivos locales que pueda haber, la parte más voluminosa de la actividad del trabajador circula a través del servidor central. Ello permite al empresario tener acceso a ella sin acceder al ordenador personal del trabajador, y sin ni siquiera estar en el mismo centro de trabajo en el que este presta sus servicios. De nuevo, la existencia de una política de control clara y debidamente comunicada será nuclear para poder definir los límites de la facultad empresarial.

Un 56% de las empresas cuentan con personal formado para efectuar el análisis forense del ordenador del trabajador; mientras que un 36% contactaría con una empresa especializada. Un 8% asegura que, pese a no tener personal especializado, sus técnicos informáticos serían capaces de hacer ese trabajo.

El mantenimiento de la cadena de custodia y la realización de estudios acordes con el principio de proporcionalidad constitucional son cuestiones esenciales que con frecuencia se gestionan con más garantías de forma externalizada.

En cuanto a si la empresa tiene un sistema de almacenamiento de correo electrónico para recuperar mensajes enviados o recibidos de hace tres meses, solo un 51% dice disponer de uno. Y únicamente un 44% asegura poder acceder a los *logs* para determinar la persona y el ordenador utilizado.

Finalmente, un 42% de las empresas, tras realizar la encuesta-simulacro, admitió la existencia de algunas discrepancias entre la implementación teórica de los sistemas de seguridad disponibles y la implementación real en la práctica del ejercicio. Dicho ejercicio simulado permitió identificar carencias en los mecanismos de control en un 15% de las empresas; un 35% afirmó que ya eran conscientes de tales carencias; un 23% dijo disponer de la *mayoría* de la información requerida en el simulacro; y un 27% de *toda* la información.

5.3. Finalidad de las políticas de uso de las TIC y reacción de la empresa

(i) **Finalidad declarada de las políticas de uso**. En cuanto a la finalidad declarada en las políticas de uso, la mayoría de las empresas manifiestan que obedece a una necesidad de proteger la empresa frente a posibles daños, en un 48,6% de los casos; un 25,7% afirma tener como finalidad el control frente a abusos en los sistemas informáticos; un 2,9% se refiere al control del rendimiento laboral; y un 22,9% no declara finalidad alguna. Ninguna empresa manifiesta como objetivo la prevención del delito.

La percepción del daño potencial es baja, de ahí que no se asignen más recursos al control y no se adopten más medidas de sanción.

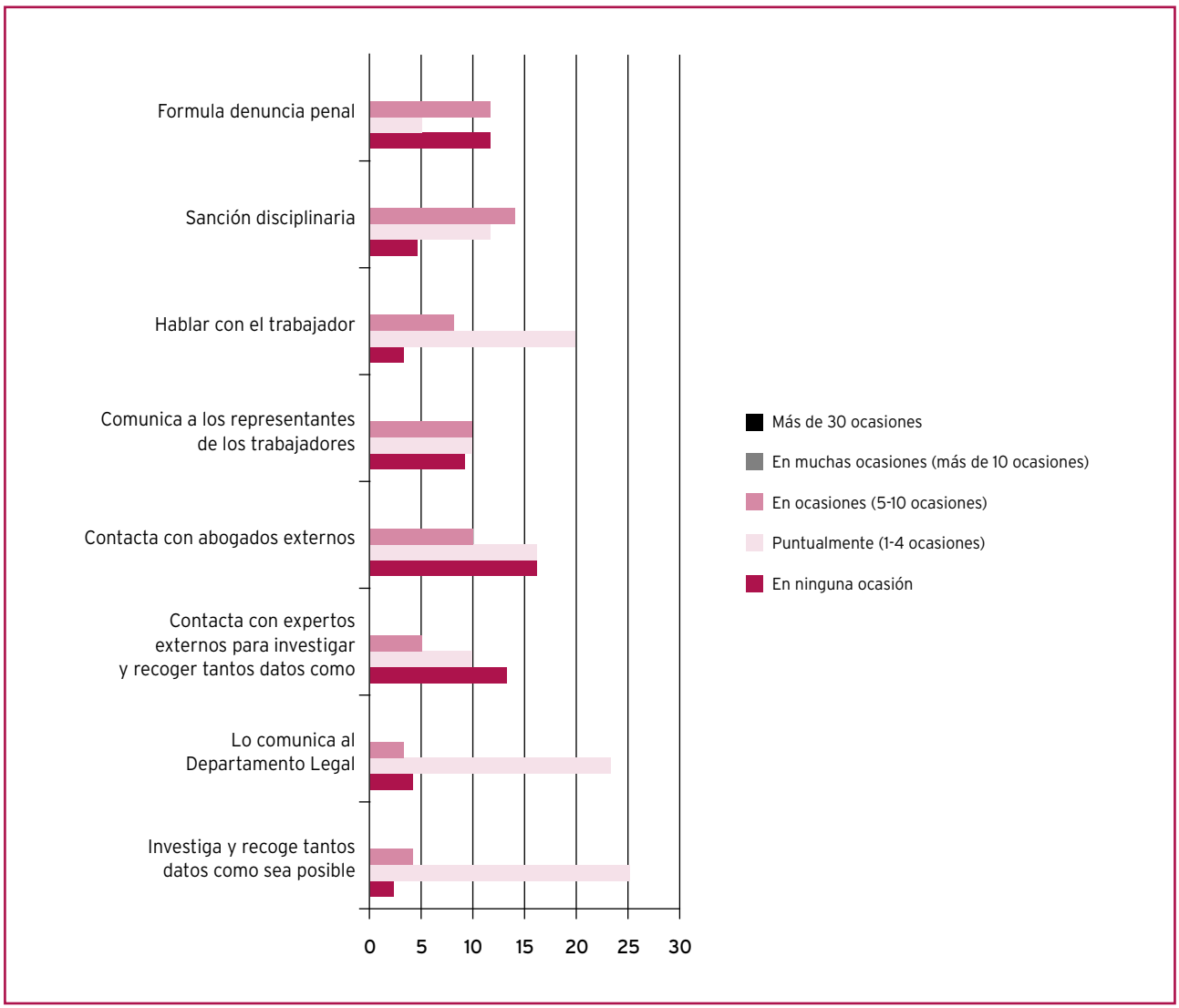
(ii) **Primera reacción de la empresa**. Sobre un periodo de tres años, un 38,8% de las empresas encuestadas afirmó haber formulado ocasionalmente denuncia penal contra el trabajador (entre 5 y 10 ocasiones), junto a un idéntico 38,8% que no lo hizo nunca, y un 16,1% que lo hizo tan solo puntualmente (entre 1 y 4 ocasiones).

Respecto a la sanción disciplinaria, un 45,2% de las empresas manifestó haber acudido a dicha opción ocasionalmente (en 5-10 ocasiones); mientras que un 64,5% dijo que solo puntualmente (en 1-4 ocasiones) optó por hablar con el trabajador. Solo un 32,3% de las empresas dijo haber comunicado a los representantes de los trabajadores el incumplimiento en 5-10 ocasiones.

En cuanto si la empresa comunicó el incumplimiento al departamento legal propio o contactó con abogados externos, un 32,2% acudió a la primera opción en 5-10 ocasiones, mientras que ese mismo porcentaje de empresas contactó en 1-4 ocasiones con abogados externos a la compañía. La opción de contactar con expertos externos para investigar y recoger la máxima información posible se limitó a un 16,1% de empresas (en 5-10 ocasiones) y a un 32,3% (en 1-4 ocasiones).

(ii) **¿Cuál ha sido la reacción habitual de las empresas una vez constatado el incumplimiento?** En un 37% de los casos, la reacción habitual consistió en advertir informalmente al trabajador; en el 22% de los casos se sancionó disciplinariamente al trabajador (pero sin llegar al despido); se le despidió en el 13% de casos. En un 12% no se realizó actuación alguna, y en un 6% se negoció con el trabajador algún tipo de solución. Solo en el 3% de casos se presentó denuncia penal. A este respecto nos extenderemos en el epígrafe número 7, sobre las motivaciones de las empresas al decidir si reacciona o no de algún modo ante incidentes o delitos de los trabajadores (*vid. infra*).

Gráfico 3. ¿Cómo reacciona la empresa en un primer momento en el caso de detectar un incumplimiento (por orden de actuación, del 1 al 8)?



Ante la pregunta de *qué porcentaje de casos detectados fueron sancionados disciplinariamente*, un 70,4% de las empresas que respondieron declaró que fueron menos del 30%; un 7,4% dijo haber sancionado entre el 30% y el 70% de los casos, y un 22,2% lo hizo en más del 90% de los casos.

¿Y cuáles fueron los motivos principales para decidir no sancionar al trabajador? En un 30% de los casos se debió a la falta de gravedad del incumplimiento o del daño, y en un 29% a la falta de pruebas suficientes para sancionar. Solo en un 10% se adujeron razones de no dar publicidad al incumplimiento; mientras que en un 8% se debió a la tolerancia de la empresa en casos anteriores similares; el mismo porcentaje de ocasiones en que las que el motivo de no sancionar tuvo como causa prevenir la reacción de los trabajadores y/o de sus representantes. En un 6% se debió a la prescripción de la acción;[18] en un 5% al coste derivado de la obtención de pruebas, y un 2% al coste del asesoramiento jurídico necesario.

18. Téngase en cuenta que el art. 60.2 del Estatuto de los Trabajadores establece que las faltas leves prescribirán a los diez días; las graves, a los veinte días, y las muy graves, a los sesenta días a partir de la fecha en que la empresa tuvo conocimiento de su comisión, y, en todo caso, a los seis meses de haberse cometido.

Respecto al tipo de sanción adoptada, (i) se despidió al trabajador aceptando la improcedencia del despido (1-4 ocasiones, siempre dentro de los últimos tres años) en un 30,8% de las empresas, frente al 3,8% que dijo haberlo hecho en *muchas ocasiones* (más de 10); (ii) los casos de sanción no seguida de recurso por parte del trabajador son sensiblemente inferiores (15,4% *puntualmente*, 11,5% en 5-10 ocasiones, y 3,8% en *muchas ocasiones*) frente a aquellos casos en los que sí fue discutida y se resolvió posteriormente, bien en la fase de conciliación (23% puntualmente, o 7,7% en *muchas ocasiones*), bien tras el procedimiento judicial correspondiente (19,2% puntualmente).

El despido de un trabajador por motivos disciplinarios supone la imposición de la máxima sanción que permite el sistema laboral. Teniendo en cuenta la fórmula tasada para el cálculo de la indemnización, en ocasiones, la adopción de medidas alternativas a una extinción reconocida como improcedente puede ser mucho más costosa. Sin embargo, el coste no es el único parámetro de valoración, ya que existen conductas que la empresa debe combatir, con independencia de que el proceso pueda obligar a generar una inversión económicamente superior. Además, la reciente reforma introducida mediante el Real decreto ley 3/2012, de 10 de febrero, ha suprimido los salarios de tramitación. Ello hará que se asuma en mayor número de ocasiones el riesgo de defender la procedencia de las extinciones.

A este respecto es interesante tener en cuenta que la percepción de la gravedad de una conducta puede variar no solo en función de la cultura de empresa en cada caso, sino también en función del país en el que se encuentren las personas que deben tomar la decisión disciplinaria. Así, en grupos empresariales internacionales no es infrecuente que se produzcan valoraciones significativamente distintas de un mismo hecho desde la empresa filial y la matriz.

5.4. Tipología de incumplimientos detectados, origen de la detección y sus consecuencias

(i) **Tipología de infracciones**. Un 90,5% de las empresas manifestó haber detectado casos de absentismo o pérdida de tiempo (uso para fines particulares de medios profesionales). En cuanto al resto de los incumplimientos detectados, los porcentajes son sensiblemente inferiores: infracciones de la propiedad intelectual, como descargas ilegales (40,5%); daños informáticos (38,1%); uso inadecuado o revelación de información confidencial (35,8%); suplantación de identidad (19%); daños a la imagen o reputación de la empresa (11,9%); actos de competencia desleal (11,9%); acceso a contenidos de pornografía infantil (7,1%); acoso moral o sexual a otros trabajadores (2,4%).

El sistema sancionador en una empresa debe respetar los principios de progresividad y proporcionalidad. Por tanto, como se indicaba antes, debe evitarse generar una situación de tolerancia empresarial que dificulte la aplicación del régimen sancionador.

(ii) **Origen de la detección**.

(iii) **Consecuencias derivadas de la infracción**. Una vez excluidos los costes derivados del propio procedimiento sancionador, un 11,9% de empresas manifestó que puntualmente (en 1-4 ocasiones) los daños oscilaron entre 3.000 y 10.000 euros, y un 4,8% entre 10.000 y 30.000 euros. Además, un 4,8% de empresas reveló que también puntualmente los daños habían sido superiores a 30.000 euros.

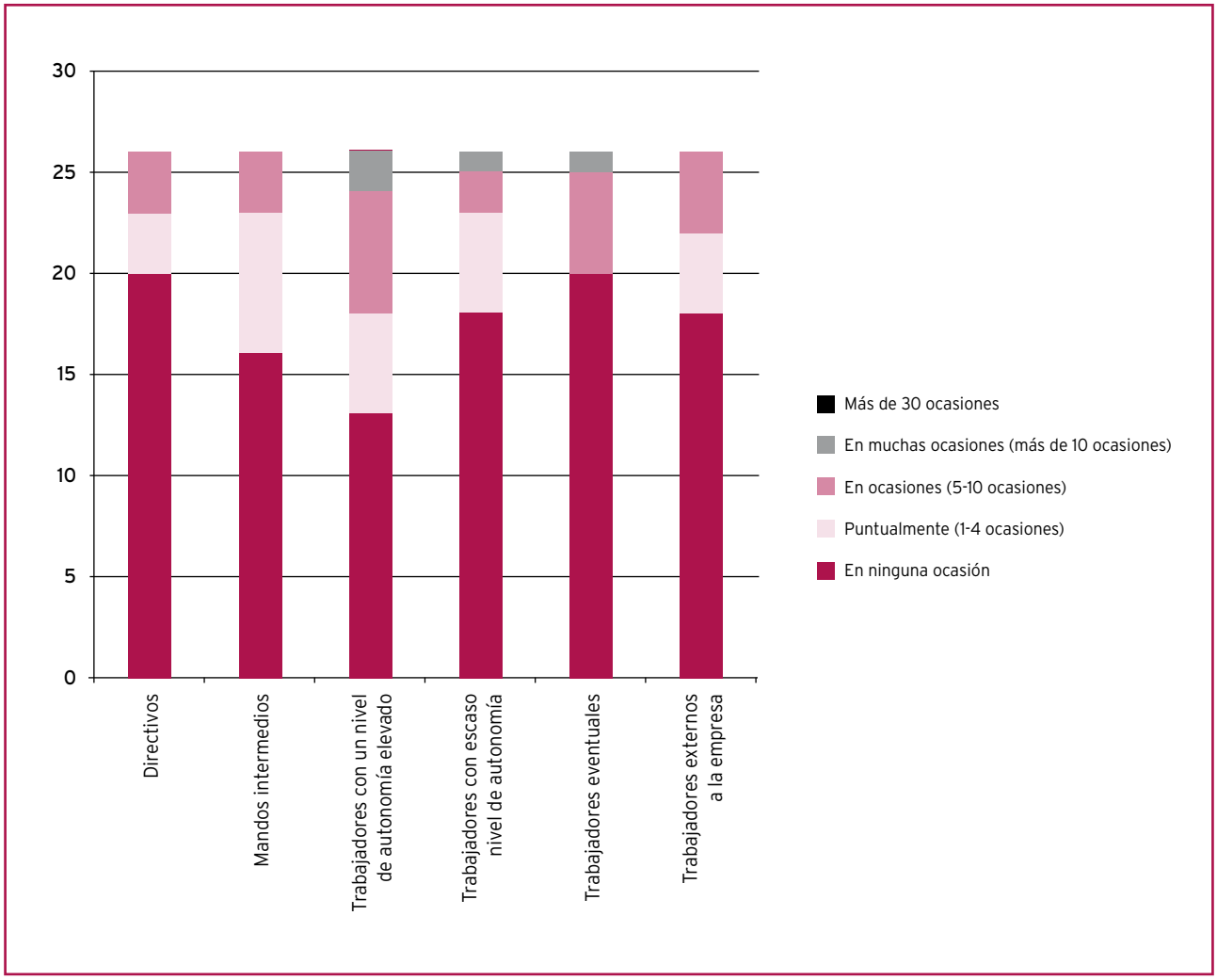
En cuanto al tipo de daños sufridos por las empresas, un 47% consistió en la reducción del rendimiento laboral de los trabajadores; un 18% en daños materiales; un 16% en daños relativos a la propiedad intelectual o industrial (incluidas las infracciones al deber de confidencialidad respecto de datos de terceros); un 11% en daños a la imagen o reputación de la compañía; y un 8% en daños personales (injurias, acoso, pornografía infantil, etc.).

5.5. Perfiles de los trabajadores infractores

El grupo de trabajadores con mayor tendencia a cometer infracciones es el de aquellos que gozan de *un elevado nivel de autonomía*, seguidos de los *mandos intermedios*, los trabajadores con *escaso nivel de autonomía*, los trabajadores *eventuales* y los que son *externos a la empresa*. Lógicamente, los *directivos* ocupan el último lugar, al tener una menor representación (*vid.* gráfico relativo a la pregunta 34).

A este respecto, Gerard Mars describió, en función de las variables relativas a las características del tipo de trabajo (*grid dimension*) y a la integración en el grupo (*group dimension*), cuatro tipos de perfiles criminológicos en el lugar de trabajo. La proclividad delictiva derivada de la clasificación que propuso en su obra *Cheats at Work. An*

Gráfico 4. ¿Qué tipo de trabajadores han cometido los incumplimientos?



Anthropology of Workplace Crime (1982) ilustra la relación existente entre tipos de trabajadores y clases de conductas abusivas o delictivas, y, por lo que aquí respecta, puede dar cuenta también de la clase de riesgos delictivos derivados del acceso a información, de la autonomía del trabajador y del acceso facilitado a las TIC en el entorno laboral:

(1) *Contornos difusos individualmente y vínculos débiles desde un punto de vista grupal* (*weak-grid and weak-group*). En primer lugar, describe a aquellas personas que ocupan puestos de trabajo caracterizados por una gran autonomía organizativa, con tendencia al individualismo en el modo de funcionar y un nivel alto de competitividad por el tipo de trabajo que llevan a cabo. El control que ejercen sobre otras personas es muy superior al que se lleva a cabo sobre este tipo de profesionales. En este tipo de puestos de trabajo, es especialmente valorada la iniciativa personal y el espíritu emprendedor, la discrecionalidad para negociar con autonomía. En un primer momento, Mars sitúa en este grupo de trabajadores (a los que denomina *hawks*) a directivos de empresa, académicos que han alcanzado cierto nivel de éxito profesional y a pequeños empresarios que han creado su propia empresa. Sin embargo, el perfil profesional que caracteriza a este tipo de profesionales no se limita a las categorías sociales de más alto nivel: en cierto modo, también entrarían el taxista que es propietario del automóvil que emplea para su trabajo, o el camarero que goza de cierta autonomía y experiencia. El *carácter competitivo* como rasgo dominante en esta clase de profesionales, junto a los débiles vínculos que se generan entre sus iguales, conlleva que las alianzas entre *hawks* tiendan a cambiar con relativa

frecuencia y que el clima que se respire entre los miembros del grupo esté dominado más por la sospecha más que por la confianza mutua.[19]

De este modo, el carácter independiente, la tendencia dinámica a la búsqueda de nuevas oportunidades, la capacidad de adaptación..., todas las características presentes en tales perfiles laborales inducen a este tipo de profesionales a abrirse su propio camino y a aprovechar las ventajas y la flexibilidad que define su puesto de trabajo. En parte, esta forma flexible de convivencia junto con las ventajas adicionales a una autonomía y ausencia de controles pueden explicar cómo y por qué funciona el sistema.[20] Los *hawks* están a menudo protegidos frente a cualquier forma de control, por razón de su estatus y de su *statelessness* (condición de apátrida, en cuanto a la ausencia de vínculos respecto de cualquier grupo).[21] Mars describe algunas situaciones en las que un profesional de estas características puede ver peligrar su posición: cuando su jefe inmediato deja el cargo y tiene que renegociar de nuevo sus condiciones contractuales, cuando organizaciones que deberían basarse en el instinto emprendedor se ven aplastadas por una burocracia paralizante, o cuando un directivo es rebajado de nivel y se le retira de un cargo. En tales situaciones, los *hawks* no pueden explotar sus mejores cualidades y se ven capitidisminuidos. Sin embargo, saben sobreponerse y sortear los obstáculos que limitan su potencial, y se reafirman en otros campos en los que sí pueden gozar de libertad de movimientos.[22]

El tipo de trampas (*fiddles*) a las que recurren los *hawks* son parte de la propia elasticidad que configura su clase de puestos de trabajo. En este sentido, las inclinaciones a aprovecharse de las circunstancias mediante recompensas ilícitas son *intrínsecas* al tipo de trabajo, y no *extrínsecas*. Si a un *donkey* (*vid.* al respecto *infra*) le remueves las condiciones que le permiten aprovecharse del sistema y crearse ventajas paralelas o recompensas, no alterará su forma de trabajar: no suele ocurrir así cuando le quitas a un *hawk* las recompensas paralelas en su trabajo.[23]

(2) *Contornos bien delimitados individualmente y vínculos débiles en grupos* (*strong-grid and weak-group*). En segundo lugar, describe a aquellas personas que ocupan puestos caracterizados por el aislamiento y la subordinación (*donkey*). El ejemplo paradigmático de este tipo de profesiones o puestos de trabajo son los *skivvies*, aquellos sirvientes personales en el ámbito familiar, que era común tener en los hogares en el siglo XIX (Douglas, 1978). Los *donkeys* se hallan en una paradójica posición, entre una extrema fragilidad y un enorme poder. Pueden llegar a gozar de enorme poder, en el sentido de que, cuando se los rechaza (o no se los acoge debidamente), los efectos que pueden llegar a provocar podrían suponer un trastorno importante. Es relativamente frecuente que este tipo de trabajos generen *resentimiento*. Y, por tanto, no es inusual que haya un *alto nivel de rotación* en tales oficios o que el trabajador busque otras alternativas para escapar de la desagradable realidad laboral en que convive mediante el recurso al *absentismo* o la *enfermedad*. También pueden darse diferentes formas de *sabotaje*, especialmente cuando los límites y controles son de naturaleza mecánica (Taylor and Watson, 1971).[24]

(3) *Contornos bien delimitados individualmente y vínculos fuertes en grupos* (*strong-grid and strong-group*). Se refiere a aquellos tipos de trabajo tradicionales de las clases trabajadoras (*traditional working-class occupations*), tales como los obreros en el sector de la minería o los estibadores portuarios. Estos grupos de trabajadores se basan en la mutua interdependencia y en la definición de funciones o roles estratificados (*wolves*). En ocasiones, el trabajo y la vida en grupo se fusionan en instituciones omniabarcantes como la convivencia laboral en prisiones, hospitales o algunos hoteles. En tales entornos, el control que ejerce el grupo sobre el individuo puede llegar a ser considerable, y exigir la dedicación de tiempo y la definición de lealtades.

(4) *Contornos poco delimitados individualmente pero con vínculos fuertes en cuanto al grupo, aunque sean a menudo latentes* (*weak-grid and strong-group*). En último lugar, se

19. G. Mars (1982, pág. 29).
20. Estos factores pueden explicar por qué, por ejemplo, algunos cirujanos de prestigio permanecen en el National Health Service, donde los salarios son formalmente más bajos, o algunos cerebros tecnológicos no siempre se van al extranjero: *Ibid.*, pág. 42 y ss.
21. *Ibid.*, pág. 54.
22. En el contexto de tal cambio de circunstancias, menciona dos casos prototípicos de la flexibilidad y adaptabilidad del *hawk*: la tendencia al pluriempleo (*moonlighters*) y las tensiones entre el control y el fomento de la creatividad de los trabajadores para evitar que se vayan a la competencia (*breakaways*). *Ibid.*, pág. 61 y ss.
23. *Ibid.*, pág. 65. Así, si se implementan mecanismos para prevenir que una dependienta de un supermercado no cometa pequeñas sustracciones de la caja registradora, esa medida no alterará la forma de trabajar de este tipo de trabajadores.
24. *Ibid.*, pág. 31.

refiere a aquellos tipos de trabajo que ofrecen una considerable autonomía y libertad de movimientos, pero en los que tal libertad está sujeta a un control burocrático por clases que lleva a uniformizar a los trabajadores, y los clasifica en distintas unidades y, por tanto, generan un sentimiento colectivo. Los trabajadores se sienten miembros de un grupo junto a sus compañeros de trabajo para algunos propósitos determinados, mientras que actúan de forma individualista y movidos por la competitividad en otros (*vultures*). No gozan de la libertad de los *hawks*, ni del encorsetamiento asfixiante que atenaza a los *donkeys*. Su pertenencia al grupo no tiene los efectos intrusivos y controladores propios de una *manada de lobos* (*wolves*). Entre tales tipos de trabajo se encuentran los agentes comerciales o los representantes de negocios. Los repartidores ejemplifican bien el grado de unidad en las condiciones laborales y las tareas profesionales, y en la discrecionalidad y la considerable libertad de cada miembro en el día a día de su trabajo.[25]

Como conclusión, se puede afirmar, en líneas generales, que el conocimiento de la psicología individual y colectiva en torno a cada tipo de trabajo resulta de utilidad para definir las estrategias de prevención y adaptar el necesario control a las características y circunstancias particulares; así se encuentra el punto de equilibrio entre confianza y control.

Aunque no se puedan establecer reglas generales que definan el modo en que interaccionan (cuando menos, a efectos criminológicos) los rasgos personales y las características del entorno laboral, se puede tratar de identificar algunos nexos de unión entre tipos de trabajo y características de los delitos más comunes, sus condiciones y lugares de ejecución (*fiddle factors and fiddle-proneness*).[26]

Así, el empresario debería conocer *ex ante* con mayor profundidad la potencialidad delictiva del entorno en que coloca a cada trabajador. Ciertamente, desde el punto de vista jurídico-penal será difícil que pueda asumir parte de responsabilidad si puso su confianza en una persona que no la merecía (*culpa in eligendo*), o si al otorgarle sus funciones y capacidades (tal vez por un exceso de confianza) omitió un sistema de vigilancia o de reducción de las oportunidades delictivas (*culpa in vigilando*). Sin embargo, la relevancia penal no es el único análisis posible respecto de una negligente estrategia preventiva.

5.6. A propósito de la opacidad de lo que ocurre en el interior de la empresa

El trabajo de James W. Williams ayuda a comprender cómo una de las primeras razones que aducen los ejecutivos empresariales para dejar de denunciar a la policía casos relativos a irregularidades financieras es que pierden el control sobre el problema y sacrifican, de esta manera, algunos de los bienes más altamente valorados por las empresas: la discreción, la confidencialidad y el control (*secrecy, discretion and control*). La importancia del control de la situación por parte de la empresa en tales casos pivota sobre tres cuestiones relacionadas entre sí:

a) Efectos en la imagen corporativa

La primera, y tal vez la más importante, se refiere a los efectos en la imagen de la empresa derivados de la publicidad del caso (*dimensión corporativa*). Tal y como apunta Williams, los directivos desean evitar a toda costa la embarazosa situación y la publicidad negativa como consecuencia de este tipo de incidentes. Si estos trascienden y llegan a ser de conocimiento público, las acusaciones de fraude podrían tener efectos devastadores en la reputación y en el valor bursátil de la compañía. Esta apreciación es especialmente certera si el núcleo del negocio de la empresa depende de la confianza pública relativa a la integridad de los mecanismos de control y sistemas de dirección, como es el caso del sector bancario y de las compañías de seguros, o si puede dar lugar a una sospecha en cuanto a la complicidad corporativa en el incidente. En este sentido, el problema de acudir a la policía (incluso en el mejor de los escenarios posibles) es que la empresa pierde el control sobre la medida en que el asunto llega a convertirse en un conocimiento público. Por el contrario, es precisamente la preservación del secreto y la confidencialidad, así como la capacidad de limitar la visibilidad pública de un incidente, lo que proporciona a la investigación privada (FACI) una ventaja estratégica y un factor clave.[27]

b) Efectos en la dimensión personal

La segunda razón aducida por Williams se refiere a que los directivos no solo quieren tener la capacidad de controlar si el caso se hace público y en qué manera para no deteriorar la imagen de la empresa, sino que también desean determinar qué aspectos del caso exactamente van a ser investigados (*dimensión personal*). Este hecho aporta un valor añadido

25. *Ibid.*, págs. 32-33.
26. *Ibid.*, pág. 136 y ss.
27. J. W. Williams (2005).

de gran importancia, sin duda carente de legitimidad, ya que al acudir a los servicios de una empresa privada (FACI) se garantiza que las líneas de investigación de posibles responsabilidades personales u organizacionales derivadas de un supuesto fraude pueden ser llevadas a cabo de forma restrictiva, con la finalidad de limitar la responsabilidad de otras personas potencialmente implicadas o de la compañía en su conjunto. Este factor es especialmente relevante para los directivos del más alto nivel, en tanto que podrían tener que someterse a formas adicionales de registro y control si las pesquisas en la investigación del respectivo fraude acaban conduciendo a los investigadores «hasta la puerta de su propio despacho».[28]

c) Efectos imprevisibles derivados

Un tercer aspecto nada despreciable relacionado con el control de la situación es la misma *imprevisibilidad de las consecuencias* como resultado de una investigación oficial. En el momento en que la policía inicia una investigación en el interior de la empresa, pueden aflorar otras prácticas irregulares no del todo relacionadas con el caso: anteriores tramas delictivas vinculadas tan solo tangencialmente o de forma secundaria a la investigación principal.[29] En la medida en que la policía tiene el derecho y la autoridad para investigar, en ese contexto, cualquier faceta relacionada con la actividad empresarial, el alcance de la investigación policial puede descubrir y desvelar también irregularidades no conocidas por la misma dirección de la empresa, o prácticas bien conocidas pero de las que se ignoraba su ilicitud.

6. Conclusiones y sugerencias para futuras investigaciones

Del análisis anterior, y con las obvias limitaciones derivadas del número de respuestas obtenidas, entendemos que se puede llegar a varias conclusiones. La más importante es, sin duda, que las empresas no están aprovechando el margen legal que la reciente jurisprudencia del Tribunal Supremo les concede para controlar el uso de las nuevas tecnologías en la empresa.

Como hemos visto, existen todavía empresas de gran tamaño que no disponen de política de uso, cosa que impide en buena medida la posibilidad de llevar a cabo un control razonable del uso de los medios informáticos proporcionados a los trabajadores. Por otro lado, la inmensa mayoría de las empresas que disponen de esa política de uso no han implementado mecanismos técnicos de prevención ni sancionan debidamente la infracción.

En este contexto, sorprende que un 44% de las empresas encuestadas consideren que detectan *prácticamente todos* o *la mayoría* de los incumplimientos que se producen en la empresa.

Estos resultados se podrían explicar porque la mayoría de las empresas continúan pensando que el daño que se les puede ocasionar por el mal uso de los sistemas de información por parte de los empleados es bajo. Más concretamente, la mayoría de las empresas españolas trabajarían sobre la base de que el único daño al que están expuestas por este motivo es a una bajada de la productividad de determinados empleados. Si la empresa trabaja sobre estas premisas, es probable que tenga la sensación de que controla la mayoría de las infracciones, no porque disponga de los medios técnicos necesarios (de los que efectivamente no dispone), sino porque percibiría una bajada de rendimiento del trabajador por otros medios e identificaría el mal uso de los sistemas de información como causa de esa bajada.

Sin embargo, de acuerdo con estas mismas empresas, «solo» un 47% de los daños consisten en la reducción del rendimiento laboral del trabajador, dividiéndose el 53% restante entre daños materiales o a la propiedad intelectual, industrial o *know-how*, entre otros.

Llevando a cabo una visión de conjunto, entendemos que hay que llegar a la conclusión de que un número significativo de empresas encuestadas (el citado 44% de empresas que consideraban que detectan *prácticamente todos* o *la mayoría* de los incumplimientos) no han hecho un estudio riguroso de los riesgos a los que están expuestas como consecuencia del uso de los sistemas de información por parte de los empleados. Esta conclusión se puede generalizar todavía más si sumamos a aquellas empresas que consideran que han detectado *solo los casos más graves*, teniendo en cuenta que de forma

28. *Ibid.*, pág. 328. A este respecto, es especialmente ilustrativa la estrategia seguida en el control de los tiempos y de las formas en el reciente caso Société Générale, a la luz de las noticias aparecidas en la prensa (véase al respecto la noticia publicada en *La Vanguardia* el 24 de enero de 2008).
29. «The problem is when you start with the police you have no control» (*cfr.* Former Police Officer 5: 6-7). Si se tratara de una investigación o consultoría privada, el alcance de las pesquisas se limitaría por la misma causa por la que se han contratado los servicios (*Ibid.*, 45, pág. 328).

mayoritaria las empresas encuestadas han valorado los daños causados por cada incidente en menos de tres mil euros.

Así, un 74% de las empresas encuestadas consideran que detectan, como mínimo, los casos más graves, que en ningún caso superan los tres mil euros por incidente.

En nuestra opinión, lo que las respuestas ponen de manifiesto es una falta de análisis profundo de los riesgos asociados al uso de las nuevas tecnologías. Esta falta de análisis no se debería a un desconocimiento de los riesgos en sí, sino a una indebida (posiblemente inexistente) evaluación de los daños que se podrían producir.

La aplicación de un sistema de control de los sistemas de información debe partir de una análisis de lo que la empresa desea proteger por considerarlo más valioso. En determinados sectores, es posible que lo que tenga más valor en la empresa sea el tiempo de los empleados. Sin embargo, hemos podido observar que en apenas un 10% de los casos se discrimina el control por salario o por posición jerárquica. En el mismo sentido, si el gran valor de la empresa fuesen sus empleados, tendría sentido diferenciar el control ejercido sobre aquellas posiciones cuya retribución va en mayor medida ligada a resultados concretos, del que se debería ejercer sobre empleados con salarios fijos proporcionalmente más importantes.

Quizás es todavía más importante llamar la atención sobre la falta de sensibilidad frente a la posibilidad de incurrir en otro tipo de daños inmateriales. Sin entrar en detalles sobre la diferente casuística, parece evidente que los daños por perder a un cliente, no ganar un contrato o, ya en casos más extremos, divulgar determinada tecnología deben superar ampliamente a los que se puedan derivar de una reducción de la productividad del trabajador.

Es esta falta de conciencia de los daños que se han producido y de los que se pueden producir la que, a nuestro entender, está condicionando el tratamiento preventivo y reactivo de las empresas. Es evidente que la evaluación de muchos de los activos inmateriales de las empresas es una asignatura pendiente, y no es la menor de las razones para esto la dificultad intrínseca de este ejercicio. Sin embargo, a diferencia de otros ámbitos (como en el contable o el fiscal), la aplicación de medidas de control en el uso de los sistemas de información no requiere de una valoración detallada, pero sí de un ejercicio de priorización y sensibilización, sin el cual las empresas se instalarán en la falsa sensación de tener controlado el riesgo.

A la vista del estudio realizado y de las conclusiones que se acaban de exponer, sintetizamos en el siguiente cuadro las principales orientaciones prácticas que deberían implementar las empresas para el buen gobierno de las TIC.

Decálogo para empresas: orientaciones prácticas para el buen gobierno de las TIC

1. *Evalúe adecuadamente los distintos tipos de daños que se le pueden ocasionar a la empresa a través de los sistemas de información.*
2. *Delimite claramente el ámbito de lo permitido.*
3. *Distinga adecuadamente las necesidades de control de cada tipo de trabajador y cada tipo de riesgo.*
4. *Supervise periódicamente las* e-policies*, y establezca sanciones o medidas efectivas.*
5. *Actualice las* e-policies *en función de los incidentes producidos.*
6. *Disponga de instrumentos técnicos necesarios para detectar los incumplimientos y establezca protocolos de actuación.*
7. *Evalúe adecuadamente las estrategias de reacción.*
8. *En todo el proceso, mantenga el debido asesoramiento jurídico.*
9. *Informe periódicamente a los trabajadores del impacto económico de los incumplimientos habidos.*
10. *Demuestre con hechos que las políticas de control no están reñidas con unas relaciones laborales basadas en la confianza, pero también en la responsabilidad.*

Bibliografía

AGUSTINA, J. R. (2009a). *El delito en la empresa*. Barcelona: Atelier.

AGUSTINA, J. R. (2009b). *El delito de descubrimiento y revelación de secretos en su aplicación al control del correo electrónico del trabajador*. Madrid: La Ley.

AGUSTINA, J. R. (2009c). «Expectativa de privacidad en el correo electrónico laboral y prevención del delito (Reflexiones en torno a la Sentencia del Tribunal Supremo de 26 de septiembre de 2007)». *La ley penal: revista de derecho penal, procesal y penitenciario*. N.º 63.

AGUSTINA, J. R. (2009d). «El factor confianza y la lógica del control en la empresa: algunas reflexiones ético-jurídicas a propósito de las estrategias de prevención del delito de los trabajadores». *Revista Empresa y Humanismo*, XII. N.º 2, págs. 13-60.

AGUSTINA, J. R. (2010). «Fenomenología del *"employee crime"*: bases para definir estrategias de prevención del delito intraempresarial». *Política Criminal. Revista Electrónica Semestral de Políticas Públicas en Materias Penales*, 5. N.º 10, págs. 352-409.

BAYLOS GRAU, A.; TERRADILLOS BASOCO, J. (1997). *Derecho penal del trabajo*. (2.ª ed.) Madrid: Trotta.

BUSSMANN, K. D. (2003). «Causes of Economic Crime and the Impact of Values: Business Ethics as a Crime Prevention Measure». En: Swiss Conference on Coping with Economic Crime. Zúrich: Risks and Strategies.

FRIEDRICHS, D. O. (2002). «Occupational crime, occupational deviance, and workplace crime: Sorting out the difference». *Criminal Justice*. Vol. 2, n.º 3, págs. 243-256.

GREEN, G. S. (1997). *Occupational Crime* (2. ed.). Chicago: Nelson Hall.

BLOUNT, E. C. (2003). *Occupational Crime. Deterrence, Investigation, and Reporting in Compliance with Federal Guidelines*. Nueva York: CRC Press.

MARS, G. (1982). *Cheats at Work. An Anthropology of Workplace Crime*. Londres-Boston: Allen & Unwin.

PRICE WATERHOUSE COOPER'S 4TH BIENNIAL GLOBAL ECONOMIC CRIME SURVEY (2007). *Economic crime: people, culture and controls.*

SÁNCHEZ ÁLVAREZ, M. (1986). *Los delitos societarios*. Pamplona: Aranzadi.

SNIDER, L. (2001). «Crimes against capital: Discovering theft of time». *Social Justice*. Vol. 28, n.º 3, págs. 105-120.

SOLIVETTI, L. M. (1987). «*La criminalità di impresa: alcuni commenti sul problema delle cause*». *Sociologia del Diritto*, Nº 1, pág. 65.

SUTHERLAND, E. H. (1939). *Principles of Criminology*. Nueva York: Rowman & Littlefield.

WECKERT, J. (2002). «Trust, corruption, and surveillance in the electronic workplace». En Klaus Brunnstein and Jacques Berleur (eds.), *Human Choice and Computers: Issues of Choice and Quality of Life in the Information Society*, Kluwer, Boston, 17th IFIP World Computer Congress, Montreal. Págs. 109-120.

WILLIAMS, J. W. (2005). *Reflections on the private versus public policing of economic crime*. *British Journal of Criminology*, 45. Págs. 327-328.›

Cita recomendada

AGUSTINA, JOSE R. (2013). «¿Cómo prevenir conductas abusivas y delitos tecnológicos en la empresa?». *IDP. Revista de Internet, Derecho y Política*. Número 16, pág. 7-26. UOC. [Fecha de consulta: dd/mm/aa]
<http://idp.uoc.edu/ojs/index.php/idp/article/view/n16-agustina/n16-agustina-es>
DOI: http://10.7238/idp.v0i16.1806

Sobre el autor
Jose R. Agustina
jragustina@uic.es
Profesor contratado doctor de la Universitat Internacional de Catalunya
http://www.uic.es/es/es/personal-page?id_user=jragustina

Facultad de Ciencias Jurídicas y Políticas
Universitat Internacional de Catalunya
C/ Immaculada, 22
08017 Barcelona