La videovigilancia en el trabajo en tiempos de inteligencia artificial

Video surveillance at the workplace in times of artificial intelligence

Miguel Rodríguez-Piñero Royo
Universidad de Sevilla
ORCID ID: 0000-0001-7926-6175

doi: 10.20318/labos.2024.9032

Resumen: Este trabajo analiza los efectos de la integración de sistemas de IA en la videovigilancia en las empresas, y qué regulación se aplica cuando esto ocurre. Se estudia la aplicación conjunta de las reglas sobre videovigilancia del Derecho digital del trabajo con las del Derecho Algorítmico. La conclusión es que dispone de reglas bastante completas para ordenar estos sistemas, sin que se detecten grandes contradicciones entre ambos sectores. Estos dispositivos y la analítica de imágenes incrementan los riesgos de vulneración de derechos para los trabajadores, pero también proporcionan a los empleadores un importante instrumento para la mejora de la salud y la seguridad, la toma de decisiones y el cumplimiento normativo, por lo que debe avanzarse en su regulación.

Palabras clave: Videovigilancia, Inteligencia Artificial, poderes empresariales, cumplimiento normativo, derechos de los trabajadores.

Abstract: This paper analyzes the effects of integrating AI systems into workplace surveillance and the applicable regulations when this occurs. It examines the joint application of digital labor law surveillance rules with those of Algorithmic Law. The conclusion is that there are fairly comprehensive rules to regulate these surveillance systems, without significant contradictions between the two sectors. These devices and image analytics increase the risk of rights violations for workers, but also provide employers with an important tool for improving health and safety, decision-making, and regulatory compliance. Therefore, progress must be made in their regulation.

Keywords: Videosurveillance, Artificial Intelligence, managerial powers, compliance, workers' rights.

1. Presentación: control, tecnología y derecho

El Derecho del Trabajo que hoy conocemos es, todavía, el del trabajado asalariado y por cuenta ajena, al que calificamos como subordinado porque la nota que lo caracteriza, frente a otras formas de empleo retribuido, es el sometimiento de la persona que lo desempeña a otra. La evolución del ordenamiento jurídico ha llevado a que esta dependencia sea una estrictamente contractual, derivada de la voluntad de la persona que acepta formar parte de un vínculo obligacional, lejos ya de compromisos personales o de estatus de clase. La dependencia supone, como es bien sabido, el sometimiento a tres poderes empresariales, que generan derechos para los empleadores y correlativas obligaciones para quiénes trabajan para ellos: poder de dirección, poder disciplinario y poder de control. Del último de ellos me ocuparé en este trabajo.

Se trata de un poder legalmente reconocido, justificado y finalista en la medida en que se ejercita en relación con una serie limitada de finalidades, amén de otras restricciones derivadas por la forma en que afecta a derechos fundamentales de la persona, tanto los generalmente conocidos como "inespecíficos", como otros que podemos considerar específicos del trabajador, que es titular de una especie de "intimidad laboral" que ha estado reconocida desde un primer momento, antes incluso de que se pensara en términos de derechos de éstos. Es un poder marcadamente pro empresario, para el cuidado de sus intereses en la relación de trabajo, aunque no exclusivamente desde el momento en que se ejercita para verificar el cumplimiento de determinados derechos de los trabajadores.

Estos tres poderes, por más que como laboralistas nos hayamos acostumbrados a ellos hasta normalizarnos, no dejan de ser anómalos en un contexto contractual, con un Derecho de obligaciones construido sobre modelos completamente diferentes. La función histórica del Derecho del Trabajo, en el marco del Derecho privado, ha sido la de establecer un marco normativo que permita su ejercicio de acuerdo con unos estándares de dignidad y de derechos.

Poder de dirección y poder de control comparten estar directamente condicionados por el estatus quo tecnológico del momento en que se ejercitan. Es la tecnología la que determina cómo se trabaja, y cómo se supervisa lo que se trabaja. De ahí que su ordenación sea en gran medida la de los medios técnicos utilizados por la empresa, cuyos avances generan problemas crónicos de obsolescencia regulatoria. El impacto de la innovación no se produce sólo en el ejercicio de las facultades de dirección y supervisión, pero no cabe duda de que incide especialmente en éstas.

Las últimas revoluciones tecnológicas, digitalización e inteligencia artificial (IA), han tenido un especial impacto en este ámbito, al haber generado nuevos instrumentos y haber extendido los ya existentes. Puede decirse incluso que, en las últimas décadas, y como consecuencia de ellas, se está produciendo un cambio en el peso específico de cada uno de ellos en la relación de trabajo: los medios disponibles han permitido una mayor autonomía en la prestación de trabajo, con lo que la relevancia de la dirección se reduce, a la vez que se han incrementado las posibilidades de controlar, haciendo que la

supervisión resulte más importante. En los centros de trabajo del siglo XXI la autonomía en el trabajo no se ve acompañada de un aligeramiento del control, sino más bien de lo contrario, siendo éste a lo que las empresas han recurrido para mantener el gobierno de la organización.

Tradicionalmente entre los indicios de laboralidad manejados por nuestros tribunales escaseaban los que tenían que ver con el control de la actividad del trabajador, en detrimento de aquellos vinculados con el ejercicio de los poderes directivos. El desafío del trabajo digital, en particular el de las nuevas formas de empleo generadas por éste, está haciendo que el foco vaya dirigiéndose también a este aspecto, alineando esta tarea con la realidad del trabajo en este siglo.

El cambio en los soportes que facilitan el control empresarial se ha percibido por lo general en términos de riesgo para los trabajadores, conceptuándose la idea de la "empresa panóptica" (MERCADER UGUINA), como un prototipo ucrónico en el que los derechos de éstos podían verse sistemáticamente limitados. Y es cierto que tanto los espacios tradicionales de intimidad como las expectativas de privacidad se ven afectados por las capacidades ampliadas de supervisión, todo ello en un contexto jurídico de mayor sensibilidad hacia los derechos vinculados con la protección de datos y la intimidad. Sin embargo, y de una manera ciertamente paradójica, el control de la empresa está mutando para desarrollar otra de sus facetas, la de la garantía del cumplimiento normativo en lo laboral. Esta doble naturaleza no es nueva, pero sí se ha visto potenciada con figuras tales como el registro de jornada, originalmente diseñado para asegurar el cumplimiento de las obligaciones laborales, hoy orientado también hacia la evitación de abusos en el tiempo de trabajo. Esto debe ser tenido en cuenta, a mi juicio, cuando se analizan los instrumentos de vigilancia en el nuevo entorno tecnológico, para aprovechar al máximo las posibilidades que se generan.

En este trabajo voy a analizar un mecanismo particular de control empresarial, la videovigilancia, cuyo análisis resulta especialmente interesante por una serie de motivos: es una forma con una larga tradición, que precede la existencia de soportes tecnológicos que lo faciliten (un supervisor en un centro de trabajo está vigilando la actividad de los empleados utilizando su propia vista); ha experimentado sucesivas innovaciones técnicas, que han tenido el efecto de hacerla ubicua en el siglo XXI; su régimen jurídico ha ido evolucionando, de acuerdo con el contexto regulatorio de la tecnología en cada momento; y, finalmente, puede verse especialmente afectada por el desarrollo de la IA, de la que nos estamos ocupando en este número monográfico.

La hipótesis de partida de este estudio es que se está produciendo la construcción de un Derecho algorítmico del trabajo, constituido por un conjunto de respuestas jurídicas a los problemas que se percibe puede generar la utilización de sistemas de inteligencia artificial en el ámbito laboral. A la vez, la videovigilancia se está transformando por la integración de estos sistemas, de tal modo que su utilidad, alcance y efectos van a cambiar radicalmente. Las reglas jurídicas ya aplicables deberán actualizarse para adecuarse a estos nuevos usos, a la vez que se ajustan a los principios e instrumentos del Derecho algorítmico.

2. La videovigilancia en el derecho del trabajo anterior a la inteligencia artifical

Como ya se ha dicho, la videovigilancia es anterior a la digitalización, surgiendo en un entorno analógico, lo que hizo que originalmente tuviera poco impacto en la práctica, por su escaso alcance y limitada utilización. Su regulación estuvo condicionada por este estatus quo tecnológico, lo que se tradujo en un tratamiento legal limitado, cuando existía, y la aplicación de la normativa general sobre intimidad de la persona trabajadora y poderes empresariales. Tampoco era frecuente su tratamiento en los convenios colectivos, lo que dejaba el protagonismo a la jurisprudencia, tanto laboral como constitucional, que se realizaba aplicando la regulación del derecho a la intimidad e importando reglas de otros sectores del ordenamiento (como el Derecho procesal en torno a la validez de las grabaciones como prueba).

Con el tiempo una serie de cambios afectó a este mecanismo de control, algunos técnicos y otros de distinta naturaleza. Así, uno de los factores que más cambió su utilización fue el abaratamiento de los soportes técnicos utilizados, tanto para la obtención de imágenes como para su almacenamiento. Esto permitió un uso extensivo de la videovigilancia. También ayudó la miniaturización de las cámaras, que permitió su ubicación en todo tipo de entornos, así como su inclusión en otros soportes (como ordenadores y monitores), lo que llevó una especie de invisibilidad, al perderse la consciencia de estar siendo monitorizado. No en vano una de las principales medidas de control que se le impone es, precisamente, la señalética para avisar de su presencia.

La digitalización alteró profundamente su utilización. Al pasarse las imágenes obtenidos a un formato digital se facilitó su almacenamiento, tratamiento, transferencia y manipulación. Convertida en un dato, la imagen de las personas se hace merecedora de tutela por la legislación de protección de datos.

Hoy está presente en todo tipo de entornos laborales, así como en aquellos otros que, no siéndolo en sentido estricto, pueden exponer a las personas que trabajan al control de su imagen, como las vías públicas durante los desplazamientos causados por la actividad profesional.

Estos avances han cambiado radicalmente la percepción de riesgos asociados a su presencia, lo que ha impulsado el desarrollo de su régimen jurídico. Éste se ha construido sobre jurisprudencia anterior, y ha combinado reglas generales y especiales. En particular se ha definido un nuevo derecho fundamental laboral, encuadrado en los derechos digitales, que es el derecho a la tutela frente a la videovigilancia abusiva o excesiva (no frente al control de imágenes en sí mismo). De esta materia, la Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital (2023/C 23/01) afirma que "*nos comprometemos a (…) la protección frente a una vigilancia ilegal e injustificada*". En España la Carta de Derechos Digitales dispone que "*en los entornos digitales y el teletrabajo las personas trabajadoras del sector público o privado tienen derecho con arreglo a la normativa vigente, a la protección de sus derechos a la intimidad personal y familiar, el honor, la propia imagen, la protección de datos y el secreto de las comunicaciones frente al uso de dispositivos de videovigilancia*".

Este derecho, que es autónomo frente a los genéricos de intimidad y protección de datos, es la base para un régimen jurídico diferenciado, que en nuestro país incluye dos preceptos que no llegan a ser monográficos, aunque sí aportan mandatos para definir éste. Por un lado, el artículo 20 bis del Texto Refundido del Estatuto de los Trabajadores (TRET), que contempla los derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión, entre los que se incluye el de la intimidad frente al uso de dispositivos de videovigilancia. El precepto estatutario se remite a los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales en cuanto al ejercicio de este derecho, para lo que disponemos, como segundo referente normativo, del artículo 89 de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, que reconoce el derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.

La combinación de estos preceptos con las construcciones jurisprudenciales anteriores resulta en un régimen caracterizado por siguientes notas:

— Relevancia del dispositivo, de tal modo que esta regulación se aplica a un tipo determinado de éstos, los que recogen imágenes.
— Relevancia del tipo de dato, dado que se trata de reglas específicas para las imágenes.
— Legitimidad del uso de estos dispositivos por parte de las empresas, pero limitado al ejercicio de las funciones de control de personas trabajadoras que emplean, y en relación con la actividad productiva y la seguridad de las personas.
— Sometimiento de este control mediante videovigilancia al marco legal y a los límites inherentes al mismo. Esto incluye la legislación de protección de datos
— Deber de información a las personas trabajadoras que van a ser objeto de esta medida de control; esta información deberá suministrarse con carácter previo, y de forma expresa, clara y concisa.
— Deber de información a los representantes de la plantilla, en caso de estar constituida ésta, en los mismos términos que a los trabajadores individuales.
— Aplicación de criterios de necesidad, idoneidad y proporcionalidad en cuanto a la utilización de este control.
— Deber de minimización, que supone (AEPD) que se valore si realmente es necesaria la instalación de la videovigilancia, o si el fin perseguido se puede alcanzar de otra forma. Además, cuando realice la instalación, que se tenga en cuenta la proporcionalidad en función del número de cámaras, tipo de las mismas y la opción de utilizar "máscaras de privacidad".
— Respeto a las expectativas de intimidad, de tal modo que, si existen motivos justificados para considerar que no se va a ser objeto de este control, su utilización resultará ilegítima.

— Respeto a los espacios de intimidad, en los que no se admite su uso, y que incluyen los lugares destinados al descanso o esparcimiento, como vestuarios, aseos, comedores y análogos.
— Reconocimiento del papel de los representantes de los trabajadores, aunque desde nuestra perspectiva nos parece un rol bastante discreto.

Por su propia naturaleza, las reglas propias de la videovigilancia se superponían frecuentemente con otros contenidos del Derecho digital, desde el punto de vista de la utilización de las imágenes obtenidas. Es frecuente que estos dispositivos sean instrumentales para el establecimiento de controles biométricos, que están admitidos pero sujetos a exigencias rigurosas, por su carácter intrusivo y porque los riesgos vinculados a este tipo de controles van más allá de los ya identificados para los de imagen. La videovigilancia entra igualmente dentro del ámbito de aplicación de la normativa de protección de datos, en cuanto la imagen es considerada legalmente como un dato, y estos sistemas permiten el almacenamiento y la transmisión de éstas. Es posible que este control se realice mediante dispositivos empresariales puestos a disposición de los trabajadores, como las cámaras de los ordenadores portátiles. Si además estos se utilizan en relaciones de teletrabajo en el domicilio de la persona trabajadora, se le aplica el conjunto normativo especial que regula esta forma de empleo.

Comparte la regulación de la videovigilancia con otras formas del Derecho Digital la presencia de una gran diversidad de elementos normativos, ya que junto a las normas legales encontramos otras propias del soft-law, cláusulas convencionales, guías de uso, cláusulas contractuales y normativas internas de las empresas.

3. Del Derecho digital al Derecho algorítmico

La aparición de los sistemas de IA está suponiendo una verdadera revolución, que ha impulsado una nueva fase en la evolución del tratamiento de los instrumentos tecnológicos por el ordenamiento jurídico. En efecto, si realizamos un análisis histórico superficial del tratamiento de esta cuestión, podemos identificar diferentes fases o momentos, comenzando por regulaciones concretas para los mecanismos de control más generalizados (por ejemplo, para los registros en la persona del trabajador), para llegar a la utilización de los llamados "derechos inespecíficos" para garantizar ciertos niveles de protección a las personas. El desarrollo de la legislación de protección de datos afectó igualmente a los sistemas de vigilancia en la empresa. A finales del siglo pasado se manejó una categoría, la de "derechos on-line", que no tuvo mucho impacto en el Derecho positivo pero que sí sirvió para llamar la atención sobre los riesgos derivados de la utilización de mecanismos avanzados de control y de la generalización de las entonces conocidas como TIC. La fase siguiente, en la que todavía nos encontramos, es la del Derecho Digital del Trabajo, que dedica una parte importante de su regulación a la tutela de las personas frente a los mecanismos de supervisión basados en esta tecnología, videovigilancia incluida.

Ahora estamos asistiendo al surgimiento de un nuevo conjunto regulador, conocido generalmente como Derecho Algorítmico o Derecho de la IA, que tiene una vertiente laboral en cuanto regula la utilización de tales sistemas en la gestión de personas, incluyendo su supervisión y control. Esta rama no debe entenderse estrictamente como una nueva fase en la evolución del Derecho de la tecnología en el trabajo, sino como un desarrollo monográfico de una parte de éste, ya que supone una regulación propia para un tipo particular de instrumento empresarial que podría considerarse como parte de la tecnología digital, o que al menos se combina con ésta. Podríamos hablar, así, de que esta rama emergente como un "spin-off" del Derecho digital, centrado en la ordenación de los sistemas de IA que van a utilizarse en las empresas y en las administraciones públicas. Como tal derivación tienen un código genético compartido con éste, ya que comparte muchos de sus objetivos, principios e instrumentos. Tiene, aun así, señas de identidad propias, que lo diferencian y caracterizan como una regulación verdaderamente original.

Entre estas señas de identidad podemos señalar su construcción acelerada, ya que en un corto plazo se dispone ya de un conjunto de normas bastante extenso, resultado de una intervención multinivel que también lo caracteriza. Este desarrollo rápido es consecuencia de su carácter preventivo, no en el sentido de que se elaborara antes de que los sistemas de IA fueran una realidad en las empresas, sino que su construcción comenzó cuando surgió la preocupación por los potenciales riesgos que se atribuían a ésta IA. Esto es, que no se ha esperado a que se generaran los problemas para comenzar a diseñar sus soluciones, sino que éstas los han precedido, a partir de previsiones y expectativas razonables. En este sentido el Derecho algorítmico ha surgido con un marcado carácter académico y tecnocrático, puesto que está siendo elaborado por expertos de diversas disciplinas a partir de la constatación de sus efectos potenciales (o reales, como en el caso del trabajo en plataformas digitales), con el objetivo de adelantarse y anticiparse a éstos.

Esta es una importante diferencia con el Derecho Digital, al menos tal y como éste se había venido construyendo. Éste es igualmente de elaboración multinivel, y utiliza también una pluralidad de instrumentos reguladores. Ahora bien, éste ha tardado mucho más en desarrollarse, ya que sus grandes productos normativos se han aprobado cuando las consecuencias de la utilización de la tecnología digital en las empresas eran ya evidentes. Son muchas las reglas que codifican soluciones preexistentes, elaboradas por los tribunales internacionales o nacionales a partir de regulaciones sobre derechos fundamentales.

Su peculiar origen y su objeto material de regulación han dado lugar a otro rasgo característico del Derecho Algorítmico, su complicación y sofisticación técnicas. Vamos a encontrar regulaciones de realidades tecnológicas complejas y exigentes, cuya elaboración y aplicación exigen un alto nivel de conocimiento previo. A diferencia de las del Derecho Digital, sus normas son muchas más precisas, identificando con detalle su ámbito de aplicación y sus mandatos. Esto tiene que ver con tanto con la realidad material que regula como son su origen tecnocrático. Pero también con el hecho de que el Derecho Algorítmico, especialmente el de la Unión Europea, se ocupa de regular unos programas que van a desarrollarse, comprarse, exportarse. Pretende estandarizar unos

productos de nueva creación para facilitar su uso y circulación. El Reglamento de Inteligencia Artificial afirma en este sentido que su objetivo es "*mejorar el funcionamiento del mercado interior y promover la adopción de una inteligencia artificial (IA) centrada en el ser humano y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta, incluidos la democracia, el Estado de Derecho y la protección del medio ambiente, frente a los efectos perjudiciales de los sistemas de IA en la Unión así como prestar apoyo a la innovación*". Estamos ante una regulación que tutela derechos, pero que a la vez promociona un mercado y facilita el avance de la tecnología. Para ello establece, entre otras cosas, normas armonizadas para la introducción en el mercado, la puesta en servicio y la utilización de sistemas de IA en la Unión; así como medidas en apoyo de la innovación.

La regulación algorítmica es transversal, en el sentido de que se ocupa de unos sistemas que pueden adoptar distintos formatos y manejar datos de diferente naturaleza, dado que lo relevante para su categorización es un factor que opera en un plano diferente, el de los riesgos. Ser calificado con un mismo nivel de riesgo determina la aplicación de un régimen jurídico común; y este nivel se asigna en función del uso que se de al sistema de IA. El Derecho digital es, por el contrario, mucho más específico, ya que diferencia según el dispositivo de control que se utilice y el dato que se recopile, puesto que en la mayoría de los casos la intervención del empleador se hace con una misma función, monitorizar al empleado. Por poner un ejemplo, el Reglamento de Inteligencia Artificial maneja un concepto de sistema de identificación biométrica remota que incluye a todos los destinados a identificar a personas físicas sin su participación activa, con independencia de la tecnología, los procesos o los tipos de datos biométricos concretos que se usen

Finalmente, y si lo comparamos con el Derecho digital previo, el de la IA es algo más sentible a la dimensión colectiva de las relaciones laborales, a la que presta mayor atención. Se reconoce, en este sentido, el papel de los representantes de los trabajadores y las organizaciones sindicales, y se identifican los derechos sindicales como una realidad a tutelar.

4. El impacto de la IA en la videovigilancia

La IA se suma a los cambios tecnológicos experimentados por la videovigilancia en las últimas décadas, ya señalados previamente. Ésta ha mejorado tanto por los avances en el hardware, mediante incrementos de alcance y calidad de las imágenes, capacidad de tratamiento, minutarización y conectividad, como por el software. Y éste, a su vez, ha recibido mejoras tanto en los programas de gestión como con la introducción de la IA en su manejo. La IA se combina con una tecnología ya avanzada para incrementar las capacidades de monitarización, y esto ha llevado a que no se quede en esta función sino que va a servir también para apoyar la toma de decisiones por parte de las empresas, en ejercicio de su poder de dirección.

Esta combinación, que produce lo que en el lenguaje comercial de las empresas de seguridad se llama "cámaras inteligentes", está teniendo un gran impacto tanto por su generalización y extensión, muy rápida, como por los riesgos que se identifican en ella. Es la videovigilancia inteligente en algunas áreas, como la seguridad pública, la que ha movilizado muchos de los debates sobre los riesgos para los derechos fundamentales y las libertades públicas, y lo que ha dado lugar a regulaciones restrictivas, que encontramos en el mismo Reglamento de Inteligencia Artificial. Junto a ello se ha desarrollado la "analítica de imágenes", que consiste en la obtención de información por medio de herramientas de IA a partir de las imágenes obtenidas por un sistema de captación de éstas.

La videovigilancia inteligente está muy extendida, hablándose entonces de "videovigilancia masiva". Puede resultar invisible, no tanto por sus dimensiones o colocación, sino por su presencia generalizada en todos los ámbitos, que hace que se acabe por ignorarlas. En sentido contrario, el "sentimiento de vigilancia masiva", la consciencia de estar continuamente monitorizado, puede afectar negativamente a las personas, produciendo ansiedad y condicionando sus comportamientos.

La videovigilancia inteligente es instrumental para otras actuaciones, como el reconocimiento facial o la detección o deducción de emociones. El Reglamento de IA define los sistemas de identificación biométrica remota como aquellos destinados a identificar a personas físicas sin su participación activa, generalmente a distancia. Éstos pueden ser en tiempo real, si la recogida de los datos biométricos, la comparación y la identificación se producen de manera instantánea, e implican el uso de materiales en directo o casi en directo, como grabaciones de vídeo, generados por una cámara u otro dispositivo con funciones similares. En los sistemas en diferido también se utilizan imágenes o grabaciones de vídeo captadas por cámaras de televisión en circuito cerrado generados con anterioridad a la utilización del sistema en relación con las personas físicas afectadas.

En cuanto a la deducción de emociones de los trabajadores ésta puede basarse en las imágenes obtenidas mediante estos sistemas, tanto de expresiones faciales como de pautas de comportamiento y conductas concretas. No entraré en esta cuestión, dado que ésta será objeto de un análisis completo en otra colaboración a este número monográfico, por parte de una gran experta en este tema.

Las imágenes obtenidas mediante estos sistemas se utilizan para el desarrollo y el entrenamiento de los modelos de IA de uso general, en particular los grandes modelos de IA generativos, capaces ellos mismos de generar imágenes. Esta capacidad de generar imágenes con un alto grado de realismo y verosimilitud produce el riesgo de pruebas falsas, creadas o manipuladas, sobre las que basar decisiones empresariales, algo que con la videovigilancia digital resultaba mucho más complicado.

Se ha señalado igualmente que estos sistemas pueden extender su utilidad más allá del control de la realidad de la actividad laboral, para alcanzar otros aspectos como su cantidad y calidad, convirtiéndose en una fuente de información para la evaluación del desempeño. Una cámara inteligente controla automáticamente lo que se hace, cómo se hace, quién lo hace, en cuánto tiempo, etc.

La IA introducida en los aparatos de videovigilancia se utiliza combinación con otras tecnologías, como los drones y las cámaras "on board" en vehículos. Se diseñan para moverse en función de la información que estén recibiendo, siguiendo a personas y vehículos para tenerlos controlados de manera continuada. También se dotan de sensores para medir la temperatura y otros parámetros físicos y químicos del medio de trabajo. Pueden incluir herramientas de cómputo para determinar el número de personas presentes en un espacio determinado. Se activan o desactivan según se identifique la presencia de elementos predeterminados.

Además, en la medida en que se trata de un software que puede ser instruido fácilmente demuestra una gran capacidad de adaptación al usuario. Así, existen cámaras que descartan las imágenes de las mascotas en los domicilios dotados con estos sistemas de seguridad, o que se adaptan para la custodia a distancia de bebés.

La integración de la IA en la videovigilancia permite el análisis de las imágenes grabadas, su interpretación y la predicción de eventos, de manera inmediata. También hace posible el análisis en tiempo real de la información obtenida por las cámaras, y el aprendizaje automático a partir de ésta.

El sistema de IA inserto en la cámara identifica los elementos que aparecen en la grabación, lo que facilita la extracción de información de ésta, y así hace posible un control que con cantidades ingentes de imágenes resultaría imposible. La actividad de los responsables de seguridad se facilita enormemente, aunque con ello también el riesgo de intrusiones excesivas en la intimidad de las personas trabajadoras.

Las cámaras inteligentes no sólo captan imágenes, sino que detectan patrones y tendencias en la realidad observada, y esto genera el riesgo de control de emociones, como se ha dicho. También introduce el factor de los errores experimentados por la IA, que puede llegar a conclusiones equivocadas, experimentar alucinaciones o sufrir sesgos. De la misma manera, la IA puede concentrar la atención y la captación de imágenes en algunas personas, identificadas a partir de pautas constatadas o de predicciones, y esto genera un riesgo real de discriminación algorítmica.

Como resultado, la IA está transformando el uso que se hace de la videovigilancia en las empresas, permitiéndoles un nivel de control desconocido hasta ahora, tanto por la cantidad y calidad de la información visual que se recoge como por la posibilidad de obtener otra información a partir de ésta. Con las imágenes recogidas y tratadas se basan decisiones empresariales que nada tienen que ver con el cumplimiento de las obligaciones laborales por las personas empleadas por la entidad, sino en la búsqueda de eficiencia, la mejora de la productividad, el ahorro de costes, el incremento de la seguridad y otras finalidades, que no siempre resultan legítimas. Pensemos en la utilización de imágenes para predecir el comportamiento de los trabajadores frente a una huelga, unas elecciones sindicales o un proceso de certificación sindical (como efectivamente parece haber ocurrido en los Estados Unidos); o simplemente para calibrar el clima laboral o el impacto de decisiones empresariales que afectan a la plantilla.

Por todo ello se ha asociado su utilización con la aparición de nuevos riegos para los derechos de los trabajadores. Entre estos riesgos se pueden citar un uso extensivo y

sistemático del control de imágenes; la manipulación y generación de éstas; la posibilidad de alucinaciones y deducciones equivocadas; el control selectivo de ciertas personas o grupos de éstas, como consecuencia de sesgos que pueden suponer una verdadera discriminación; y el agotamiento del personal monitorizado.

Es igualmente cierto que la integración de la IA en los sistemas de control de imágenes proporciona a éstos nuevas utilidades, mejorando la gestión empresarial y la situación de los mismos trabajadores. Podemos pensar en la mejora en la seguridad de los centros de trabajo frente a la actuación de personas, empleadas o no, que puedan detectarse a tiempo o incluso con anticipación; la prevención de accidentes, especialmente incendios (ya se utiliza la videovigilancia inteligente para combatir los incendios forestales); el control sanitario (utilizado durante la pandemia, al poder detectarse la temperatura corporal y otros parámetros, así como detectar cuando una persona tose); la mejora de la salud de los trabajadores (al detectar problemas posturales o conductas indicativas de problemas en ésta); la prevención de violencia y acoso en el trabajo; la tutela de las trabajadoras víctimas de violencia de género (al identificarse a las personas sobre las que recaigan órdenes de alejamiento); la objetivización de la evaluación del desempeño y del control de calidad; y el control real del tiempo de trabajo, entre otras posibilidades.

En particular se ha señalado su utilidad para asegurar el respeto de la normativa preventiva, detectando posibles incumplimientos en el uso de equipos de protección individual, o en el mantenimiento de las distancias de seguridad. Este uso es especialmente adecuado en el caso de trabajadores que, por la naturaleza de su actividad, prestan sus servicios en solitario. Desde otra perspectiva, resulta muy eficiente para mejorar algunos aspectos de la seguridad para las personas, cuando se aplica a colectivos críticos como conductores o pilotos, detectando problemas físicos o inobservancia de descansos obligatorios y otras restricciones; o alertando de situaciones de violencia física que puedan afectar a usuarios de instalaciones y clientes.

5. La videovigilancia en el derecho algorítmico

Una vez identificada la existencia de una combinación entre sistemas de videovigilancia y modelos de IA, que dan lugar a la videovigilancia inteligente y al análisis de la imagen, corresponde señalar, siquiera someramente, cuáles serían las consecuencias jurídicas. Porque, como hemos indicado antes, nos encontramos en una zona de confluencia y superposición de regulaciones, las propias del Derecho Algorítmico con las específicas para esta forma de control elaboradas en el seno del Derecho Digital del Trabajo. Porque las cámaras inteligentes, por el hecho de serlo, no suponen la inaplicación de las reglas que se aplican al conjunto de mecanismos de control de imagen; antes bien, unas y otras se aplicarán de manera simultánea, lo que podría dar lugar a problemas de coordinación entre las distintas regulaciones.

Un dato importante es que el Derecho digital contiene regulaciones específicas para la monitorización por imágenes, lo que no ocurre con el de la IA, que es general y

se ocupa a todo tipo de sistemas. Encontramos algunas reglas específicas para estos dispositivos, pero no una ordenación propia. Esto obliga a un esfuerzo de interpretación y adaptación mayor.

En la práctica, en muchos casos la utilización de cámaras inteligentes va a suponer una acumulación de obligaciones para los empleadores que las usan. También para las empresas que las construyen, comercializan a instalan, puesto que el Reglamento de IA les impone un conjunto elevado de deberes, a diferencia de una regulación de los aspectos digitales que los ignoraba más allá de alguna exigencia de carácter técnico, en normas con este carácter. En esta regulación, y como consecuencia de su naturaleza y objetivos, el foco no se pone sólo en quién utiliza el mecanismo de control sino también en quién se lo proporciona.

Un concepto importante en la aplicación del Derecho Algorítmico de la Unión Europea es el de "espacio de acceso público", que es definido como "*cualquier espacio físico al que pueda acceder un número indeterminado de personas físicas y con independencia de si es de propiedad privada o pública y de la actividad para la que pueda utilizarse el espacio*". No se consideran de esta naturaleza, según el Considerando 19 del Reglamento IA, los locales de empresas y fábricas, así como las oficinas y lugares de trabajo a los que solo se pretende que accedan los empleados y proveedores de servicios pertinentes. Esto condiciona el régimen jurídico de la utilización de los sistemas inteligentes de control de imágenes en numerosos centros de trabajo, aunque habrá otros en los que la presencia de clientes y usuarios dará lugar a esta calificación.

La integración de IA supone que los sistemas de control de imagen deban distinguirse según el riesgo, siguiendo la clasificación en cuatro niveles establecida por el Reglamento. Esto hace que resulten jurídicamente relevantes las finalidades y los usos que se les van a dar a las imágenes que se obtienen, que pueden ser, como se ha visto, múltiples, muchos más que los de control y vigilancia tradicionalmente asociados a este tipo de dispositivos.

El Reglamento de IA incluye entre las prácticas de IA prohibidas algunas que pueden estar entre en las que estamos estudiando. Dentro de los ocho supuestos contemplados por su artículo 5 están los sistemas se usan para inferir las emociones de una persona física en los lugares de trabajo y en los centros educativos (salvo los que estén justificados por motivos médicos o de seguridad). El Reglamento define el concepto de "sistema de reconocimiento de emociones" como aquellos que, utilizando la IA, distinguen o deducen las emociones o las intenciones de las personas físicas a partir de sus datos biométricos. Las imágenes obtenidas bien por circuito cerrado, bien a partir de los ordenadores de los empleados, son una gran fuente de información para ello.

Se excluyen de este concepto los estados físicos como el dolor o el cansancio, y la norma unioneuropea pone como ejemplo los sistemas utilizados para detectar el cansancio de los pilotos o conductores profesionales con el fin de evitar accidentes, lo que permite la analítica de imágenes en el marco de las políticas de seguridad y salud de los trabajadores, seguridad de los usuarios o incluso de bienestar físico general de la plantilla.

Si el sistema de análisis de las imágenes captadas en la empresa va a dar soporte a decisiones de recursos humanos o de producción, o incluso si va a adoptar las mismas decisiones, entonces nos encontraríamos en un supuesto de los contemplados en el Anexo III del Reglamento como de alto riesgo, que como es sabido incluyen los sistemas de IA destinados a ser utilizados para tomar "*decisiones que afecten a las condiciones de las relaciones de índole laboral o a la promoción o rescisión de relaciones contractuales de índole laboral, para la asignación de tareas a partir de comportamientos individuales o rasgos o características personales o para supervisar y evaluar el rendimiento y el comportamiento de las personas en el marco de dichas relaciones*". Idéntica calificación de sistemas de alto riesgo merecen para el Reglamento los de identificación biométrica remota, salvo aquellos cuya finalidad sea exclusivamente de verificación biométrica para confirmar que una persona física concreta es la persona que afirma ser; así como los utilizados para la categorización biométrica y el reconocimiento de emociones.

Tal calificación supone, como es sabido, la exigencia en cascada de una serie de medidas, como la necesidad de implantar un sistema de gestión de riesgos, la elaboración de una documentación técnica, prácticas de gobernanza y gestión de datos adecuadas, un nivel de transparencia suficiente, un registro automático de acontecimientos y una supervisión humana, además de exigencias concretas de precisión, solidez y ciberseguridad.

Va a cambiar radicalmente la naturaleza y el alcance del deber de información a la representación de la plantilla. La LOPDGDD impone en su artículo 89 el deber de la empresa que imponga sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores de informar con carácter previo a éstos y a sus representantes. La inclusión de la IA activa la aplicación del artículo 64.4 TRET, que como es sabido reconoce el derecho de comités de empresa y delegados de personal de ser informado por la empresa de los parámetros, reglas e instrucciones en los que se basan los algoritmos o sistemas de inteligencia artificial que afectan a la toma de decisiones que pueden incidir en las condiciones de trabajo, el acceso y mantenimiento del empleo, incluida la elaboración de perfiles. El conocido como "derecho de información algorítmico" existiría respecto de los sistemas de análisis de imágenes vinculados a aparatos para la captación de éstas. Igualmente se aplicaría el artículo 26.7 del Reglamento IA, que impone que antes de utilizar un sistema de IA de alto riesgo en el lugar de trabajo la empresa informe a los representantes de los trabajadores afectados de que estarán expuestos. Esta obligación se cumplirá siguiendo la regulación vigente en el Derecho de la Unión y nacional y conforme a las prácticas en materia de información a los representantes de los trabajadores. Así lo prevé el Considerando 90 del Reglamento, que señala que sus disposiciones son independientes de las que puedan existir en materia de información y consulta a los trabajadores o a sus representantes en virtud del Derecho o las prácticas nacionales.

El deber de información individual a los trabajadores afectados del artículo 89 LOPDGDD se completa con el previsto por el artículo 26.7 del Reglamento IA cuando el control de imágenes se caracteriza como de alto riego por su finalidad y alcance. Para la implementación de este deber la norma unioneuropea se remite igualmente al Derecho

aplicable en materia de información a los trabajadores, y a las prácticas nacionales que pudieran existir. Este derecho de información individual se completa con el derecho a recibir una explicación de decisiones que le afecten previsto en el artículo 86 del Reglamento, lo que supone que el trabajador afectado por una decisión basada en los resultados un sistema que integre IA y captación de imágenes tendrá derecho a obtener del responsable de su implantación, su empleador, explicaciones claras y significativas acerca del papel que ésta ha tenido en todo el proceso decisión y en su resultado.

En relación con la posibilidad de manipulación y generación de imágenes, que puedan hacerse pasar por las obtenidas por el sistema de videovigilancia de la empresa, el artículo 50 del Reglamento de Inteligencia Artificial indica que los proveedores del sistema velarán por que los resultados de salida del sistema de IA estén marcados en un formato legible por máquina y que sea posible detectar que han sido generados o manipulados de manera artificial. Además, éstos deberán velar por que sus soluciones técnicas sean eficaces, interoperables, sólidas y fiables en la medida en que sea técnicamente viable, teniendo en cuenta las particularidades y limitaciones de los diversos tipos de contenido, los costes de aplicación y el estado actual de la técnica generalmente reconocido, según se refleje en las normas técnicas pertinentes.

Finalmente, el uso de sistemas inteligentes de control de imágenes impone a las empresas el deber de alfabetización en materia de IA, en tanto sus empleados van a ser personas afectadas. Ello supone la adquisición de los conceptos necesarios para tomar decisiones con conocimiento de causa en relación con tales sistemas. El Reglamento de IA (Considerando 20) dispone además que la puesta en práctica general de medidas de alfabetización en materia de IA y la introducción de acciones de seguimiento adecuadas podrían contribuir a mejorar las condiciones de trabajo. En general la alfabetización en materia de IA incluye la sensibilización pública y la comprensión de los beneficios, los riesgos, las salvaguardias, los derechos y las obligaciones en relación con el uso de sistemas de IA.

6. Reflexiones conclusivas

La IA se está desarrollando y se está extendiendo por todos los entornos de trabajo, afectando a la forma en que se prestan los servicios y se organiza la actividad productiva. También al modo en que se supervisa a las personas que trabajan. Esto se hace, en muchos casos, integrando los dispositivos tradicionalmente utilizados en esta tarea con programas que optimizan su uso y manejan la información suministrada por éstos. La videovigilancia se convierte, así, en un control inteligente, que hace posible además una analítica de imágenes.

Este avance técnico incrementa los riesgos para los trabajadores, ya importantes en un control de por sí intrusivo. También mejora sus utilidades, que incluyen algunas que debemos considerar positivas para los trabajadores y la sociedad en su conjunto, en aspectos tales como la salud y seguridad laborales y la seguridad de las personas. Esto

obliga a un análisis del marco normativo de aplicación, que es lo que se ha pretendido hacer en estas páginas.

Pero los efectos de los avances algorítmicos en el control de imágenes van más allá, ya que se convierten en un instrumento adicional en el proceso de toma de decisiones previo al ejercicio del poder de dirección. De la misma manera en que, como dijimos al principio de estas páginas, la revolución tecnológica está haciendo cambiar el peso real de los dos principales poderes empresariales en las relaciones laborales, el de dirección y el de control, potenciando la supervisión de personas que prestan sus servicios con mayor autonomía, la utilidad de estos mecanismos está mutando. Junto a la original de velar por el cumplimiento de las obligaciones laborales de los empleadores, las nuevas utilidades están permitiendo que sean instrumentales también para el ejercicio del poder de dirección. Y ello porque dan soporte a decisiones empresariales de todo tipo con la mejora de la información obtenida, y con el tratamiento de ésta para identificar patrones y pautas, predecir acontecimientos y proponer actuaciones.

La videovigilancia inteligente es útil también para una función de creciente importancia, la del control del cumplimiento de obligaciones de empresarios y trabajadores, porque puede orientarse a la identificación de posibles violaciones de éstas. En momentos en los que el compliance adquiere una mayor relevancia en las empresas, este apoyo merece ser destacado.

Estos mecanismos suponen una zona de confluencia entre el Derecho Digital tradicional y el Derecho Algorítmico, en la medida en que ambos sectores del ordenamiento resultan aplicables. La acumulación de obligaciones que se deriva de ello no generará, a mi juicio, grandes problemas, en la medida en que resultan compatibles. Unos mismos instrumentos aparecen en las dos regulaciones, aunque la de la IA va más allá y contiene otros de nueva creación. El origen común y el hecho de compartir unas mismas finalidades de tutela de las personas explica esta compatibilidad. Sí será necesario, por supuesto, una mayor coordinación. Seguramente también más avances en la regulación algorítmica, que como se dijo en su momento no ha producido hasta ahora reglas específicas para el mecanismo de control que nos ocupa; es de esperar que comencemos a verlas a medida que la utilización de estos productos se vaya extendiendo.

Estos avances resultan especialmente recomendables, a mi juicio, porque la videovigilancia inteligente debe disponer un marco regulatorio adecuado que le permita extenderse y alcanzar todas sus posibilidades, evitando a la vez los riesgos para las personas que trabajan sometidos a ella. Estamos en un momento de transición tecnológica, que está siendo acompañado de una reordenación normativa que, en esta materia como en otras, debe esforzarse para mantenerse a la altura.