COMENTARIOS LABORALES

El impacto de las nuevas tecnologías en las relaciones laborales*

Pedro Morales Corrales (†)**
Universidad de Lima, Lima, Perú

Alejandro Morales Cáceres***
Universidad de Lima, Lima, Perú
alejandro.morales@tytl.com.pe

Recibido: 24/1/2021 Aprobado: 1/2/2021
doi: https://doi.org/10.26439/iusetpraxis2021.n052.5072

RESUMEN. En los últimos años, el desarrollo de las nuevas tecnologías ha venido transformando la forma de producir y trabajar, lo que indudablemente impacta en el derecho laboral. En primer lugar, se realiza una explicación sobre el tratamiento de las plataformas digitales en el derecho laboral. A continuación, se expone cómo es que la implementación de nuevas tecnologías como las cámaras de videovigilancia, los dispositivos de geolocalización y la fiscalización de los dispositivos corporativos impactan en la privacidad de los trabajadores. Luego, se plantean los desafíos del teletrabajo en torno al derecho a la protección de los datos personales. Finalmente, se analiza el derecho a la desconexión laboral.

PALABRAS CLAVE: derecho laboral / tecnología / plataformas digitales / privacidad / teletrabajo / desconexión laboral

* Este artículo reúne algunos trabajos publicados en el 2020 por Alejandro Morales Cáceres sobre las nuevas tecnologías y el derecho laboral, que hoy adquieren gran relevancia. Se han integrado bajo la atenta mirada de Pedro Morales Corrales y de Alejandro Morales Cáceres para ofrecer un panorama actual sobre este tema.

** Abogado por la Universidad Nacional Mayor de San Marcos. Magíster en Derecho por la Universidad de San Martín de Porres. Expresidente de la Sociedad Peruana de Derecho y Trabajo y de la Seguridad Social. Profesor de Derecho Laboral Individual en la Universidad de Lima. Socio del Estudio Echecopar asociado a Baker & McKenzie International.

*** Abogado por la Universidad de Lima. Máster en Derecho de las TIC, Redes Sociales y Propiedad Intelectual en ESADE Business & Law School. Jefe de prácticas de Derecho Comercial I y II en la Universidad de Lima. Jefe del Área de Derecho y Nuevas Tecnologías en el Estudio Torres y Torres Lara Abogados.

THE IMPACT OF NEW TECHNOLOGIES ON EMPLOYMENT RELATIONSHIPS

ABSTRACT. In recent years, the development of new technologies has been transforming the way of producing and working, which undoubtedly has an impact on labor law. First, the authors explain the treatment of digital platforms in labor law. Next, they illustrate how the implementation of new technologies such as video surveillance cameras, geolocation devices and the control of corporate devices affects the privacy of employees. Then, they present the challenges of remote working in relation to the right to personal data protection. Finally, they analyze the right to disconnect from work.

KEYWORDS: labor law / technology / digital platforms / privacy / remote working / right to disconnect

INTRODUCCIÓN

En los últimos años, hemos sido testigos de la profunda transformación de la sociedad, producida al compás de los avances tecnológicos. Las nuevas tecnologías de la información y la comunicación han pasado a formar parte de nuestros hábitos diarios, cambiando nuestra forma de relacionarnos, de pensar y hasta de vivir.

No cabe duda de que la irrupción de nuevas tecnologías en nuestras sociedades está generando una serie de cambios en la economía, en el consumo, en los negocios y en el mundo del trabajo, cuya profundidad y trascendencia nos coloca frente al surgimiento de una nueva época signada por el avance exponencial e incesante del conocimiento.

La tecnología y el acceso a internet nos han facilitado la vida, el conocimiento y las comunicaciones, y nos permiten estar permanentemente conectados, lo que supone sin duda una ventaja o un avance. Si bien la actividad productiva se ha visto enormemente facilitada y agilizada, es importante resaltar que estas indudables ventajas no han evitado que la implantación generalizada de las nuevas técnicas, particularmente, en los sistemas de gestión del personal, haya puesto de relieve su potencial lesividad para la esfera de los derechos fundamentales de la persona y, en concreto, para algunos de los aspectos más vulnerables de la personalidad: la dignidad e intimidad del trabajador.

En efecto, esta nueva realidad pone en cuestión, con mucha más intensidad que antes, la vigencia de los derechos fundamentales de los trabajadores en el seno de las empresas y en el desarrollo de sus actividades productivas. Este nuevo contexto trae consigo una serie de inquietudes tales como (i) la "uberización" del trabajo; (ii) la fiscalización y control laboral a través de las nuevas tecnologías por parte de los empleadores a los trabajadores; (iii) la importancia creciente que, previsiblemente, asumirá a futuro el teletrabajo en la empresa; (iv) la libertad de expresión de los trabajadores a través de las redes sociales; (v) la dimensión reforzada que debe asumir el derecho a la protección de datos en el seno de la relación laboral.

¿EXISTE RELACIÓN LABORAL EN LAS PLATAFORMAS DIGITALES?

Plataformas digitales y relación laboral[1]

La irrupción de las plataformas digitales es uno de los cambios más importantes en la economía global, pues su aparición supone que las personas puedan conseguir en línea a conductores, mensajeros, repartidores de comida, profesores particulares, entrenadores personales, gasfiteros, entre otros servicios, en cuestión de segundos.

1 Adaptado del artículo "Relación laboral en las plataformas digitales", por A. Morales Cáceres, 15 de febrero del 2020, *Agnitio*. Todos los derechos reservados [2020] por AGNITIO. Adaptado con permiso del autor.

Desde un punto de vista económico, lo que sucede es que un grupo de personas se encuentra dispuesto a ofrecer un determinado servicio y se apalanca, tecnológicamente, de estas sociedades titulares de estas aplicaciones tecnológicas, quienes los contactan con miles de consumidores. La doctrina estadounidense la conoce como *Uber economy*, que consiste en tomar una prestación de un servicio, tradicionalmente realizada por un trabajador, y descentralizarla a través de internet hacia un gran número de personas.

Este nuevo modelo económico supone un reto jurídico, pues no es del todo claro si estas nuevas formas de trabajo atípicas conducen a la creación de una relación laboral, en donde las plataformas digitales como Uber, Cabify o Glovo podrían ser consideradas como empleadores de aquellos que prestan los servicios. Actualmente, en el Perú existen iniciativas legislativas[2] que pretenden regular la relación entre la plataforma digital y el prestador del servicio, enmarcándola en una relación laboral con el objetivo de proteger al segundo. Por otro lado, tenemos a los titulares de las plataformas, quienes niegan la condición de empleador y se definen como intermediarias entre los proveedores de servicios y sus clientes (consumidores finales). Ante esta "zona gris" del derecho, ¿podría un chofer de Uber o Cabify reclamar una indemnización laboral a estas plataformas? ¿Acaso un *rider* de Glovo o Rappi son trabajadores de dichas empresas?

Para responder estas preguntas, debemos analizar si es que en cada caso se presentan los elementos esenciales de la relación laboral. Esto es, si existe una prestación personal de servicios, si se paga una retribución económica y si es que hay subordinación. Es claro que los dos primeros supuestos se cumplen, pues un *rider* presta el servicio de un motorizado y, por ello, recibe una comisión. Lo mismo sucede con un chofer de Easy Taxi, quien es el que conduce el vehículo y, como consecuencia de ello, percibe una retribución a cambio. Sin embargo, la cuestión fundamental radica, entonces, en determinar si existe o no subordinación laboral.

La subordinación es el vínculo de sujeción que tiene el empleador frente al trabajador en una relación laboral. De este surge el poder de dirección, que es la facultad del empleador de dirigir, fiscalizar y, en última instancia, sancionar al trabajador. Este es el elemento distintivo que permite diferenciar al contrato de trabajo de un contrato de prestación de servicios, en donde se brindan servicios de forma autónoma e independiente. En ese sentido, se debe analizar si quien pone a disposición la plataforma digital lleva a cabo un control comercial o si, en cambio, cruza esta línea y se convierte en un control laboral. En términos prácticos, lo que se debe analizar es si el titular de la plataforma es

2 Actualmente, existen dos proyectos de ley: el Proyecto de Ley N.° 4144/2018-CR, que regula la labor del trabajador por plataforma digital; y el Proyecto de Ley N.° 4243/2018-CR del empleo digno, que regula a los trabajadores de plataformas digitales.

quien determina dónde se presta el servicio, cómo se presta el servicio, de qué manera se presta el servicio y en qué momento se presta el servicio.

Asimismo, la Organización Internacional del Trabajo (OIT), en el artículo 13 de la Recomendación N.° 198 sobre la relación de trabajo (2006), establece indicios específicos que permitan determinar la existencia de una relación de trabajo. Entre esos indicios se encuentran los siguientes:

a. El hecho de que el trabajo se realiza según las instrucciones y bajo el control de otra persona; que el mismo implica la integración del trabajador en la organización de la empresa; que es efectuado única o principalmente en beneficio de otra persona; que debe ser ejecutado personalmente por el trabajador, dentro de un horario determinado, o en el lugar indicado o aceptado por quien solicita el trabajo; que el trabajo es de cierta duración y tiene cierta continuidad, o requiere la disponibilidad del trabajador, que implica el suministro de herramientas, materiales y maquinarias por parte de la persona que requiere el trabajo.

b. El hecho de que se paga una remuneración periódica al trabajador; de que dicha remuneración constituye la única o la principal fuente de ingresos del trabajador; de que incluye pagos en especie tales como alimentación, vivienda, transporte u otros; de que se reconocen derechos como el descanso semanal y las vacaciones anuales; de que la parte que solicita el trabajo paga los viajes que ha de emprender el trabajador para ejecutar su trabajo y el hecho de que no existen riesgos financieros para el trabajador.

Tratamiento de las plataformas digitales en el Perú

En una reciente decisión, el Tribunal de la Sala Especializada en Defensa de la Competencia del Indecopi, a través de la Resolución N.° 0084-2020/SDC-INDECOPI (2020), declaró que Uber es una empresa de tecnología y no de transporte, por lo que tampoco realiza competencia desleal contra los servicios de transporte público. Se advierte que Uber se dedica exclusivamente a conectar usuarios taxistas con usuarios solicitantes de servicios de transporte, no constituyendo prestación directa del servicio de transporte.

En efecto, las empresas como Uber, Glovo, Cabify, Rappi, Airbnb, eBay, entre otras, son ejemplos típicos de plataformas digitales. Para entender este concepto, primero debemos entender qué es un modelo lineal. Este modelo es aquel que crea valor de forma lineal a sus clientes. Es decir, se crea valor desde el primer cliente hasta el último. Por ejemplo, Subaru vendiendo carros, Ripley vendiendo ropa, un estudio de abogados prestando servicios a sus clientes. En un modelo lineal, hay un intercambio de dinero por un producto o servicio. El empresario es propietario de los medios productivos tradicionales.

En cambio, en el modelo de plataformas digitales, existen dos lados que se conectan en la plataforma: la oferta y la demanda. La plataforma digital crea valor para ambos lados; sin embargo, no necesariamente hay valor al inicio, pues para ello se necesita de una masa crítica en ambos lados. Uber no sería atractivo si solo tuviese personas que demandan transporte privado, pero no contara con choferes afiliados a la aplicación. Airbnb no sería atractivo si solo hubiera oferta de alojamientos, pero no contara con usuarios que demanden estos. El valor crece en la medida que haya más usuarios, tanto del lado de la oferta como de la demanda. Por ejemplo, Tinder aporta más valor en la medida que hay más usuarios. Facebook tiene más valor si hay más personas que utilizan esta red social. Sin masa crítica, no hay valor (lo que se conoce como *network effect*). Las plataformas digitales no necesitan ser propietarias de los medios productivos tradicionales. Es decir, se apalancan de forma tecnológica para ser un intermediario que conecta a usuarios.

En ese sentido, es acertado que la Sala de Competencia (Resolución N.° 0084-2020/SDC-INDECOPI, 2020) considere a Uber como una plataforma digital de transporte de pasajeros; es decir, es un servicio de intermediación, "el cual tiene como finalidad poner en contacto dos demandas: la demanda del servicio de transporte (conductores) y la demanda de pasajeros que requieren su traslado físico hacia otro lugar". Por su parte, "el conductor del vehículo (chofer) es quien presta el referido servicio de taxi" y, por lo tanto, quien debe cumplir con las autorizaciones correspondientes.

Asimismo, según la Sala de Competencia (Resolución N.° 0084-2020/SDC-INDECOPI, 2020), "el éxito de una plataforma no está determinado únicamente por el número de miembros o interacciones en los que participan, sino también por su calidad". Así, una plataforma podrá utilizar reglas de gobernanza (que rigen el acceso, el uso y la convivencia dentro de la plataforma) para resolver ciertas fallas de mercado. Estas reglas incluyen "ciertos filtros" antes de permitir el acceso a determinados proveedores, con la finalidad de que únicamente puedan ingresar aquellos agentes económicos que brinden un servicio y/o producto idóneo (por ejemplo, revisar los antecedentes penales, el récord de multas que Uber aplica para sus socios conductores). En palabras de la Sala de Competencia, estas reglas de gobernanza son propias de un administrador de plataforma.

En ese sentido, siguiendo lo señalado por el Indecopi, una plataforma digital, al ser un intermediario, no podría ser considerado como empleador, pues simplemente funciona como un nexo para que los que prestan el servicio subyacente consigan clientes de una forma más sencilla. Además, aquellos filtros, en teoría, no pueden ser considerados como una selección de personal de trabajo, sino más bien como un filtro comercial. Aunado a ello, lo lógico sería no confundir el control empresarial (como el que un franquiciante puede tener con un franquiciado) con el control laboral. Sin embargo, es importante manifestar que a la fecha no existe ningún pronunciamiento sobre alguna

autoridad laboral al respecto, es por ello que es de vital importancia revisar criterios jurisprudenciales de ordenamientos jurídicos internacionales.

Tratamiento de las plataformas digitales en el extranjero

A nivel internacional, encontramos que no hay un criterio uniforme sobre si existe relación laboral o no entre las plataformas digitales y aquellos que prestan el servicio. A continuación, presentaremos una serie de casos que analizan este aspecto.

Caso Deliveroo[3]

El 1 de junio del 2018, el Juzgado de lo Social N.° 6 de Valencia determinó que la relación que une a la plataforma digital Deliveroo y a uno de sus *riders* no es una relación mercantil como locador de servicios, sino una laboral como asalariado por los siguientes motivos:

> – La empresa es la titular de la plataforma virtual, careciendo los *riders* de organización empresarial alguna y estando obligados a descargar la correspondiente aplicación e integrarse en un grupo de Telegram.
>
> – La empresa geolocaliza en todo momento al trabajador, llevando un control de tiempos de cada reparto, utilizando la tecnología como un mecanismo de fiscalización laboral.
>
> – La empresa imparte las instrucciones y fija los tiempos y normas de comportamiento que el *rider* debe seguir cuando lleva a cabo el reparto. Asimismo, es la plataforma quien decide, dentro de las franjas que previamente el trabajador escoge, cuál es su horario.
>
> – La empresa fija los precios de los servicios que realiza el trabajador.
>
> – Los *riders*, dentro de su horario, carecen de libertad para rechazar pedidos. De hecho, el supuesto enjuiciado trae su causa precisamente en la extinción derivada de los reiterados rechazos y faltas de disponibilidad por parte del trabajador para realizar entregas.
>
> – Es la empresa quien establece las condiciones de los restaurantes adheridos y de los clientes a los que presta sus servicios, desconociendo el trabajador cuáles son estos restaurantes, así como la identidad de los clientes que solicitan el servicio.
>
> – Por último, los *riders* son utilizados como la marca de Deliveroo, dado que son "la imagen de la compañía de cara al cliente". (Villaverde, 7 de junio del 2018, párrs. 4-10)

3 Adaptado del artículo "Relación laboral en las plataformas digitales", por A. Morales Cáceres, 15 de febrero del 2020, *Agnitio.* Todos los derechos reservados [2020] por AGNITIO. Adaptado con permiso del autor.

Cabe señalar que, el 22 de julio del 2019, el Juzgado de lo Social N.° 19 de Madrid le dio la razón al órgano de Inspección de Trabajo de la Seguridad Social en Madrid, señalando, de igual manera que en el caso anterior, que los *riders* de Deliveroo son trabajadores y no "falsos autónomos", debido a que los repartidores esencialmente han ejecutado un trabajo personal en unas condiciones organizadas y dirigidas por la empresa, que es la única que controla la marca Deliveroo, su aplicación informática y toda la información que se desprende de ella. Esta sentencia fue confirmada el 17 de enero del 2020 por el Tribunal Superior de Justicia de Madrid (TSJM, 2020) indicando que los *riders* de Deliveroo son falsos autónomos (falsos locadores de servicios); así dio la razón a la Seguridad Social y confirmó la primera decisión de la Inspección de Trabajo.

Caso Glovo[4]

El 3 de septiembre del año 2018, el Juzgado de lo Social N.° 39 de Madrid señaló que la relación entre la plataforma digital y sus *glovers* no es de naturaleza laboral, sino de naturaleza mercantil; se trata, por lo tanto, de verdaderos profesionales autónomos (locadores de servicios). En este caso, se concluyó que la prestación de servicios desarrollada por el *rider* no podía clasificarse como laboral por no existir subordinación por las siguientes razones:

> – El *rider* no estaba sujeto a jornada ni horario, puesto que él decidía la hora en la que deseaba trabajar y los pedidos, pudiendo incluso rechazarlos una vez aceptados. Asimismo, el repartidor tenía dominio completo de su actividad, dado que decidía con libertad la ruta a seguir por cada pedido y su forma de realización.
>
> – Glovo no ejerce ningún poder disciplinario sobre el *rider*, por lo que este se autoorganiza, lo que es una característica propia de una relación mercantil.
>
> – El *rider* asume el riesgo de cada pedido, lo que indica que este no está sometido a la estructura organizativa interna de la empresa. Las principales herramientas de trabajo (moto y teléfono celular) son propiedad del trabajador.
>
> – La retribución que percibe el *rider* depende directamente de la cantidad de recados que haga, siendo distinta de un mes a otro.
>
> – Glovo no exige justificaciones a los *riders* por sus ausencias, sino que estas simplemente deben comunicarse.
>
> – Finalmente, no existe pacto de exclusividad entre las partes, de manera que el *rider* puede prestar servicios para otras empresas. (Villaverde, 1 de octubre del 2018, párrs. 3-8)

4 Adaptado del artículo "Relación laboral en las plataformas digitales", por A. Morales Cáceres, 15 de febrero del 2020, *Agnitio*. Todos los derechos reservados [2020] por AGNITIO. Adaptado con permiso del autor.

Podemos apreciar que una de las diferencias más llamativas radica en la diferente concepción que en las sentencias se tiene acerca de la estructura empresarial. En el caso de Glovo, entiende la jueza que la moto y el celular son las principales herramientas de trabajo. Sin embargo, en la sentencia de Deliveroo, se afirma que, pese a que el teléfono móvil y la bicicleta son propiedad del repartidor, este carece de organización empresarial, dado que lo relevante, a efectos de organización de la actividad empresarial, es la aplicación informática, propiedad de la plataforma digital. Asimismo, mientras que el sistema de geolocalización de los *riders* de Deliveroo fue considerado un elemento de dependencia de los repartidores frente a la plataforma digital, propio de una relación laboral, en el caso de Glovo, a juicio de la magistrada-jueza, este no es un instrumento de control, sino la forma de contabilizar el kilometraje para su posterior abono en la factura. Estas sentencias nos demuestran la diferente valoración que subjetivamente realizan los jueces respecto a las circunstancias que rodean la prestación del servicio.

Caso Uber Reino Unido[5]

El 10 de noviembre del año 2017, el Employment Appeal Tribunal (EAT) del Reino Unido resolvió el recurso de Uber BB, Uber London Ltd. y Uber Britannia Ltd. contra la sentencia del London Central Employment Tribunal (ET) de octubre del 2016, que reconocía a los conductores de Uber su condición de *workers*. Cabe precisar que en el ordenamiento jurídico del Reino Unido existen tres categorías para clasificar la prestación de servicios realizada por personas naturales, a saber:

> – *Employee:* figura equivalente al trabajador en la legislación peruana, al que le resulta de aplicación toda la normativa laboral: beneficios laborales, indemnización por despido, vacaciones, etc.
>
> – *Self-employed* o *contractor:* figura equivalente a nuestro trabajador autónomo o locador de servicios, cuya relación no tiene naturaleza laboral, sino civil o mercantil.
>
> – *Worker:* figura inexistente en España, se refiere a personas trabajadoras con (a) contrato de trabajo o (b) contrato de cualquier otro tipo, incluso verbal, en el que se compromete a prestar servicios personalísimos, cuya prestación puede ser irregular en el tiempo. Si bien al *worker* le resulta de aplicación, entre otros, el salario mínimo, las vacaciones retribuidas, los límites de tiempo de trabajo... esta figura no tiene acceso a otros derechos laborales, como a una indemnización por despido o al preaviso por extinción. (Agote, 14 de noviembre del 2017, párrs. 3-5)

5 Adaptado del artículo "Relación laboral en las plataformas digitales", por A. Morales Cáceres, 15 de febrero del 2020, *Agnitio*. Todos los derechos reservados [2020] por AGNITIO. Adaptado con permiso del autor.

El EAT, en su sentencia, declara la condición de *worker* a los choferes de Uber, pues existen indicios de un vínculo laboral, tales como la monitorización del conductor, la imposición de normas o de un precio máximo por servicio, consecuencias del incumplimiento de aquellas, asunción de Uber de determinados gastos del conductor (limpieza), el hecho de que los choferes conducen bajo una marca ajena y que, además, Uber publicita su marca, no a los conductores o prestadores de servicios, lo cual imposibilita el crecimiento de sus negocios, así como el poder que tiene Uber de modificar unilateralmente los términos y condiciones del contrato. Sin embargo, reconoce que esta relación se encuentra contextualizada por la circunstancia de la libertad del conductor de prestar sus servicios cuando quiera, sin sujeción a compromiso de tiempo previo. A diferencia de la relación laboral tradicional, la mayoría de prestadores de servicios a través de plataformas *on demand* definen su horario de trabajo, su tiempo de descanso, su jornada e incluso sus vacaciones. En ese sentido, se puede decir que el chofer de Uber goza de cierta autonomía, por lo que no se podría hablar de subordinación laboral en términos tradicionales.

Sin embargo, en el Perú no existe esta figura, que es una suerte de híbrido legal entre el trabajador y el locador de servicios. Por eso, la realidad hace que muchas veces sea difícil encajarla, ya sea como "trabajador" o como "locador".

Caso Hilfr en Dinamarca

> El 10 de abril del año 2018, se firmó el que sería, según reivindican las partes, el primer convenio en el ámbito de la *gig economy* de una plataforma digital. Hilfr.dk, una empresa danesa dedicada a poner en contacto a limpiadores y usuarios, llegó a un acuerdo pionero con 3F, el principal sindicato del país escandinavo, cuya firma contó incluso con la presencia del primer ministro. (Bel y García, 2018, párr. 1)

El acuerdo distingue entre trabajadores autónomos y Super Hilfr, siendo estos últimos los beneficiarios de las condiciones pactadas. Los limpiadores adquieren la condición de Super Hilfr una vez trabajadas cien horas a través de la plataforma, si bien aquellos que no alcancen este umbral podrán solicitar igualmente su inscripción en dicha categoría.

Los limpiadores Super Hilfr pasan a tener reconocidos determinados derechos laborales:

- Una retribución mínima de 141 coronas (19 euros) por hora de servicio
- Cotizaciones al seguro de pensiones
- Devengo del pago de vacaciones
- Prestación por enfermedad

Esta es una prueba de cómo el mismo mercado puede llevar a que las partes regulen mejor sus necesidades (Bel y García, 2018, párrs. 8-12).

Caso Tortas Gaby en el Perú[6]

Si bien este caso no está relacionado con una plataforma digital (ni en el extranjero), es bastante interesante puesto que señala que una persona que brinda el servicio de repartición de tortas no se encuentra en una relación laboral. El 13 Juzgado Laboral de Lima determinó que esta relación era comercial, pues el *rider* utilizaba su propia movilidad y corría con gastos tales como el de gasolina, reparaciones y seguro. Asimismo, él era quien decidía cuándo realizar mantenimiento a su motocicleta. Finalmente, su ingreso dependía exclusivamente de la cantidad de pedidos y las tarifas según los distritos.

En ese sentido, si en este caso se ha determinado que no existe vínculo laboral, en el caso de las plataformas digitales sería inclusive más difícil poder establecer la naturaleza jurídica de la relación.

Más allá del derecho laboral: los *riders* o *drivers* como empresarios[7]

"Cada uno ve lo que quiere ver", dice el popular refrán. La discusión de un abogado laboralista siempre se centrará en si existe o no vínculo laboral, pues, tal como dijo el filósofo británico Aldous Huxley, "hay cosas conocidas y hay cosas desconocidas, y en el medio están las puertas de la percepción". Por lo tanto, es natural que se centren en este análisis. Sin embargo, abogados de otras ramas del derecho, probablemente, lleguen a conclusiones distintas, porque la percepción siempre precede a la realidad. En ese sentido, un abogado comercial o tributario podría identificar a un *rider* o a un chofer de estas plataformas digitales como un empresario (Morales Cáceres, 15 de febrero del 2020, párr. 41)

Recordemos que un empresario es el titular de la empresa. Es el sujeto de derecho que organiza el capital y trabajo a fin de producir bienes o proveer servicios en favor de la sociedad. Las características que definen a un empresario son las siguientes:

- *Gestión*: capacidad de administrar y organizar el capital y el trabajo.
- *Riesgo*: el empresario es responsable de todos los daños que su actividad jurídica pueda derivar.
- *Resultado económico*: dado que en el ejercicio económico pueden producirse ganancias o pérdidas, el empresario asume las consecuencias de su explotación económica.

6 Adaptado del artículo "Relación laboral en las plataformas digitales", por A. Morales Cáceres, 15 de febrero del 2020, *Agnitio*. Todos los derechos reservados [2020] por AGNITIO. Adaptado con permiso del autor.

7 Adaptado del artículo "Relación laboral en las plataformas digitales", por A. Morales Cáceres, 15 de febrero del 2020, *Agnitio*. Todos los derechos reservados [2020] por AGNITIO. Adaptado con permiso del autor.

De acuerdo con esta concepción, se puede considerar que tanto los *riders* como los choferes pueden ser calificados como empresarios, pues ellos gestionan su capital (dinero, vehículo, teléfono celular) y disponen su tiempo combinándolo con su habilidad (trabajo) para poder llevar a cabo el servicio. Ellos son los que deciden cuánto tiempo trabajar, las horas y los días, así como la elección de la gasolina, el período de mantenimientos, las mejoras del vehículo, la elección del seguro, etcétera. Igualmente, son los responsables de todos los daños que sucedan mientras realizan el servicio, en caso de que sufran un accidente. Finalmente, de su actividad económica depende si ellos generan utilidades o pérdidas.

Inclusive, desde un punto de vista tributario, existen cinco categorías de impuesto a la renta. Las dos primeras corresponden a rentas de capital, mientras que la cuarta y la quinta categoría pertenecen a las rentas de trabajo. En las rentas de capital, se grava todas las ganancias que se obtengan por la explotación de un capital (bien mueble, inmueble, acciones, bonos, propiedad industrial, etcétera), mientras que en las rentas de trabajo se grava las ganancias que se consigan por trabajos dependientes o independientes. En cambio, la renta de tercera categoría, llamada también *renta empresarial*, grava todas aquellas ganancias que se generen como consecuencia de una actividad empresarial, esto es, aquellas que se producen por la participación conjunta de la inversión del capital y el trabajo. ¿Uber puede funcionar sin un chofer? No. ¿Puede funcionar sin un vehículo o un celular? Tampoco. En estos modelos tanto el capital como el trabajo son igual de importantes.

A nivel europeo, en algunas de las sentencias antes mencionadas, se decía que el prestador del servicio tenía nulas posibilidades de crecimiento como empresario, pues todo el *marketing* y la publicidad iba para la marca de la plataforma digital, mas no para quien prestaba el servicio. Sin embargo, esto también ocurre con las microfranquicias o las agencias mercantiles, cuya naturaleza jurídica es mercantil. En este punto, los jueces hacen una valoración subjetiva que limita el ingenio empresarial, pues me parece completamente factible que un empresario inicie su negocio prestando directamente sus servicios personales, pero, a medida que pase el tiempo, este podrá invertir en más vehículos y arrendarlos para que nuevos choferes lo empleen en estas plataformas. Es decir, el nivel de crecimiento depende exclusivamente de lo que se trace la persona.

¿Empleados o empresarios?

Tal como se ha podido apreciar, existe mucha controversia a nivel internacional en cuanto a determinar si los titulares de las plataformas digitales son empleadores de aquellos que proveen el servicio subyacente. Entendiendo a la plataforma como un mero intermediario, consideramos que no debería existir una relación laboral. Sin

embargo, lo más apropiado es analizar caso por caso, pues existe una línea gris entre el control comercial y el control laboral. Para ello, al momento de analizar cada caso debemos preguntarnos si el titular de la plataforma determina dónde se presta el servicio, cómo se presta el servicio, de qué manera se presta el servicio y cuándo se presta el servicio. Si se puede probar ello, nos encontraremos ante una relación laboral. De lo contrario, la relación será meramente comercial.

LA VIDEOVIGILANCIA EN EL CENTRO LABORAL

Cada vez es más frecuente la instalación de cámaras de vigilancia en los centros de trabajo de las empresas por motivos de seguridad. Sin embargo, cabe preguntarse si esta medida podría ser considerada ilícita en algunos supuestos. ¿Un empleador puede colocar de forma arbitraria cámaras de seguridad por todo el centro de trabajo? Es necesario precisar que un sistema de videovigilancia, en buena cuenta, es una estructura de captación de imágenes, e incluso sonido, en un espacio concreto, cuyas imágenes puedan ser visualizadas, grabadas y/o reproducidas.

Esto significa que un sistema de videovigilancia es un banco de datos personales, pues tanto la imagen como la voz, en la medida que identifiquen o puedan identificar a una persona, constituyen datos de carácter personal y pueden ser objeto de tratamiento para diversas finalidades. Si bien la más común consiste en utilizar las cámaras con la finalidad de garantizar la seguridad de personas, bienes e instalaciones, también pueden usarse con otros fines, como la investigación, la asistencia sanitaria o el control de la prestación laboral por parte de los trabajadores. Por ello, la instalación de estos sistemas no debe ser algo arbitrario o casual, sino que debe responder a fines concretos y justificados.

¿Puede un empleador utilizar esta tecnología para fiscalizar a sus trabajadores? Al respecto, el artículo 9 del Decreto Supremo N.° 003-97-TR, Texto Único Ordenado del Decreto Legislativo N.° 728, Ley de Productividad y Competitividad Laboral (1997), señala que el empleador se encuentra facultado a realizar controles y medidas para vigilar el ejercicio de las actividades laborales de sus trabajadores. En ese sentido, el empleador podrá adoptar las medidas que estime oportunas de vigilancia y control a fin de verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales[8].

En efecto, la mencionada ley le reconoce atribuciones o facultades al empleador, como son (a) la facultad directiva, es decir, la potestad de impartir órdenes al trabajador para que realice una adecuada prestación de sus servicios; (b) la facultad fiscalizadora que consiste en supervisar el cumplimiento de las obligaciones que surgen del contrato de

8 Adaptado del artículo "Videovigilancia en el centro de trabajo", por A. Morales Cáceres, 22 de enero del 2020, *Agnitio*. Todos los derechos reservados [2020] por AGNITIO. Adaptado con permiso del autor.

trabajo; (c) la facultad disciplinaria expresada en la posibilidad que tiene el empleador de sancionar las acciones u omisiones que signifiquen el incumplimiento de las labores encomendadas o actos de indisciplina en el trabajo (STC. Exp. N.º 02208-2017-PA/TC, 2020).

Si bien el empleador goza de esa facultad de control, esto no significa que se encuentre exento de cumplir con la Ley de Protección de Datos Personales, dado que almacenar imágenes —o, en su defecto, voces— en un sistema de videovigilancia supone un tratamiento de datos de carácter personal y, por tanto, el empresario debe ajustarse a los principios y obligaciones que establece la normativa de protección de datos.

El hecho de que se tenga que cumplir con la Ley de Protección de Datos Personales no significa que se deba solicitar el consentimiento de los trabajadores para poder utilizar el sistema de videovigilancia y grabarlos, puesto que, tal como se explicó previamente, el tratamiento de los datos personales del empleador para fines de control empresarial no requiere del consentimiento del trabajador, por encontrarse en el marco de la ejecución de la relación contractual, en razón de lo dispuesto por el numeral 5 del artículo 14 de la Ley de Protección de Datos Personales, Ley N.° 29733 (2011). Por lo tanto, el empleador puede tratar los datos personales de sus trabajadores para fines laborales, sin el consentimiento de los mismos.

Asimismo, el tratamiento de los datos de los trabajadores se limita a las finalidades propias del control y supervisión de la prestación laboral, de tal forma que no pueden utilizarse los medios o el sistema de videovigilancia para fines distintos[9], salvo que se cuente con el consentimiento del trabajador o se trate de alguna de las excepciones señaladas en el artículo 14 de la Ley de Protección de Datos Personales, Ley N.° 29733 (2011), tales como cuando la empresa requiera dar tratamiento a sus datos en cumplimiento de una norma u obligación legal, y para la preparación y/o ejecución de una relación contractual de la que el trabajador forma parte, entre otras.

Sin embargo, a efectos de acatar la normativa de protección de datos personales, el empleador debe cumplir con informar a sus trabajadores sobre las cámaras de videovigilancia de forma previa. Así, el hecho de no ser necesario el consentimiento de los trabajadores no significa que el empleador no deba cumplir con informar al trabajador sobre el tratamiento de los datos personales captados mediante sistemas de videovigilancia, lo que puede realizarse a través de carteles informativos, ello sin perjuicio de informar de manera individualizada a cada trabajador del tratamiento que se realizará de sus datos personales.

9 De acuerdo con la Directiva N.° 01-2020-JUS/DGTAIPD, son fines legítimos para el control y la supervisión de la prestación laboral, la protección de bienes y recursos del empleador; la verificación de la adopción de medidas de seguridad en el trabajo; y aquellos otros que la legislación laboral y sectorial prevea.

Al respecto, la Directiva N.° 01-2020-JUS/DGTAIPD, directiva de videovigilancia emitida por la Autoridad Nacional de Protección de Datos Personales, establece qué es lo que deben contener estos carteles informativos. Cada acceso a la zona videovigilada debe tener un cartel o anuncio visible con fondo amarillo o cualquier otro que contraste con el color de la pared y que lo haga suficientemente visible. Su contenido mínimo debe indicar (i) la identidad y domicilio del empleador; (ii) ante quién y cómo se pueden ejercitar los derechos establecidos en la Ley de Protección de Datos Personales; (iii) el lugar donde puede acceder a una política de privacidad que le informe sobre el tratamiento de sus datos personales conforme al artículo 18 de la referida ley (Directiva N° 01-2020-JUS/DGTAIPD, 2020). Este documento informativo debe estar disponible, ya sea a través de medios informáticos, digitalizados o impresos, y debe señalar qué datos se recopilan, las finalidades del tratamiento, los posibles receptores de la información tanto a nivel nacional e internacional y el plazo durante el cual se conservarán los datos personales[10].

La jurisprudencia española precisa algunos puntos importantes sobre el deber de información respecto a las finalidades del sistema de videovigilancia[11]:

- No basta con la mera indicación de una "zona videovigilada".
- Se debe ofrecer a los trabajadores información previa clara, precisa y concisa acerca de la medida de videovigilancia.
- Se debe concretar la finalidad sancionadora si se captan incumplimientos laborales de los trabajadores.
- El momento en que debe suministrarse la información es cuando se instala el sistema de videovigilancia, y cada vez que se incorpore a la empresa un nuevo trabajador.
- Si no se dispone de un sistema de videovigilancia, pero se instala por sospechas de irregularidades, se deberá informar a los trabajadores en el momento en que se instalen las cámaras, incluyendo la finalidad sancionadora de incumplimientos laborales.
- Las cámaras encubiertas u ocultas, no informadas a los trabajadores, quedan totalmente prohibidas. ("La videovigilancia en las empresas, ¿medio de prueba válido en el procedimiento laboral?", 2019, párrs. 11-16)

10 Adaptado del artículo "Videovigilancia en el centro de trabajo", por A. Morales Cáceres, 22 de enero del 2020, *Agnitio*. Todos los derechos reservados [2020] por AGNITIO. Adaptado con permiso del autor.

11 Adaptado del artículo "Videovigilancia en el centro de trabajo", por A. Morales Cáceres, 22 de enero del 2020, *Agnitio*. Todos los derechos reservados [2020] por AGNITIO. Adaptado con permiso del autor.

En esta misma línea, en la reciente sentencia recaída en el Expediente N.º 02208-2017-PA/TC (2020), el Tribunal Constitucional precisó que los empleadores tienen el deber de identificar, evaluar y prevenir riesgos laborales a los que podrían exponerse los trabajadores al implementar mecanismos necesarios para asegurar las condiciones de seguridad en el establecimiento laboral, por lo que, en dicho marco, es posible implementar uso de tecnologías como la videovigilancia.

Como bien recuerda el Tribunal Constitucional, la fiscalización laboral no es una facultad discrecional del empleador que justifica un trato arbitrario, pues su límite se encuentra establecido en el tercer párrafo del artículo 23 de la Constitución Política del Perú (1993), que contempla expresamente que ninguna relación laboral puede limitar el ejercicio de los derechos constitucionales, ni desconocer o rebajar la dignidad del trabajador.

Ahora bien, cabe preguntarse qué sucede si el empleador no cumple con el deber de información. Desde la perspectiva del derecho a la protección de datos personales, el empleador podría ser sancionado por la comisión de una falta grave al no respetar los derechos de los titulares de datos personales, la cual tiene prevista una multa que fluctúa entre cinco y cincuenta unidades impositivas tributarias. Desde el ámbito del derecho laboral, si un empleador utiliza un sistema de videovigilancia sin comunicárselo a sus trabajadores, se estaría vulnerando sus derechos fundamentales a la privacidad y a la protección de datos personales. En ese sentido, si se quisiera emplear una grabación como prueba en un proceso, esta podría ser considerada como una prueba ilícita (STC. Exp. N.° 00655-2010-PHC/TC)[12] y, por tanto, podría traer como consecuencia que el despido sea considerado como incausado.

En esta misma línea, la Dirección General de Protección de Datos Personales señala en su Opinión Consultiva N.° 49-2018-JUS/DGTAIPD (2018), en su numeral 11, que a través de los sistemas de videovigilancia el empleador puede captar algún incumplimiento laboral y, por tanto, el registro de tal captación puede ser usado como prueba para imputar faltas de carácter disciplinario a los trabajadores o utilizarse para fines de un proceso judicial laboral, siempre que este medio haya sido empleado cumpliendo con los principios establecidos en la Ley de Protección de Datos Personales[13].

12 El Tribunal Constitucional considera que la prueba prohibida es un derecho constitucional que garantiza a todas las personas que el medio probatorio obtenido con vulneración de algún derecho fundamental sea excluido en cualquier clase de procedimiento o proceso para decidir la situación jurídica de una persona, o que prohíbe que este tipo de prueba sea utilizada o valorada para decidir la situación jurídica de una persona.

13 El Tribunal Supremo Español también ha tomado parte en el debate de la videovigilancia. Una de sus resoluciones más reseñables es la STS 817/2017, del 2 de febrero, que resolvía un recurso de casación que traía causa de la improcedencia de un despido disciplinario de un trabajador por el incumplimiento reiterado de su jornada. El incumplimiento se probó gracias a las videocámaras instaladas en el centro de trabajo, si bien *no se contemplaba la finalidad de control de horario laboral ni la utilización disciplinaria para con los trabajadores, que no habían sido informados de ello.* Dentro

De otro lado, los empleadores no deben colocar cámaras de seguridad en cualquier ambiente. Siguiendo con lo establecido por el principio de proporcionalidad, solo podrá ser utilizado cuando sea pertinente, adecuado y no excesivo para el cumplimiento del control laboral. En ese sentido, la instalación de cámaras o, en todo caso, su ámbito de aplicación debe restringirse a los espacios indispensables para satisfacer las finalidades de control laboral. Por tanto, en ningún caso se admite la instalación de grabación o captación de sonido o de videovigilancia en los lugares destinados al descanso o esparcimiento de trabajadores, como vestuarios, comedores, lactarios o análogos. Tampoco se permitirá en los servicios higiénicos.

A modo de ejemplo, será proporcional colocar una cámara que grabe las manos de una cajera a fin de ver si esta pudo hurtar dinero en la caja registradora. También será proporcional videovigilar al personal que trabaja en un espacio lleno de maquinarias. No lo será, en cambio, videovigilar a alguien en una oficina personal. A fin de verificar si las medidas son proporcionales o no, se recomienda realizar el siguiente test:

– Juicio de idoneidad: ¿la medida sirve para conseguir el objetivo?

– Juicio de necesidad: ¿existe otro recurso menos intrusivo para la consecución del mismo?

– Juicio de proporcionalidad: ¿existe un equilibrio entre el perjuicio causado (intromisión a la privacidad) y los beneficios que suponga el uso de esta medida (control laboral)?

A modo de conclusión, un empleador podrá utilizar la videovigilancia como forma de control laboral, siempre que dicho tratamiento sea proporcional a la finalidad. Para ello, se debe cumplir con informar al trabajador sobre las características del tratamiento. De esta forma, tanto los derechos de los empleadores como el de los trabajadores se ven reforzados, pues no se priva al primero de emplear este método de fiscalización laboral, sino que se regula de tal manera que las grabaciones puedan ser utilizadas en la medida

---

del ámbito laboral, según el Tribunal Supremo, *el consentimiento del trabajador se entiende implícito en la relación negocial, siempre que el tratamiento de datos de carácter personal sea necesario para el mantenimiento y el cumplimiento del contrato de trabajo.* Por el contrario, *el consentimiento de los trabajadores sí será necesario cuando el tratamiento de datos se utilice con finalidad ajena al cumplimiento del contrato. No obstante, el deber de información previa sobre el uso y destino de los datos forma parte del contenido esencial del derecho a la protección de datos, y persiste a la dispensa del consentimiento.*

Esta idea se vio reforzada en el 2018, cuando el Tribunal Europeo de Derechos Humanos emitió su sentencia por el caso López Ribalda y otros contra España. En el caso, ante sospechas sobre pérdidas en la caja, el empleador decidió instalar un *sistema de videovigilancia consistente en cámaras visibles y ocultas, pero los empleados solo tenían conocimiento de las visibles.* La videovigilancia encubierta en el puesto de trabajo fue considerada como una considerable intrusión en la vida privada de las demandantes, que vulnera el artículo 8 del Convenio Europeo de Derechos Humanos.

que garanticen y respeten los derechos fundamentales de los segundos, de acuerdo con lo dispuesto en la Constitución, la legislación laboral y la normativa en materia de protección de datos personales[14].

LA REVISIÓN DE LOS DISPOSITIVOS TECNOLÓGICOS CORPORATIVOS

Como he mencionado anteriormente:

> Son muchos los casos en los que las computadoras del trabajo, el correo corporativo, la conexión a internet de la oficina, el WhatsApp o Facebook del celular de la empresa se utilizan para cuestiones personales. ¿Quién no ha enviado alguna vez un correo electrónico a su pareja para coordinar una salida a algún restaurante o sus amigos para coordinar una reunión? ¿Quién no ha navegado por internet a fin de buscar destinos turísticos? ¿Quién no dedica tiempo a leer columnas de opinión en los sitios web de los periódicos? Sin embargo, muy pocas personas se detienen a reflexionar si el empleador puede leer el correo electrónico corporativo o verificar las páginas por las que uno ha navegado.
>
> La razón por la que los empleadores ponen a disposición de sus trabajadores una conexión a internet, correos corporativos, chats internos, *smartphones*, entre otras nuevas tecnologías, es para que estos ejerzan sus actividades profesionales de la manera más eficiente posible. En consecuencia, resultaría lógico, desde ese punto de vista, que estos se encuentren legitimados para vigilar a sus empleados a fin de evaluar su productividad laboral.
>
> Sin embargo, debemos recordar que el trabajador llega a la relación laboral con todos los derechos constitucionales que le corresponden como persona, tales como el derecho a la intimidad, al secreto de las telecomunicaciones y a la protección de datos personales, por lo que el empleador debe respetarlos. En ese sentido, cabe preguntarse hasta qué punto es legal que una empresa revise el correo de sus empleados.
>
> Al respecto, debemos mencionar que el legislador peruano no ha regulado de forma expresa el tema en cuestión, por lo que caben múltiples interpretaciones. La Corte Suprema, por su parte, mediante la Casación N.° 14614-2016-LIMA (caso Nestlé) establece que constituiría un exceso que el empleador al ser propietario de las cuentas de correo pudiese revisar el contenido de ellas, puesto que admitirlo implicaría colisionar con el derecho fundamental a la intimidad e inviolabilidad de las comunicaciones de los trabajadores. (Morales Cáceres, 11 de enero del 2019, párrs. 1-4)

Sin embargo, esta postura no se adaptaba a la realidad empresarial ni a las tendencias internacionales. ¿Cómo podía un empleador revisar el correo corporativo de un trabajador si este se encontraba en vacaciones o había cesado en sus funciones? ¿Acaso

14 Adaptado del artículo "Videovigilancia en el centro de trabajo", por A. Morales Cáceres, 22 de enero del 2020, *Agnitio*. Todos los derechos reservados [2020] por AGNITIO. Adaptado con permiso del autor.

se requería de un mandato judicial para ello? Inclusive, desde el punto de vista de la protección de datos personales, el empleador es un titular de bancos de datos personales y, como tal, debe cumplir con una serie de obligaciones de seguridad. ¿Cómo podía el empleador revisar que sus trabajadores estén cumpliendo con todas las medidas de seguridad necesarias? ¿Cómo podía el empleador verificar una posible fuga de datos personales si no se implementaban mecanismos de trazabilidad? No cabe duda de que la posición esbozada hasta ese momento por la jurisprudencia no se adaptaba al impacto de las tecnologías en las relaciones laborales.

Hasta ese momento, doctrina autorizada sostenía que, para efectos de cumplir con el criterio establecido por la Corte Suprema, el empleador podría acceder al correo electrónico de sus trabajadores en dos circunstancias: la primera, cuando cuente con una autorización judicial; y la segunda, cuando el propio trabajador haya autorizado el acceso dando su consentimiento informado ("Empleadores que ingresen a correos de trabajadores sin permiso recibirían multa de hasta S/ 20,250", 2017, párr. 2).

Por otro lado, César Puntriano, en una entrevista en el diario *El Peruano*, de fecha 6 de junio del año 2017, recomendaba

> diferenciar entre las herramientas informáticas de carácter personal que pueda tener el trabajador, de aquellas que le proporciona el empleador como medio de trabajo, ya que estas últimas deben emplearse para fines laborales, no siendo inconstitucional que el empleador acceda a su contenido. [Para ello], la intervención se debe efectuar en forma excepcional, no discriminatoria y con la participación del trabajador involucrado. (párr. 6)

Sin perjuicio de lo interpretado por los juristas, lo cierto era que, ante esta postura adoptada por la jurisprudencia nacional, los empleadores se veían limitados a revisar los dispositivos corporativos proporcionados sin contar con un mandato judicial.

Es a raíz de la Sentencia 412/2020, de fecha 8 de septiembre del 2020, que el Tribunal Constitucional analiza dos cuestiones relacionadas con la evolución de las tecnologías de la información y comunicación que han generado un gran impacto en las relaciones laborales: (i) los límites al uso extralaboral de los medios informáticos de propiedad de la empresa por parte de los trabajadores, y (ii) la legitimidad de los controles empresariales y de vigilancia de dicho uso frente a los nuevos avances tecnológicos (STC. Exp. N.° 00943-2016-PA/TC, 2020). En esta sentencia, el Tribunal Constitucional sostiene que "una aplicación de la actual línea jurisprudencial seguida por este Tribunal conllevaría que el empleador no cuente con la posibilidad de controlar el contenido de las comunicaciones del correo electrónico institucional" (fundamento jurídico 22). Dicho con otras palabras, no tendría posibilidad alguna de poder monitorear si es que existe alguna filtración de información confidencial que pueda generar grandes perjuicios a la empresa.

A fin de cambiar dicha postura, el Tribunal Constitucional se basa en los criterios establecidos en el caso Barbulesco vs. Rumanía, de fecha 12 de enero del 2016:

> [En este caso], el Tribunal Europeo de Derechos Humanos (TEDH) estableció que el empleador vulneró el derecho a la intimidad y al secreto de las comunicaciones al vigilar los mensajes enviados en un chat privado por un trabajador mediante medios propios de la empresa y acceder al contenido de los mismos, si no había sido previamente informado de esta posibilidad, incluso existiendo normas en la empresa que prohibían su utilización con fines personales. En ese sentido, lo relevante en esta sentencia es que la inexistencia de un protocolo interno es lo que infringe el derecho a la intimidad. En otras palabras, el empleador debió informar al trabajador sobre la posibilidad de que su actividad puede ser monitorizada. Asimismo, debió establecer el grado de intromisión estableciendo a qué archivos se accede y cuántas personas tienen acceso a los datos personales e información de carácter privado. Finalmente, para realizar esto debe existir una razón legítima empresarial que justifique la monitorización. (Morales Cáceres, 11 de enero del 2019, párr. 12)

Al respecto, el Tribunal Constitucional señala:

> En esa línea, la Gran Sala del TEDH ha establecido los siguientes criterios para determinar si es que el empleador puede o no monitorear las comunicaciones de sus trabajadores.
>
> – El trabajador debe haber sido informado con claridad y con carácter previo de las medidas de control que pueden utilizarse, y del alcance de las mismas, y no únicamente de la posibilidad de que el empresario puede emplear medidas de vigilancia.
>
> – El empleador debe prestar atención y valorar la proporcionalidad de su actuación, estimando qué grado de intromisión comporta la medida en la vida personal y familiar del empleado, debiendo optar por aquella actuación menos intrusiva.
>
> – El empleador debe poder acreditar la existencia de motivos concretos previos al control que justifiquen la necesidad y procedencia de tal medida.
>
> – La medida debe llevarse a cabo de forma previa al inicio del procedimiento disciplinario por parte del empresario, no siendo posible iniciar tal procedimiento y posteriormente determinar los hechos que lo puedan justificar. (STC. Exp. N.° 00943-2016-PA/TC, 2020, fundamento jurídico 25)

Ello permite determinar una posición a favor de la posibilidad de controlar el contenido de los correos electrónicos desde los medios informáticos otorgados por el empleador si es que se cumple con los criterios antes señalados, dejándose de lado una posición que cierre de forma absoluta la fiscalización de su contenido por parte del empleador.

Igualmente, se puede apreciar que la legislación española respalda esta posición, ya que el artículo 87 de la nueva Ley Orgánica de Protección de Datos Personales y Garantía

de los Derechos Digitales establece que los trabajadores tendrán derecho a la protección de su intimidad cuando utilicen dispositivos digitales puestos a disposición por su empleador (Ley Orgánica 3/2018). Este podrá acceder a los contenidos siempre que sea para controlar el cumplimiento de las obligaciones laborales y para garantizar la integridad de dichos dispositivos. Para ello, los empleadores deberán establecer criterios de utilización de los dispositivos digitales, así como todas las medidas técnicas y organizativas que garanticen la preservación de la intimidad de los empleados.

En ese sentido, se puede apreciar que en España los empleadores deberán respetar el derecho fundamental a la intimidad personal de sus trabajadores y no podrán revisar sus correos electrónicos, salvo que exista un protocolo aprobado de uso, o se haya informado de forma clara, expresa y con lenguaje sencillo el reglamento de uso y de verificación de dichos dispositivos digitales. Cabe indicar que esto no excluye que el empleador pueda controlar el uso que el trabajador le otorga a dichos dispositivos (no su contenido) para garantizar su integridad, que no solo será física, sino que deberá verificar que no tengan virus como consecuencia de acceder a páginas prohibidas.

En atención a esta línea argumental, el Tribunal Constitucional en la Sentencia 412/2020 reconoce la "facultad del empleador de fiscalizar e intervenir en el correo electrónico institucional si es que previamente ha comunicado al trabajador tanto de la posibilidad de la monitorización de sus comunicaciones a través de este medio, así como de las condiciones de uso permitido por la empresa" (fundamento jurídico 29). Asimismo, precisa

> que dicha intervención debe respetar ciertos criterios, los cuales se encuentran relacionados con el respeto del principio de proporcionalidad entre el fin que se persigue lograr con dicha intervención y la intensidad de la eventual vulneración o amenaza de violación del derecho fundamental al secreto e inviolabilidad de las comunicaciones. (STC. Exp. N.° 00943-2016-PA/TC, 2020, fundamento jurídico 30).

Como consecuencia, cabe advertir lo siguiente:

> Tomando en consideración lo anteriormente expuesto, consideramos que para que un empleador en el Perú pudiese revisar los correos, chats, archivos personales y navegaciones por internet necesitaría cumplir con lo siguiente:
>
> 1. Respetar el principio de información en materia de protección de datos personales, informando al trabajador que podrá monitorizar el correo electrónico corporativo, así como toda la tecnología puesta a disposición a fin de que pueda controlar el uso que se les otorga a dichos dispositivos (no su contenido) y para que pueda garantizar la integridad de los mismos.
> 2. Deberá elaborar un protocolo de monitoreo en donde se establezca cómo se llevará a cabo la monitorización de los dispositivos (los motivos, cada cuánto tiempo, a qué archivos se accede, quiénes pueden acceder a dicha información, etc.), así como las conductas prohibidas por parte de los trabajadores respecto

al uso de la tecnología entregada por la compañía. Este documento deberá ser entregado al inicio de la relación laboral o ni bien sea aprobado por la empresa.

3. Implementar las medidas legales, técnicas y organizativas necesarias que garanticen la preservación de la intimidad de los empleados. En ese sentido, se deberán utilizar los métodos de vigilancia menos intrusivos posibles.
4. Notificar al trabajador de forma previa sobre la posibilidad de que se supervisarán sus comunicaciones, informando sobre la naturaleza y el alcance de dicho monitoreo.
5. Garantizar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los trabajadores.

En resumen, los dispositivos digitales puestos a disposición por el empleador pueden estar sujetos a las facultades de supervisión laboral siempre que, previamente, marque las pautas sobre el uso de los medios informáticos y advierta que existen controles. Caso contrario, vulneraría el derecho a la intimidad, al secreto de las telecomunicaciones y a la protección de datos personales. (Morales Cáceres, 11 de enero del 2019, párrs. 14-20)

LA GEOLOCALIZACIÓN COMO MÉTODO DE FISCALIZACIÓN LABORAL

Una de las tecnologías que cada vez es más utilizada por las empresas es el GPS (*Global Positioning System*), mecanismo que permite geolocalizar a un objeto y, por ende, suele ser empleado por las empresas para posiciones cuyas funciones se desarrollan centralmente fuera del centro de trabajo.

Al respecto, la geolocalización es la capacidad para obtener la ubicación geográfica real de un objeto, como un radar, un teléfono celular, una tableta, una *laptop* o cualquier otro *wearable* (como un *smartwatch*) que se encuentre conectado a internet. La ubicación geográfica del objeto es medida en coordenadas; en otras palabras, es un concepto que hace referencia a la situación que ocupa un objeto en el espacio y que se mide en coordenadas de latitud (x), longitud (y) y altura (z).

Esta tecnología es utilizada con mayor frecuencia a nivel mundial, principalmente porque los *smartphones* tienen este sistema que permite saber la ubicación geográfica del celular. Así, son muchos los usuarios que están familiarizados con los beneficios de la geolocalización, que van desde (i) solicitar un taxi por aplicativo, (ii) pedir un *delivery*, (iii) prevenir delitos, (iv) hacer *marketing* personalizado, entre otros.

Hace algunos días leíamos con cierta preocupación, como si se tratara de un capítulo de *Black Mirror*, que algunas empresas en Estados Unidos han comenzado a implantar microchips en diferentes partes del cuerpo de sus trabajadores, con el objetivo de geolocalizarlos y verificar que efectivamente se encuentren en el centro de trabajo en su horario laboral. Esto ha llevado a que los legisladores en Michigan, Estados Unidos,

propongan un proyecto de ley que prohibiría a las empresas implantar microchips a sus trabajadores, salvo que se ofrezcan como voluntarios. Si bien en el Perú una práctica así sería contraria al derecho fundamental a la intimidad, esto nos lleva a cuestionarnos la validez de la utilización del GPS como herramienta de fiscalización en el marco de una relación de trabajo.

Tal como mencionamos anteriormente, el artículo 9 del Decreto Supremo N.° 003-97-TR (2020), Texto Único Ordenado del Decreto Legislativo N.° 728, Ley de Productividad y Competitividad Laboral, señala que el empleador se encuentra facultado a realizar controles y medidas para vigilar el ejercicio de las actividades laborales de sus trabajadores. Al igual que ocurre con las cámaras de videovigilancia, la introducción de nuevas tecnologías, como la utilización del GPS, está produciendo en la relación laboral un aumento del poder de control del empleador sobre la prestación de trabajo y sobre el trabajador mismo.

Esto se debe a que resulta más económico y eficiente fiscalizar a los trabajadores a través de las nuevas tecnologías que hacerlo de forma "tradicional" o presencial. Sin embargo, esto puede terminar vulnerando derechos fundamentales como la intimidad, la protección de datos personales y la dignidad. La primera pregunta que debemos respondernos es si es que un empleador puede utilizar un sistema GPS para geolocalizar a sus trabajadores. En principio, el empleador puede utilizar esta tecnología para supervisar a sus trabajadores o para cuidar su patrimonio. En el Perú, se ha utilizado el GPS en las unidades de transporte o vehículos motorizados, tanto para fines de seguridad o de fiscalización laboral.

Debido a que la geolocalización es un dato personal debido a que a través de ella se hace identificable a una persona natural, la Ley de Protección de Datos Personales y su reglamento es aplicable. En tal sentido, el acceso a los datos de geolocalización se considera un tratamiento de datos de carácter personal, por lo que es necesario con dicha normativa en aras de salvaguardar la privacidad del trabajador. Se considera dato de geolocalización a cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal del usuario de un servicio de comunicaciones electrónicas disponible para el público.

Cabe indicar que este tratamiento de datos personales no necesita del consentimiento del trabajador, puesto que dicho tratamiento se realiza en el marco de una relación contractual. Por tanto, no sería necesario solicitar el consentimiento para dicho tratamiento de datos, aunque sí sería necesario informarle del mismo.

Además, el empleador debe tener cuidado en caso de que esos datos de localización geográfica revelen información no concerniente a la actividad laboral, ya que supondría una vulneración del derecho fundamental de los trabajadores a su privacidad. Se exige, por tanto, observar en ese tratamiento de los datos el principio de proporcionalidad, lo

que significa utilizar la menor cantidad de datos posible y tratarlos de tal manera para que sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades para las que se hayan obtenido. Para ello, se recomienda realizar una evaluación de impacto a la privacidad antes de proceder con la incorporación de la tecnología.

En España, la Audiencia Nacional dictó una importante sentencia que trata sobre los límites a la geolocalización de los empleados (Sentencia núm. 13/2019, del 6 de febrero del año 2019). Telepizza implementó un sistema de geolocalización a través de una aplicación instalada en el celular de los propios empleados, con la finalidad de que los clientes puedan hacer un seguimiento en directo de sus encargos (como sucede actualmente con muchas plataformas tecnológicas de reparto de comida a domicilio).

En esa resolución, se estableció que para la implantación del sistema de geolocalización por parte de la empresa se prescindió de proporcionar a los trabajadores la información relativa al tratamiento de datos personales. De hecho, la sentencia analiza la cláusula prevista en el contrato de trabajo, en la que no se menciona la posibilidad de que los trabajadores sean geolocalizados ni se informa del resto de aspectos que resultan obligatorios, tales como la base jurídica del tratamiento, el plazo de conservación de los datos o la posibilidad de ejercer los derechos de acceso, rectificación, cancelación, etcétera (SAN 136/2019, 2019).

Asimismo, se determinó que la geolocalización no supera el principio de proporcionalidad. La Audiencia Nacional sostiene que la finalidad perseguida por la empresa —que el cliente conozca en todo momento el lugar en que se encuentra su pedido— se podría haber obtenido con medidas que suponen una menor injerencia en los derechos fundamentales de los empleados, como, por ejemplo, la implantación de sistemas de geolocalización en las motocicletas en las que se transportan los pedidos o las pulseras con tales dispositivos, que no implican para el empleado la necesidad de aportar medios propios ni, sobre todo, obtener datos de carácter personal como son el número de teléfono o la dirección de correo electrónico en la que han de recibir el código de descarga de la aplicación informática que activa el sistema (SAN 136/2019, 2019).

En efecto, para que el uso del GPS no sea considerado ilícito debe respetar, en primer lugar, los derechos fundamentales de los trabajadores. El empleador debe entender que aquello que legitima el control o la supervisión del trabajador mediante un sistema de geolocalización estriba en que el empresario goza de la facultad de dirección y gestión de los recursos de su empresa. Sin embargo, una vez culminada la jornada laboral, también finaliza la prestación laboral y, por tanto, debe cesar toda medida de control que interfiera en la vida privada del empleado. Asimismo, para garantizar los controles menos intrusivos, el empleador deberá realizar un análisis y ver si supera el test de idoneidad y proporcionalidad.

Adicionalmente, en virtud de lo establecido por la Ley de Protección de Datos Personales, el trabajador debe ser informado de forma previa respecto de los medios de control y vigilancia que utilice el empleador. El conocimiento previo resulta trascendente, ya que de ese modo no se genera una expectativa de confidencialidad a los trabajadores.

Finalmente, el empleador debe preferir aquellos mecanismos tecnológicos que tengan el menor impacto en la vida privada del trabajador, pese a que estos puedan resultar más idóneos para el control de los trabajadores. En ese sentido, el empleador, al momento de elegir el medio de fiscalización, debe evaluar el impacto que este puede tener en los derechos de los trabajadores, a través de una evaluación de impacto a la privacidad del trabajador.

EL TELETRABAJO Y LA PROTECCIÓN DE DATOS PERSONALES

El teletrabajo[15] es una modalidad de prestación de servicios en las instituciones públicas y privadas que se caracteriza por la utilización de tecnologías de la información y las comunicaciones (TIC) sin la presencia física del trabajador en el centro de labores. A través del uso de las TIC, el empleador ejerce el control y la supervisión de las labores. Esta modalidad de trabajo no solo implica un cambio para el trabajador; sin lugar a dudas, también representa un cambio para los empleadores, quienes, en su calidad de responsables del tratamiento de datos personales, deben considerar cuestiones que van desde dónde accede el empleado a la información hasta la forma en la que ingresa a los sistemas.

El teletrabajo pone de relieve la utilidad de la tecnología para permitir el incremento de la eficiencia en la gestión de las relaciones laborales; sin embargo, el uso de las TIC también da pie a importantes interrogantes en relación con la privacidad y la protección de datos personales: ¿qué formas de acceso remoto se permiten? ¿Qué tipo de dispositivos pueden ser utilizados en el teletrabajo? ¿Se permite el trabajo mediante el uso de los dispositivos personales por parte de los trabajadores? ¿Cuáles son las responsabilidades y obligaciones que asumen las partes? ¿Cómo puede fiscalizar el empleador el trabajo realizado por el trabajador? ¿Qué ocurre ante una brecha de seguridad en uno de los dispositivos de los trabajadores? Por ende, en un contexto de teletrabajo, que se apoya necesaria y fundamentalmente en el uso de las TIC, resulta necesario que el empleador delimite un marco normativo en donde se fijen los derechos y obligaciones entre las partes, de forma previa.

No cabe duda de que, al permitir que los trabajadores accedan y manipulen información fuera del entorno corporativo, se amplía la frontera de implicancias en seguridad.

15 Lo señalado en el presente artículo también aplica para el trabajo remoto, pues el empleador debe cumplir con las normas de protección de datos personales y garantizar el derecho fundamental a la privacidad por parte del trabajador.

Las vulnerabilidades y amenazas informáticas en este nuevo contexto plantean riesgos que deben ser mitigados implementando medidas de control adecuadas, ya que, de no tenerlas, se podría estar abriendo la puerta a brechas de seguridad, fugas de información, infecciones con códigos maliciosos o accesos no autorizados a información privilegiada. La tabla 1 presenta algunas de las vulnerabilidades y amenazas en un entorno relacionado con el teletrabajo.

Tabla 1
Vulnerabilidades y amenazas en el entorno del teletrabajo

Vulnerabilidades (Factor interno)	Amenazas (Factor externo)
• Conexión desde redes inseguras	• Infección con códigos maliciosos
• Contraseñas débiles	• Daño de los equipos
• Ausencia de soluciones de seguridad	• *Phishing*
• Falta de respaldos de información	• Pérdida o robo de dispositivos
• Dispositivos con información sin cifrar	• Engaños basados en ingeniería social
• Reglas corporativas oscuras	
• Uso de aplicaciones no seguras	
• Utilización de *software* gratuito	
• Falta de actualización de sistemas y dispositivos	

Elaboración propia

Como se puede apreciar, el empleador se enfrenta a un doble reto, pues debe proteger, por un lado, la información confidencial y datos personales de sus clientes y, por el otro, respetar el derecho a la intimidad de sus trabajadores, de conformidad con lo dispuesto en el literal c) del artículo 6 del Reglamento de la Ley N.° 30036, Ley que regula el Teletrabajo. Esto significa que, al momento de fiscalizar el cumplimiento de las obligaciones de seguridad de la información, a su vez debe garantizar los derechos fundamentales a la privacidad, protección de datos personales e inviolabilidad de las comunicaciones y documentos privados del trabajador.

En este sentido, el empleador deberá plasmar todas las funciones y obligaciones que el trabajador deberá tener en cuenta al momento de prestar sus servicios bajo esta modalidad en el Manual de Teletrabajo. Dicho documento deberá tener en cuenta lo siguiente:

– *Uso de dispositivos corporativos*: el empleador debe incluir una Política de Uso de Medios Tecnológicos, en donde se debe establecer qué puede hacer y qué no puede hacer el trabajador con los dispositivos corporativos y sistemas que son de propiedad del empleador (por ejemplo, teléfonos celulares corporativos, *laptops* corporativas, entre otros).

- *Uso de dispositivos propios*: en el supuesto en que se permita a los trabajadores utilizar sus dispositivos propios, de igual manera, se deberán establecer las políticas de seguridad de la información por implementar.
- *Seguridad de la información*: se recomienda que la información de la empresa se almacene en la nube, pues es más seguro que tenerla almacenada en el propio dispositivo. Asimismo, para evitar el acceso de personal no autorizado a la información de estos dispositivos, se debe hacer uso de un sistema de cifrado de la información.
- *Uso de VPN*: además, se deberá implementar algún sistema que permita sincronizar la información que los trabajadores guardan en sus dispositivos con los sistemas centralizados; de esa manera, no se perderá información. También resulta importante verificar las conexiones entre los dispositivos en el régimen de teletrabajo y, también, cuidar que los servidores centrales estén cifrados. Para ello deberían establecerse redes privadas virtuales o VPN, o bien acceder por escritorio remoto.
- *Entorno laboral*: tanto si el trabajador se encuentra trabajando con un dispositivo habilitado por la empresa como si es un dispositivo personal, es importante establecer la obligación de bloquear siempre el ordenador o cerrar la sesión en caso de ausencia. El entorno laboral en la casa difiere del de la oficina, pues nos encontramos en un lugar en donde compartimos nuestro espacio con terceros (niños, mascotas), que no son tan conscientes de sus actos y podrían borrar o compartir información confidencial de manera involuntaria.
- *Información*: debe informarse a los trabajadores sobre las principales amenazas a las que se encuentra sometido el teletrabajo y las consecuencias en caso de que se quebrante alguna directriz en torno a la seguridad de la información, tanto para el titular de datos personales como para los mismos trabajadores.
- *Gestión de incidencias de seguridad*: resulta imprescindible tener preparados planes de contingencia y protocolos de brechas de seguridad que permitan actuar rápidamente ante situaciones de riesgo, o ante la ocurrencia de incidencias o brechas. La empresa debe estar preparada para atender cualquier pérdida o robo de información, comportamientos anómalos en los sistemas, entrada de virus o cualquier otro incidente que pueda poner en riesgo la información de la empresa. Cualquier anomalía que pueda afectar a la seguridad de la información y a los datos personales tratados debe notificarse al responsable de seguridad del banco de datos personales o al jefe de área (si se trata de información comercial), sin dilación y a la mayor brevedad posible, a través de los canales definidos para tal efecto.

– *Protección a la privacidad de los trabajadores*: es esencial que se establezcan los procedimientos de fiscalización a fin de que el empleador pueda revisar (i) el correcto uso de estos dispositivos, (ii) los contenidos derivados del uso para controlar el cumplimiento de las obligaciones laborales y (iii) que se estén cumpliendo las normas de ciberseguridad de la compañía. Para ello, el empleador debe establecer criterios de utilización de los dispositivos digitales respetando estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos en la Constitución. El empleador deberá detallar las formas en que se llevarán a cabo las fiscalizaciones y el acceso al contenido de los dispositivos. Asimismo, deberá establecer las garantías que se tomarán para preservar la intimidad de los trabajadores.

De otro lado, con el objetivo de que se respete el espacio privado de los trabajadores, el empleador deberá respetar su "derecho a la desconexión digital en el ámbito laboral". Dicho de otro modo, se deberá respetar la jornada laboral estableciendo mecanismos para evitar el riesgo de una fatiga informática. Una manera de plasmar esto será, por ejemplo, señalando que el empleado no se encuentra obligado a responder comunicaciones electrónicas fuera de su jornada de trabajo.

Como reflexión final, consideramos que la figura del teletrabajo, que será utilizada a mayor escala una vez culminada la pandemia del COVID-19, representa indudablemente un avance importante en la nueva mecánica de trabajo. Sin embargo, todo avance debe venir equiparado con el debido cumplimiento de la normatividad que lo regula en distintos ámbitos y relaciones humanas a fin de no dejar desprotegidos los derechos tanto de los trabajadores, empleadores y terceros[16].

EL DERECHO A LA DESCONEXIÓN LABORAL

Tal como se mencionó en la introducción, las tecnologías de la información son parte de nuestra vida, forman parte de nuestros hábitos diarios, transformando nuestra forma de relacionarnos, de pensar y hasta de vivir. El trabajo, al ser un componente tan importante en la vida del ser humano, no es ajeno a esta realidad.

El incremento de una comunicación continua, impulsada por el empleo de nuevas tecnologías como herramientas para el desarrollo de la prestación de servicios laboral, tales como el correo electrónico, el WhatsApp, los chats por redes sociales, etcétera, propicia que muchos trabajadores se encuentren permanentemente "conectados" al trabajo, a través de diferentes dispositivos tecnológicos tales como *smartphones*,

16 Adaptado del artículo "Aspectos legales en torno a la privacidad, ciberseguridad y protección de datos personales en el teletrabajo", por A. Morales Cáceres, 10 de junio del 2020, *Agnitio*. Todos los derechos reservados [2020] por AGNITIO. Adaptado con permiso del autor.

computadoras, tabletas, entre otros. A su vez, las tecnologías móviles se han convertido en uno de los pilares que dan sustento a la transformación digital que actualmente están experimentando las empresas.

El empleador, como es sabido, tiene el deber de proteger la salud de los trabajadores en el desempeño de todos los aspectos relacionados con su labor, en el centro de trabajo o con ocasión del mismo. En ese sentido, el empresario debe respetar de manera efectiva su derecho al descanso, lo cual muchas veces se torna en una práctica compleja, pues la revolución tecnológica y la digitalización de los procesos, así como la globalización —lo cual se ha acentuado aún más con la pandemia del COVID-19—, han dado lugar a un fenómeno de conectividad permanente que impacta en todos los ámbitos de la actividad humana, incluido el laboral, donde las fronteras entre tiempo de trabajo y descanso se tornan cada vez más grises.

En consecuencia, la aparición de las nuevas tecnologías ha proporcionado ventajas, tales como la libertad para trabajar fuera de la oficina, pero también inconvenientes, en especial, lo difícil que resulta desconectarse del trabajo. Esta circunstancia provoca estrés, agotamiento, y dificulta la conciliación de la vida familiar y personal con el trabajo. Así pues, los trabajadores corren el riesgo de padecer síndromes relacionados con las tecnologías, como la fatiga informática, esto es, el cansancio provocado por la continua exposición a la tecnología informática, así como el estrés que genera la espera de un correo electrónico fuera del horario laboral. En definitiva, el abuso digital, es decir, una sobrecarga de información y comunicación puede llegar a ser un riesgo psicosocial nocivo para la salud de un trabajador, y que no garantiza el derecho al descanso, ni la conciliación entre trabajo y la vida personal y familiar (Aragüez, 2018, p. 393).

Esta situación ha abierto un gran debate acerca de la necesidad de regular el denominado *derecho a la desconexión laboral*. Este derecho fue regulado por primera vez en Francia a través de la *Loi* 1088-2016, conocida también como *Loi Travail* o *Loi El Khomri*. Asimismo, en diciembre del 2018, España lo incorporó a través de la Ley Orgánica 3/2018 de Protección de Datos y Garantías de los Derechos Digitales. En el Perú, finalmente se ha materializado en el Decreto de Urgencia que modifica el artículo 18 del Decreto de Urgencia N.° 026-2020, Decreto de Urgencia que establece diversas medidas excepcionales y temporales para prevenir la propagación del coronavirus (COVID-19) en el territorio nacional, el cual versa sobre el trabajo remoto (Decreto de Urgencia N.° 127-2020, 2020):

> 18.1. Son obligaciones del empleador:
>
> [...]
>
> 18.1.4. *Respetar el derecho a la desconexión digital del trabajador, por el cual este último tiene derecho a desconectarse de los medios informáticos, de telecomunicaciones y análogos utilizados para la prestación de servicios durante los días*

> *de descanso, licencias y períodos de suspensión de la relación laboral* [cursivas añadidas].
>
> 18.1.5. Para el caso del sector privado, *observar las disposiciones sobre jornada máxima de trabajo que resulten aplicables conforme a las normas del régimen laboral correspondiente.*
>
> *El empleador no puede exigir al trabajador la realización de tareas o coordinaciones de carácter laboral durante el tiempo de desconexión digital* [cursivas añadidas].
>
> Tratándose de trabajadores no comprendidos en la jornada máxima de trabajo, de conformidad con la normativa vigente en la materia, el tiempo de desconexión debe ser de, al menos, doce horas continuas en un período de veinticuatro horas, además de los días de descanso, licencias y períodos de suspensión de la relación laboral.
>
> 18.1.6. Para el caso del sector público, la Autoridad Nacional del Servicio Civil - SERVIR podrá emitir disposiciones complementarias sobre la presente materia.

En tal sentido, el derecho a la desconexión digital se conceptúa como la limitación en el uso de las tecnologías de la comunicación para garantizar el tiempo de descanso y vacaciones de los trabajadores. Por tanto, este derecho tiene por fin garantizar el derecho al descanso laboral de los trabajadores, así como las jornadas máximas de trabajo, consagrados en la Constitución.

Al respecto, el derecho a la desconexión digital persigue un triple objetivo: (i) garantizar el descanso del trabajador, (ii) permitir la conciliación de la vida personal y familiar, y (iii) prevenir riesgos para la salud de los trabajadores. Es por esta razón que la norma establece que el empleador no pueda exigir al trabajador la realización de tareas o coordinaciones de carácter laboral fuera de la jornada de trabajo o durante los días de descanso, licencias y períodos de suspensión de la relación laboral.

Para ello, se recomienda a los empleadores la elaboración de una política de desconexión digital tomando en consideración la realidad empresarial y el tipo de trabajador que labora en la empresa. En dicho protocolo se debe:

a. Establecer las reglas de desconexión digital de acuerdo con el tipo de trabajador (fiscalizados, no sujetos a fiscalización, intermitentes, personal directivo, entre otros). Asimismo, se debe tener en cuenta la dinámica de la industria o sector económico, así como las funciones y responsabilidades del trabajador.

b. Determinar en qué momentos se aplica, como las horas fuera de la jornada de trabajo, el día de descanso semanal obligatorio, las vacaciones o las licencias de trabajo, así como cualquier permiso concedido por el propio empleador.

c. Prever y coordinar aquellas situaciones excepcionales que requieran de atención inmediata debido a su importancia y urgencia.

d. Señalar las medidas disciplinarias para los jefes de área que incumplan esta política.

La práctica mundial nos demuestra que el respeto al derecho a la desconexión digital se materializa de distintas formas. Una de ellas es determinando que, salvo causa de fuerza mayor o circunstancias excepcionales, el empleador reconoce el derecho de los trabajadores a no responder a los correos electrónicos o mensajes profesionales fuera de su horario de trabajo. Esto implica la obligación de los directivos de no enviar comunicaciones a sus trabajadores fuera del horario laboral. Otra forma de sensibilizar este derecho es a través de la difusión y capacitación de todos los trabajadores, informando sobre los riesgos, desafíos y buenas prácticas relacionados con el uso de las herramientas digitales.

Hay empresas que van más allá de lo señalado por la norma, a fin de ser socialmente responsables con sus trabajadores. A modo de ejemplo, en el año 2016, Michelin implementó una herramienta para enviar avisos a aquellos trabajadores que realizaban más de cinco conexiones laborales fuera de su horario para advertirles de la necesidad de desconectar. En Alemania (sin tener norma expresa), Volkswagen tiene como política apagar el servidor de correo para todos los *smartphones* media hora después de terminar la jornada de trabajo y no los vuelve a encender hasta media hora antes del inicio de jornada. También la empresa Mercedes-Benz ofrece a sus empleados acogerse a un sistema de trabajo *mail on holiday*, por medio del cual los correos enviados a trabajadores que se encuentran de vacaciones son automáticamente redirigidos a otros contactos disponibles dentro de la empresa, evitando que lleguen a sus destinatarios durante las fechas en que estos se encuentran de vacaciones.

A modo de reflexión, si bien se reconoce el esfuerzo hecho por el Poder Ejecutivo al reconocer por primera vez el derecho a la desconexión digital en el Perú y convertirnos en un país que se encuentra a la vanguardia del derecho laboral, esta norma resulta insuficiente. Tal como se ha explicado, este derecho surge como consecuencia del uso masificado de las nuevas tecnologías en el trabajo y no solo a raíz de la incorporación del trabajo remoto, el cual fue establecido como una medida excepcional y temporal para prevenir la propagación del COVID-19. Este derecho no puede limitarse al trabajo remoto (el cual tiene un carácter temporal), sino que debe ser incorporado en la legislación laboral, dado que, cuando el Perú logre superar la pandemia, aún existirán empleadores que abusen de las nuevas tecnologías. En esta nueva realidad, el derecho a la desconexión digital de los trabajadores se perfila como un aspecto clave para el trabajo propio de la era digital, donde las garantías de seguridad y salud solo quedarán fortalecidas con la incorporación de nuevos límites, un cambio de mentalidad y una regulación específica.

CONCLUSIONES

1. Con relación a las plataformas digitales, hay mucha controversia a nivel internacional para determinar si los titulares de las plataformas digitales son empleadores de aquellos que proveen el servicio subyacente. Entendiendo a la plataforma como un mero intermediario, consideramos que no debería existir una relación laboral. Sin embargo, lo más apropiado es analizar caso por caso, pues existe una línea gris entre el control comercial y el control laboral. Para ello, al momento de analizar cada caso, debemos preguntarnos si el titular de la plataforma determina dónde se presta el servicio, cómo se presta el servicio, de qué manera se presta el servicio y cuándo se presta el servicio. Si se puede probar ello, nos encontraremos ante una relación laboral. De lo contrario, la relación será meramente comercial.

2. Respecto al tema de supervisión laboral, para los casos de videovigilancia, geolocalización y revisión de los dispositivos corporativos, es imperativo que el empleador informe con antelación cómo es que llevará a cabo la fiscalización y cuáles son los derechos que tienen los trabajadores en torno a este. Debido a que la tecnología nos presenta situaciones "grises", el empleador deberá realizar un análisis de proporcionalidad y razonabilidad en la medida, a fin de garantizar los derechos fundamentales de los empleados.

3. El teletrabajo pone de relieve la utilidad de la tecnología para permitir el incremento de la eficiencia en la gestión de las relaciones laborales; sin embargo, el uso de las TIC también da pie a importantes interrogantes acerca de la privacidad y la protección de datos personales, por lo que resulta fundamental que los empleadores implementen las medidas legales, organizativas y técnicas a fin de garantizar el correcto tratamiento de datos personales dentro de la empresa.

4. El derecho a la desconexión digital de los trabajadores se perfila como un aspecto clave para el trabajo propio de la era digital, donde las garantías de seguridad y salud solo quedarán fortalecidas con la incorporación de nuevos límites, un cambio de mentalidad y una regulación específica. Es por esta razón que, una vez culminado el estado de emergencia, se debería crear una norma que regule específicamente este derecho.

REFERENCIAS

Agote, R. (14 de noviembre del 2017). Los conductores de Uber son *workers* en lugar de *employees*, pero esa figura no existe en España [mensaje en un blog]. Recuperado de https://blog.cuatrecasas.com/laboral/los-conductores-de-uber-son-workers/

Aragüez, L. (2018). El impacto de las nuevas tecnologías de la información y de la comunicación en el tiempo de trabajo: una especial referencia a la desconexión digital. En J. M. Miranda Boto (Dir.), *El derecho del trabajo español ante el Tribunal de Justicia: problemas y soluciones* (pp. 387-409). Madrid: CINCA.

Bel, J., y García, E. (24 de abril del 2018). Negociación colectiva en la *gig economy*: claves del primer convenio de una plataforma digital [mensaje en un blog]. Recuperado de https://blog.cuatrecasas.com/laboral/economy-convenio-digital/

Casación N.° 14614-2016 (Lima). (2017). Corte Suprema de Justicia de la República: Segunda Sala de Derecho Constitucional y Social Transitoria.

Decreto Supremo N.° 003-97-TR, Texto Único Ordenado del Decreto Legislativo N.° 728, Ley de Productividad y Competitividad Laboral. (21 de marzo de 1997). Recuperado del sitio web del Congreso de la República del Perú: https://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/BE35EA4B0DF56C0A05257E2200538D4C/$FILE/1_DECRETO_SUPREMO_003_27_03_1997.pdf

Directiva N.° 01-2020-JUS/DGTAIPD, Tratamiento de datos personales mediante sistemas de videovigilancia. (10 de enero del 2020). Ministerio de Justicia y Derechos Humanos: Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales. Recuperado de file:///C:/Users/User/Downloads/Directiva-N%C2%B0-01-2020.pdf

Empleadores que ingresen a correos de trabajadores sin permiso recibirían multa de hasta S/ 20,250. (19 de junio del 2017). *Gestión*. Recuperado de https://gestion.pe/tendencias/management-empleo/empleadores-ingresen-correos-trabajadores-permiso-recibirian-multa-s-20-250-137607

La videovigilancia en las empresas, ¿medio de prueba válido en el procedimiento laboral? (14 de junio del 2019). *Diario Constitucional*. Recuperado de https://www.diarioconstitucional.cl/2019/06/14/la-videovigilancia-en-las-empresas-medio-de-prueba-valido-en-el-procedimiento-laboral/

Morales Cáceres, A. (11 de enero del 2019). ¿Puede mi empleador revisar mis correos y navegaciones por internet? *Agnitio.* Recuperado de http://agnitio.pe/articulo/puede-mi-empleador-revisar-mis-correos-y-mis-navegaciones-por-internet/

Morales Cáceres, A. (22 de enero del 2020). Videovigilancia en el centro de trabajo. *Agnitio.* Recuperado de http://agnitio.pe/articulo/videovigilancia-en-el-centro-de-trabajo/

Morales Cáceres, A. (15 de febrero del 2020). Relación laboral en las plataformas digitales. *Agnitio*. Recuperado de http://agnitio.pe/articulo/relacion-laboral-en-las-plataformas-digitales/

Morales Cáceres, A. (10 de junio del 2020.). Aspectos legales en torno a la privacidad, ciberseguridad y protección de datos personales en el teletrabajo. *Agnitio*. Recuperado de http://agnitio.pe/articulo/aspectos-legales-en-torno-a-la-privacidad-ciberseguridad-y-proteccion-de-datos-personales-en-el-teletrabajo/

Opinión Consultiva N.° 49-2018-JUS/DGTAIPD, Sobre el tratamiento de datos personales captados mediante sistemas de videovigilancia en el marco del control laboral. (11 de septiembre del 2018). Ministerio de Justicia y Derechos Humanos: Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales. Recuperado de https://www.gob.pe/institucion/anpd/informes-publicaciones/1373158-oc-n-49-2018-jus-dgtaipd-sobre-el-tratamiento-de-datos-personales-captados-mediante-sistemas-de-videovigilancia-en-el-marco-del-control-laboral

Proyecto de Ley N.° 4144/2018-CR, Ley que regula la labor del trabajador por plataforma digital. Recuperado del sitio web del Congreso de la República del Perú: http://www.congreso.gob.pe/comisiones2018/Trabajo/Expediente/PL4144

Proyecto de Ley N.° 4243/2018-CR, Ley del empleo digno que regula a los trabajadores de plataformas digitales. Recuperado del sitio web del Congreso de la República del Perú: http://www.congreso.gob.pe/comisiones2018/Trabajo/Expediente/PL4243

SAN 136/2019. (6 de febrero del 2019). Audiencia Nacional: Sala de lo Social. Recuperado del sitito web del Poder Judicial de España: https://www.poderjudicial.es/search/AN/openDocument/8ed60e51766c4e3e/20190219

Sentencia recaída en el Expediente N.° 00655-2010-PHC/TC. (2010). Tribunal Constitucional del Perú. Recuperado de https://www.tc.gob.pe/jurisprudencia/2010/00655-2010-HC.html

Sentencia recaída en el Expediente N.° 00943-2016-PA/TC. (2020). Tribunal Constitucional del Perú. Recuperado de https://tc.gob.pe/jurisprudencia/2020/00943-2016-AA.pdf

Sentencia recaída en el Expediente N.° 02208-2017-PA/TC. (2020). Tribunal Constitucional del Perú. Recuperado de https://tc.gob.pe/jurisprudencia/2020/02208-2017-AA.pdf

STS 817/2017. (2 de febrero del 2017). Tribunal Supremo Español: Sala de lo Social. Recuperado del sitito web del Poder Judicial de España: https://www.poderjudicial.es/search/openDocument/b5f9f44350651dc7

STSJ M 1/2020. (17 de enero del 2020). Tribunal Superior de Justicia de Madrid: Sala de lo Social. Recuperado del sitito web del Poder Judicial de España: https://www.

poderjudicial.es/search/AN/openCDocument/53b1b1721a75d34a10b129baa45c19bf179e3f439af7b2cc

Suprema limita acceso al correo electrónico laboral. (6 de junio del 2017). *El Peruano*. Recuperado de https://elperuano.pe/noticia/56482-suprema-limita-acceso-al-correo-electronico-laboral

Villaverde, M. (7 de junio de 2018). Golpe judicial a las plataformas de economía colaborativa: existe relación laboral entre un *rider* y Deliveroo [mensaje en un blog]. Recuperado de https://blog.cuatrecasas.com/laboral/rider-deliveroo-sentencia/

Villaverde, M. (1 de octubre del 2018). Diferencias entre el caso Glovo y los casos Deliveroo y Take Eat Easy: ¿los *riders* tienen relación mercantil o laboral? [mensaje en un blog]. Recuperado de https://blog.cuatrecasas.com/laboral/glovo-deliveroo-take-eat-easy/