MONITORIZACIÓN DE LA NAVEGACIÓN EN INTERNET EN EL «BYOD»: EXIGENCIAS DEL EMPLEADOR EN EL MARCO DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES

FÁTIMA DEYANIRA ARRIVASPLATA REYES

Especialista Legal en Juzgado Especializado de Trabajo de la Corte Superior de Justicia de Lima.

I. INTRODUCCIÓN

El escenario de emergencia sanitaria a causa del COVID-19, ha mostrado la vital importancia que cobran las Tecnologías de la Información y Telecomunicaciones (TICs) en el ámbito de la organización y gestión del trabajo en general, aunque en mayor medida, en aquellas formas de empleo a distancia. Un ejemplo reciente de ello lo constituye la regulación de la modalidad del trabajo remoto establecida en virtud del Decreto de Urgencia N.° 026-2020 y desarrollada en el Decreto Supremo N.° 010-2020-TR. Sin embargo, la consumerización de las TICs también ha jugado un rol gravitante en el desarrollo de la actividad laboral situada en esta crisis sanitaria, aunque ciertamente la transciende. Así pues, una de las aristas de este complejo fenómeno se configura con la posibilidad -cada vez más frecuente- de que el trabajo sea efectuado con los propios dispositivos digitales del empleado, quien generalmente, valiéndose de las elevadas prestaciones técnicas que ellos ofrecen, los aportan a un uso productivo. Ahora bien, aunque dicha técnica de organización del trabajo, conocido como «Bring Your Own Device» (BYOD) cuenta con un lacónico reconocimiento en las normas precitadas, no es menos cierto que de ella se desprenden múltiples aspectos que merecen ser estudiados. Uno de ellos recae en el ejercicio intensivo de la vigilancia empresarial que pudiera suscitarse a fin de controlar el modo en que los trabajadores utilizan sus propios dispositivos -muchas veces- no homologados a los estándares de seguridad informática de la empresa, suponiendo un elevado riesgo potencial por virus, hackers, etc., en razón de que a través de ellos se puede acceder a información sensible de la base informática empresarial.

En el contexto descrito, no es de extrañar que la empresa –a modo de precaución- asuma ciertas acciones de control que al conllevar el tratamiento de información personal del trabajador, pudieran afectar sus

derechos fundamentales. De ahí que, nos resulta razonable sostener que en ese escenario, alcanzan plena virtualidad el derecho fundamental a la protección de datos personales como sus principios rectores incardinados en su normativa de desarrollo, la Ley 29733 (Ley de Protección de Datos Personales; en adelante, LPDP).

No obstante, dado que, por razones de espacio, no nos es posible abordar todas las implicancias generadas a partir de la proyección laboral del derecho en alusión, de su normativa ni de la totalidad de sus principios rectores, esta ponencia se enfoca en *establecer parte de las exigencias que derivan para el empleador a raíz de la aplicación de los principios de legalidad, finalidad y proporcionalidad -recogidos en la LPDP- a las medidas que conlleven la monitorización de la actividad de navegación en internet desplegada por el trabajador en el ámbito BYOD.*

Ciertamente, la informatización del trabajo en la coyuntura COVID-19 perfila hoy la importancia de este pequeño aporte por cuanto su producto robustece la garantía de los derechos fundamentales del trabajador al posibilitársele un mayor control sobre su información personal en el contexto de la supervisión laboral, específicamente, cuando ésta conlleve el registro de su actividad de navegación en internet, en tanto que al empleador le confiere una serie de parámetros a los que debe ajustarse cuando pretenda poner en marcha tales medidas de control.

Es así que, la presente investigación tiene un enfoque teórico fundamentado en el estudio sistemático de la cuestión, el cual inicia contextualizando la necesidad empresarial de monitorizar la navegación en internet en el BYOD, reconociéndose la directa implicación del derecho del trabajador a la protección de sus datos personales, y por ende, la aplicabilidad a tal supuesto de los principios que rigen su normativa de desarrollo recaída en la LPDP. Aunque, por razones de espacio nos enfocamos solo en los principios de legalidad, finalidad y proporcionalidad, a partir de los cuales se derivan para el empleador ciertas exigencias observables ante la adopción de dicho control informático, cuya formulación compone el propósito asumido en esta ponencia.

II. UNA APROXIMACIÓN A LA MODALIDAD BYOD

1. Principales ventajas y riesgos del BYOD

La adopción del BYOD como técnica de organización del trabajo se enmarca en la amplia funcionalidad y sofisticación que han adquirido los dispositivos electrónicos destinados al consumo final (Grupo de Protección de Datos «Artículo 29», 2017, p. 18). De ella, a primera vista se advierte que la posibilidad -contemplada a nivel de normatividad laboral heterónoma- que tiene el trabajador -asalariado- de aportar su propia herramienta de trabajo, en este caso su propio dispositivo electrónico para ejecutar su prestación, confirma el hecho de que el criterio de propiedad exclusiva empresarial de los medios productivos, no es determinante de cara a establecer la laboralidad de la actividad contratada. Desde esa perspectiva, cabe subrayar que la adopción del BYOD presenta como principales ventajas (Puyol, 2015, pp. 42-43): el ahorro de costes para el empleador en la adquisición de nuevos equipos informáticos, así como la promoción de una mayor flexibilidad en cuanto a la organización y gestión de la actividad laboral, principalmente cuando por la naturaleza de la labor, ésta deba llevarse a cabo en distintas locaciones, por ejemplo, los trabajos de reparto de mercadería o los que supongan visitas a clientes o proveedores.

Por otra parte, entre sus principales desventajas, se encuentra el riesgo informático incrementado concretado en el peligro de que se produzcan accesos no autorizados a información sensible de la empresa, fuga de datos e introducción de softwares maliciosos por descarga de aplicaciones no autorizadas (Cremades Chueca, 2018, pp. 107-108), por nombrar a los más comunes. Empero, a la par de dicho riesgo empresarial, concurre también otro para el trabajador, por cuanto pueden resultar afectados sus derechos fundamentales merced al potencial lesivo que suelen albergar los programas informáticos que pudieran ser instalados a iniciativa del empleador en los dispositivos afectos al BYOD -bajo la causa legítima de garantizar la integridad y seguridad de la infraestructura informática corporativa-, en la medida que tales mecanismos generalmente operan sobre

la base del recojo y procesamiento de cuantiosa información personal del usuario trabajador (Baz Rodríguez, 2019, apartado 5.2).

2. Algunas recomendaciones de seguridad aplicadas al BYOD

Dado que en virtud de esta modalidad, al trabajador le es posible acceder desde su propio dispositivo a información de carácter corporativo, es razonable colegir que la seguridad de dicha base informática empresarial puede verse seriamente afectada ante el ataque cibernético que pretenda burlarla, comprometiéndose con ello la imagen o el prestigio empresarial ya alcanzado. Sin perjuicio de la protección normativa que le asista al trabajador -en este escenario potencialmente adverso para su contraparte-, las recomendaciones técnicas informáticas usualmente propuestas son las que a continuación se señalan:

a) La delimitación del ámbito subjetivo que alcanza la modalidad BYOD, definiéndose perfiles informáticos, según la cualificación técnica y grado de responsabilidad del trabajador (Puyol, 2015, pp. 219-220).

b) El establecimiento de criterios de utilización de las herramientas informáticas puestas a disposición del trabajador (correo electrónico, programas, aplicaciones, bases de datos, etc.) e incluso respecto de sus propios dispositivos móviles, tipificándose, de ser el caso, las infracciones a dichos parámetros como faltas pasibles de sanción (Puyol, 2015, p. 218).

c) En el supuesto de que el trabajador tenga acceso a banco de datos personales concernientes a clientes, proveedores e inclusive de otros trabajadores, en rigor de lo preceptuado por el principio de seguridad de los datos recogido en el artículo 9 de la LPDP[1] y según lo expuesto sobre el particular por la Dirección de Protección de Datos Personales, el empleador debe hallarse premunido

1 El artículo 9 del referido dispositivo legal prescribe: «[e]l titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales»

de controles de acceso respecto a los datos que allí se conservan, estableciendo quienes se hallan autorizados para ello, acorde con el perfil profesional de cada uno (cargo y funciones) además de los alcances que tendría dicho acceso. También le corresponde la provisión a los usuarios de contraseñas o códigos de ingreso, aparte de un examen periódico de los privilegios otorgados, a fin de adoptar las modificaciones que resulten pertinentes conforme hayan ido variando las circunstancias (DPD, Informe 03-2018-JUS/DGTAIPD-DPDP, p. 5).

d) La implementación de la modalidad en mención, debe finalmente protocolizarse mediante el pacto bilateral celebrado con el trabajador, en el que se plasme su libre consentimiento para su incorporación al BYOD, estipulándose en dicho instrumento los usos autorizados y prohibidos del respectivo dispositivo como de los recursos virtuales que sean puestos a disposición del empleado (Baz Rodríguez, 2019, apartado 5.2).

III. LA PROTECCIÓN DE DATOS COMO DERECHO FUNDAMENTAL IMPLICADO EN EL CONTEXTO DE LA MONITORIZACIÓN DEL USO DE LOS DISPOSITIVOS DIGITALES

En el marco del ejercicio del poder directivo del empleador es habitual que éste, amparado en el propósito de garantizar el adecuado funcionamiento de los sistemas informáticos de la empresa, resuelva recurrir a la instalación de programas o aplicaciones encargadas de la monitorización del uso de los dispositivos digitales afectos a la modalidad BYOD, justificándose en su legítimo interés de prevenir una utilización inadecuada o indebida de ellos sea por la acción de terceros -en situaciones de robo, extravío, ciberataque, *jailbreak*, *phishing*, etc.- o bien por actuaciones irregulares imputables al trabajador. Sin embargo, no puede soslayarse que dichas operaciones también suelen implantarse con el objeto de supervisar el correcto desarrollo de la actividad laboral, así como el adecuado cumplimiento de las respectivas obligaciones de trabajo[2].

2 Estas obligaciones laborales en el campo del BYOD, generalmente se reconducen a los

Bajo tales alcances y aun cuando la referida vigilancia electrónica efectuada por el empleador se enmarque dentro de sus facultades de fiscalización o control, las cuales conforman el contenido del poder de dirección[3] que le asiste en virtud del reconocimiento de la libertad de empresa consagrada en el artículo 59° de nuestra Norma Fundamental[4] -sin dejar de mencionar la previsión contemplada el artículo 9° del Texto Único Ordenado de la Ley de Productividad y Competitividad Laboral aprobado por Decreto Supremo N.° 003-97-TR[5]; sin embargo, como ya es sabido, dichos poderes no se encuentran exentos de límites y restricciones; todo lo contrario, a ese respecto, el Tribunal Constitucional ha dejado sentado que el ejercicio de las facultades de fiscalización -y disciplinarias- deben observar las limitaciones previstas en la Constitución además de satisfacer el canon de razonabilidad, en el sentido de ser adecuadas para cumplir un objetivo laboral sin alterar el contenido de los derechos fundamentales involucrados (Sentencia del Tribunal Constitucional del 18 de agosto de 2004, FJ. 20)[6]. Lo postulado por este Colegiado, sin duda, cobra plena

deberes de reserva o confidencialidad de la información corporativa almacenada en los dispositivos de titularidad del trabajador, siguiéndole otros compromisos, como los de no concurrencia, uso adecuado de las plataformas de comunicación digitales, cumplimiento del tiempo de trabajo prefijado, gestión diligente de los equipos informáticos aplicados a la ejecución de la prestación, entre otros.

3 El poder directivo del empleador no puede ser comprendido si no es relacionándolo con el contrato de trabajo, pues en virtud de éste, el trabajador se compromete a ejecutar a favor del primero una determinada actividad en condiciones de subordinación, siéndole correlativa la posición jurídica de su contraparte, la cual se conforma de «(…) una pluralidad de facultades que el ordenamiento jurídico reconoce como necesarias e indispensables para el funcionamiento normal de la empresa, para su organización económica, técnica y funcional» (Hernández Rueda, 1997, p. 405).

4 El Tribunal Constitucional la ha definido como "(…) la facultad de poder elegir la organización y efectuar el desarrollo de una unidad de producción de bienes o prestación de servicios (…)" (Sentencia del Tribunal Constitucional de fecha 18 de abril de 2007, FJ. 37).

5 El artículo 9° del TUO de la LPCL establece que: «Por la subordinación, el trabajador presta sus servicios bajo dirección de su empleador, el cual tiene facultades para normar reglamentariamente las labores, dictar las órdenes necesarias para la ejecución de las mismas, y sancionar disciplinariamente, dentro de los límites de la razonabilidad, cualquier infracción o incumplimiento de las obligaciones a cargo del trabajador».

6 En todo caso, el carácter limitado de la potestad empresarial en cuestión viene expre-

vigencia ante la progresiva sofisticación técnica que han ido adquiriendo los mecanismos de control del empleador al permitirle ejercer una supervisión laboral ubicua, lo que a su vez comporta un serio riesgo para los derechos fundamentales del trabajador.

En esa medida, cabe subrayar que el derecho a la intimidad personal[7] se ha venido perfilando como uno de los atributos del trabajador directamente implicados en el despliegue de la fiscalización empresarial y en especial, de las medidas que conllevan el registro o seguimiento de la navegación web desplegada por el trabajador, puesto que a través de tales operaciones se puede acceder a cuantiosa información personal que a él concierne (ideologías, condición médica, orientación sexual, aficiones, etc.), a partir de la cual es factible igualmente construir un perfil de su personalidad. No obstante, como quiera que actualmente dicha vigilancia es puesta en marcha mediante la instalación de programas informáticos que operan en base a técnicas de recolección y procesamiento de numerosa data laboral, resulta insoslayable la intervención de otra garantía adicional, recaída a nuestro juicio, en el derecho fundamental a la protección

samente impuesto por el artículo 23 de la Constitución, cuyo tenor sanciona que «[n]inguna relación laboral puede limitar los derechos constitucionales ni rebajar la dignidad del trabajador»

7 Este derecho se encuentra consagrado en el artículo 2, inciso 7 de la Constitución y en palabras de nuestro Tribunal Constitucional, su contenido esencial lo representa la protección de un ámbito estrictamente personal, cuya reserva es indispensable para el libre desarrollo de la personalidad de su titular; tanto así que su exposición pública podría conllevar la causación de un perjuicio psicológico irreparable para aquel (Sentencia del Tribunal Constitucional de fecha 29 de agosto de 2007, FJ. 41). Por lo menos en la jurisprudencia del Tribunal Europeo de Derechos Humanos (véase apartado IV, infra), ese derecho ha sido comúnmente aplicado en los conflictos generados por el uso –extralaboral- de las herramientas informáticas corporativas por parte de los trabajadores, enjuiciándolos bajo el estándar de la expectativa razonable de privacidad, la cual ha entrado a tallar en aquellas situaciones en las que el empleador no ha establecido ni informado a sus trabajadores respecto a las reglas de uso que debe dispensarse a tales herramientas o cuando se ha venido permitiendo su utilización para propósitos privados, independientemente de quien haya detentado la titularidad real de los mismos (Goñi Sein, 2017, p. 13).

de datos personales, el cual se perfila como otro de los límites oponibles ante el desarrollo de las referidas actuaciones empresariales[8].

Con base ello, se tiene que el derecho fundamental invocado, por expresa declaración de la LPDP, cuenta con reconocimiento constitucional en el artículo 2, inciso 6 de nuestra Norma Fundamental, el cual se configura como un derecho de titularidad inespecífica del trabajador en el marco de la relación laboral, cuyo contenido constitucionalmente protegido puede analizarse desde una perspectiva subjetiva como objetiva. Para arribar a dicho entendimiento, previamente es preciso situarse dentro del marco conceptual que propugna el carácter dual predicable de todo derecho fundamental, en virtud del cual estos poseen una dimensión subjetiva la cual vincula tanto al poder público como a los particulares –en razón de su eficacia horizontal- a través de la imposición de un deber negativo de no obstaculizar el ejercicio de las facultades conferidas al titular, mientras que su dimensión objetiva o institucional instaura -para el poder público- una obligación positiva de promoción del ejercicio real y eficaz del derecho fundamental implicado (Preciado Domenech, 2019, párr. RB-2.2), reclamándole un despliegue prestacional a todos los niveles, legislativo, judicial y ejecutivo (Castillo Córdova, 2003, pp. 9-14).

Proyectando esa base conceptual sobre el derecho fundamental a la protección de datos, es posible sostener que la dimensión subjetiva del mismo, en efecto, comprende una «(…) serie de facultades que tiene toda persona para ejercer control sobre la información personal que le concierne, contenida en registros ya sean públicos, privados o informáticos, a fin de enfrentar las posibles extralimitaciones de los mismos» (Sentencia del Tribunal Constitucional del 15 de octubre de 2007, Fundamento 2). Así, sobre ese particular, nuestro Colegiado Constitucional ha dejado sentado que el derecho fundamental en estudio garantiza al titular de los datos personales, la posibilidad de "[c]onocer, actualizar, incluir y suprimir o

8 El citado derecho fundamental y su normativa de desarrollo cobran plena virtualidad si se trata de preservar, ya no únicamente la intimidad personal sino cualquier otro derecho que pudiera verse afectado por las sofisticadas técnicas informáticas de recolección, procesamiento y análisis de datos personales (Rodríguez Escanciano, 2019).

rectificar la información o datos referidos a su persona que se encuentren almacenados o registrados (…) en bancos de datos de (…) instituciones privadas (…)" (Sentencia del Tribunal Constitucional del 30 de mayo de 2011, FJ. 8). Por otra parte, a nivel infraconstitucional, cabe destacar que, en su norma de desarrollo, esto es, la LPDP, tales prerrogativas se concretan en los derechos de acceso[9], rectificación[10], cancelación[11] y oposición[12] (conocidos como derechos «ARCO»).

9 El derecho de acceso reconocido en el artículo 19 de la LPDP, habilita al titular a obtener información respecto a qué datos suyos están siendo objeto de tratamiento, de qué modo, con qué propósitos y a instancia de quién aquellos fueron recogidos, así como con quiénes se comparte la información personal y para qué fines; qué transferencias de sus datos personales han realizado, realizan o prevén realizar; en qué condiciones están siendo tratados sus datos personales; o, cuánto tiempo se conservarán dichos datos. Así, el derecho de acceso posibilita el ejercicio de los demás derechos de rectificación, cancelación y oposición, por cuanto esto último solo puede concretarse si es que al titular de los datos le es posible conocer todos los detalles antes descritos respecto de la información que le concierne (Castro Cruzatt, 2008, p. 270)

10 El derecho de rectificación recogido en el artículo 20 de la LPDP, confiere a su titular la facultad de exigir al titular del banco de datos o al encargado del tratamiento, que modifique los datos personales que resulten ser parcial o totalmente inexactos e incompletos o cuando se advierta algún tipo de omisión, error o falsedad. Este derecho comprende la posibilidad de actualizar los datos que han sido modificados a la fecha del ejercicio del derecho. Es así que, a criterio del TC, "(…) la única manera de que a través de los datos se pueda proyectar una imagen real del comportamiento de una persona (…) es que estos sean constantemente actualizados" (Sentencia del Tribunal Constitucional de fecha 30 de mayo de 2011, FJ. 9). Asimismo, se acoge la facultad de incluir aquella información faltante además de corregir o modificar la que resulte errada o inexacta.

11 El derecho de supresión o cancelación sustentado en el artículo 20 de la LPDP y en el artículo 67° del RGPD, faculta a su titular a solicitar la cancelación o supresión de los datos que le conciernen cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hayan sido recopilados, cuando hubiera vencido el plazo establecido para su tratamiento, cuando haya revocado su consentimiento y, en general, en todos aquellos casos en los que sus datos personales no están siendo tratados conforme a la LPDP y su reglamento. A ese respecto, cabe indicar que cuando media relación contractual entre el responsable y el titular de los datos personales y se encuentra justificado el tratamiento de estos últimos, no procederá la cancelación comentada, sin embargo, en esos casos se prevé que, en cuanto sea posible, se empleen mecanismos de anonimización o disociación, de acuerdo con lo prescrito por los artículos 69 y 70 del RGPD precitado

12 El derecho de oposición previsto en el artículo 22 de la LPDP y artículo 71 del RGPD, confiere al titular de los datos el derecho a que no se efectúe el tratamiento de su información personal o a que esta operación se detenga, cuando no haya prestado su consentimiento para ello por haber sido aquella tomada de fuentes de acceso público. Mientras

En cuanto a la dimensión objetiva del derecho en cuestión, se tiene que en este ámbito, se consideran comprendidos los principios rectores del tratamiento de datos personales recogidos en la LPDP, dentro de los cuales se encuentran aquellos que integran el propósito asumido en esta ponencia, a saber, los de legalidad, finalidad y proporcionalidad, respecto a los que se volverá más adelante. En efecto, a tales directrices se les reputa parte de la citada dimensión por cuanto su estipulación a cargo del Legislador de la LPDP, a modo de contenidos obligacionales dirigidos principalmente al titular del banco de datos respectivo, no constituyen sino garantías objetivas destinadas a promover, en favor del titular de los datos, el ejercicio eficaz de las facultades conferidas por el derecho sub examine, las mismas que, como se vio supra, hace parte de su dimensión subjetiva.

Ahora bien, tras exponerse ambas dimensiones del derecho fundamental a la protección de datos, es preciso sin embargo, subrayar que el tratamiento a profundidad de los referidos derechos «ARCO» dista del objetivo de este trabajo -enmarcado en el ámbito de los principios contemplados en la LPDP, es decir, en su dimensión objetiva-. De ahí que se considera conveniente centrarse en el análisis de estos últimos, específicamente en su aplicación a las medidas de control y vigilancia de la navegación en internet; tanto más si –a criterio de la autora- las aludidas pautas rectoras -exigibles a los sujetos responsables del tratamiento de los datos desde su fase inicial de acopio o recolección, hasta su etapa final de cancelación, supresión o eliminación- han sido estipuladas para presidir toda operación que conlleve el tratamiento de los datos personales -potenciando así la virtualidad tuitiva conferida por el derecho fundamental sub examine- independientemente de si su titular resuelve actuar las facultades de control antes enunciadas, no siendo éstas últimas posiciones correlativas de las primeras. Es por ello que se asume viable su exclusión en este estudio, por cuanto, de cara al propósito que nos concierne, su abordaje tendría una utilidad netamente informativa.

que, en caso de haberse prestado el consentimiento, el interesado haya acreditado la concurrencia de razones legítimas que justifiquen el ejercicio del derecho aludido.

IV. CASO BARBULESCU C. RUMANÍA: CRITERIOS DEL TEDH PARA LA MONITORIZACIÓN DE LOS DISPOSITIVOS ELECTRÓNICOS EN EL ÁMBITO DEL TRABAJO

Aunque en nuestro medio no se reportan antecedentes jurisprudenciales conocidos -a nivel del Tribunal Constitucional[13] y de la Corte Suprema- sobre el supuesto de estudio aquí abordado, podría afirmarse que aquellos *sí se han encontrado en la jurisprudencia del* Tribunal Europeo de Derechos Humanos (en adelante, TEDH), adquiriendo singular importancia, por su aporte y pertinencia de cara al propósito que nos reúne, la Sentencia del 05 de setiembre de 2017 recaída en el Caso Barbulescu contra Rumanía. Ciertamente, la relevancia de este fallo reside en la contribución de diversos criterios *útiles* para evaluar la validez de las medidas empresariales que conlleven la monitorización del uso de los equipos y herramientas informáticas por parte de los trabajadores, siendo que aunque ellos se encuentren referidos a los dispositivos digitales de propiedad corporativa, cierto es que no existe razón objetiva que impida extenderlos a las situaciones en que el mencionado control informático se instale en el propio equipo del empleado. Bajo ese entendido, de tales parámetros merece especial énfasis el deber de información previa atribuible al empleador, en tanto presupuesto sustantivo habilitante para llevar a cabo, no solo el registro de las comunicaciones electrónicas de los trabajadores (asunto materia del fallo en mención) por cuanto la aludida exigencia se ha hecho extensiva a los casos referidos al control del uso del internet[14],

13 Los casos que han suscitado la atención de este Colegiado – e inclusive de la Corte Suprema- así como de la doctrina nacional han recaído primordialmente en la cuestión referida al registro empresarial de las comunicaciones electrónicas de los trabajadores, cuyo abordaje se ha efectuado desde la exclusiva base de la garantía del secreto e inviolabilidad de las comunicaciones y los documentos privados consagrada en el artículo 2 inciso 10 de la Constitución, postulándose la exigencia irrestricta de una investigación de tipo judicial que habilite al empleador a fiscalizar y eventualmente sancionar a sus empleados por utilizar el correo electrónico corporativo para fines opuestos a los que le imponen sus obligaciones laborales (Véase, Exp. N.° 1058-2004-AA/TC, Exp. N.° 04224-2009-PA/TC, Exp. N.° 00114-2011-PA/TC (10 de enero de 2012), Exp. N.° 03599-2010-PA/TC (10 de enero de 2012), Exp. N.° 05532-2014-PA/TC y Sentencia de Casación 14614-2016-LIMA de fecha 10 de marzo de 2017.

14 Con ocasión de este fallo, el TEDH reiteró el criterio sostenido en la Sentencia del 03 de abril de 2007 (Caso Copland c. Reino Unido), según el cual la noción de vida privada

dentro de cuyo ámbito se inserta la vigilancia de la navegación en red, cuestión ésta que nos concierne.

1. Los hechos del caso

Dicho lo anterior, en torno al Asunto Barbulescu se sabe que la Sentencia de la Gran Sala del TEDH de fecha de 5 de septiembre de 2017 tuvo como antecesora a la Sentencia de fecha 12 de enero de 2016 dictada por la Sección Cuarta del referido Tribunal. Así pues, el hecho principal que motivó la expedición de estos fallos fue el del despido de un trabajador producido tras constatarse que aquel intercambiaba comunicaciones de carácter personal con sus parientes valiéndose de una cuenta de mensajería de Yahoo Messenger cuya creación se había efectuado a instancia del empleador para una finalidad exclusivamente laboral, reputándose infringida la prohibición empresarial de emplear el citado canal de mensajería para propósitos extralaborales.

2. Valoraciones del TEDH

Ante tales sucesos, la primera Sentencia del año 2016, declaró no vulnerado el derecho del recurrente a su vida privada y correspondencia reconocido en el artículo 8° del Convenio Europeo de Derechos Humanos. Sin embargo, frente a ese resultado desfavorable, el demandante llevó el caso a la Gran Sala, cuya decisión final dio lugar a la Sentencia del año 2017, la cual, tras reputar insuficiente la preexistencia de la prohibición empresarial de utilizar los recursos de la empresa para actividades personales, decretó que las autoridades nacionales no brindaron la protección adecuada al referido derecho, señalando a esos efectos que aquellas debieron valorar los siguientes factores o exigencias -atribuibles al empleador-, a saber: (a) la información al trabajador sobre la posibilidad de control sobre sus comunicaciones; (b) la información al trabajador sobre la natu-

-y de correspondencia- también concurre en el campo de la actividad profesional, de ahí que ingresen dentro de la cobertura del derecho a la vida privada -además de las comunicaciones electrónicas del trabajador- la información derivada de la monitorización del uso de Internet de una persona, inclusive en el contexto de las relaciones laborales.

raleza, alcance e intensidad de la supervisión; (c) la formulación de una justificación suficiente que legitime la adopción de las medidas de control; (d) la indagación sobre otras medidas menos intrusivas para la privacidad y la confidencialidad de las comunicaciones del trabajador; (e) la determinación de los resultados de la medida de supervisión implementada y si estos fueron aplicados para alcanzar el propósito de la misma; y (f) la adopción de garantías dirigidas a impedir que el empleador acceda a las comunicaciones del trabajador sin que éste haya sido avisado de la oportunidad en que tendrá lugar el registro (FJ 120). En ese orden de ideas, considerando que a juicio del Tribunal, las regulaciones restrictivas que adopte el empleador respecto al uso de sus recursos informáticos por parte de sus empleados no puede anular la expectativa de privacidad que a ellos les es reconocida en esas situaciones, la estipulación de dichos parámetros ha operado favorablemente a la preservación del estándar aludido, el cual nos resulta pertinente abordar aunque sea de forma exploratoria, cometido al que se dirigen las líneas siguientes.

V. UN COMENTARIO EXPLORATORIO ACERCA DE LA EXPECTATIVA RAZONABLE DE PRIVACIDAD

Conforme se expuso previamente, dado que los parámetros enunciados en el Caso Barbulescu se dirigen a proteger la expectativa razonable de privacidad que les es reconocida a los trabajadores en el uso de los recursos informáticos corporativos. Es por ello que, cual estándar habitualmente empleado en el análisis de los asuntos referidos a la vigilancia informática desplegada por el empleador, es destacable su incidencia en el abordaje de nuestro supuesto de estudio como probable también es su eventual aplicación en el medio local[15], de ahí que se justifica proseguir con una breve aproximación al parámetro en mención desde la perspectiva de su aplicación a los casos atinentes al registro empresarial de la navegación en

15 Estándar que, conforme se señaló supra, fue alguna vez invocado, sin mayor impacto resolutivo en algunos fallos de nuestro Tribunal Constitucional referidos a la problemática del acceso a las comunicaciones electrónicas de los trabajadores (véase en los fundamentos de voto emitidos por el Magistrado Eto Cruz en los Exp. N.° 00114-2011-PA/TC y Exp. N.° 03599-2010-PA/TC.

internet, tomando como referentes a esos efectos, dos importantes fallos del Tribunal Supremo de España alusivos al supuesto en cuestión a partir de los cuales se esboza un sucinto comentario en torno a su idoneidad como canon de enjuiciamiento de tales medidas de control informático.

1. Sentencia 966/2006 del Tribunal Supremo de España de fecha 26 de setiembre de 2007

Este fallo respondió al hecho del despido de un trabajador de alta dirección producido tras constatarse en el ordenador asignado por su empleador la existencia de una carpeta de archivos temporales de "antiguos accesos a páginas pornográficas". Se sabe que el acceso al mismo respondió originalmente a una revisión técnica, con ocasión de la cual se detectaron virus informáticos causados por "la navegación por páginas poco seguras de Internet", utilizándose ulteriormente los resultados obtenidos para propósitos disciplinarios. Tales sucesos fueron valorados por dicho Colegiado, habiendo postulado que es posible compaginar la intimidad del trabajador -y por ende su expectativa razonable de privacidad- con la fiscalización empresarial respecto a la utilización correcta de sus recursos informáticos siempre que previamente se hayan establecido las reglas de uso de los mismos, se le haya informado al afectado de la posibilidad de ejercer control para comprobar la observancia de dicha reglamentación así como que se le haya notificado de los mecanismos seleccionados a tal efecto (Fundamente Jurídico N.° 4).

2. Sentencia 8876/2011 del Tribunal Supremo de España de fecha 06 de octubre de 2011

Este fallo posterior tuvo como antecedente de hecho, el despido de una trabajadora suscitado tras comprobarse la utilización del Internet para cometidos personales habiéndose constatado numerosas visitas a sitios Web no autorizados. Anótese que dicha verificación fue factible gracias a la instalación -no informada- de un "software" de monitorización que operaba capturando lo reflejado en la pantalla del ordenador, para su sucesiva visualización. Es así que, tales sucesos conllevaron sin embargo

a que el Colegiado flexibilizara las exigencias informativas plasmadas en el fallo precedente, concluyendo que la expectativa de privacidad decaía con la sola prohibición de usar el ordenador o cualquier otro recurso del empleador para asuntos personales, reputándose irrelevante la ausencia de información respecto al control ejercido (FJ. 4).

Ahora bien, pese a que lo destacable del estándar de la expectativa razonable de privacidad reside en la relevancia que a través de ella adquiere la exigencia empresarial de transparentar los criterios bajo los cuales debe regirse el uso de la infraestructura informática que pone a disposición de sus empleados, sin perjuicio de quien detente la titularidad del equipo o dispositivo respectivo. Sin embargo, atendiendo a la volubilidad con la que -a nivel jurisprudencial- se ha tratado dicha expectativa al punto de entender que ésta «(…) puede ser desconectada por casi cualquier elemento que muestre al trabajador la ilicitud de su conducta al utilizar para fines personales los medios tecnológicos empresariales (…)» (Tascón López, 2017, p. 77); entonces, difícilmente aquella pueda fungir de canon de enjuiciamiento predecible de las medidas de control tecnológico implantadas por el empleador, tanto más si en el contexto del BYOD -a raíz de los peculiares riesgos concurrentes- se reclama el estricto cumplimiento de un estándar de transparencia informativa adecuadamente delimitado, no sujeto a los vaivenes observados en el tratamiento dispensado al citado parámetro.

VI. SEGUIMIENTO DE LA ACTIVIDAD DE NAVEGACIÓN EN INTERNET DESPLEGADA POR EL TRABAJADOR: EXIGENCIAS DERIVADAS PARA EL EMPLEADOR

Lo expuesto hasta este punto conlleva a sostener que los supuestos de monitorización de los dispositivos electrónicos en el ámbito del trabajo y específicamente los casos referidos al seguimiento de la navegación web desplegada por el trabajador desde el ordenador de la empresa han venido siendo comunmente enjuiciados desde la perspectiva de la protección de la privacidad del empleado. Sin embargo, habiéndose dejado sentada la directa implicancia del derecho fundamental a la protección de datos

personales en el despliegue de las medidas empresariales objeto de estudio, al reconocerse que estas operan mediante el tratamiento masivo de información personal de los empleados, entonces, a raíz de ello, se hace posible postular que aquellas se insertan en el ámbito de la normativa de protección de datos y por ende de los principios rectores recogidos en la LPDP, perfilándose estos como contrapesos de las facultades de vigilancia del empleador. A pesar de ello, dado que a la fecha han sido poco exploradas las exigencias que para la parte empleadora, se derivan de la aplicación de tales principios a los supuestos de control tecnólogico empresarial como el aquí analizado; concretamente, de la aplicación de los principios de legalidad, finalidad y proporcionalidad contemplados en la LPDP, en consecuencia, a ese propósito se dirigen los contenidos desarrollados en los párrafos siguientes.

1. La ineficacia del consentimiento del trabajador como base jurídica habilitante para la monitorización de la navegación en internet en el contexto del BYOD

Recurriendo al tenor preceptivo del principio de legalidad[16] precitado se deduce que toda operación que conlleve el tratamiento de datos personales debe sustentarse en una base o título legal habilitante, la cual como regla debe residir en la manifestación de voluntad previa, libre, informada, expresa e inequívoca del titular de los datos, según lo informa el principio del consentimiento igualmente previsto en la LPDP. En efecto, en e*l consentimiento se reconoce a la base jurídica por excelencia sobre la cual se ha vertebrado la infraestructura normativa de la protección de datos personales,* perfilándose esta como el punto de partida para el tratamiento de la información personal. Sin embargo, en el terreno de las relaciones laborales, dicho título jurídico habilitante se reputa excepcional, en la medida que «[l]os trabajadores casi nunca están en condiciones de dar, denegar o revocar el consentimiento libremente, habida cuenta de la de-

16 El artículo 4 de la LPDP establece que: «El tratamiento de los datos personales se debe realizar conforme a lo establecido en la ley. Se prohíbe la recopilación de los datos personales por medios fraudulentos, desleales o ilícitos»

pendencia que resulta de la relación empresario/trabajador (…)» (Grupo de Protección de Datos «Artículo 29», 2017, p. 25).

Es así que, el carácter residual del consentimiento en ese escenario se traduce en su restringida operatividad, circunscrita a aquellas situaciones en que se garantice a los trabajadores que no se les anudará perjuicio alguno para sus intereses personales o profesionales, sea cual fuere la decisión que adopten al respecto (Grupo de Protección de Datos «Artículo 29», 2011, p. 15). De ahí que, desde dicho anclaje argumental difícilmente pueden encuadrarse en el ámbito del consentimiento, los procedimientos que conlleven el tratamiento de información personal de los trabajadores cuando aquellos se instalen en el marco de la implementación de medidas de control informático por parte del empleador, como el registro de la navegación web, al ser plausible que de estas se deriven consecuencias disciplinarias, aún en el caso de que la supervisión tenga lugar en el ordenador del trabajador en el contexto BYOD.

Antes bien, en escenarios como éste, se considera que la base legal que subyace a la adopción de tales controles informáticos no puede ser otra que su carácter necesario para la ejecución de la relación laboral entablada con el trabajador implicado -titular de los datos personales respectivos-, encuadrándose dicha base habilitante en la causal prevista en el artículo 14, inciso 5 de la LPDP[17], la misma que de cara al supuesto en estudio, se traduce en la necesidad empresarial de actuar esos registros digitales motivada por el legítimo interés del empleador de preservar la seguridad de su base informática así como de supervisar el uso adecuado de los recursos virtuales que pone a disposición de sus trabajadores para el desarrollo de la prestación laboral, lo cual a su vez cobra una importancia gravitante en la modalidad BYOD en razón del elevado riesgo informático que en ésta concurre.

17 «Cuando los datos personales sean necesarios para la preparación, celebración y ejecución de una relación contractual en la que el titular de datos personales sea parte, o cuando se trate de datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento»

Es así que, desde esa perspectiva, q*uedaría excluida para el empleador la posibilidad de recurrir al consentimiento del trabajador como título jurídico habilitante para monitorizar su actividad de navegación en internet en el contexto del BYOD*[18], tornándose cuestionables las cláusulas que directa o indirectamente estipulen la aquiescencia del trabajador para la instalación de determinados programas o softwares en los dispositivos que éste aporte como herramienta productiva, en la medida que ellos permitan llevar a cabo una vigilancia o seguimiento permanente e indiscriminado de su actividad informática.

2. La finalidad lícita y explícita en el registro digital de la navegación en internet

No obstante haberse establecido la base legal habilitante que sustenta el seguimiento de la navegación en internet, cierto es que ella solo configura un marco genérico a partir del cual se justifica el tratamiento de la información personal de los trabajadores a través de la puesta en marcha de tales medidas de control. Es por ello que cabe introducir al caso otra de las garantías objetivas incardinadas en la normativa de protección de datos, la cual reside en el *carácter determinado, lícito y explícito que debe(n) poseer el(los) propósito(s) que se persigue(n) a través de dicha monitorización*, según se desprende del tenor preceptivo del principio de finalidad[19] recogido en la LPDP.

18 Si bien en el apartado II.2 supra, se ha señalado que el BYOD debe protocolizarse vía pacto con el trabajador, debe distinguirse entre el consentimiento requerido para su incorporación a dicha modalidad y el título que legitima el ejercicio de la tecnovigilancia laboral a través de las medidas aquí discutidas, el cual no reside en la voluntad laboral sino en el ejercicio del poder de dirección empresarial, según se desprende de las causales de limitación del consentimiento para el tratamiento de datos (ex art. 14.5 de la LPDP).

19 El artículo 6 de la LPDP establece que: «Los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita. El tratamiento de los datos personales no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización»

Ahora bien, en rigor del contenido prescriptivo asignado al principio en cuestión, se tiene que del mismo se deriva para el empleador la exigencia según la cual la implementación de las medidas de registro informático objeto de estudio debe dirigirse a uno o más propósitos cuya formulación observe los requerimientos anteriormente enunciados. Así, a nuestro juicio, *las finalidades que pueden ser legítimamente invocadas en el supuesto que nos concierne, se reconducen a: i) la verificación del cumplimiento de las obligaciones laborales contraídas en el marco de la modalidad BYOD y ii) la preservación de la integridad y seguridad de la base informática empresarial*, la cual se muestra especialmente vulnerable dada la configuración propia de dicha modalidad.

En relación al primero de tales propósitos, se considera que éste debe reputarse excepcional en razón de lo intrusivas que pudieran resultar siendo las medidas de control digital sub examine[20], tanto más si el dispositivo sobre el cual se implementan es de titularidad del trabajador. En orden al carácter residual postulado, es que se admite que éste tenga cabida, primordialmente en aquellas situaciones en las que previamente se haya detectado -por otros cauces- la comisión de inconductas laborales graves (p.ej. competencia desleal, infracciones a reglas de seguridad y de la confidencialidad, entre otras) o bien cuando se tengan sospechas fundadas de su existencia, de modo que se recurra al referido mecanismo solo a efectos confirmatorios (Baz Rodríguez, 2019, pág. 144). De lo contrario, si se normaliza el registro de la actividad informática desplegada por el trabajador desde su dispositivo, a modo de método ordinario de supervisión de la actividad laboral, se terminaría validando un control empresarial permanente e indiscriminado (Navarro Nieto, 2019, p. 84).

Por otra parte, en cuanto al segundo propósito, se tiene que éste, a criterio de la Organización Internacional del Trabajo, «(…) es uno de los

20 Esto se sustenta en que la monitorización remota de los dispositivos informáticos del trabajador -concretamente cuando esta se traduce en el registro o indexación de la navegación web- puede acarrear el posible acceso a la información relativa a la vida personal del trabajador, como su afiliación política o ideológica, gustos personales, orientación sexual o inclusive, su condición de salud, datos personales éstos a partir de los cuales puede construirse un perfil del empleado (Rodríguez Escanciano, 2019, párr. RB-10.10).

pocos casos en que se reconoce como indispensable la vigilancia continua de los trabajadores (…)» (Organización Internacional del Trabajo, 1997, p. 15). Así, bajo dicha finalidad, se acoge la implementación del control de la actividad informática del trabajador en el contexto BYOD, en respuesta al riesgo informático cualificado que esta modalidad reporta[21].

Como colofón de todo lo expuesto, resta agregar que otra de las pautas normativas que se desprende del principio en cuestión apunta a garantizar la circunscripción del tratamiento respectivo al propósito específico programado, proscribiéndose los usos desviados de los datos personales recabados. Así pues, al proyectar dicha regla sobre nuestro supuesto de estudio hace posible colegir que la vigilancia permanente a la que se encuentra expuesto el trabajador merced a la monitorización de su actividad en internet implantada con el propósito de resguardar la seguridad de la base informática corporativa, debe tener su contrapeso en la restricción de los usos o destinos a los que se aplican los datos recogidos con ocasión de ella, lo que a su vez implica que el empleador pueda utilizar la información recabada en ese contexto para una finalidad distinta, siempre que se notifique previa y explícitamente de ello. Esto último significa que debe procurarse la correspondencia entre la finalidad preestablecida y el uso real dispensado a la información recopilada, de modo que, en principio, le es exigible al empleador programar el(los) propósito(s) que pretende satisfacer a través de las mencionadas técnicas digitales de supervisión, previniéndose así la sobremonitorización al trabajador so pretexto de preservar la integridad de la data corporativa (Organización Internacional del Trabajo, 1997, p. 15).

21 Es por ello que cada vez es más común la contratación de servicios de «Movile Device Management» o «MDM», los cuales viabilizan una monitorización en tiempo real del funcionamiento y de la localización del dispositivo, permitiéndole implementar diversas configuraciones que posibilitan el bloqueo de los referidos equipos o el borrado automático del contenido allí almacenado, en casos de pérdida o robo; no obstante, también es cierto que tales programas pueden ser tan invasivos como sean configurados por quien los administra en este caso, el empleador (Baz Rodríguez, 2019, apartado 5.3).

3. La exigencia de transparencia informativa en el control digital de la navegación en internet

Como ya es sabido, el derecho a la protección de datos personales confiere a su titular un haz de facultades de disposición y control sobre la información que le concierne, en cuanto a su registro, uso y revelación por y hacia terceros (Sentencia del Tribunal Constitucional del 15 de octubre de 2007, FJ. 2-4). Sin embargo, es pertinente subrayar que el referido derecho fundamental devendría impracticable «(…) si el afectado desconoce qué datos suyos son los que terceros poseen, quiénes los poseen, y con qué fin lo hacen» (Sentencia 29/2013 del Tribunal Constitucional de España, del 11 de febrero de 2013, FJ. 6). De ahí que, la garantía de transparencia informativa previa, expresa y precisa[22] sea considerada, con razón, parte del contenido constitucionalmente protegido del derecho en cuestión (Castillo Córdova, 2012, párr. 3-4). Ahora bien, acudiendo a la LPDP, específicamente, al tenor de sus principios rectores, se advierte que el sustento de dicha garantía reside en el principio de legalidad precitado, cuando en su tenor se contempla la expresa prohibición de efectuar tratamientos desleales de los datos personales.

En esa línea de criterio, aun cuando por lo general no se precise del consentimiento del trabajador en caso de que el tratamiento de su información personal obedezca a la adopción de medidas empresariales que no son sino concreciones de las facultades de ordenación y fiscalización del empleador, cierto es que ello no le exime de la obligación de

22 El contenido detallado que debe predicarse de la obligación de transparencia dirigida al titular del banco de datos, condición que en nuestro caso recae en el empleador, se contempla en el artículo 18 de la LPDP, el cual confiere al titular de los datos personales, el «(…) derecho a ser informado a ser informado en forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación, sobre la finalidad para la que sus datos personales serán tratados; quiénes son o pueden ser sus destinatarios, la existencia del banco de datos en que se almacenarán, así como la identidad y domicilio de su titular y, de ser el caso, del encargado del tratamiento de sus datos personales; el carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles; la transferencia de los datos personales; las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo; el tiempo durante el cual se conserven sus datos personales; y la posibilidad de ejercer los derechos que la ley le concede y los medios previstos para ello»

proporcionarle información previa y detallada sobre quién, cómo y para qué se están recogiendo y procesando sus datos, quienes pueden ser sus destinatarios, durante cuánto tiempo serán conservados así como de la posibilidad de ejercer los precitados derechos «ARCO». Dicho esto, al proyectar el subrayado deber empresarial de transparencia sobre el supuesto en estudio -registro de la navegación en internet-, es plausible formular algunas pautas normativas consideradas relevantes de cara al propósito que nos convoca, aunque su aplicabilidad puede también hacerse extensiva a la implementación de otras formas de control informático en la medida que estas operen a través de técnicas de recolección y procesamiento de la data personal de los empleados:

(A) El establecimiento de una política que fije los criterios de utilización de los dispositivos digitales de los trabajadores inmersos en la modalidad BYOD así como de los recursos virtuales puestos a su disposición por el empleador con fines de productividad, procurándose la especificación de los usos autorizados como de los proscritos[23].

(B) La previa notificación respecto a las características y alcances de las medidas técnicas de seguridad adoptadas por el empleador con el propósito de preservar la integridad y confidencialidad de la infraestructura informática corporativa a la que el trabajador pudiera tener acceso desde su propio dispositivo.

(C) La previa información sobre la posibilidad de instalar programas o soluciones informáticas que permitan llevar a cabo un seguimiento o vigilancia de la actividad del trabajador en internet -navegación web-, debiendo asegurarse el empleador de trans-

23 Bajo tales alcances, si bien se admite que el empleador puede establecer inclusive prohibiciones absolutas respecto al uso personal del internet como de otros recursos virtuales que ponga a disposición de sus empleados, es importante considerar que en el contexto BYOD se encuentra implicado el dispositivo de titularidad del trabajador- coexistiendo en el mismo una dualidad de usos, entre privados y profesionales. Debido a esta particularidad, las prohibiciones absolutas y tajantes del aprovechamiento extralaboral de las funcionalidades del equipo en cuestión no se perfila como la opción más adecuada; antes bien se sugiere la implantación de una política de usos razonables de los mismos (Baz Rodríguez, 2019, apartado 5.2).

parentar la clase de datos personales que serán objeto de tratamiento, sus destinatarios, así como las características y alcances que pudieran tener dichas medidas de control digital, el(los) propósito(s) que con éstas se persigue(n), las implicancias -organizativas, disciplinarias, etc.- que de ellas podrían derivarse para el trabajador además del plazo y modo de la conservación de sus datos.

A ese respecto, cabe destacar que la mayor o menor rigidez que adopten los criterios mencionados supra, ciertamente dependerá de diversos factores como los referidos a si el dispositivo fue de exclusivo uso personal del empleado con anterioridad a la implementación del BYOD o si el equipo se adquirió a partir de la adopción de dicha modalidad; así como por quién solventó la adquisición y/o el uso del mismo (Cremades Chueca, 2018, p. 114), siendo igualmente relevante tomar en cuenta el aspecto locativo en el que tiene lugar el BYOD, valorándose en ese sentido si la prestación con el propio equipo se viene ejecutando en las instalaciones del empleador o fuera de ellas, sin soslayar lo atinente al grado de flexibilidad con que cuenta el trabajador para gestionar el desarrollo de su labor. No obstante, cualquiera que sea la política que se decida al respecto, sí que es cierto que el *trabajador no puede ver anulados sus atributos iusfundamentales, especialmente su privacidad y el derecho a la protección de sus datos personales en el entorno laboral, configurando garantía mínima de los mismos, el estricto cumplimiento previo del estándar de transparencia* abordado supra[24] (Luque Parra & Ramón Lacomba, 2020, párr. RB-12.36).

24 De ahí que, se haya asentado en la jurisprudencia del TEDH, el concepto de «vida privada social», el cual responde a la posibilidad de que su titular desarrolle su identidad social mediante la comunicación y las relaciones con sus semejantes, lo que, comprende las actividades profesionales, pues se considera que la vida laboral representa uno de los espacios donde las personas tienen la mayoría de oportunidades para forjar vínculos con sus pares (Sentencia del TEDH de fecha 3 de abril de 2007, Caso *Copland vs. Reino Unido*).

4. La proporcionalidad del tratamiento de los datos personales de los trabajadores en la monitorización de la navegación en internet

Es sabido que las medidas de monitorización informática materia de este estudio sin duda pueden comprometer múltiples derechos fundamentales del trabajador, por lo que, para su válida implementación se precisa que aquellas también satisfagan las exigencias derivadas del principio de proporcionalidad previsto en el artículo 7 de la LPDP, en virtud del cual «[t]odo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados»[25].

Ahora bien, aun cuando en este apartado se aborda el principio de proporcionalidad consagrado en la LPDP, no puede perderse de vista su indudable sustento constitucional, habiéndolo así ratificado nuestro Tribunal Constitucional, al considerarlo un principio vigente en la integridad del ordenamiento jurídico nacional, reconociendo en la cláusula del Estado de Derecho uno de sus principales fundamentos, en la medida que ella expresa la sujeción de todo acto de poder –sea público o privado, normativo o no normativo- a la Constitución y especialmente a las previsiones que garantizan derechos fundamentales, a partir de la cual se arriba al entendimiento de que ante una eventual afectación de los mismos, ésta deba ser equilibrada y proporcional (Sentencia del Tribunal Constitucional del 03 de enero de 2003, FJ. 138).

En esa línea de criterio, la lógica operativa que acompaña al principio en alusión consiste en establecer si en el supuesto en cuestión se verifica una correlación entre la limitación que grava al derecho fundamental implicado y la satisfacción del bien jurídico relevante invocado como causa justificante de la afectación iusfundamental alegada. En otras palabras, dicho principio comporta una "(…) relación lógico– axiológica entre la circunstancia motivante, el objeto buscado y el medio empleado" (Sentencia del Tribunal Constitucional del 05 de julio de 2004, FJ. 35). Es

25 No obstante, a dicho principio lo complementa el de calidad igualmente contemplado en el citado dispositivo legal, en la medida que éste último prevé, entre otros aspectos, la exigencia de que la información personal recabada sea la necesaria, pertinente y adecuada en relación a la finalidad programada

así que, dicho cometido se concreta sometiendo a la medida limitativa del derecho a un triple juicio ponderativo: (i) de idoneidad, el cual vela tanto por la legitimidad del fin u objetivo perseguido como por la adecuación de la medida aludida para la realización del primero; (ii) de necesidad, dirigida a preservar la indispensabilidad del medio empleado ante la inexistencia de alternativas igualmente eficaces pero menos intrusivas para el derecho fundamental intervenido; y (iii) de proporcionalidad en sentido estricto, que apunta a garantizar el equilibrio razonable entre el grado de realización del objetivo buscado y el grado de intervención en el derecho fundamental respectivo, procurándose que las desventajas o sacrificios acarreados no superen las ventajas o beneficios reportados (Sentencia del Tribunal Constitucional de fecha 18 de febrero de 2005, FJ 6).

Desde ese marco conceptual y volviendo sobre tenor preceptivo asignado al principio de proporcionalidad recogido en la LPDP, es posible apreciar que en él se encuentran contempladas las tres precitadas dimensiones que tradicionalmente han conformado su contenido, llegándose a identificar, a estos efectos, la idoneidad con la exigencia de adecuación; la necesidad con la exigencia de relevancia y la proporcionalidad en sentido estricto con la proscripción de los excesos en el tratamiento respectivo, cuya proyección a nuestro supuesto de estudio propicia que aquellas adquieran perfiles específicos, los mismos que pasarán a desarrollarse en las líneas que siguen.

(A) Exigencia de adecuación o idoneidad: en virtud de esta exigencia, el tratamiento de los datos personales de los trabajadores llevado a cabo mediante el registro de la navegación en internet debe ser adecuado o idóneo para satisfacer eficazmente la finalidad legítima y específica que lo motiva, la cual si bien se encuentra en principio encaminada a preservar la infraestructura informática corporativa a raíz del riesgo informático implícito en el BYOD, tampoco se descarta la posibilidad de que excepcionalmente dicho registro pueda servir al estricto propósito de fiscalizar la actividad laboral, conforme se ha explicado en el apartado VI.2 supra. En ese sentido, de cara a alcanzar

tales propósitos, se tiene que la idoneidad requerida al referido control informático por lo general no exige mayor problematización si se atiende a sus múltiples funcionalidades técnicas sujetas a la exclusiva disposición del empleador. En efecto, ello responde al hecho de que la monitorización de la navegación reporta al empresario eventuales peligros e irregularidades que pudieran estar afectando la infraestructura informática corporativa, sin soslayar el potencial que aquella alberga para informar de otros aspectos del desarrollo de la actividad laboral, tales como el cumplimiento de las obligaciones, desempeño o inclusive perfiles del trabajador.

(B) Exigencia de indispensabilidad o relevancia: en razón de esta exigencia, resulta pertinente señalar que el recurso a técnicas de monitorización como las aquí abordadas, solo se concibe cuando ello sea relevante en razón de su carácter indispensable para alcanzar el objetivo o propósito programado, ante la falta de otras medidas alternativas menos invasivas e igualmente eficaces para esos efectos. De ahí que, a partir de ello se postule el carácter preferente –dada su reducida lesividad- de las medidas de índole preventiva que en ese contexto se adopten, considerándose entre estas, la instalación de programas que bloqueen automáticamente el acceso a determinadas páginas web riesgosas, el establecimiento de políticas informativas dirigidas a los empleados respecto a las aplicaciones prohibidas, advertencias sobre los problemas de seguridad que puede acarrear la descarga de programas no autorizados, técnicas de encriptado de datos, políticas formativas sobre usos razonables y diligentes de las nuevas tecnologías, etc.. En suma, «(…) la prevención de los usos desviados de los dispositivos digitales debe ser más importante que su detección (…)» (Baz Rodríguez, 2019, p. 140), aunque ciertamente el examen caso por caso será lo más adecuado para establecer cuán indispensable puede llegar a ser la implementación de los registros informáticos en cuestión de cara a la satisfacción de los específicos propósitos buscados.

(C) Proscripción de los excesos en el tratamiento de datos personales: el tratamiento de la información personal del empleado sobre cuya base opera la monitorización de la navegación en internet debe finalmente ser equilibrado o en términos de la LPDP, no excesivo. Ciertamente esto se traduce en el alcance limitado que le es requerido a las medidas de control aquí abordadas, de modo que se garantice la relación razonable que debe verificarse entre el grado de satisfacción del propósito empresarial perseguido a través de ellas y el grado de intromisión en el derecho fundamental a la protección de datos así como en otros de su mismo rango que también pudieran estar implicados, según las particularidades del caso concreto. Desde esa perspectiva, se arriba al entendimiento de que las medidas de control digital en cuestión deben obedecer a una configuración tal que puedan operar con la mínima información personal del trabajador implicado, perfilándose así incompatibles con dicha exigencia, las técnicas de vigilancia informática capaces de recabar datos innecesarios o cuyo despliegue sea irrazonablemente prolongado o indiscriminado (Baz Rodríguez, 2019, apartado 2.6). Por lo que, tras esas consideraciones conviene introducir algunas pautas avocadas a minimizar el impacto de la monitorización bajo examen:

(i) El alcance subjetivo que se plantee el empleador al implementar las medidas de monitorización estudiadas, debe procurar hallarse en función del perfil informático que ostente el trabajador concernido, aspecto éste que a su vez depende de su cualificación profesional, así como del tipo de información corporativa a la que aquel puede acceder desde su propio dispositivo en razón de su concreta función.

(ii) Especialmente, cuando las medidas sub examine se orientan hacia un propósito referido al control laboral, debe procurarse que su despliegue tenga lugar durante un intervalo temporal acotado, el estrictamente necesario para alcanzar su cometido, de ahí que, se recomiende la implementación de mecanismos

-preferentemente automáticos- de desconexión de dichos sistemas de control durante un rango horario predeterminado, independientemente de cuán flexible se perfile el régimen contractual del trabajador implicado. En efecto, esta última posibilidad redunda en beneficio de ciertos bienes humanos fundamentales habitualmente intervenidos con las prácticas empresariales bajo análisis, tales como el descanso y la conciliación entre la vida personal y profesional, por nombrar algunos.

(iii) Por otra parte, si por razones de seguridad, se requiere de una permanente monitorización, repárese que, aún en este contexto -y a modo de contrapeso-, ésta debe observar la mayor corresponderse posible con dicho propósito, procurándose optar por configuraciones que impidan la visualización de los datos personales recolectados, sino hasta que ello sea realmente necesario, es decir, ante el acaecimiento de situaciones de robo, extravío, detección de actividad informática irregular, entre otras análogas.

VII. CONCLUSIONES

a) A pesar de que la incorporación del trabajador a la modalidad BYOD deba ser protocolizada a través de un convenio celebrado entre ambas partes de la relación laboral, el aspecto concerniente a *la monitorización de la navegación en internet no puede dejarse a merced del consentimiento del empleado, al no ser éste título jurídico habilitante para ello, quedando consecuentemente excluida para empleador la posibilidad de ampararse en* él, tornándose entonces cuestionable la validez de ciertas cláusulas contractuales, que apoyándose en la aquiescencia del trabajador, terminen legitimando una vigilancia indiscriminada en sus propios dispositivos.

b) El seguimiento de la navegación en internet debe responder a una *finalidad determinada, lícita y explícita, perfilándose como unos de los propósitos plausibles en el marco de tales operaciones*, a saber: i) la preservación de la seguridad de la base informática

empresarial, de cara a los riesgos implícitos en el BYOD y ii) la supervisión del correcto desarrollo de la actividad laboral, especialmente si se trata de fiscalizar el uso de los recursos virtuales proporcionados a los trabajadores.

c) *Las medidas de monitorización digital aquí abordadas no pueden ser desleales o clandestinas*. Todo lo contrario, la información previa que se proporcione respecto a su instalación, características, propósito, alcances e implicancias se constituye en un *prius* ineludible de cara a su válida implementación, más aún si la referida vigilancia informática tiene lugar en un dispositivo de titularidad del trabajador inmerso en la modalidad BYOD.

d) El cumplimiento del estándar de transparencia en la implementación del registro de la navegación en internet, habilita el sucesivo examen de su proporcionalidad, comprendida en su triple juicio ponderativo. En virtud de este último, *el empleador debe garantizar, en primer orden, la adecuación de dicha medida de control de cara al logro del propósito que justifica su adopción.* Asimismo, aquel debe asegurar su relevancia, en el sentido de asegurarse de que su puesta en marcha sea realmente indispensable tras haberse descartado -dada su reducida eficacia-, otras alternativas menos intrusivas. Y, finalmente, se le exige *preservar el equilibrio razonable entre el grado de restricción que dicha medida pueda generar en los derechos fundamentales del trabajador implicado y la relevancia del propósito empresarial que con ella se intenta satisfacer*, lo cual se traduce en la exigencia de limitar sus alcances y concreto ámbito de operatividad.

VIII. BIBLIOGRAFÍA

Baz Rodríguez, J. (2019). *Privacidad y protección de datos de los trabajadores en el entorno digital.* Madrid: Wolters Kluwer.

Baz Rodríguez, J. (Junio de 2019). Protección de datos y garantía de los derechos digitales laborales en el nuevo marco normativo europeo e interno. *Ars Iuris Salmanticensis, 7*, 129-171.

Castillo Córdova, L. (2003). Principales consecuencias de la aplicación de la doble dimensión de los derechos fundamentales. *Anuario da Facultade de Dereito da Universidade da Coruña*(7), 183-196. Obtenido de: https://pirhua.udep.edu.pe/bitstream/handle/11042/1959

Castillo Córdova, L. (31 de julio de 2012). *La finalidad del derecho a la autodeterminación informativa y su afianzamiento a través del hábeas data*. [Entrada de Blog]: https://sumaciudadana.wordpress.com/2012/07/31/la-finalidad-del-derecho-de-autodeterminacion-informativa-y-su-afianzamiento-a-traves-del-habeas-data

Castro Cruzatt, K. (2008). El derecho fundamental a la protección de datos personales: aportes para su desarrollo en el Perú. *Ius et Veritas*(37), 260-276.

Cremades Chueca, O. (junio de 2018). Impacto teórico-práctico del BYOD en el derecho del trabajo. (CEF, Ed.) *Revista de Trabajo y Seguridad Social*(423), 103-122.

Goñi Sein, J. L. (2017). Nuevas tecnologías digitales, poderes empresariales y derechos de los trabajadores: análisis desde la perspectiva del Reglamento Europeo de Protección de Datos de 2016. *Revista de Derecho Social*(78), 1-29.

Grupo de Protección de Datos del Artículo 29. (GT 29). Dictamen 15/2011 sobre la definición del consentimiento, WP 187, 13 de julio de 2011.

Grupo de Protección de Datos del Artículo 29. (GT 29). Dictamen 2/2017 sobre el tratamiento de datos en el trabajo, WP 249, 8 de junio de 2017.

Luque Parra, M., & Ramón Lacomba, F. (2020). Acceso a dispositivos digitales del trabajador facilitados por la empresa. En M. Rodríguez-Piñero Royo, & A. Todolí Signes, *Vigilancia y control en el Derecho del Trabajo Digital.* Cizur Menor: Aranzadi, S.A.U. Obtenido de https://proview.thomsonreuters.com/

Navarro Nieto, F. (2019). Las facultades de control a distancia del trabajador: videovigilancia y grabación del sonido. *Temas Laborales: Revista Andaluza de Trabajo y Bienestar Social* (150), 71-89. Obtenido de: https://dialnet.unirioja.es/servlet/articulo?codigo=7224368

Organización Internacional del Trabajo. (1997). Repertorio de recomendaciones prácticas de la OIT: Protección de los datos personales de los trabajadores. Ginebra: Oficina Internacional del Trabajo.

Preciado Domenech, C. (2019). *Los derechos digitales de las personas trabajadoras. Aspectos Laborales de la L.O 3/2018, de 5 de diciembre de protección de datos y garantía de los derechos digitales.* Cizur Menor: Aranzadi, S.A.U. Obtenido de https://proview.thomsonreuters.com/

Puyol, J. (2015). *Una aproximación a la técnica "BYOD" y al control estratégico de las nuevas tecnologías en la empresa.* Valencia: Tirant lo Blanch.

Rodriguez Escanciano, S. (2019). *Derechos laborales digitales: garantías e interrogantes.* Cizur Menor: Aranzadi, S.A.U. Obtenido de https://proview.thomsonreuters.com/

Tascón López, R. (octubre de 2017). Tecnovigilancia empresarial y derechos de los trabajadores (intento de construcción de una regla conceptual en el derecho del trabajo español). *Revista de Trabajo y Seguridad Social*(415), 53-92.

Jurisprudencia, normativa y otros documentos legales

Constitución Política del Perú (1993).

Decreto supremo 003-97-TR, Texto Único Ordenado del decreto legislativo 728. *Diario Oficial El Peruano*, 27 de marzo de 1997.

Decreto supremo 003-2013-JUS. Reglamento de la Ley No 29733, Ley de Protección de Datos Personales [RLPDP]. *Diario Oficial El Peruano*, 22 de marzo de 2013.

Decreto supremo N.° 010-2020-TR. Desarrolla disposiciones para el Sector Privado, sobre el trabajo remoto previsto en el Decreto de Urgencia N.° 026-2020. *Diario Oficial El Peruano*, 24 de marzo de 2020.

Decreto de Urgencia N.° 026-2020. Establece diversas medidas excepcionales y temporales para prevenir la propagación del coronavirus (COVID-19) en el territorio nacional. *Diario Oficial El Peruano*, 15 de marzo de 2020.

Dirección de Protección de Datos Personales. (2018). Informe 03-2018-JUS/DGTAIPD-DPDP. Miraflores, 30 de enero de 2018.

Ley 29733 [LPDP]. Ley de Protección de Datos Personales. *Diario Oficial El Peruano*, 3 de julio de 2011.

Tribunal Constitucional [Perú].Sentencia de 03 de enero de 2003. Exp. N.º 0010–2000–AI/TC

Tribunal Constitucional [Perú].Sentencia de 05 de julio de 2004. Exp. N.º 0090–2004–AA/TC

Tribunal Constitucional [Perú].Sentencia de 18 de agosto de 2004. Exp. N.º 1058-2004-AA/TC.

Tribunal Constitucional [Perú].Sentencia de 18 de febrero de 2005. Exp. N.º 2235–2004–AA/TC

Tribunal Constitucional [Perú].Sentencia de 18 de abril de 2007. Exp. N.º 4637-2006-PA/TC

Tribunal Constitucional [Perú].Sentencia de 29 de agosto de 2007. Exp. N.º 0009-2007-PI/TC

Tribunal Constitucional [Perú].Sentencia de 15 de octubre de 2007.Exp. N.º 4739-2007-HD/TC

Tribunal Constitucional [Perú].Sentencia del 30 de mayo de 2011. Exp. N.º 4227-2009-HD/TC

Sentencia del Tribunal Europeo de Derechos Humanos (Sección Cuarta). Caso Copland contra Reino Unido, del 3 de abril de 2007

Sentencia del Tribunal Europeo de Derechos Humanos (Gran Sala). Caso Barbulescu contra Rumanía, del 5 de septiembre de 2017.

Sentencia del Tribunal Supremo de España (Sala de lo Social, Sección 1ª) n.° 966/2006 de 26 de setiembre de 2007.

Sentencia del Tribunal Supremo de España (Sala de lo Social, Sección 1ª) n.° 8876-2011 de 6 de octubre de 2011.

Sentencia del Tribunal Constitucional [España]. Sentencia 29/2013, del 11 de febrero de 2013. BOE 61, del 12 de marzo de 2013.