LA CIBERSEGURIDAD DE LA INFORMACIÓN DEL EMPLEADOR Y LA FISCALIZACIÓN DEL TRABAJO REMOTO: ALCANCES Y LÍMITES

André Jorge Cossio Peralta.

Resumen:

En este artículo, el autor aborda la problemática de la implementación de mecanismos de ciberseguridad de la información del empleador en el contexto de la masificación de la modalidad de trabajo remoto implementado en el Perú a propósito de la pandemia generada por la Covid-19. El autor analiza si el monitoreo de la prestación de servicios bajo esta modalidad, así como la fiscalización de los correos electrónicos del empleador, resultan compatibles con el respeto a los derechos fundamentales a la intimidad, vida privada y secreto e inviolabilidad de las comunicaciones del trabajador.

Abstract:

In this article, the author addresses the problem of the implementation of cybersecurity mechanisms for employer information in the context of the massification of the remote work modality implemented in Perú in connection with the pandemic generated by Covid-19. The author analyzes whether the monitoring of the provision of services under this modality, as well as the control of the employer's emails, are compatible with respect for the fundamental rights to privacy, private life and secrecy and inviolability of the worker's communication´s.

Palabras clave:
Ciberseguridad, información, empleador, trabajador, intimidad.

Keywords
Cybersecurity, information, employer, worker, privacy.

* Abogado y Magíster en Derecho del Trabajo y de la Seguridad Social por la Pontificia Universidad Católica del Perú (PUCP). Profesor de Derecho Laboral Especial en la PUCP. Asociado Principal de Rubio, Leguía, Normand. Miembro de la Sociedad Peruana de Derecho del Trabajo y de la Seguridad Social.
Correos electrónicos: acossio@rubio.pe y acossio@pucp.pe

Introducción

La relación de trabajo ha pasado por diversas etapas. Mucho antes de lo que nosotros conocemos como contrato de trabajo o relación laboral, hasta el siglo XVI el término "trabajo" se utilizaba para denominar la actividad del verdugo; en paralelo, surgieron las ocupaciones bajo un concepto negativo del trabajo como castigo; en el siglo XVI pasa a ser una obligación para obtener la salvación divina que luego es aprovechado por sectores emergentes para que surja el trabajo asalariado de aquellas personas que realizan sus actividades dentro de las fábricas[1]; con ello, a fines del siglo XIX e inicios del XX, se pasa a una organización del trabajo bajo el modelo Taylor-Fordista; y, a finales de los años setenta del siglo XX, a los modelos *just in time* y de especialización flexible[2].

La pandemia generada por el brote del nuevo coronavirus SARS-CoV2 que causa la enfermedad Covid-19 ha ocasionado que se acelere el paso hacia la nueva organización del trabajo. Así, quedará registrado en los libros de historia que, a inicios de la década del veinte del siglo XXI, el trabajo se organizó en: trabajo presencial; esto es, el desarrollado al interior de un centro de labores o de operaciones; y, el trabajo no presencial, caracterizado por una prestación de servicios que se ejecuta en cualquier lugar fuera de un establecimiento o espacio de trabajo, siendo indispensable la conexión o vinculación con el empleador mediante el uso de las Tecnologías de la Información y Comunicación (TIC).

1 Cfr. ALBALATE, Joaquín Juan. *"Trabajo, Mercado de Trabajo y Relaciones Laborales"*. Madrid: Tecnos, 2015, págs. 60-74.

2 Ídem, págs. 111-131.

La distancia social, como medida de prevención frente a la Covid-19, trajo consigo la necesidad de que los empleadores deban reorganizar sus actividades para que estas sigan ejecutándose, a pesar de las cuarentenas obligatorias dispuestas en un sinnúmero de países a nivel mundial. La Organización Internacional del Trabajo (OIT) ha señalado que la pandemia obligó a que tanto los empleadores que ya tenían experiencia aplicando trabajo remoto, como las que no, tengan que crear las condiciones para enviar a sus trabajadores a sus domicilios, con lo que se ha producido el mayor experimento masivo de teletrabajo en la historia[3]. La OIT ha observado que los países más afectados por la pandemia y que ya tenían alguna experiencia con el teletrabajo, han sido los que han presentado un mayor incremento del teletrabajo, siendo que, por ejemplo, en Finlandia el 60% de los trabajadores pasaron a laborar en sus domicilios; 50% en Luxemburgo, los Países Bajos, Bélgica y Dinamarca; y, 40% en países como Suecia, Irlanda, Austria e Italia[4].

En nuestro país, contamos con una Ley del Teletrabajo, Ley Nº 30036, publicada el 5 de junio de 2013; y, su Reglamento, aprobado por Decreto Supremo Nº 017-2015-TR, publicado el 2 de noviembre de 2015; regulación que podría haber sido utilizada para afrontar las medidas de distanciamiento social y paralización de actividades decretadas por el Gobierno desde el 15 de marzo de 2020. Sin embargo, a pesar de contar con una legislación particular sobre la materia con algunos años de vigencia previos a la aparición de la pandemia por Covid-19, lo cierto es que esta modalidad ha sido escasamente utilizada por los empleadores[5]. Quizá por el carácter voluntario del teletrabajo o quizá por otros diversos factores que no serán materia de este trabajo, mediante Decreto de Urgencia Nº 026-2020 del 15 de marzo de 2020, el Gobierno creó una modalidad especial de prestación de labores subordinadas denominada "trabajo remoto", la

3 ORGANIZACIÓN INTERNACIONAL DEL TRABAJO. *"Teleworking during the COVID-19 pandemic and beyond. A practical guide"*. Génova: Oficina Internacional del Trabajo, 2020, pág. 1.

4 Ídem, pág. 3.

5 Cabe destacar que a la fecha no existe información oficial sobre la cantidad de teletrabajadores existente en el Perú, a pesar de que el 11 de julio de 2016 el entonces titular del Ministerio de Trabajo y Promoción del Empleo (MTPE) Daniel Maurate anunció la publicación de una estadística oficial que permita registrar la cantidad de teletrabajadores en el Perú. Ver: https://andina.pe/agencia/noticia-teletrabajo-mtpe-contarapronto-estadistica-a-nivel-nacional-620835.aspx

cual estará en vigencia durante el tiempo que se prolongue la emergencia sanitaria nacional[6]. A diferencia del Teletrabajo, el Trabajo Remoto es asignado de forma unilateral por el empleador[7]; es decir, se prescinde del carácter voluntario por parte del trabajador—aspecto característico del Teletrabajo—para facilitar la migración masiva de los trabajadores a esta modalidad y así asegurar la continuidad de las actividades en esta "nueva normalidad".

Sin embargo, existen múltiples actividades que, necesariamente, tienen que ejecutarse de forma presencial; y, otras que sí pueden ser objeto de trabajo no presencial. Al interior de una entidad o empresa, el trabajo no presencial—en mayor medida—ha sido aplicado a los denominados *"White collar workers"*; es decir, aquellos que realizan actividades administrativas, de oficina al servicio de la empresa y no ejecutan actividades físicas, manuales o de otro tipo; y, no para los *"Blue collar workers",* aquellos que realizan trabajo manual, en agricultura, manufactura, construcción, minería, mantenimiento, y, en general, actividades operativas[8]. Esta diferenciación permite recurrir a la clásica categorización entre empleados—los que ejecutan labores de oficina—y obreros—los que realizan actividades manuales u operativas—.

Esta clásica categorización sigue siendo utilizada en las estadísticas oficiales del Ministerio de Trabajo y Promoción del Empleo (MTPE). Por ejemplo, al cierre del año 2019, en las Planillas Mensuales de Pagos y T-Registro de los empleadores de los diversos sectores económicos, según categoría ocupacional, existían registrados del total de 3'641,577 trabajadores declarados en las planillas electrónicas a nivel nacional: 84,891 trabajadores ejecutivos (2.33%); 2'502,041

6 De acuerdo con la única disposición complementaria modificatoria del Decreto de Urgencia Nº 127-2020, se modificó la cuarta disposición complementaria del Decreto de Urgencia N° 026-2020, por lo cual el régimen de trabajo remoto estará en vigencia hasta el 31 de julio de 2021.

7 Con excepción de la asignación de trabajo remoto a las Personas con Discapacidad (PCD). En efecto, en el artículo 4.7 del Decreto Legislativo Nº 1468, publicado en el diario oficial "el Peruano" el 23 de abril de 2020, precisó que el trabajo remoto se aplicará de común acuerdo con la PCD. De este modo, si dada la incompatibilidad de las actividades que desarrolla una PCD con el trabajo remoto; o, a falta de acuerdo, el empleador deberá otorgar una licencia con goce de haber hasta la fecha que culmine la emergencia sanitaria.

8 PARIETTI, Melissa. *"Blue Collar vs. White Collar: What´s the Difference?* En: Investopedia. https://www.investopedia.com/articles/wealth-management/120215/blue-collar-vs-white-collar-differente-social-classes.asp hrs. 09/09/2020 19:01 hrs.

trabajadores empleados (68.71%); 978,401 trabajadores obreros (26.87%); y, 76,244 trabajadores no determinados en una categoría ocupacional, lo que representa el 2.09%[9].

En este contexto, los empleadores han asignado trabajo remoto a todos aquellos trabajadores cuyas actividades son compatibles con dicha modalidad, por lo que resultaría probable que, a la fecha, el 70% de los trabajadores ejecutivos y empleados—conforme a la categorización del MTPE—se encuentre prestando servicios bajo esta modalidad. Para este efecto, diversos empleadores han permitido que sus trabajadores retiren las computadoras de sus oficinas; o, han solicitado que accedan a una Red Privada Virtual (VPN, por sus siglas en inglés) desde sus computadoras personales, *tablets*, *iPads*, entre otros dispositivos (BYOD, por las siglas en inglés de *Bring Your Own Device*) y así continúen prestando servicios de forma remota. En ambos casos, el acceso o la conexión a internet se realiza a través de la red doméstica de cada trabajador, la cual, conforme al régimen de trabajo remoto, no necesariamente requiere una compensación económica por parte del empleador[10].

No obstante, la prestación de servicios a través del trabajo remoto ha preocupado aún más a los empleadores respecto a los mecanismos de seguridad que deben implementar para proteger la información corporativa; y, al mismo tiempo, fiscalizar la adecuada realización de las actividades de su personal. De este modo, cobra particular relevancia el análisis de la procedencia del uso de softwares que el empleador puede emplear para instalar softwares de rastreo de correos electrónicos corporativos, de los datos de navegación, bloqueo de páginas web, de ventanas emergentes, efectuar grabaciones de las reuniones en plataformas digitales de videoconferencias, intervención de plataformas de mensajería instantánea, entre otros.

9 Datos extraídos del cuadro Nº 66 del Anuario Estadístico del 2019 del Ministerio de Trabajo y Promoción del Empleo. https://cdn.www.gob.pe/uploads/document/file/920578/ANUARIO_2019_.pdf

10 Conforme a lo dispuesto en el artículo 19º del Decreto de Urgencia Nº 026-2020 y el artículo 7º del Decreto Supremo Nº 010-2020-TR, las partes pueden acordar la compensación de los gastos adicionales, cuando los medios o mecanismos para el desarrollo del trabajo remoto son proporcionados por el trabajador.

Esta nueva forma de ejercicio de las facultades de fiscalización del empleador podría afectar derechos fundamentales del trabajador, tales como el secreto e inviolabilidad de sus comunicaciones y documentos privados; la intimidad personal y vida privada. En el presente artículo, y conforme a las limitaciones de espacio, pretendemos examinar las particularidades de la protección de la información durante la masiva migración del trabajo remoto, las formas de control de esta modalidad y cómo ello se conjuga con el respeto de los referidos derechos fundamentales del trabajador.

1. La protección de la información del empleador durante el trabajo remoto: la ciberseguridad

El Instituto Nacional de Normas y Tecnología (NIST por sus siglas en inglés) del Departamento de Comercio de los Estados Unidos de América (EUA) sostiene que los equipos utilizados para el teletrabajo se encuentran generalmente en mayor riesgo de ataques cibernéticos en ambientes externos a la empresa que dentro de las mismas, por lo que las compañías deben implementar superiores elementos de seguridad que permitan cautelar la información corporativa[11]. En este contexto de masiva migración al trabajo remoto a causa de la Covid-19, se ha incrementado la vulnerabilidad de las plataformas de conectividad, dado que existen diversos hackers alrededor del mundo que pretenden sacar provecho del incremento de las actividades en línea, mediante ataques de *fishing*, virus y otros atentados cibernéticos[12].

Por ejemplo, en el sector financiero, el Fondo Monetario Internacional (FMI) ha identificado que las personas que no se encuentran familiarizadas con el teletrabajo y que están bajo el estrés de la pandemia son un blanco fácil para ataques de *fishing*, pues los ciber hackers se aprovechan de esta situación para enviar invitaciones y enlaces dañinos que pueden infectar los dispositivos

11 NATIONAL INSTITUTE OF STANDARS AND TECHNOLOGY. *"Guide to Enterprise Telework, Remote Access, and BYOD Security. NIST SP 800-46, Rev. 2"*. Gaithersburg: NIST, 2016, pág. vii.

12 OKEREAFOR, Kenneth y MANNY, Philip. *"Understanding Cybersecurity Challenges of Telecommuting and Conferencing Applications in the COVID-19 Pandemic"*. En: *International Journal in IT & Engineering* (IJITE), Volumen 8, Número 6, junio de 2020, pág. 14.

y sistemas operativos de las compañías[13]. De ahí que el FMI haya efectuado una serie de recomendaciones para las instituciones financieras, tales como limitar los servicios de acceso remoto a red y con perfiles de usuario; evaluación previa de almacenamiento de datos en la nube; utilizar plataformas de videoconferencias que tengan sistemas de protección de información adecuados; sensibilizar al personal sobre la ciberseguridad durante el teletrabajo, entre otras[14].

El NIST de los EUA considera que los más comunes objetivos de seguridad de todas las herramientas implementadas para asegurar la prestación de servicios de forma remota son: a) confidencialidad, garantizando que los mecanismos de acceso remoto no sean accesibles para partes no autorizadas; b) integridad, detectando cualquier cambio intencional o no intencional en los mecanismos de acceso remoto; y, c) disponibilidad, es decir, que los trabajadores puedan tener acceso remoto a la información en cualquier momento[15]. Esta misma entidad resalta que los métodos más frecuentes de acceso remoto que los empleadores utilizan para facilitar el teletrabajo son: la tunelización (mediante la creación de VPN's del empleador a la cual accede el trabajador a través de su dispositivo); portales de aplicación (a través de un servidor que ofrece el acceso a diversas aplicaciones del empleador mediante una interface); acceso al escritorio remoto (el trabajador accede directa o indirectamente desde su computadora o dispositivo personal a la computadora de la organización); y, aplicaciones de acceso directo (no se usa algún software de acceso remoto, pues el trabajador accede directamente a las aplicaciones del empleador a través del internet, como por ejemplo el correo web de la compañía)[16].

Okereafor y Manny han identificado algunos factores directos e indirectos que comprometen la seguridad de la prestación de servicios de forma remota o desde los hogares (WFH, por las siglas en inglés de *"Work From Home"*), tales como: (i) redes inseguras e inadecuados ancho de banda en plataformas de videoconferencias, las cuales permiten la irrupción de ciber ataques durante

13 FONDO MONETARIO INTERNACIONAL. "*Ciberseguridad del teletrabajo durante la pandemia*". En: https://www.imf.org/~/media/Files/Publications/covid19-special-notes/Spanish/sp-special-series-on-covid-19-cybersecurity-of-remote-work-during-pandemic.ashx 10/09/2020 19:28 horas, pág. 2.

14 Ídem, pág. 3.

15 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Op. cit., pág. 2.

16 Ídem, págs. 5-10.

las sesiones; (ii) desconocimiento de los trabajadores sobre elementales medidas de ciberseguridad, como por ejemplo no compartir datos de usuario o ID de reuniones virtuales en redes sociales; (iii) problemas al compartir información confidencial en redes abiertas durante el trabajo remoto; (iv) utilización de terminales inseguros para desarrollar el trabajo remoto; (v) colusión interna por parte de los propios trabajadores que comparten intencionalmente los ID de las sesiones remotas o credenciales a terceras personas con intención de perjudicar a la compañía; (vi) ataques de ingeniería social mediante la utilización trucos psicológicos para generar un sentimiento de decepción en el trabajador y que este divulgue información confidencial; y, (vi) errores de distracción inadvertidos por parte de los trabajadores[17].

En la migración masiva del trabajo remoto, ya sea con la entrega de dispositivos de propiedad del empleador o mediante políticas de BYOD—bajo VPN's, aplicaciones a los sistemas de la empresa, acceso a escritorio remoto, entre otras—no cabe duda de que existe un legítimo derecho del empleador de tutelar o proteger la información correspondiente a la marcha de sus actividades. En efecto, el empleador recurre a diversos activos tangibles e intangibles para el desarrollo de sus actividades. Así, las plataformas virtuales, sistemas de información, programas operativos, softwares de organización de labores, entre otros, constituyen bienes o activos intangibles de particular valor para el empleador, por lo que éste encuentra válida justificación para implementar políticas y/o protocolos que los protejan y/o preserven.

En situaciones normales—en las que los trabajadores desarrollan sus actividades desde las oficinas del empleador—claramente existe un mayor nivel de seguridad de la información corporativa, puesto que el personal accede a computadores o dispositivos que, por lo general, cuentan con antivirus o softwares necesarios para proteger el sistema operativo de ataques cibernéticos. Más aún, los trabajadores acceden al internet a través de una red corporativa privada que cuenta con estos programas informáticos de protección, como por ejemplo, antivirus, antispams, bloqueo de ventanas emergentes, de determinadas páginas web, entre otras. El personal, debido a la relación de subordinación y como parte del deber general de buena fe en el ejercicio de sus funciones, tiene la obligación

17 OKEREAFOR, Kenneth y MANNY, Philip. Op. Cit., pág. 19.

de acatar—en tanto no se afecten derechos fundamentales, como veremos más adelante—las políticas de seguridad de la información de su empleador.

Así, de una parte, en esta nueva normalidad, el empleador debe reforzar, e incluso duplicar, los niveles de protección de la información, debido a que ya no cuenta con las mismas herramientas de seguridad que aplicaba cuando los trabajadores prestaban servicios a través de sus redes corporativas dentro de las instalaciones de la empresa, lo que implica que el trabajador deba cumplir con las directivas y políticas de seguridad de la información que para este efecto le sean impartidas. De otra parte, esa facultad del empleador no podría aplicarse con la misma intensidad cuando los servicios son prestados de forma remota, ya sea desde las computadoras de la empresa o de sus BYOD, utilizando sus redes de navegación domésticas.

Precisamente, la posibilidad de que los trabajadores puedan conectarse desde sus redes domésticas o mediante cualquier red *wi-fi* pública para ingresar a las plataformas de acceso remoto diseñadas por el empleador, incrementa el riesgo de ataques cibernéticos a los sistemas e información confidencial de éste. Ejemplos de ataques cibernéticos pueden darse mediante la interceptación de mensajes del correo electrónico, obtención de datos de compañeros de trabajo, acceder a información confidencial o infectar los mecanismos de comunicación de la empresa[18]. En este sentido, se justifica que el empleador adopte protocolos más estrictos de seguridad de la información, los cuales deberán observar los trabajadores durante la prestación de servicios a través de la modalidad de trabajo remoto.

Así, y como una forma de reconocer el mayor riesgo al que se encuentra expuesta la información de los empleadores en la prestación de servicios fuera del centro de trabajo, en el régimen de trabajo remoto aprobado por el Decreto de Urgencia Nº 026-2020 se ha establecido literalmente que el personal está obligado a "(…) cumplir con la normativa vigente sobre seguridad de la información, protección de la confidencialidad de los datos, así como guardar confidencialidad de la información proporcionada por el empleador para la

18 GÓMEZ BLANCO, Ana. *"Teletrabajo y ciberseguridad: ¿cómo proteger nuestra información corporativa durante el confinamiento?"*. En: https://www.bbva.com/es/teletrabajo-y-ciberseguridad-como-proteger-nuestra-informacion-corporativa-durante-el-confinamiento/ 11/09/2020 18:45 horas.

prestación de los servicios"[19]. Por su parte, el Decreto Supremo Nº 010-2020-TR precisa que el empleador debe otorgar las instrucciones necesarias para la adecuada utilización de los sistemas, plataformas o aplicativos informáticos para el desarrollo de la actividad bajo esta modalidad[20]; y, que se encuentra facultado a restringir el acceso a sus sistemas de información, así como a comunicar las responsabilidades que asumirá el trabajador, en caso de un uso indebido de estos sistemas[21].

En consecuencia, en el particular régimen del trabajo remoto aprobado en nuestro país, se reconoce el derecho y/o facultad del empleador de establecer mecanismos que permitan proteger adecuadamente su información. De esta forma, los empleadores podrán implementar herramientas de ciberseguridad que el trabajador deberá acatar, como parte de su deber general de buena fe durante la prestación de sus servicios. Resulta relevante resaltar, como bien sostuvo Livellara, que durante la ejecución del contrato de trabajo, el trabajador tiene que prestar sus servicios de forma idónea a los fines de la empresa, actuando con diligencia y colaboración, observando los deberes de fidelidad que sean acordes a las labores desempeñadas; preservando la confidencialidad o secreto de la información a la que tenga acceso; y cumpliendo las órdenes e instrucciones que brinde el empleador para la ejecución de sus servicios[22].

2. Mecanismos de vigilancia de la productividad durante el trabajo remoto: el nuevo ejercicio del poder de dirección

El artículo 16º del Decreto de Urgencia Nº 026-2020 enfatizó que la modalidad de trabajo remoto se caracteriza por tratarse de una prestación *subordinada* de servicios que se ejecuta fuera del centro de trabajo a través de las TICs. A pesar de que el servicio se preste fuera de las instalaciones del empleador, el trabajador permanece bajo el poder de dirección y control de aquel.

19 Artículo 18.2.1 del Decreto de Urgencia 026-2020.

20 Artículo 6.2 del Decreto Supremo Nº 010-2020-TR.

21 Artículo 6.3 del Decreto Supremo Nº 010-2020-TR.

22 LIVELLARA, Carlos. *"Derechos y deberes de las partes"*. En: Tratado de Derecho del Trabajo. Director: Antonio Vásquez Vialard. Tomo 3. Capítulo XI. Buenos Aires: Editorial Astrea, 1982, pág. 603.

Recordemos que, por el poder de dirección, el empleador detenta las facultades de reglamentación, organización de las actividades, fiscalización y supervisión del adecuado desarrollo de la prestación de servicios de los trabajadores. Hernández Rueda señalaba que una de las manifestaciones de este poder se concreta en la facultad de implementar mecanismos de control y vigilancia del servicio prestado por el trabajador, de modo que se ejecute conforme a las necesidades de la empresa[23]. Estas facultades se encuentran expresamente reconocidas por nuestro ordenamiento legal, dado que "(…) por la subordinación, el trabajador presta sus servicios bajo dirección del empleador, el cual tiene facultades para normar reglamentariamente las labores, dictar las órdenes necesarias para la ejecución de las mismas, y sancionar disciplinariamente (…)"[24].

En la ejecución de las labores dentro de las instalaciones de la empresa y durante la jornada de trabajo, no existe discusión alguna sobre las facultades del empleador de fiscalizar, supervisar y/o controlar la productividad y adecuada prestación de los servicios de su personal[25]. Así, por ejemplo, el empleador puede fiscalizar y sancionar a aquellos trabajadores que utilicen las horas de trabajo para atender asuntos personales (p.ejm. emails, redes sociales, páginas de mensajería instantánea, entre otras) afectando así su productividad. A este tipo de conductas se le ha denominado *"cyberloafing"*, pues el personal utiliza las computadoras y el internet proporcionado por el empleador para fines ajenos a sus obligaciones laborales durante las horas de trabajo[26].

Estas facultades de control se trasladan a la modalidad de trabajo remoto, con la complejidad que el personal está fuera del centro de trabajo y, por lo general,

23 HERNANDEZ RUEDA, Lupo. *"Poder de Dirección del Empleador"*. En: Instituciones del Derecho del Trabajo y de la Seguridad Social. Coordinadores: Néstor de Buen y Emilio Morgado Valenzuela. Primera Edición. Ciudad de México: Universidad Autónoma de México, 1997, págs. 406 – 407.

24 Artículo 9º del Texto Único Ordenado del Decreto Legislativo Nº 728, Ley de Productividad y Competitividad Laboral, aprobado por Decreto Supremo Nº 003-97-TR.

25 Para los fines de este trabajo solo nos referiremos al personal sujeto a fiscalización inmediata del empleador y, por ende, sujeto al cumplimiento de los límites máximos de jornada de 8 horas diarias o 48 horas semanales.

26 KIDWELL, Roland E. y Robert SPRAGUE. *"Electronic surveillance in the global workplace: laws, ethics, research and practice"*. En: *New Technology, Work and Employment.* Oxford: *Blackwell Publishing Ltd*. Volumen 2, Número 24, 2009, pág. 196.

utiliza una red doméstica e, inclusive, una red pública (wifi). Sin embargo, esta particular circunstancia no exonera al trabajador de sujetarse a los mecanismos de vigilancia y control de su productividad que pueda haber implementado su empleador.

Más aún, esta facultad del empleador ha sido reconocida de forma expresa en el artículo 5.5 del Decreto Supremo Nº 010-2020-TR, toda vez que será responsabilidad de éste:

> "(…) la implementación de los mecanismos de supervisión y reporte de las labores realizadas durante la jornada laboral, de ser el caso, mediante el empleo de mecanismos virtuales. El/la empleador/a no podrá alegar el incumplimiento de las obligaciones del/la trabajador/a si no ha previsto o no ha dejado constancia explícita de las labores asignadas al/la trabajador/a y sus mecanismos de supervisión y reporte".

De la norma antes citada se desprende de forma clara que el empleador debe implementar alguna herramienta de supervisión y control de la prestación de servicios de su personal bajo esta modalidad; y, a la vez, deberá informar cuáles serán sus alcances. De lo contrario, el empleador no podrá acusar e imputar de forma legítima algún tipo de incumplimiento de obligaciones laborales por parte de su personal.

Estas herramientas o mecanismos de control de la productividad del personal se conocen como *"Electronic perfomance monitoring"* (EPM)[27] o *"Electronic Surveillance"* (ES)[28]. Para Kidwell y Sprague, estas herramientas consisten en la utilización de instrumentos tecnológicos por parte del empleador para recolectar información relativa al rendimiento y conducta de la fuerza de trabajo, con el objetivo de mejorar la productividad, controlar el centro de trabajo, entre otros[29]. Por su parte, Jeske y Santuzzi acotan que la implementación de un EPM tiene por objeto verificar un adecuado nivel de rendimiento del personal, midiendo el ritmo de trabajo y la precisión, con la diferencia de que estas herramientas—a

27 JESKE, Debora y Alecia M. SANTUZZI. *"Monitoring what and how: psychological implications of electronic performance monitoring"*. En: *New Technology, Work and Employment.* Oxford: *John Wiley & Sons Ltd.* Volumen 1, Número 30, 2015, pág. 62.

28 KIDWELL, Roland E. y Robert SPRAGUE. Op. Cit., pág. 194.

29 Ídem, pág. 196.

diferencia de los métodos tradicionales o convencionales—brindan datos más precisos enfocados en el desempeño y la productividad de los trabajadores[30].

No obstante, la implementación de medidas de ciberseguridad de la información del empleador y de EPM's en el marco de la masiva transición al trabajo remoto, deberán examinarse a la luz de criterios de razonabilidad, vale decir, que se adecúen a legítimos propósitos de tutela de los bienes intangibles de las organizaciones y de control de la idoneidad de la prestación de servicios por parte del trabajador. A la vez, deberá ser objeto de ponderación entre el derecho a libertad de empresa, que en esta materia se manifiesta a través del poder de dirección del empleador, y el respeto de los derechos fundamentales del trabajador, máxime si, conforme se encuentra reconocido en nuestra Constitución, ninguna relación laboral—incluyendo la que se ejecuta bajo la modalidad de trabajo remoto—puede desconocer o limitar los derechos fundamentales, ni rebajar la dignidad del trabajador[31].

En las líneas que siguen nos proponemos examinar—con las limitaciones de espacio que corresponden a este trabajo—cómo se conjuga la facultad del empleador para implementar estas formas protección de la información de la empresa y control del trabajo remoto del trabajador en un contexto de masiva transición a esta modalidad de prestación de servicios, con los derechos fundamentales de los trabajadores relativos al secreto y la inviolabilidad de las comunicaciones y documentos privados; intimidad personal y vida privada.

3. La ciberseguridad y el derecho al secreto e inviolabilidad de las comunicaciones y documentos privados del trabajador

En el primer punto del presente trabajo, hemos señalado los mecanismos de ciberseguridad que puede implementar el empleador para proteger sus bienes intangibles, como lo es la información, sistemas informáticos u otras plataformas virtuales; y que, en un contexto de migración masiva a la modalidad de trabajo remoto, se justifica la adopción de medidas de seguridad más intensas para proteger la información sensible y confidencial de la empresa.

30 JESKE, Debora y Alecia M. SANTUZZI. Op. Cit., pág. 63.

31 Artículo 23 de la Constitución de 1993.

Dada esta coyuntura, diversas organizaciones cuentan con protocolos de ciberseguridad respecto a la utilización de las cuentas de correo corporativo asignadas a su personal, tales como rastreo de mensajería instantánea desde tales cuentas hacia las cuentas de correo personal, o mediante aplicativos web que facilitan este tipo de comunicación, con el objetivo de preservar o cautelar que los trabajadores no filtren información sensible y/o confidencial que comprometa la seguridad—en el sentido amplio del término—de sus operaciones. No obstante, y en la medida que el personal—por lo general—utiliza sus datos de navegación (red doméstica) y no los de sus empleadores (red privada), podría cuestionarse que estos mecanismos afectan derechos fundamentales tales como al secreto e inviolabilidad de sus comunicaciones y documentos privados; o, incluso, lesionar el derecho a la intimidad personal y vida privada.

A continuación, sólo analizaremos la problemática del rastreo y acceso a los correos electrónicos corporativos; y, las restricciones de uso de aplicativos webs de mensajería instantánea.

A) Monitoreo de correos electrónicos corporativos

El inciso 10º del artículo 2º de la Constitución de 1993 reconoce el derecho de toda persona al secreto e inviolabilidad de sus comunicaciones y documentos privados. El procedimiento para la intervención de este derecho también se encuentra regulado en la Constitución, estableciéndose de forma expresa que las comunicaciones, telecomunicaciones o sus instrumentos solo pueden ser abiertos, interceptados, incautados u otro, únicamente mediante mandamiento motivado de juez o con las garantías previstas en la ley. No tendrán validez aquellos documentos privados que se obtengan infringiendo tales disposiciones.

La extensión de este derecho fundamental al ámbito laboral ha sido reconocida por el Tribunal Constitucional (TC) y la Corte Suprema de Justicia de la República (CSJR), al haber tenido la oportunidad de pronunciarse sobre la posibilidad de que el empleador de intervenga o acceda al contenido del correo electrónico corporativo que otorga a su personal.

En el año 2004, vale decir hace 16 años, en el conocido caso Serpost, el TC consideró que, a pesar de que el empleador sea el propietario de la fuente o soporte de las comunicaciones, este hecho no determina que aquel pueda tener

una titularidad exclusiva sobre estas y así no pueda garantizar el respeto a la inviolabilidad de las comunicaciones privadas por la existencia de una relación de trabajo. De ahí que el TC, sin perjuicio de reconocer las facultades de fiscalización del empleador, reitera que este debe utilizar los mecanismos previstos en la Constitución y en la ley para acceder al correo corporativo de sus trabajadores[32].

Por su parte, la CSJR, acogiendo los criterios vertidos por el TC en el caso Serpost, en la Casación Laboral Nº 14614-2016-LIMA consideró que constituía un exceso que el empleador establezca dentro del reglamento interno de trabajo que es propietario tanto de las cuentas de correo electrónico que otorga al personal, así como de su contenido y de los programas, página web e información. La CSJR añadió que admitir la validez de tal disposición implica colisionar con el derecho constitucional al secreto e inviolabilidad de las comunicaciones[33].

Con relación al caso Serpost, Blancas Bustamante recuerda que el TC reiteró su criterio en las sentencias recaídas en los Expedientes Nos. 04224-2009-PA/TC, 03599-2010-PA/TC y 00114-2011-PA/TC[34]. Este autor considera que la intervención del correo electrónico sin presencia del trabajador resulta ilegítima; y efectúa una distinción a partir de si el acceso a este medio de comunicación se realiza a través de la internet o de la intranet[35]. Así, acota que, en el primer supuesto, sólo el servidor es de propiedad del empleador, por lo que éste no podría intervenir directamente el correo electrónico; en cambio, en el segundo, tanto el correo como el servidor son de propiedad del empleador, lo que permite que éste último pueda controlar su uso y no se afectaría la intimidad del trabajador[36].

No obstante, consideramos que esta diferenciación no podría efectuarse en este tránsito masivo al trabajo remoto. El servidor de correo electrónico seguirá siendo del empleador, pero los datos de navegación o la red que se utilizará para

32 Cfr. Fundamentos jurídicos Nos. 18, 19, 20 y 21 de la sentencia recaída en el Expediente Nº 01058-2004-AA/TC.

33 Cfr. Considerandos décimo sexto a décimo octavo de la Casación Laboral Nº 14614-2016-LIMA publicada en el diario oficial "el Peruano" el día 30 de mayo de 2017.

34 BLANCAS BUSTAMANTE, Carlos. *"Derechos Fundamentales de la Persona y Relación de Trabajo"*. Segunda edición aumentada. Lima: Fondo Editorial de la Pontificia Universidad Católica del Perú, 2013, pág. 221.

35 Ídem, pág. 220.

36 Ibídem.

ingresar a los mecanismos de acceso remoto son propiedad del trabajador, ya sea que utilicen las computadoras de la empresa o los dispositivos de propiedad de los trabajadores. En este nuevo escenario, cobra mayor relevancia determinar si el derecho al secreto e inviolabilidad de las comunicaciones del trabajador resulta oponible, en mayor o menor grado de intensidad, respecto del correo corporativo proporcionado por el empleador. Para este efecto, será necesario recordar los alcances de este derecho.

Como bien sostiene Abad Yupanqui, el derecho al secreto de las comunicaciones constituye un derecho formal que comprende a toda forma de comunicación que no es equivalente al derecho a la intimidad; y que sirve de instrumento de protección de otros derechos, pero no de un derecho al "secreto de las conversaciones"[37]. Este derecho es de titularidad de las personas que participan en el proceso comunicativo, por lo que, acota el referido autor, es oponible a terceros (los que no participan en la comunicación); e, inclusive, como ha precisado la Corte Interamericana de Derechos Humanos, se opone tanto a las operaciones técnicas que registran el contenido, así como a cualquier elemento del proceso comunicativo en sí mismo (identidad de los interlocutores, registro y duración de las llamadas, entre otros)[38].

En la actualidad, a través del correo electrónico corporativo se brindan instrucciones, directivas u otras relacionadas con las labores, siendo lo usual que una empresa asigne una cuenta de correo a su personal[39]. Empero, y más aún en el contexto del tránsito masivo al trabajo remoto, el correo electrónico corporativo no solo constituye una herramienta de trabajo que los empleadores proporcionan al personal con fines de comunicación, sino también tiene la utilidad de ser la clave de acceso a todos sus sistemas de información.

---

37 ABAD YUPANQUI, Samuel. *"El derecho al secreto de las comunicaciones. Alcances, límites y desarrollo jurisprudencial".* En: Pensamiento Constitucional. Lima: Maestría de Derecho Constitucional de la Pontificia Universidad Católica del Perú. Año XVI, Número 16, 2012, pág. 15.

38 Ídem, pág. 17.

39 DE LAS CASAS DE LA TORRE UGARTE, Orlando. *"El poder de dirección y el uso de nuevas tecnologías".* En: QUIÑONES, Sergio (coord.). "*El Derecho del Trabajo en la Actualidad: Problemática y Prospectiva. Estudios en Homenaje a la Facultad de Derecho PUCP en su centenario".* Lima: Pontificia Universidad Católica del Perú, 2019, pág. 129.

Supongamos que Juan Pérez ingresa a trabajar a la empresa "La Sociedad S.R.L" y se le asigna la cuenta jperez@lasociedad.com. Con la clave y contraseña de este correo electrónico, Juan podrá ingresar a los ordenadores o plataformas digitales de la empresa, se comunicará con clientes de la compañía, terceras personas u otros compañeros de trabajo, que podrán identificarlo como parte de dicha empresa. De ahí que—en principio—los correos electrónicos que envíe se remitirán como un trabajador de la compañía, y no necesariamente a título personal, como así sucedería si utilizara su cuenta de correo personal jperez@gmail.com. La cuenta de correo corporativo tiene, por tanto, mayor utilidad en la actualidad, al constituir la credencial con la que el trabajador puede ingresar a las plataformas y sistemas de información del empleador. Resulta difícil que, a la fecha, alguna organización de cierto nivel permita que sus trabajadores accedan a sus sistemas de información, plataformas institucionales, entre otras, a través de cuentas de correo personales.

En el ejemplo planteado, la Sociedad, a propósito de la pandemia de la Covid-19, ha asignado trabajo remoto a Juan, quien utilizará su propia laptop y red doméstica para ingresar a la VPN creada por la empresa para que este pueda desarrollar sus actividades desde su domicilio. Como parte de los protocolos de seguridad de la información, se le ha comunicado que el correo electrónico se encontrará constantemente monitoreado para evitar la filtración de información confidencial, se prohibirá la remisión de correos electrónicos a su cuenta de correo personal, y que todos los correos que curse mediante su cuenta de correo corporativo deberán ser guardados/subidos en la nube / servidor de almacenamiento online diseñado por la empresa.

La empresa ha accedido al contenido de los correos electrónicos cursados por el trabajador, ¿se vulneró el derecho al secreto e inviolabilidad de las comunicaciones y documentos privados? Consideramos que no, toda vez que, en este escenario, el trabajador ha sido informado de los protocolos de seguridad de la información de la empresa y no tendría una expectativa de intimidad o privacidad de las comunicaciones que se cursen mediante el correo corporativo.

Este concepto (expectativa de intimidad o privacidad) ha sido utilizado por el Tribunal Europeo de Derechos Humanos (TEDH) en algunos casos en los que ha examinado la intervención de los correos electrónicos, datos de navegación

de internet, llamadas telefónicas, entre otros. En el Asunto Copland contra el Reino Unido, el TEDH consideró que los correos electrónicos remitidos desde el lugar de trabajo estaban protegidos por el derecho a la no intervención en la vida privada y correspondencia; a la vez, se reconoce que la demandante tenía una expectativa fundada de privacidad sobre esta comunicación, dado que no fue informada por su empleador del monitoreo de sus correos electrónicos[40]. En el caso Libert contra Francia, el TEDH consideró que legítimamente el empleador puede pretender verificar que sus trabajadores utilicen los equipos informáticos que se encuentran a su disposición para el desarrollo de sus funciones, conforme las obligaciones contractuales convenidas y a la regulación que resulte aplicable, pues este tiene un válido interés en asegurar el buen funcionamiento de sus actividades[41].

Este mismo tribunal, en el caso Barbulescu contra Rumanía, desarrolló y/o estableció diversos requisitos para admitir la validez los mecanismos de monitoreo del uso de la internet y correos corporativos del empleador: (i) el trabajador debe haber sido informado de forma clara y precisa del mecanismo de supervisión de sus comunicaciones y de forma previa a su implementación; (ii) los alcances de la supervisión realizada por el empleador y el número de personas que han accedido a los resultados; (iii) existencia objetivos legítimos que justifiquen la vigilancia de las comunicaciones y el acceso al contenido por parte del empleador; (iv) verificación de la existencia de mecanismos menos intrusivos; (iv) información de las consecuencias de la supervisión y si esta cumple con los objetivos establecidos por el empleador; entre otros[42].

Recientemente, los magistrados del TC, señores Blume Fortini, Ramos Núñez y Espinosa-Saldaña Barrera, presentaron un voto singular en minoría la sentencia recaída en el Expediente N° 00943-2016-PA/TC, en el que, recogiendo los criterios establecidos por el TEDH en el caso Barbulescu vs Rumanía, reconocieron la facultad del empleador de fiscalizar e intervenir el correo electrónico institucional que el empleador ha otorgado al trabajador, siempre

40 Cfr. párrafo 74 de la sentencia emitida por el TEDH en el Asunto Copland c. Reino Unido (Demanda nº 62617/00) del 3 de abril de 2007.

41 Cfr. párrafo 46º de la sentencia emitida por el TEDH en el Asunto Libert c. Francia (Demanda nº 588/2013) del 22 de febrero de 2018.

42 Cfr. párrafo 120 de la sentencia emitida por el TEDH en el Asunto Barbulescu c. Rumanía (Demanda nº 61496/2008) del 5 de setiembre de 2017.

que se haya cumplido con comunicar a este dicha posibilidad de monitorear sus conversaciones, así como las condiciones aplicables para la utilización de los bienes entregados por el empleador[43]. Este voto singular en minoría no constituye un cambio del criterio adoptado en el caso Serpost, prueba de ello es que en la sentencia recaída en el Expediente N° 04386-2017-PA/TC, en el que la mayoría de magistrados del TC ratificó íntegramente el criterio contenido en la sentencia del caso Serpost[44].

La expectativa de intimidad y privacidad también ha sido empleada por la Corte Suprema de los Estados Unidos de América para analizar los mecanismos de vigilancia del empleador. En efecto, Kidwell y Sprague recuerdan que en dicho país no existe derecho a la privacidad, a menos que exista una expectativa de intimidad (Katz vs. USA, 1967); si los trabajadores utilizan los equipos proporcionados por el empleador para el desarrollo de sus labores, entonces aquellos deberían tener una mínima expectativa de privacidad e intimidad; y, la mínima expectativa de intimidad quedará destruida si los empleadores notifican previamente a los trabajadores (EUA vs. Simons, 2000; TBG Ins. Services Corp. vs. Corte Superior, 2002)[45].

Sobre la base del concepto expectativa de intimidad, y teniendo en cuenta los mayores riesgos a los que se encuentra expuesta la información de los empleadores en este particular contexto de migración masiva al trabajo remoto, estimamos que si los empleadores cumplen con informar adecuada, precisa y minuciosa los alcances de las políticas de seguridad de la información a sus trabajadores para la utilización de los correos corporativos, disposiciones como las indicadas en

43 Ver fundamentos jurídicos Nos. 24 al 29 del voto singular de la sentencia recaída en el Expediente N° 00943-2016-AA/TC del 14 de julio de 2020. Cabe destacar que esta posición fue aceptada por la minoría de magistrados del TC, pues la mayoría de magistrados del TC votaron por declarar improcedente la demanda de amparo.

44 Los magistrados Ledesma Narváez, Miranda Canales, Blume Fortini, Ramos Núñez y Espinosa-Saldaña Barrera votaron por declarar fundada la demanda de amparo, pues estimaron que la Caja Municipal de Ahorro y Crédito de Piura había vulnerado el derecho al secreto e inviolabilidad de las comunicaciones del señor Edward Antonio Muñoz Salazar, al acceder indebidamente a sus correos electrónicos institucionales para sustentar su despido por la comisión de faltas graves. Así, se consideró que dichos correos electrónicos constituían una prueba ilícita que carece de todo valor probatorio. La sentencia fue emitida el 27 de octubre de 2020.

45 KIDWELL, Roland E. y Robert SPRAGUE. Op. Cit., págs. 198 y 199.

el ejemplo de líneas arriba (caso señor Juan Pérez), no constituirán una lesión o vulneración del derecho al secreto e inviolabilidad de las comunicaciones. En rigor, y si los empleadores adoptan parámetros como los descritos por el TEDH, el correo electrónico corporativo no se encontraría protegido por el derecho al secreto e inviolabilidad de las comunicaciones, pues se habría neutralizado la expectativa de privacidad del trabajador y, de esta forma, el empleador podría acceder—inclusive—al contenido de los correos cursados y recibidos por este.

No incidiría en esta conclusión el hecho que el trabajador utilice su red doméstica para ingresar a las plataformas de acceso remoto creadas por el trabajador. Creemos que, en estos casos, el análisis debe estar centrado en las políticas de seguridad de la información que deberá observar el trabajador durante la prestación efectiva de servicios bajo esta modalidad, ya sea que ejecute dicha prestación en la computadora o dispositivos proporcionados por su empleador, o se hayan adoptado políticas de BYOD. En ambos casos, la expectativa de privacidad quedará restringida al uso de las cuentas de correo personales distintas a las cuentas de correo corporativas asignadas por el empleador. La cuenta de correo personal será el espacio que se encontrará fuera del ámbito de fiscalización y control del empleador; por ende, este correo sí estará protegido por el derecho fundamental en referencia y solo podrá accederse a su contenido o ser intervenido, mediando las garantías previstas en la Constitución, es decir, por mandamiento motivado del Juez.

Inversamente, si el empleador no cumple con comunicar sus políticas y/o protocolos de ciberseguridad durante la prestación del trabajo remoto; o, incluso, si antes del paso a esta modalidad no se contaba con alguna directiva respecto al control y fiscalización de los correos electrónicos corporativos; entonces este medio de comunicación sí estará protegido por el derecho fundamental en referencia. En efecto, si el empleador no contó con una política de utilización y control del correo corporativo, probablemente los trabajadores habrán "personalizado" esta herramienta, de modo tal que no solo habría sido empleada para fines laborales, sino también personales. De forma evidente, en este supuesto no podría discernirse qué contenido del correo es de índole profesional y cuál corresponde al ámbito privado o personalísimo del trabajador, quedando protegido por las garantías previstas por la Constitución. Así, el empleador sólo podrá acceder al correo corporativo o por una autorización expresa del trabajador o por mandato judicial.

B) Restricciones al uso de aplicativos webs de mensajería instantánea

Proliferan en la internet múltiples páginas o aplicativos webs de mensajería instantánea, tales como *Whatsapp, Telegram, Facebook Messenger, Instagram Messenger* que pueden utilizarse desde las computadoras. Así, es frecuente que muchos usuarios (trabajadores, estudiantes, locadores de servicios, etc.) de estos aplicativos prefieren recurrir a las páginas web para no afectar el paquete de datos de sus dispositivos móviles (celulares). Estos aplicativos no solo permiten la transmisión de texto, sino también de fotografías, videos, archivos Word, pdf y, en general, de cualquier clase de archivo digital. Por este motivo, en el contexto de la aplicación masiva del trabajo remoto, los equipos de Tecnología de la Información de algunas organizaciones, como parte de los protocolos de seguridad de la información, recomiendan la implementación de restricciones a estas formas de comunicación instantánea.

Empero, la legalidad y/o validez este tipo de restricciones deben examinarse teniendo en cuenta que, dada la coyuntura, los trabajadores se encuentran prestando servicios de forma remota a través de sus redes de navegación domésticas. Particularmente, estimamos que el análisis de la validez de estas restricciones dependerá de si el titular del dispositivo es el empleador o el trabajador. Veamos:

a) *De propiedad del empleador:* Por lo general, las computadoras del empleador cuentan con todos los programas, aplicativos y antivirus necesarios para preservar la seguridad de la información. Por ende, a pesar de que los datos de navegación sean de propiedad del trabajador, este no podría tener una expectativa de uso pleno e irrestricto de los aplicativos de mensajería instantánea. Inclusive, los empleadores podrían instalar un software que detecte cualquier tipo de intento de transmisión de mensajes o archivos mediante estas aplicaciones. A la intervención de estos aplicativos por parte del empleador no podría oponérsele el derecho al secreto e inviolabilidad de las comunicaciones. No advertimos que exista una expectativa legítima de privacidad e intimidad del trabajador respecto de estos aplicativos cuando utilice la computadora de propiedad de la empresa.

b) *De propiedad del trabajador:* Si para la prestación del trabajo remoto el trabajador accede a una VPN creada por la empresa o ingresa al escritorio remoto de su computadora corporativa, aquel se encontrará sujeto al cumplimiento las restricciones dispuestas por esta para la utiliza-

ción de aplicativos webs de mensajería instantánea. Sin embargo, estas restricciones no podrían ejecutarse mientras el trabajador hace uso de su escritorio personal. En este último caso, el trabajador goza de las más amplías libertades de navegación a través del internet, incluyendo la utilización de la mensajería instantánea por web, sin perjuicio de adoptar las medidas comunes de seguridad de navegación por internet (no compartir contraseñas, actualizar antivirus, no responder correos inseguros, entre otros).

4. Monitoreo del trabajo remoto: intimidad, vida privada y la fiscalización de los datos de navegación de los trabajadores

En el segundo punto del presente trabajo examinamos los EPM o ES que tienen por objeto monitorear el desempeño y la productividad de los trabajadores, y, de este modo, evitar el *cyberloafing*. Sin embargo, en el trabajo remoto, el servicio es prestado desde sus domicilios y a través de su red de navegación. Por tanto, los sistemas o mecanismos de control del trabajo efectivo por parte del empleador deben de considerar esta particularidad.

Respecto de los trabajadores sujetos a fiscalización inmediata del tiempo de trabajo que se encuentran en esta modalidad, el empleador cuenta con un interés legítimo de verificar que aquellos cumplan de forma efectiva con cada una de las obligaciones propias al cargo que desempeñan en la empresa, así como de observar la jornada de trabajo convenida. Ciertamente, no debe soslayarse que, en el régimen del trabajo remoto, se ha previsto que el trabajador *"(…) debe estar disponible durante la jornada de trabajo para las coordinaciones de carácter laboral que resulten necesarias (…)"*[46].

No obstante, y como toda medida de control y vigilancia de la prestación de trabajo por parte del empleador, los EPM que se implementen para verificar la productividad y desempeño durante el trabajo remoto deberán respetar o encontrarán un límite en los derechos fundamentales del trabajador, como por ejemplo a la intimidad y vida privada, máxime si la prestación se ejecuta—primordialmente—dentro del domicilio del trabajador, el cual constituye un espacio hermético de éste que se encuentra fuera de la esfera de control del empleador.

46 Artículo 9.4 del Decreto Supremo Nº 010-2020-TR.

En este sentido, la OIT ha señalado que la instalación de softwares que rastreen la actividad de los trabajadores, tales como verificación de la utilización del teclado, movimientos del *mouse* e, incluso, el traslado o desplazamiento del personal tienen una naturaleza particularmente intrusiva y, por ende, no son recomendados[47]. Así, pues, resultaría intrusivo y lesivo al derecho a la intimidad personal, la implementación de directivas que obliguen al trabajador a tener encendida en todo momento la cámara web de la computadora o dispositivo con el que presta servicios, con la finalidad de verificar que, de manera efectiva, cumple con la jornada de trabajo convenida con la empresa.

De igual forma, una directiva que obligue al personal a no editar el *backing* mientras se hace uso de las plataformas de videoconferencias (*Google meet*, *Microsoft teams*, *webex mettings*, zoom, etc.) resultaría invasiva a la esfera privada del trabajador, pues este no se encuentra obligado a exhibir el entorno en el que desarrolla su actividad, salvo que existan razones justificadas vinculadas—esencialmente—a las medidas de seguridad y salud en el trabajo. En el ámbito de las videoconferencias existen herramientas que permiten al empleador analizar la atención del personal, grabación de las reuniones en la nube con los datos de la imagen y voz que, incluso, puede filtrar sonidos del domicilio del trabajador[48].

Para Prous y Crouzet la utilización de estas medidas en el contexto del Covid-19 debe observar: a) un objetivo limitado, específico y legítimo; b) solo debe obtenerse la información que resulte necesaria y proporcional; c) transparencia, todos los trabajadores deben ser informados de los mecanismos que se utilizarán para monitorear la actividad; entre otros[49].

En definitiva, la validez de estas medidas de monitoreo del trabajo remoto quedará sujetas al *test* de proporcionalidad y razonabilidad: (i) idoneidad, adecuación de la medida con el objetivo legítimo; (ii) necesidad, que no existan medidas menos invasivas o lesivas al derecho fundamental; y, (iii) proporcionalidad en

47 ORGANIZACIÓN INTERNACIONAL DEL TRABAJO. Op. Cit., pág. 9.

48 PROUST, Olivier y Sixtine CROUZET. *"The risks of online employee monitoring during the COVID-19 crisis"*. En:https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/the-risks-of-online-employee-monitoring-during-the 13/09/20 00:06 horas

49 Ibídem.

sentido estricto, a mayor injerencia en el derecho fundamental, mayor deberá ser el objetivo o interés del empleador que se pretenda tutelar con la medida.

Reflexiones finales

La Covid-19 aceleró la migración a las actividades no presenciales y, con ello, a la utilización masiva del trabajo remoto. Si bien esta modalidad estará en vigencia hasta el 31 de julio de 2021, lo cierto es que—seguramente—se realizarán modificaciones o se aprobará una nueva Ley de Teletrabajo que permita la continuidad de una prestación laboral de servicios a distancia, mediante la utilización de TICs.

Como se ha examinado en este trabajo, la abrupta migración al trabajo remoto está obligando a las organizaciones a adoptar mayores medidas de ciberseguridad para preservar la confidencialidad e integridad de sus sistemas operativos. Para este efecto, los protocolos de monitoreo, seguimiento y fiscalización de las cuentas de correo corporativo del personal constituyen materias ineludibles por parte de los equipos de TI de las organizaciones. Estos protocolos deberán ser debidamente comunicados a los trabajadores, detallando sus alcances, objetivos y consecuencias ante eventuales incumplimientos. Así, se neutralizaría la expectativa de intimidad y privacidad y el correo electrónico corporativo quedaría fuera de los alcances del derecho al secreto e inviolabilidad de las comunicaciones.

La enorme facilidad y variedad de opciones con la que disponen los trabajadores para acceder a cuentas de correo gratuitas (*Gmail*, *Hotmail*, *Yahoo*, entre otras) permitiría una clara diferenciación entre un medio de comunicación privado y uno laboral. El correo electrónico personal será el medio infranqueable por el empleador y sujeto a las garantías previstas en la Constitución. El trabajador estará en plena capacidad de discernir el medio de comunicación que empleará para fines privados y personales.

Los pronunciamientos del TC y de la CSJR no fueron expedidos con carácter de precedente vinculante[50] y, como es obvio, se emitieron en una coyuntura

50 Si bien es cierto que la primera disposición final de la Ley Orgánica del TC dispone que los jueces y tribunales aplican las leyes y toda norma con rango de ley, conforme a los preceptos y principios constitucionales emanados de las sentencias del TC, también lo es que estas nuevas circunstancias demandan nuevas reflexiones que se adecúen a una etapa

distinta. La nueva "normalidad" exigirá por parte de las autoridades jurisdiccionales criterios que se adecúen a los riesgos cibernéticos presentes en la masiva en la migración al trabajo remoto. Por lo menos, los votos singulares en minoría emitidos en la sentencia recaída en el Expediente N° 00943-2016-AA/TC del 14 de julio de 2020 constituyen una positiva muestra—aunque débil—de pretender adecuar el criterio del caso Serpost a un contexto en el que predomina la utilización de las TICs por parte del empleador.

Por su parte, los mecanismos de fiscalización del trabajo remoto que se implementen encontrarán un límite en el respeto de los derechos fundamentales del trabajador. Es en este contexto en el que cobra mayor vigencia lo señalado por Valdez Dal Ré, quien sostuvo: *"el ejercicio de los derechos fundamentales ha de efectuarse en unos términos que resulten compatibles con el resto de derechos, bienes y valores constitucionalmente amparados, compatibilidad ésta que se garantiza mediante la imposición de unos límites a aquel ejercicio"*[51].

En resumen, las facultades de dirección del empleador y los derechos fundamentales de los trabajadores colisionan en esta nueva normalidad de prestación de servicios subordinados. La responsabilidad para resolver estos conflictos recaerá en los jueces, quienes tendrán que recurrir al *test* de proporcionalidad y razonabilidad. Aguardemos expectantes por su actuación.

de mayor intervención e innovación tecnológica.

51 VALDEZ DAL RÉ, Fernando. *"Los derechos fundamentales de la persona del trabajador"*. En: AA.VV. Libro de Informes Generales del XVII Congreso Mundial de Derecho del Trabajo y de la Seguridad Social. Montevideo: Asociación Uruguaya de Derecho del Trabajo y de la Seguridad Social, 2003, pág. 96.