SOBRE DATOS Y METADATOS

La nueva vigilancia y los retos que impone al derecho laboral

CAMILA SUZANA TARAMONA BARA

Estudiante de la Universidad del Pacifico.
Segundo puesto del Concurso Laboral Universitario.

1. LOS RETOS DE LA NUEVA TECNOLOGÍA

La vigilancia de trabajadores ha sido siempre un tema sensible y de amplio debate. La búsqueda del balance entre el poder de fiscalización y la privacidad e intimidad de los trabajadores parece no tener fin, sobre todo si sumamos a la ecuación la aparición de nuevas tecnologías casi a diario. Si bien la tecnología resulta de suma ayuda e importancia para el día a día laboral, lo cierto es que también impone nuevos retos para el empleador al comenzar a desdibujar los limites de sus facultades de control sobre los trabajadores.

Tomando como ejemplo un caso común, la regulación del uso del correo electrónico ha roto más de una cabeza jurídica al intentar delimitar las facultades y derechos de cada parte de la relación laboral. Como resulta evidente, esta gran herramienta fue utilizada, no solo como un elemento para facilitar la realización del trabajo, sino también para vigilar las labores de los trabajadores por parte del empleador.

El ejemplo del correo electrónico (caso que nos acompañará a lo largo del presente ensayo) resulta sumamente ilustrativo y no hace más que resaltar la constante pugna entre los derechos fundamentales del trabajador y el poder de fiscalización del empleador. Sin embargo, aún cuando hoy en día tenemos claros ciertos límites existentes a la vigilancia del correo electrónico, nuevos retos parecen estar a la vuelta de cada esquina.

El famoso caso Serpost, dio las primeras luces sobre la regulación del correo y el recorte de facultades del empleador, indicando, en pocas palabras, que el contenido de los mensajes electrónicos se encuentra fuera del alcance de este último. Sin embargo, como explicaremos luego, esta solución únicamente trae más preguntas que respuestas.

El principal problema radica en que, cuando pensamos en protección de las comunicaciones y correos electrónicos, lo primero que se nos viene a la cabeza es proteger el mensaje. Resulta plenamente razonable que no quiera que nadie vea lo que estoy escribiendo o enviado, en tanto tengo el derecho constitucional a la intimidad. Sin embargo, muchos no han reparado en que existen otros elementos paralelos y complementarios al contenido de un mensaje que pueden brindar incluso más información que el mensaje en sí: **los metadatos**.

2. SOBRE DATOS Y METADATOS: UNAS ACLARACIONES INICIALES

Antes que nada, resulta importante establecer claramente dos definiciones que ayudarán a entender mejor el problema planteado: el dato y el metadato. El dato es aquella información referente al contenido de la comunicación, la conversación, la foto que es transmitida de un usuario a otro. Se trata del mensaje comunicado. Mientras tanto, el metadato es la información sobre la comunicación mantenida. En el caso de un correo electrónico se incluye el usuario emisor y receptor, la hora en la que se envió un mensaje, la dirección IP, el asunto del correo. En el caso de las llamadas telefónicas, se considera metadato los usuarios intervinientes en la comunicación, la duración de la llamada, la geolocalización, etc. El metadato es información sobre la información.

Tomando como ejemplo un caso sencillo de la vida real tenemos lo siguiente: Cuando recibimos una carta, el dato es la carta en sí, el mensaje escrito. Mientras tanto, el metadato es la información que aparece en el sobre, referente al emisor y destinatario de la carta, la dirección de envío, etc. El metadato (la información del sobre) acompaña al dato (el mensaje de la carta). En palabras de Bruce Schneier, experto en seguridad informática y fundador de *Counterpane Internet Security*, *"Los datos son contenido y los metadatos el contexto"*[1]

1 Schneier, Bruce; *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World (*2015); obtenido de https://www.wired.com/2015/03/data-and-goliath-nsa-metadata-spying-your-secrets/. Texto original: "*Data is content, and metadata context"*

Tanto el dato como el metadato son informaciones sumamente relevantes y claves para que la comunicación se lleve a cabo efectivamente. No hay dato sin metadato, ni metadato sin dato. Se trata de dos caras de una misma moneda.

Inicialmente puede pensarse que el metadato, siendo únicamente contexto y no la comunicación o mensaje en sí, importa muy poco. En el caso del correo electrónico o de las llamadas telefónica, resulta natural que, antes que nada, me preocupe que alguien vea lo que escribo o escuche lo que digo. Sin embargo, los metadatos pueden abrir una gran ventana para observar nuestras actividades diarias.

Segun afirma Schneier *"Los metadatos pueden ser mucho más reveladores que los datos, especialmente cuando se recopilan en conjunto."* Asimismo, refiriéndose a los metdatos obtenidos de llamadas telefonicas[2], indica que *"[…] los metadatos telefónicos por sí solos revelan mucho sobre nosotros. El momento, la duración y la frecuencia de nuestras conversaciones revelan nuestras relaciones entre nosotros: nuestros amigos íntimos, socios comerciales y todos los demás. Los metadatos del teléfono revelan qué y en quién estamos interesados y qué es importante para nosotros, sin importar cuán privados sean. Proporciona una ventana a nuestras personalidades. Proporciona un resumen detallado de lo que nos está sucediendo en cualquier momento".* [3]

Como resulta evidente, no es necesario tener acceso al contenido de un mensaje o llamada para adentrarse en la vida y privacidad de una per-

2 Si bien no es nuestro ejemplo central (el correo electrónico), en el caso de los metadatos telefonicos tambien representan un caso preocupante ya que puede obtenerse informacion sobre el destinatario de la llamada, el tiempo de duracion de la conversacion, la frecuencia de las llamadas, la geolocalizacion, etc.

3 Schneier, Bruce; *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (2015); obtenido de https://www.wired.com/2015/03/data-and-goliath-nsa-metadata-spying-your-secrets/. Texto original en inglés: "*Metadata can be much more revealing than data, especially when collected in the aggregate. […] Telephone metadata alone reveals a lot about us. The timing, length, and frequency of our conversations reveal our relationships with each other: our intimate friends, business associates, and everyone in-between. Phone metadata reveals what and who we're interested in and what's important to us, no matter how private. It provides a window into our personalities. It provides a detailed summary of what's happening to us at any point in time."*

sona. El metadato es más que suficiente. De hecho, según ex oficiales del gobierno americano, *"si tienes suficientes metadatos, realmente no necesitas el contenido"*, agrega también que, tratándose de ofensas criminales, *"nosotros matamos basándonos en los metadatos"*.[4] (énfasis agregado).

Un elemento adicional a tomar en cuenta es que, los metadatos son fácilmente accesibles. En el caso del correo electrónico, basta con instalar un software de extracción de datos o revisar la información del servidor por el que pasan los correos, para obtener los metadatos. Utilizando fórmulas tecnológicas sencillas, es fácil separar el mensaje de los metadatos y recopilar y vigilar estos últimos.

En este sentido, tenemos que los metadatos sobre las comunicaciones son un tipo de información fácilmente obtenible que, bajo ningún concepto, representan datos secundarios ni complementarios al mensaje en sí. Se trata de información sumamente valiosa y que da un amplio margen de datos sobre una persona, sus actividades, vida diaria, etc. En este sentido, resulta relevante analizar el tratamiento y protección que la ley laboral peruana garantiza a este tipo de información.

3. LA SOBRE-CONCENTRACIÓN EN EL CONTENIDO Y EL ABANDONO DE LOS METADATOS

La experiencia nacional sobre protección de comunicaciones y limitación de facultados de vigilancia de los empleadores nos ha enseñado que existe cierta tendencia a la concentración por el contenido. La protección de los derechos fundamentales de los trabajadores frente a la vigilancia del empleador se ha centrado principal (y casi únicamente) en garantizar la privacidad del contenido de mensajes, es decir, de los datos.

En el ámbito constitucional, nuestras comunicaciones se encuentran protegidas bajo los derechos a la intimidad y al secreto y la inviolabilidad

4 Gilad, Yossi: Metadata-Private Communication for the 99%, MIT and Boston University (2019); Obtenido de: http://www.mit.edu/~yossigi/metadata.pdf. Texto original en inglés: "*If you have enough metadata you don't really need content*", "*we kill people based on metadata*".

de las comunicaciones. Particularmente, el inciso 10 del artículo 2 de nuestra Constitución, establece que:

> *"Toda persona tiene derecho:* ***el secreto y a la inviolabilidad de sus comunicaciones y documentos privados. Las comunicaciones, telecomunicaciones o sus instrumentos*** *solo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado del juez, con las garantías previstas en la ley. [...]" (Énfasis agregado)*

Este artículo constitucional ha sido entendido durante mucho tiempo como aquel que garantiza el secretismo y protección del contenido de las comunicaciones. Así, esta norma es la capa y espada utilizada en todo proceso relacionado con la intervención o "chuponeo" de comunicaciones, sea cual sea el soporte de estas. En efecto, el Tribunal Constitucional a través de la sentencia 2863-2002-AA/TC señaló que:

> *"El concepto de "secreto" e "inviolabilidad" de las comunicaciones y documentos privados, [...], comprende a la comunicación misma, sea cual fuere su contenido y pertenezca o no el objeto de la comunicación al ámbito de lo personal, lo intimo o lo reservado. De manera que se conculca el derecho tanto cuando se produje una interceptación de las comunicaciones, es decir, cuando se aprehende la comunicación dirigida a terceros, como cuando se accede al conocimiento de lo comunicado, sin encontrarse autorizado para ello."*

En el ámbito jurisprudencial laboral, esta situación no es muy diferente. En el caso de los correos electrónicos, una breve revisión de la jurisprudencia más relevante nos revela que, al establecer los límites a la fiscalización por parte del empleador, el foco está puesto sobre el contenido del mensaje, dejando de lado a información anexa o complementaria. Atribúyase al desconocimiento sobre su existencia o importancia, lo cierto es que, jurisprudencialmente, existe cierto abandono y falta de regulación de los metadatos.

En efecto, no cabe duda que existe uniformidad jurisprudencial al reconocer que la revisión del correo electrónico o su soporte (sean estos privados o institucionales), resulta una grave vulneración a los derechos a

la intimidad y al secreto e inviolabilidad de las comunicaciones. Particularmente, el ya mencionado caso Serpost, comenzó con esta ola garantista de derechos fundamentales, siendo que se discutía la validez de un despido efectuado tras revisar el correo electrónico del trabajador y encontrar mensajes con contenido pornográfico. En este proceso se señaló que:

> ***"13) […] al revisar los archivos de dicha computadora, que anteriormente estuvo reservada al señor Javier Arévalo encontró cuatro correos electrónicos de contenido pornográfico que habían sido remitidos desde otra computadora de SERPOST,*** […].
>
> *18) En efecto, conforme lo establece el artículo 2°, inciso 10), de nuestra norma fundamental, toda persona tiene derecho a que sus comunicaciones y documentos privados sean adecuadamente protegidos […].* ***Aunque, ciertamente, puede alegarse que la fuente o el soporte de determinadas comunicaciones y documentos le pertenecen a la empresa o entidad en la que un trabajador labora, ello no significa que la misma pueda arrogarse en forma exclusiva y excluyente la titularidad de tales comunicaciones y documentos****, pues con ello evidentemente se estaría distorsionando el esquema de los atributos de la persona, como si estos pudiesen de alguna forma verse enervados por mantenerse una relación de trabajo. […]*
>
> *21) […] La demandada, lejos de inciar ua investigación como la señalada, ha pretendido sustentarse en su sola facultad fiscalizadora para acceder a los correos personales de los trabajadores, lo que evidentemente no está permitido por la Constitución […]"*[5] (Énfasis agregado)

Como puede observarse, el análisis y redacción están dirigidos a la protección del contenido del mensaje, prohibiendo que se acceda a este o que sea revisado sin autorización del autor o sin orden judicial. La solución parece clara, sencilla y obvia: los derechos a la intimidad y al secreto e inviolabilidad de comunicaciones protege lo que digo.

Hoy en día, este criterio del Tribunal Constitucional ha servido de caballo de batalla en una infinidad de casos. Como ejemplo de esto, podemos señalar las sentencias dictadas en los expedientes constitucionales 04224-2009-PA/TC, 05532-2014-PA/TC, en la Casación laboral 14614-

5 STC 1058-2004-AA/TC

2016-LIMA, entre otras. Particularmente la Casación mencionada resulta interesante siendo que señala lo siguiente:

> *"Constituye un exceso que el empleador señale que es propietario de las cuentas de correo electrónico (e-mails) y que se encuentra facultado a revisar su contenido; admitir ello, seria colisionar con el derecho a la intimidad e inviolabilidad de las comunicaciones de los trabajadores."*

Ahora bien, estamos de acuerdo con que debe protegerse el contenido del mensaje. Esto no está en duda. Lo que resulta sumamente preocupante es el cierto "abandono" de los metadatos. Nos referimos a que la protección de este tipo de información es tratada como un tema secundario o sin relevancia alguna para la discusión jurídica (en la mayoría de los casos simplemente no se hace mención alguna sobre estos). En el ámbito jurídico laboral poco se habla sobre esta información contextual. Los metadatos simplemente no han sido realmente introducidos al análisis jurídico[6].

Esta situación resulta sumamente riesgosa para cualquier trabajador en tanto, la falta de regulación puede causar un estado de indefensión del cual pocos estarán al tanto[7] y muchos otros podrán aprovechar. Como ya hemos mencionado, los metadatos traen consigo una importante carga informática. Se puede saber mucho sobre las actividades diarias de una persona con solo conocer los metadatos que producen sus comunicaciones.

---

6 Si bien han existido intentos de proteger a los metadatos, estos no han sido suficientes. El más claro ejemplo de estos esfuerzos se ve reflejado en la Sentencia del Tribunal Constitucional emitida en el expediente 03599-2010-PA/TC, donde los Magistrados Eto Cruz y Mesías Ramírez concordaron en que existen ciertos "datos externos" a las comunicaciones, referidos a la identidad de los intervinientes, la dirección de origen o destino, etc. que merecen proteccion bajo el derecho al secreto e inviolabilidad de las comunicaciones. Sin embargo, la jurisprudencia más reciente ha terminado por obviar esta parte del análisis, restándole importancia a la proteccion de los metadatos.

7 El analfabetismo digital se encuentra sumamente difundido en nuestro país. La mayoría de personas desconoce la existencia de elementos digitales como los metadatos y su relevancia dentro de las comunicaciones. Es recurrente el pensamiento que, si se encuentra protegido el contenido del mensaje, es suficiente para ganratizar los derechos a la intimidad y secreto.

Lo cierto es que la tecnología nos está obligando a replantear el ámbito de protección de los derechos fundamentales al secreto e inviolabilidad de las comunicaciones y a la intimidad y, con esto, los límites a la facultad fiscalizadora del empleador. En el caso del metadato, no se intercepta la comunicación en sí ni se accede al contenido del mensaje, sino que se procura la vigilancia sobre los datos que genera la comunicación (ej. origen y destino, asunto, etc.). Particularmente, somos de la opinión que los metadatos se encuentran debidamente protegidos por los derechos fundamentales mencionado (y por tanto fuera del ámbito de fiscalización laboral), siempre y cuando entendamos bien el sentido de la norma y los derechos involucrados.

4. ¿DEBEMOS PREOCUPARNOS POR LA PROTECCIÓN DE METADATOS EN EL ÁMBITO LABORAL?

4.1. La protección de los metadatos como garantía para el respeto del derecho al secreto e inviolabilidad de las comunicaciones

El derecho que resulta más resaltante cuando hablamos de las comunicaciones es el derecho al secreto e inviolabilidad de las mismas. Como hemos ido adelantando, la jurisprudencia laboral ha entendido durante mucho tiempo que este derecho se encuentra exclusivamente relacionado con el contenido. Esta clásica interpretación podría encontrar su origen y fundamento en el hecho que, el desarrollo de este derecho fue realizado en una época en la cual las telecomunicaciones se encontraban regidas por el teléfono y donde el contenido del mensaje era la única información que podía grabarse o registrarse. Hoy en día, pensar únicamente en el contenido como la materia protegida por el secreto de las comunicaciones no es otra cosa que resistirse al cambio y a la modernidad.

En efecto, la virtualización de las telecomunicaciones nos obliga a pensar más allá de lo evidente. Refiriéndonos a los metadatos creados por el correo de los trabajadores (sea este institucional o privado utilizado en computadoras brindadas por el empleador), creemos firmemente que estos componen un elemento esencial del derecho al secreto e inviolabilidad de las comunicaciones. Es que, en efecto, sin la proteccion de los metadatos,

todos los esfuerzos realizados para proteger a los trabajadores contra la vigilancia del contenido de los correos electrónicos, devienen en inútiles.

Nos explicamos.

En primer lugar, la protección de los metadatos es un supuesto necesario para la protección integra del derecho al secreto de las comunicaciones. En efecto, debemos tener claro que los metadatos son una consecuencia directa e inevitable de las comunicaciones. Si haces una llamada o recibes un mensaje o correo electrónico, la creación del metadato es automática: no es posible evitarlo y, en la mayoría de los casos es excesivamente difícil y costoso de ocultar o encriptar. Teniendo esto en cuenta, poco valen los esfuerzos por proteger el contenido de la comunicación si puede tenerse un razonable conocimiento de la materia discutida con solo conocer los metadatos.

Un caso práctico puede ayudarnos. Un trabajador de la empresa envía por correo electrónico un archivo confidencial a un trabajador de la competencia. En este documento se revela un secreto industrial. Un par de semanas después, la empresa de la competencia lanza un nuevo producto al mercado que es virtualmente igual. La empresa, alertada de que existe un espía entre sus trabajadores, procede a revisar los metadatos producidos los correos electrónicos y demás sistemas de comunicación digital de sus trabajadores. Haciendo esta búsqueda descubre que su trabajador intercambió varios correos con un trabajador de la competencia en el último mes. Solo observando los metadatos de los correos (usuario del trabajador, correo electrónico receptor (que coincide con correo de la competencia) y los metadatos del archivo adjunto (hora de creación y autor) que coinciden con un documento confidencial interno) puede identificar que este trabajador fue quien difundió la información confidencial a la competencia, vulnerando la buena fe y sus obligaciones laborales. En este caso, no fue necesario revisar el contenido y mensaje del correo electrónico para poder identificar la comisión de una falta grave por parte del trabajador. El contenido de la comunicación se mantuvo secreto, sin embargo, los metadatos revelaron casi lo mismo.

En este sentido, la protección de un tipo de información es inútil si no se protege el otro. El derecho al secreto de las comunicaciones pierde el sentido de ser si no hay una protección integral.

En segundo lugar, como el mismo numeral 10 del artículo 2 de la Constitución lo señala, tanto las comunicaciones, telecomunicaciones como sus instrumentos se encuentran protegidos bajo el secreto y la inviolabilidad. Para estos efectos, consideramos que los metadatos están incluidos tanto en una interpretación amplia como estricta de los que debemos entender por "instrumentos". De forma amplia, los instrumentos de las comunicaciones pueden entenderse como todos aquellos complementos y derivados de las comunicaciones, sobre todo aquellos que importan información relevante sobre esta. Los metadatos sin lugar a dudas caen dentro de esta descripción, siendo que son una consecuencia directa e inevitable de las comunicaciones y revelan tanta información sobre las conversaciones como el contenido de esta misma.

Ahora, si queremos utilizar una interpretación más estricta y literal sobre la palabra "instrumentos", entendidos como aquellas herramientas que hacen posible la comunicación, lo cierto que es los metadatos a también se encontrarían protegidos por este derecho. La existencia y creación de este tipo de información no es de ninguna manera accidental. Como bien señala Yossi Gilad, investigar en temas de seguridad de la Universidad de Boston: "*Los metadatos incluyen información crucial para la funcionalidad. Como ejemplo notable, las direcciones de origen y destino, que identifican los puntos finales de la comunicación, están incluidas en cada paquete IP y son fundamentales para establecer la comunicación a través de Internet.*"[8]

En tercer y último lugar, me gustaría resaltar que la protección de los metadatos se encuentra respaldada por la jurisprudencia internacional. Particularmente TC español en la STC 114/1984 señaló que:

8 Gilad, Yossi: Metadata-Private Communication for the 99%, MIT and Boston University (2019); Obtenido de: http://www.mit.edu/~yossigi/metadata.pdf. Texto original en inglés: "*Metadata includes crucial information for functionality. As one notable example, the source and destination addresses, which identify the communication end-points, are included in every IP packet and are fundamental for establishing communication over the Internet.*"

> *"[...] los aspectos del proceso de comunicación que no sean notorios a terceros deben quedar también protegidos [...]."*

Asimismo, la Corte Interamericana de Derechos Humanos en el Caso Escher y otros *vs*. Brasil indicó que:

> *"114. [...] el artículo 11 se aplica a las conversaciones telefónicas independientemente de su contenido e incluso, puede comprender tanto las operaciones técnicas dirigidas a registrar ese contenido, mediante su grabación y escucha, como cualquier otro elemento del proceso comunicativo mismo, por ejemplo, el destino de las llamadas que salen o el origen de las que ingresan, la identidad de los interlocutores, la frecuencia, hora y duración de las llamadas, aspectos que pueden ser constatados sin necesidad de registrar el contenido de la llamada mediante la grabación de las conversaciones."*[9]

Volviendo al ámbito nacional, creo que el deber de protección de los metadatos existe, tanto por la garantía constitucional (aun cuando no sea explicito) como por nuestra legislación vigente. Particularmente me gustaría hacer referencia a la R.M. 111-2009-MTC/03, que aprueba la Norma que establece medidas para salvaguardar el derecho a la inviolabilidad y el secreto de las telecomunicaciones y la protección de datos personales, y regula las acciones de supervisión y control a cargo del MTC, indica en su apartado número 6 que:

> *"La protección del derecho a la inviolabilidad y al secreto de las telecomunicaciones y a la protección de datos personales, comprende, entre otros aspectos, los siguientes: [...] El origen, destino, realización, curso o duración de una comunicación."* (énfasis agregado)

En este sentido, resulta claro que los metadatos merecen una debida protección. No se trata de información de libre acceso, ni de información común y corriente, sin mayor importancia. Se trata de un presupuesto

9 Si bien en este caso el punto central es la comunicación telefónica, lo cierto es que los mismos argumentos son aplicables a las comunicaciones y mensajes por correo electrónico y demás sistemas de telecomunicación. Lo relevante de este argumento, es la protección brindada a los metadatos, los cuales se encuentran presente en cualquier forma de telecomunicación.

básico para garantizar la protección de las comunicaciones y, por lo tanto, debe rechazarse todo tipo de tratamiento "ligero" que pretenda darse a este tipo de datos, particularmente si se trata de vigilancia en el ambiente laboral. Si satanizamos y limitamos tanto la vigilancia y revisión del contenido de las comunicaciones por parte del empleador, ¿por qué no hacemos lo mismo con los metadatos?

4.2. La prohibición de la vigilancia sobre los metadatos como presupuesto para garantizar el derecho a la intimidad y la protección de datos personales

Ahora bien, la protección de los metadatos y la limitación de la vigilancia laboral no solo se fundamentan en el derecho al secreto de las comunicaciones en el ambiente laboral, sino que también constituyen un presupuesto necesario para garantizar la protección de los datos personales y, por ende, de la intimidad de los trabajadores. Esta protección cobra particular importancia si tomamos en cuenta que, a raíz de la Casación Laboral 14614-2016-LIMA, la Corte Suprema dictaminó que los bienes brindados por el empleador, sea una computadora, teléfono o correo electrónico institucional, pueden ser válidamente utilizados para fines personales.

En efecto, el considerando 14 de la Casación en cuestión indicó que:

> *"El uso de estas herramientas de la tecnología moderna naturalmente estará destinada para la prestación de sus servicios y serán utilizadas dentro de la jornada de trabajo; sin embargo, el "chat", "Messenger" u otro sistema de "chateo" y el correo electrónico que pone el empleador a disposición del trabajador puede ser usado por este para fines personales (y no laborales)."*

Ahora bien, esta autorización para uso privado nos lleva a reflexionar sobre lo dispuesto por la Ley de Protección de Datos Personales. Particularmente, el inciso 4 del artículo 13 de esta Ley, indica lo siguiente:

> *"Las comunicaciones, telecomunicaciones, sistemas informáticos o sus instrumentos, cuando sean de carácter privado o uso privado, solo pueden ser abiertos, incautados, interceptados o intervenidos*

por mandamiento motivado del juez o con autorización de su titular, con las garantías previstas en la ley."

Las disposiciones arriba presentadas resultan de suma importancia para nuestro análisis, siendo que, tras una interpretación sistemática y conjunta de estos, podemos darnos cuenta que la protección de los metadatos en el ámbito laboral guarda una estrecha relación con la protección de datos personales y el derecho a la intimidad de los trabajadores.

En efecto, debemos considerar que los trabajadores se encuentran habilitados para hacer uso personal de los equipos e instrumentos tecnológicos brindados por su empleador. Siendo que existe un uso personal o privado de las herramientas tecnológicas brindadas por el empleador (telecomunicaciones, sistemas informativos o sus instrumentos del artículo arriba indicado), debemos reconocer que estas comunicaciones se encuentran debidamente protegidas por la ley protección de datos personales en términos similares a los dispuestos por la Constitución.

Este escenario no es más que una consecuencia lógica: si un trabajador se encuentra habilitado para enviar correos o mensajes privados, es necesario que estos se encuentren debidamente protegidos al, potencialmente, importar una gran carga de datos personales que los identifican o los hace identificables.[10]

Es más, las conversaciones o mensajes de uso privado suelen estar plagadas de datos sensibles los cuales se encuentran estrictamente protegidos dada su estrecha relación con datos como nuestra salud, convicciones religiosas o políticas, afiliación sindical, etc. Tratándose de información personal, nadie tiene derecho a acceder o conocer de ésta sin el consentimiento de su titular o mandato judicial.

10 Art. 2 de la Ley de Protección de datos personales: *"4. Datos personales. Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados; 5. Datos sensibles. Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos; opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual."*

Ahora bien, hablando de datos personales, resulta absolutamente necesaria no solo la prohibición de revisión del contenido sino también de la vigilancia de los metadatos. En este campo, debemos pensar más allá de lo evidente y reconocer la grave intromisión en la intimidad y vida privada que implicaría este tipo de vigilancia sobre los trabajadores. El evadir la protección de los metadatos sería como abrir una gran puerta al conocimiento no autorizado de la información personal y sensible del personal (probablemente sin conocimiento de esta situación).

En efecto, según un estudio conducido por la Universidad de Stanford[11] en el cual los voluntarios permitieron la evaluación de los metadatos producidos por su celular durante varios meses, la cantidad de información privada que puede obtenerse utilizando únicamente metadatos es mayor o igual a la que se obtiene de conocer el contenido de las comunicaciones. Por ejemplo, se tuvieron los siguientes resultados:

- Se descubrió que el participante A tenía esclerosis múltiple ya que registró múltiples llamadas clínicas neurológicas locales, farmacias especializadas, a un servicio de tratamiento de condiciones raras y una línea directa para un producto farmacéutico utilizado únicamente para tratar la esclerosis múltiple recurrente.
- Se descubrió que el participante B sufrió un ataque cardíaco ya que habló largamente con cardiólogos de un centro médico importante, recibió llamadas de farmacias y se contactó con una línea directa de informes domiciliarios para obtener un dispositivo médico utilizado para controlar la arritmia cardíaca.
- Se descubrió que el participante C tenía un arma semiautomática ya que llamó en varias oportunidades a una tienda de armas que se especializa en fusiles semiautomáticos AR y se contactó con el servicio al cliente de un fabricante de este tipo de armas de fuego.

11 Carey, Bjorn; *Stanford computer scientists show telephone metadata can reveal surprisingly sensitive personal information* (2016); Obtenido de https://news.stanford.edu/2016/05/16/stanford-computer-scientists-show-telephone-metadata-can-reveal-surprisingly-sensitive-personal-information/

En todos los casos arriba presentados, lo único que se tuvo al alcance fueron metadatos, no el contenido de las comunicaciones. Esto sin lugar a dudas demuestra que la protección de datos personales y, por ende, de la intimidad de los trabajadores, resulta gravemente amenazada si es que entendemos que el secreto de las comunicaciones abarca únicamente el contenido de estas, no la información que se crea a raíz de estas. La obtención de datos personales y sensibles no necesariamente es directa, sino indirecta (como sucedió en el experimento arriba señalado), sin embargo, ambas merecen protección. Resulta claro que, de nada vale prohibir la vigilancia de las telecomunicaciones por parte de los empleadores, volviendo ilícita cualquier prueba o documento obtenido sin autorización, si es que no entendemos que la vigilancia sobre los metadatos se encuentra también prohibida.

Si bien en el experimento arriba señalado se vigilaron los metadatos de telefonía, lo cierto es que este análisis puede aplicarse a cualquier tipo de telecomunicación. Los metadatos, sobretodo en conjunto, nos ayudan a identificar un patrón en el comportamiento y actividades de las personas. En base a esta información, puede conocerse desde nuestra rutina diaria, hasta nuestro estado de salud, orientación sexual, y demás aspectos de la vida privada. Solo es necesario observar nuestros movimientos e interacciones.

Tomando un ejemplo sencillo del ámbito laboral: un trabajador sabe que puede usar su correo y computadora de la empresa para enviar correos privados. Como es donde mejor internet tiene y donde mayor tiempo pasa en el día, decide utilizar estas herramientas para comunicarse con el sindicato ya que está pensando afiliarse. Durante varias semanas mantiene un hilo de menajes y correos con el sindicato y otro personal afiliado. El empleador, sin revisar el contenido de los mensajes sino únicamente metadatos (como receptor, asunto y demás), puede tener una idea relativamente clara de que el trabajador esta pensando en afiliarse. En este caso, el empleador (temiendo que el sindicato crezca), podría ejercer represalias o incluso despedir al trabajador bajo cualquier excusa con la finalidad de evitar que el sindicato gane fuerza.

Si bien en este caso no ponemos en duda la problemática actuación antisindical del empleador, el tema central es que, no es necesario revisar el contenido de un correo electrónico, para saber qué se esta diciendo o haciendo. Por ejemplo, podemos enterarnos de las aspiraciones sindicales de un trabajador (información protegida bajo la ley de protección de datos personales) con solo revisar los metadatos.

La vigilancia sobre los metadatos puede resultar aún más esclarecedora sobre la intimidad de las personas que el contenido de la comunicación en sí. Utilizando un ejemplo recurrente de SCHNEIER tenemos que, si contratamos un investigador privado par que intercepte las llamadas y correos de una persona, podremos conocer lo que ha dicho y conversado. Sin embargo, si contratamos al investigador para que siga a la persona constantemente (como sucede cuando vigilo sus actividades a través de los metadatos que genera) puedo saber donde está, qué hace y con quién se relaciona en cada momento del día.

En este sentido, resulta evidente que es necesario proteger tanto los datos como los metadatos. Ambos contienen información de suma relevancia para la vida privada y, como tal, merecen una debida protección en pro de salvaguardar los derechos al secreto de las comunicaciones y a la intimidad de los trabajadores. Resulta claro que este tipo de información debe mantenerse fuera del ámbito de vigilancia del empleador ya que, después de todo, de nada sirve proteger la puerta principal (el contenido) si vamos a dejar todas las ventanas y puerta traseras (los metadatos) abiertas de par en par.

5. REFLEXIONES FINALES

Como mencionamos al inicio del presente ensayo, no cabe duda que la tecnología impone nuevos retos cada día. La aparición de comunicaciones virtuales ha simplificado muchos procesos del día a día, sin embargo, también ha abiertos novedosas puertas a través de las cuales pueden generarse intromisiones y vulneraciones de derechos sin que estemos al tanto de ellas. El caso de la vigilancia laboral con uso de tecnología no es diferente.

Sin lugar a dudas hay más de una razón para abogar por la protección de los metadatos que son generados día a día por los trabajadores y que los siguen en todo lo hacen. La constitución lo autoriza, la ley lo requiere y la jurisprudencia y doctrina comparada se encuentran de acuerdo. Si queremos que la intimidad y las comunicaciones de los trabajadores se encuentren verdaderamente protegidas (como ha intentado hacer la jurisprudencia) debemos comenzar por reconocer los tipos de información que abren las puertas a las vidas de los trabajadores y comenzar a exigir garantías para se respeten los derechos fundamentales.

Tomando todo lo antedicho en consideración, podemos afirmar válidamente que los metadatos se encuentran fuera del ámbito de vigilancia del empleador. Si bien no existe regulación o jurisprudencia clara al respecto, esta protección es una consecuencia lógica de las garantías al secreto e inviolabilidad de las comunicaciones y del derecho a la intimidad por los que vela nuestra jurisprudencia. Lo cierto es que la protección del contenido por la que se ha abogado hasta la fecha, carecería de sentido si dejamos la puerta de los metadatos abierta de par en par. De nada sirve que se reconozca la protección del contenido, si es que podemos conseguir casi los mismos resultados vigilando solo los metadatos.

Es inevitable que los avances tecnológicos vayan presentando retos al derecho, sin embargo, debemos adaptarnos si no queremos llenarnos de espacios en blanco, sin regulación o abiertos a cualquier interpretación. No sirve de nada que los derechos estén redactados en papel y se garanticen formalmente si es que nos negamos a cubrir todos los agujeros que se van creando con el tiempo. Los metadatos constituyen un elemento esencial de la comunicación y, como tales, merecen protección y un espacio en la mesa de discusión sobre vigilancia laboral.

BIBLIOGRAFÍA

Guerrero, Carlos; *Ley Stalker: cuando la inocencia deja de ser una presunción* (2015); obtenido de https://hiperderecho.org/2015/09/ley-stalker-cuando-la-inocencia-deja-de-ser-una-presuncion/

Schneier, Bruce; *NSA Doesn't Need to Spy on Your Calls to Learn Your Secrets* (2015); Obtenido de https://www.wired.com/2015/03/data-and-goliath-nsa-metadata-spying-your-secrets/

Schneier, Bruce; *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World (*2015)

Elias Puelles, Ricardo; *Decreto Legislativo 1182, Geolocalizacion y proceso penal, Sacrificio de garantias a favor a favor de una supuesta eficiencia investigativa* (2016); obtenida de https://hiperderecho.org/wp-content/uploads/2016/05/elias_geolocalizacion_proceso_penal.pdf

Abad Yupanqui, Samuel; *El derecho al secreto de las comunicaciones. Alcances, límites y desarrollo jurisprudencial* (2012); Obtenido de http://revistas.pucp.edu.pe/index.php/pensamientoconstitucional/article/view/2852

Morachimo, Miguel; *Vigilancia Estatal de las Comunicaciones y Derechos Fundamentales en Perú*; Publicado por Hiperderecho (2016)

Carey, Bjorn; *Stanford computer scientists show telephone metadata can reveal surprisingly sensitive personal information* (2016); Obtenido de https://news.stanford.edu/2016/05/16/stanford-computer-scientists-show-telephone-metadata-can-reveal-surprisingly-sensitive-personal-information/

Gilad, Yossi: Metadata-Private Communication for the 99%, MIT and Boston University (2019); Obtenido de: http://www.mit.edu/~yossigi/metadata.pdf

Ulloa Millares, Daniel; *Los limites a las facultades de control del empelador en la utilizacion por parte de los trabajadores de las nuevas tecnologias (correo electronico e internet*); En: Laborem. Revista de la soceidad peruana del Derecho del Trabajo y de la Seguridad Social. Nro. 06 (2006).

Monzon Zevallos, Willy; Derecho a la intimidad, secreto de las comunicaciones y poder de dirección. A proposito de la fiscalizacion

del correo electrónico; En: TC Gaceta Constitucional y Procesal Constitucional. Nro. 95 (2015)

Plaza, Maria Eugenia Elizabeth; El correo electrónico en el ámbito laboral; En: Derecho y Sociedad. Nro. 46 (2016)

De Las Casas, Orlando; ¿Es fiscalizable el contenido del correo electrónico otorgado por el empleador?; En: TC Gaceta Constitucional y Procesal Constitucional. Nro. 83 (2014)