GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

CCN
CENTRO CRIPTOLÓGICO NACIONAL

# Guía de Seguridad de las TIC
# CCN-STIC 831

## Registro de la actividad de los usuarios


Marzo 2018

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2018.03.04 02:14:39 +01'00'


NIPO: 785-18-002-4

Fecha de Edición: marzo de 2018

El Sr. Carlos Galán ha participado en la realización y modificación del presente documento, que ha sido financiado por el Ministerio de Hacienda y Función Pública.

# PRÓLOGO

El uso masivo de las tecnologías de la información y la comunicación (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010, de 8 de enero, modificado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y la comunicación (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Marzo de 2018

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

# ÍNDICE

# 1. OBJETIVO

El artículo 23 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante) señala:

> ***Artículo 23. Registro de actividad***
>
> *Con la finalidad exclusiva de lograr el cumplimiento del objeto del presente Real Decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa*.

Como quiera, en determinadas circunstancias, el registro de las actividades de los usuarios podría comportar la colisión de diferentes derechos, de los que, alternativamente, son titulares las entidades del Sector Público, sus directivos, empleados y usuarios, es necesario delimitar el alcance de tal registro de actividad y precisar los elementos que deben tenerse en cuenta para su adecuada práctica.

Así pues, el propósito de esta Guía es presentar a los responsables y usuarios de los órganos, organismos y unidades de las entidades del ámbito subjetivo de aplicación del ENS[1], un **análisis técnico-jurídico** sobre los requisitos exigibles a la realización de las acciones contempladas en el antedicho precepto, así como determinar las condiciones que deben observarse durante su acometimiento.

# 2. MEDIOS ELECTRÓNICOS, ACCIONES CONTEMPLADAS EN EL REGISTRO DE ACTIVIDAD Y DERECHOS CONCERNIDOS

Los recursos tecnológicos contemplados en el *Registro de actividad* comprenden, en primer lugar, todos los **medios electrónicos corporativos** que la entidad pone a disposición de los empleados públicos (o del personal externo contratado), para el desempeño de sus funciones dentro de la organización, incluyendo ordenadores, tabletas, smartphones y, en general cualquier dispositivo de tratamiento de la información, incluyéndose también y con las salvedades a las que haya lugar, aquellos **dispositivos propiedad de los propios usuarios** (BYOD - *Bring Your Own Device*) autorizados por la entidad a acceder a recursos corporativos, en la medida que determine la normativa interna que resulte de aplicación.

Atendiendo a lo dispuesto en el art. 23 del ENS, las acciones que se entienden comprendidas dentro del *Registro de la actividad* de los usuarios de los sistemas de información son:

- **Retención** (almacenamiento y custodia) de información para

[1] Para un examen detallado de los ámbitos subjetivo y objetivo de aplicación del ENS puede consultarse la "Guía CCN-STIC 830 Ámbito de aplicación del ENS".

- **Monitorización**,
- **Análisis**,
- **Investigación** y
- **Documentación**,

en relación con actividades indebidas o no autorizadas, lo que incluye tanto la información generada o tratada por el usuario como los registros de su actividad.

La determinación de las denominadas "actividades indebidas o no autorizadas", cuya primera referencia suele figurar en la Política Seguridad de la Información de la organización (medida [org.1] del ENS), debe encontrarse en la Normativa Interna que regule el uso de los medios electrónicos en la organización (medida [org.2] del ENS), que, habiendo tenido en consideración las opiniones de los Responsables de la Información, de los Servicios y de Seguridad, habrá sido aprobada por el titular del órgano superior de la organización.

La Política de Seguridad de la Información o la Normativa Interna precisarán la unidad u órgano encargados de acometer las acciones señaladas en el art. 23 del ENS, la detección de las actividades indebidas o no autorizadas y la iniciación de las acciones de respuesta pertinentes[2].

No se debe olvidar, en todo caso, que el *Registro de actividad* del art. 23 del ENS debe ponerse en relación con el art. 14 (*Gestión de personal*) de dicho cuerpo legal, que además de exigir la formación e información del personal en relación con sus obligaciones de materia de seguridad, habilita la necesaria supervisión de sus actuaciones.

> ***Artículo 14. Gestión de personal***
>
> *1. Todo el personal relacionado con la información y los sistemas deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad. Sus actuaciones deben ser supervisadas para verificar que se siguen los procedimientos establecidos.*
>
> *2. El personal relacionado con la información y los sistemas, ejercitará y aplicará los principios de seguridad en el desempeño de su cometido.*
>
> *3. El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad.*
>
> *4. Para corregir, o exigir responsabilidades en su caso, cada usuario que acceda a la información del sistema debe estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado determinada actividad.*

Así pues, el ejercicio del *Registro de Actividad* puede involucrar, entre otros, los siguientes derechos:

[2] Conviene precisar que el objeto del *Registro de la actividad* tratado en la presente Guía se centra en la seguridad (de la información), excluyéndose cualesquiera otras finalidades distintas (tales como el mero control laboral o de productividad de los empleados, por ejemplo), cuyo análisis jurídico no debe entenderse comprendido en el propósito de esta publicación.

- El derecho de los usuarios[3] de los sistemas de información públicos a ver respetados sus **Derechos Fundamentales**, especialmente y por la parte que ahora interesa, la **dignidad** de las personas (art. 10 CE[4]), el derecho al **honor**, a la **intimidad** y a la **propia imagen** (art. 18.1 CE, art. 4.2 ET[5] y art. 8 CEPDH[6]) y al **secreto de las comunicaciones** (art. 18.3 CE)[7].
- El derecho de los ciudadanos de exigir el **respeto a los principios generales de funcionamiento del sector público**, expresados en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP, en adelante), entre los que destacamos: el **servicio efectivo a los ciudadanos**, la **responsabilidad por la gestión pública**, la **eficacia en el cumplimiento de los objetivos fijados,** la **eficiencia en la asignación y utilización de los recursos públicos** y, por último, la garantía **de la interoperabilidad y la seguridad** de los sistemas y soluciones adoptadas por las AA.PP. (art. 3), tal y como desarrollan el **Esquema Nacional de Interoperabilidad** (ENI-RD 4/2010) y el **Esquema Nacional de Seguridad** (ENS-RD 3/2010), respectivamente.
- El derecho al ejercicio de la **dirección y control propios de la relación jerárquica en el entorno de las entidades del sector público**, tal y como dispone el Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público (art. 37.2.d).
- El poder de **dirección y organización del empresario**[8]**,** recogido en el Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el Texto Refundido de la Ley del Estatuto de los Trabajadores[9] (art. 20.3), en el marco constitucionalmente protegido de la libertad de empresa[10].

[3] El concepto *usuario*, habitualmente interpretado como "empleado" de la organización titular del sistema de información (personal funcionario, laboral o externo contratado, sometido a la regulación que resulte de aplicación a cada caso), podrá extenderse también, cuando así se mencione y con las precisiones a las que haya lugar, a los usuarios-destinatarios de los servicios de administración electrónica.

[4] Constitución Española (1978).

[5] Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el Texto Refundido de la Ley del Estatuto de los Trabajadores.

[6] Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (Roma, 4.XI.1950).

[7] A los que hay que añadir la previsión contenida en el art. 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (CEPDH), según el cual toda persona tiene derecho al respeto de la vida privada y familiar, prohibiéndose toda injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

[8] Obsérvese que ciertas actividades públicas, cuando la ley lo posibilita, pueden ser ejercidas materialmente por terceras organizaciones (entidades privadas, entre ellas) encargadas contractualmente de desarrollar funciones específicas, entidades privadas que estarán sometidas a la dirección y control del empresario.

[9] Como es sabido, la relación de servicio de los funcionarios públicos se rige por las correspondientes normas legales y reglamentarias, así como la del personal al servicio de las Administraciones Públicas y demás entes, organismos y entidades del sector público, cuando, al amparo de una ley, dicha relación se regule por normas administrativas o estatutarias, básicamente, el Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.

[10] Esta facultad atribuida al empresario de vigilar y controlar el cumplimiento de las obligaciones laborales impuestas al trabajador ha sido reconocida por el Tribunal Supremo en la Sentencia dictada, en unificación de doctrina, el 26 de septiembre de 2007, de la que resulta que la potestad empresarial de controlar el uso adecuado de las nuevas tecnologías puestas a disposición de los trabajadores se basa en el art. 20.3 del ET, lo que incluye tanto la potestad de vigilar el cumplimiento de la prestación laboral

- La estricta observancia de lo preceptuado en la **regulación sobre Protección de Datos de Carácter Personal**, en su caso.

Como quiera que el ejercicio de alguna de las actividades señaladas en el artículo 23 del ENS (monitorización de las actividades de los usuarios de los sistemas, por ejemplo) podría oponerse, bajo ciertas circunstancias, al ejercicio de los derechos citados, en los siguientes epígrafes se examinan los conflictos potenciales entre los derechos enfrentados y la forma más adecuada de tratarlos.

Aunque lo que sigue es predicable de cualquier actividad sustentada en herramientas tecnológicas, la exposición se centrará en dos (2) de ellas, frecuentemente utilizadas por los empleados públicos (o personal contratado externo) de los sistemas de información de las entidades del ámbito subjetivo de aplicación del ENS: la **navegación por Internet** y el **uso del correo electrónico**[11].

## 3. ANÁLISIS DEL HISTORIAL DE NAVEGACIÓN Y DEL CORREO ELECTRÓNICO

Es sabido que la **navegación por Internet**, cuando se lleva a cabo sin las debidas cautelas, comporta importantes riesgos, entre ellos:

- Visitar páginas web que puedan contener código dañino, provocando la infección involuntaria del equipo del usuario y posibilitando su propagación al resto de los equipos de la red de la entidad.
- Visitar páginas web inapropiadas, lo que podría traducirse en menoscabo de la imagen o reputación del usuario y, por ende, de la institución a la que pertenece o representa[12].

Los riesgos anteriores pueden incrementarse cuando tales comportamientos obedecen a motivaciones extra-profesionales. Dicho en otras palabras, cuando los usuarios utilizan los medios electrónicos provistos por la organización para propósitos personales.

Por su parte, pese a que el **correo electrónico** constituye una herramienta de primer orden en todos los sectores de la actividad, su utilización presenta determinados riesgos que es necesario contemplar, entre otros:

- El usuario puede recibir un correo electrónico que adjunte un fichero con código dañino o que incluya un enlace a una página web previamente infectada, lo que provocaría la infección del equipo del usuario y propiciaría su ulterior propagación a la red de la organización o, incluso, a usuarios externos.
- El correo electrónico puede utilizarse como una herramienta (voluntaria o involuntaria) para la exfiltración de datos de la organización o para la participación en ataques DDoS.

realizada a través del uso profesional de estos medios, como la de asegurar que tal uso no está dirigido a la realización de fines personales o privados, y, por tanto, ajenos a la relación funcionarial o contractual.

[11] No se trata en esta Guía las repercusiones jurídicas de otros entornos, tales como el uso de las redes sociales por parte de los empleados públicos (Apéndice de la Guía CCN-STIC 821) o el uso de dispositivos móviles propiedad del empleado público (BYOD), cuestión tratada en la Guía CCN-STIC 827 Gestión y uso de dispositivos móviles.

[12] Todo ello sin tener en cuenta la pérdida de productividad derivada del tiempo empleado en tal navegación.

- El usuario podría utilizar el correo electrónico corporativo para enviar mensajes inadecuados, lo que repercutiría en la imagen o reputación de la organización a la que pertenece o representa.

Análogamente, los riesgos citados se potencian cuando tales comportamientos responden a motivaciones no-profesionales, es decir, cuando los usuarios utilizan el correo electrónico corporativo para propósitos personales.

Por todo ello, las organizaciones deben adoptar las medidas adecuadas para eliminar o, al menos, minimizar, los antedichos riesgos.

Tales medidas pueden ser de naturaleza **técnica** (filtros o reglas que impidan el acceso a determinadas páginas - *Black Listing,* por ejemplo) o de naturaleza **organizativa**: preventivamente (instando a los usuarios a evitar comportamientos inadecuados mediante la publicación, puesta a disposición o entrega de una Normativa Interna de obligado cumplimiento[13]) o reactivamente (analizando el historial de navegación o los mensajes de correo electrónico emitidos o recibidos por un determinado usuario)[14].

Sin embargo, como se ha anunciado, bajo ciertas circunstancias, la monitorización por parte de los responsables de la entidad del historial de navegación de los usuarios o del contenido de sus mensajes de correo electrónico podría ser considerada una vulneración de los derechos relativos a la intimidad o al secreto de las comunicaciones[15].

## 4. LA ADECUACIÓN LEGAL DEL REGISTRO DE ACTIVIDAD

Como se ha señalado, el *Registro de la actividad* de los empleados públicos (comprendiendo el análisis de los registros de logs, la monitorización del historial de navegación y el análisis del correo electrónico) resulta una herramienta de soporte indispensable para lograr un uso adecuado de los medios electrónicos en el seno de las organizaciones, garantizando la conformidad con la exigencia legal de respeto a los principios generales de funcionamiento del sector público, expresados en la LRJSP: el **servicio efectivo a los ciudadanos**, la **responsabilidad por la gestión pública**, la **eficacia en el cumplimiento de los objetivos fijados**, la **eficiencia en la asignación y utilización de los recursos públicos** y, por último, el **aseguramiento de la interoperabilidad y la seguridad** de los sistemas y soluciones adoptadas por las AA.PP.[16]

No hacerlo así supondría una clara dejación por parte de los responsables públicos de sus obligaciones legales, lo que, en último extremo, conduciría a una completa

[13] Tal y como la que se muestra en los modelos de Normas Internas recogidos en la Guía CCN-STIC 821, que deberán ser adaptados por las entidades a sus circunstancias específicas.

[14] De conformidad y con las salvedades impuestas por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD), especialmente, las contenidas en su artículo 9.

[15] La problemática expuesta obedece, en buena medida, a la dificultad práctica de evitar tecnológicamente el uso personal de los medios electrónicos de titularidad corporativa y, en su consecuencia, a la generalización de una cierta tolerancia cuando se usan de manera moderada, lo que ha podido generar en los usuarios equivocadamente, como se verá, una expectativa de confidencialidad sin límites.

ineficacia de las entidades públicas y al desmoronamiento del servicio público que tienen encomendado[17].

Ahora bien, tal *Registro de actividad* debe realizarse, como señala el propio ENS en su artículo 23, con plenas garantías legales y respetando el honor, intimidad y dignidad de los usuarios involucrados: empleados públicos o colaboradores externos, generalmente[18].

## 4.1 LOS LÍMITES AL EJERCICIO DE DERECHOS

Considerando la jurisprudencia del Tribunal Constitucional (TC) y la doctrina, es sabido que el ejercicio de los Derechos Fundamentales no tiene carácter absoluto, sino que debe entenderse limitado por el de otros derechos con los que, en ocasiones, pudiera estar enfrentado[19]; correspondiendo al propio TC, en última instancia, determinar los requisitos para garantizar un adecuado equilibrio entre los derechos contrapuestos[20].

En este sentido, son reiteradas las sentencias del TC[21] que consagran el llamado **juicio de proporcionalidad** como mecanismo para evaluar la prevalencia de un derecho frente a otro, cuando sus ejercicios se enfrentan simultáneamente.

Así, en virtud de este juicio de proporcionalidad, para que un derecho sea eficazmente oponible a otro, es necesario que supere los tres (3) juicios siguientes:

- Juicio de idoneidad: que la medida a adoptar sea susceptible de alcanzar el objetivo perseguido.

---

[16] En relación a la seguridad de la información, esta es también la opinión de la Agencia Española de Protección de Datos expresada en su Informe 0615/2009, recogiendo lo señalado el Documento de Trabajo del Grupo del Artículo 29, relativo a la vigilancia de las comunicaciones electrónicas en lugar de trabajo, de 29 de mayo de 2002, en el que se examina la vigilancia por el empleador de la utilización del correo electrónico e Internet por parte de los trabajadores, ofreciendo una orientación y ejemplos concretos sobre lo que constituyen actividades de control legítimas y límites aceptables de la vigilancia de los trabajadores por el empresario. Es preciso señalar que el documento de trabajo cubre toda actividad vinculada a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo, tanto la vigilancia en tiempo real como el acceso a datos almacenados.

[17] Así lo ha considerado también el Tribunal Supremo, entre otras, en las sentencias de 26.09.2007 y 08.03.2011, al entender que el trabajador no puede imponer el respeto a su intimidad cuando utiliza un equipo proporcionado por la entidad en contra de las instrucciones establecidas por ésta.

[18] Pese a que el Tribunal Constitucional ha señalado que el contrato de trabajo no puede considerarse un título legitimador de recortes en el ejercicio de los Derechos Fundamentales, no es posible obviar que la pertenencia a una organización profesional de trabajo modula el ejercicio de tales derechos. Así, este Tribunal, en sus sentencias 99/1994, 12/2003 ó 170/2013, ha señalado que, en aplicación de la adaptabilidad de los derechos del trabajador a los razonables requerimientos de la organización en la que se integra, manifestaciones del ejercicio de aquellos derechos -que en otro contexto serían legítimas-, no lo son cuando su ejercicio se valora en el marco de la relación laboral.

[19] Se dan casos muy frecuentes de colisión de derechos, por ejemplo, en el ámbito de la información, cuando se enfrentan el derecho a la libertad de expresión e información, consagrado en el artículo 20 de la Constitución, frente al derecho a la intimidad, al honor o a la propia imagen, contemplados también en el artículo 18 de la Carta Magna y desarrollados en la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

[20] El conflicto entre el derecho de la empresa a vigilar y el derecho de los empleados a la protección de su vida privada ha sido tratado en la Directiva 95/46/CE, que establecía distintos niveles que han venido regulando la vigilancia de la utilización de internet y del correo electrónico en los lugares de trabajo. Dichos principios son los siguientes: Principio de necesidad (la vigilancia -monitorización- debe ser necesaria para alcanzar un objetivo dado; Principio de finalidad (deben recogerse los datos con una finalidad específica, explícita y legítima); Principio de transparencia (el empleador debe proporcionar a los empleados todas las informaciones relativas a la vigilancia -monitorización-); Principio de legitimidad (las operaciones de tratamiento de datos solo tendrán lugar con una finalidad legítima); Principio de proporcionalidad (los datos personales objeto de la vigilancia deben ser pertinentes y adecuados respecto a la finalidad indicada) y Principio de seguridad (el empleador deberá tomar todas las medidas de seguridad al objeto de garantizar que los datos recogidos no sean accesibles a terceros).

[21] Sentencias del TC: 96/2012, de 7 de mayo; 241/2012, de 17 de diciembre y 170/2013, de 7 de octubre, entre otras.

- Juicio de necesidad: que no exista otra medida más moderada para alcanzar el propósito perseguido.
- Juicio de proporcionalidad, en sentido estricto: que la medida adoptada sea proporcional al valor de los bienes, activos o intereses en riesgo.

Este principio genérico de proporcionalidad ha sido asimismo incorporado a la LRJSP (art. 4.1) dentro de sus **Principios de intervención de las Administraciones Públicas para el desarrollo de una actividad**[22], señalándose expresamente (en su art. 4.2) que las Administraciones Públicas, velando en todo caso por el cumplimiento de los requisitos exigidos por la normativa en materia de protección de datos de carácter personal, podrán, en el ámbito de sus respectivas competencias: "comprobar, verificar, investigar e inspeccionar los hechos, actos, elementos, actividades, estimaciones y demás circunstancias que fueran necesarias".

Por todo ello, podemos afirmar que el ejercicio de los Derechos Fundamentales (derecho a la intimidad y derecho al secreto de las comunicaciones, por la parte que ahora interesa) encuentra su límite en el derecho laboral "*en la medida estrictamente imprescindible para el correcto y ordenado desenvolvimiento de la actividad productiva*", tal y como ha señalado el TC[23].

Naturalmente, y como quiera que no todos los puestos de trabajo se encuentran expuestos a los mismos riesgos (tanto por razón a la información tratada como por los derechos en riesgo de los empleados), la adopción de cualquier medida de control por parte de la entidad requiere la realización previa de un **Análisis de Riesgos** que justifique la proporcionalidad de las medidas de control que puedan adoptarse, contemplando las especiales circunstancias que concurran en cada caso, atendiendo, simultáneamente, a las funciones o competencias de los departamentos o unidades concernidas, los perfiles de los empleados públicos, la naturaleza de la información tratada y los riesgos a los derechos personales involucrados[24].

## 4.2 EL DERECHO A LA INTIMIDAD

Como la jurisprudencia y doctrina vienen afirmando, el derecho fundamental a la intimidad (art. 18.1 CE, art. 4.2 ET y art. 8 CEPDH) debe considerarse un **derecho de**

[22] *"Artículo 4. Principios de intervención de las Administraciones Públicas para el desarrollo de una actividad.*
*1. Las Administraciones Públicas que, en el ejercicio de sus respectivas competencias, establezcan medidas que limiten el ejercicio de derechos individuales o colectivos o exijan el cumplimiento de requisitos para el desarrollo de una actividad, deberán aplicar el principio de proporcionalidad y elegir la medida menos restrictiva, motivar su necesidad para la protección del interés público así como justificar su adecuación para lograr los fines que se persiguen, sin que en ningún caso se produzcan diferencias de trato discriminatorias. Asimismo, deberán evaluar periódicamente los efectos y resultados obtenidos.*
*2. Las Administraciones Públicas velarán por el cumplimiento de los requisitos previstos en la legislación que resulte aplicable, para lo cual podrán, en el ámbito de sus respectivas competencias y con los límites establecidos en la legislación de protección de datos de carácter personal, comprobar, verificar, investigar e inspeccionar los hechos, actos, elementos, actividades, estimaciones y demás circunstancias que fueran necesarias."*

[23] Sentencia TC 170/2013, de 7 de octubre.

[24] La necesidad de la realización de un análisis de riesgos en relación con los derechos de los titulares ha sido puesta claramente de manifiesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos - RGPD).

**carácter objetivo o material**, que concede a su titular la potestad de reservar ciertos ámbitos de su vida del conocimiento de terceros[25], protegiendo asimismo a su titular de la revelación, divulgación, publicidad o explotación no consentida de tales ámbitos[26].

Respecto a si la cobertura de este derecho fundamental se extiende al contenido de los mensajes electrónicos, el TC[27] ha puesto de manifiesto que el cúmulo de información que se almacena por su titular en un ordenador personal –entre otros, datos sobre su vida privada y profesional– forma parte del ámbito de la intimidad constitucionalmente protegido, siendo el ordenador un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado el derecho a la intimidad personal "*en la medida en que estos correos o email, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado*".

Este criterio es también el seguido por el Tribunal Europeo de Derechos Humanos[28], cuando señala: "*los correos electrónicos enviados desde el lugar del trabajo*" están incluidos en el ámbito de protección del art. 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, por cuanto pueden contener datos sensibles que afecten a la intimidad y al respeto a la vida privada (§ 41 y 44).

No obstante lo anterior, siguiendo la doctrina del TC que el derecho a la intimidad no es absoluto, como no lo es ningún derecho fundamental, pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el límite que aquél haya de experimentar se revele como necesario para lograr un fin constitucionalmente legítimo y sea proporcionado[29].

No es posible, por tanto, predicar la intimidad bajo cualquier supuesto ni en cualquier circunstancia[30]. Nos encontramos, pues, con la llamada **expectativa de confidencialidad** (o intimidad) que, como se verás, ha venido marcando el desenvolvimiento jurisprudencial de los últimos años[31].

En este sentido, conviene señalar la reciente sentencia, de 5 de septiembre de 2017, del Tribunal Europeo de Derechos Humanos (TEDH)[32], que señala que el despido de un trabajador por utilizar los medios de comunicación de la empresa, cuando no ha quedado acreditado que hubiera sido advertido previamente por su empleador de la posibilidad de que sus comunicaciones pudieran ser controladas; ni

[25] Tal y como ha señalado el TC en sus sentencias: 10/2002, de 17 de enero, 127/2003, de 30 de junio o 189/2004, de 2 de noviembre.

[26] Así lo señala el Tribunal Supremo, en sus sentencias 98/2000 y 186/2000.

[27] Sentencia TC 173/2011, de 7 de noviembre.

[28] De manera específica, en su Sentencia de 3 de abril de 2007 (caso Copland vs. UK).

[29] Sentencias TC: 115/2013, de 9 de mayo, FJ 5; 143/1994, de 9 de mayo, FJ 6; 70/2002, de 3 de abril, FJ 10.

[30] Obviamente, no se puede esperar el mismo grado de intimidad en una conversación telefónica cuando ésta tiene lugar en la intimidad de nuestro domicilio o en un atestado vagón de METRO.

[31] En 1967, una sentencia de un tribunal norteamericano (caso Katz vs U.S.) hablaba de la "expectativa razonable de intimidad". Este término fue acogido por el Tribunal Europeo de Derechos Humanos en su sentencia de 1997 (caso Halford vs UK), y por los tribunales españoles.

[32] TEDH, sentencia 05.09.2017, Caso Barbulescu vs Rumanía.

se la había informado de la naturaleza o el alcance de la vigilancia, ni del grado de intrusión en su vida privada y en su correspondencia, constituye un violación del artículo 8 del convenio Europeo de Derechos Humanos (derecho al respeto de la vida privada y familiar, el hogar y la correspondencia).

Así pues, en base a esta sentencia, el TEDH determina que para evaluar la legalidad de la monitorización de las comunicaciones de los empleados deben ponderarse los siguientes elementos:

- Si el empleado ha sido notificado de la posibilidad de que su actividad puede ser monitorizada (incluyendo, por ejemplo, el análisis de los registros de logs de usuario, el acceso y navegación por Internet o el uso del correo electrónico corporativo).
- El grado de intromisión de la entidad (durante cuánto tiempo se prolonga, a qué archivos se accede y cuántas personas acceden al resultado de la monitorización).
- La existencia de una razón legítima de la entidad que justifique la monitorización (al ser, por defecto, una medida intrusiva e invasiva).
- Si podrían haberse utilizado métodos de monitorización menos intrusivos que el acceso directo al contenido de las comunicaciones del empleado.
- El uso que da la entidad al resultado de la actividad de monitorización y si el mismo se utiliza para alcanzar el objetivo que justificaba la misma.

Serán estos factores los que deberán ser valorados por los tribunales nacionales para realizar la ponderación de los intereses en conflicto (poder disciplinario de la entidad frente al derecho a la intimidad y al secreto de la correspondencia del empleado) y determinar así si la monitorización es ajustada a derecho.

Por consiguiente, hay que afirmar que **el poder de control del responsable o titular del órgano de que se trate, sobre el uso de los medios electrónicos puestos a disposición de los empleados, se encuentra sometido al previo establecimiento, difusión y compromiso de cumplimiento de una Normativa**[33] -que puede, incluso, llegar a prohibir totalmente el uso de tales medios para propósitos personales- que informe sobre:

a) Las **reglas de uso de los medios tecnológicos**, con expresión de prohibiciones absolutas o parciales para usos privados.

   El TS[34] entiende que, **caso de que la prohibición fuera absoluta, tal prohibición es suficiente para destruir la expectativa de privacidad, legitimando, de este modo, la práctica de cualquier control, incluso el llevado a cabo de forma oculta**.

[33] Denominada en ocasiones como *Normativa de Seguridad, Normativa del Uso de Medios Electrónicos*, etc.) Se trata de los también llamados *Códigos de Conducta* o *Códigos de Buenas Prácticas*, tales como los modelos propuestos en la Guía CCN-STIC 821 Normas de Seguridad, debidamente adaptados a cada caso particular.

[34] Sentencia 06.10.2011, ratificada por el TC en su sentencia 241/2012.

b) La **existencia de controles** y su **intensidad**, atendiendo al Análisis de Riesgos previo[35].

c) Los **medios a aplicar para comprobar el uso correcto** (esto es, el alcance y la naturaleza del control de la entidad y la posibilidad de que la entidad acceda al contenido real de los mensajes, sin que el empleado tenga conocimiento de dicho acceso).

d) Las **medidas para garantizar la efectiva utilización laboral del medio informático**, sin perjuicio de adoptar otras medidas preventivas, como la exclusión de determinadas conexiones.

En la sentencia citada[36], el TEDH considera que, con arreglo a las normas internacionales y europeas (en particular el *Código de buenas prácticas para la protección de los datos personales del trabajador* de la OIT, de 1997, y de la *Recomendación CM/Rec 2015 del Comité de Ministros del Consejo de Europa*, sobre el tratamiento de datos personales en el ámbito de la relación laboral), para poder calificar un notificación de la empresa como aviso previo, **la advertencia de un empresario debía darse antes de que se iniciara la vigilancia**, especialmente cuando esta entraña el acceso al contenido de las comunicaciones de los empleados.

Como la jurisprudencia ha señalado**, la ausencia de la antedicha Normativa podría generar la mencionada *expectativa de confidencialidad*[37]** y, en consecuencia, la vulneración del derecho a la intimidad y la consiguiente ilicitud de la intromisión[38].

## 4.3 EL DERECHO AL SECRETO DE LAS COMUNICACIONES

Diferentes sentencias del TC[39] han venido considerando el secreto de las comunicaciones, además de como un derecho fundamental (art. 18.3 CE), un **concepto rigurosamente formal**, que sólo cede frente a una autorización judicial, el cual se "*predica de lo comunicado, sea cual sea su contenido*". Es decir, no se garantiza el secreto porque lo comunicado pueda revestir el carácter de confidencial, sino que debe extenderse a cualquier contenido, incluyendo los medios de trasmisión electrónicos.

El TC deja claro, por tanto, que el objeto de protección no es el contenido de la comunicación sino **el propio proceso de comunicación**[40], cuando se realiza a través de redes o canales cerrados[41], comprendiéndose entre los elementos protegidos las

[35] La expresión de esta "intensidad" del control ha sido especialmente recalcada por la citada sentencia del TEDH, de 5 de septiembre de 2017, caso Barbulescu vs Rumanía.

[36] TEDH, sentencia 05.09.2017 (Caso Barbulescu vs Rumanía).

[37] *A sensu contrario*, si los medios electrónicos puestos a disposición de los trabajadores se utilizan contraviniendo lo señalado en tal Normativa y con conocimiento de los controles y medidas aplicables, no podría entenderse vulnerada la expectativa de intimidad.

[38] La reciente Sentencia TC 170/2013, de 7 de octubre, ha subsumido la existencia de la información citada si, aun no existiendo la citada Normativa, el Convenio Colectivo aplicable regulaba expresamente tal posibilidad.

[39] Por todas: 114/1984, de 29 de noviembre, y 34/1996, de 11 de marzo.

[40] Sentencia TC 170/2013, citada.

[41] Es decir, cuando el acceso al contenido de la comunicación excluye el acceso de terceros no autorizados.

identidades de los comunicantes[42]. Respecto del canal de comunicaciones, conviene señalar que el TC ha excluido la protección constitucional de las comunicaciones abiertas, esto es: "*aquellas que se realizan en un canal del que no puede predicarse su confidencialidad*"[43].

En lo relativo a las comunicaciones realizadas en ambiente laboral, que se deben entender comprensivo de las relaciones laborales públicas tanto como de las privadas, el TC ha reafirmado el **poder del titular de los medios electrónicos para ordenar y controlar adecuadamente el uso de los medios electrónicos puestos a disposición de los trabajadores**, adoptando las medidas más adecuadas en función de la configuración de los sistemas utilizados y de las condiciones de uso de los antedichos medios[44], redacción actualizada de la Sentencia del Tribunal Supremo, de 25 de septiembre de 2007, dictada en un Recurso para la Unificación de la Doctrina, donde ya se confirmaba la obligación de informar al trabajador sobre las reglas de uso del ordenador y los controles que sobre los mismos podrá efectuar el empresario[45].

Lo anterior significa que, en principio y no habiéndose hecho debidamente pública la precitada Normativa, su puesta a disposición o entrega, no podría accederse al contenido de los correos electrónicos privados de los empleados[46]. Pese a ello, se admite la validez de la prueba obtenida mediante acceso por el empresario al correo recibido y emitido por el trabajador siempre que el registro informático se efectúe con las debidas garantías para preservar la dignidad del trabajador[47].

---

[42] Así lo ha señalado también la Agencia Española de Protección de Datos en su Informe, de 10 de abril de 2006, en el que se recogían las recomendaciones y dictámenes de la Unión Europea, y en el que se indicaba: "*En general el "Grupo del Artículo 29" entiende que los mensajes electrónicos deben beneficiarse de la misma protección de los derechos fundamentales que el "correo tradicional", y opina que las comunicaciones electrónicas que proceden de locales profesionales pueden estar cubiertas por los conceptos de "vida privada" y de "correspondencia" (según lo dispuesto en el Art. 8.1 del Convenio Europeo). Así, el secreto de las comunicaciones y de la correspondencia no dependen de la ubicación y la propiedad de los medios electrónicos utilizados, según se establece en constituciones y principios jurídicos fundamentales. A sensu contrario, la legitimación más idónea de la vigilancia del correo electrónico puede encontrarse en la letra f) del artículo 7 de la Directiva, que prevé que el tratamiento sólo pueda efectuarse si es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos.*"

[43] Sentencia TC 241/2012, de 17 de diciembre, FJ 7.

[44] Sentencia TC 241/2012, citada.

[45] Fundamento Jurídico Cuarto: "*… Por ello, lo que debe hacer la empresa de acuerdo con las exigencias de buena fe es establecer previamente las reglas de uso de esos medios -con aplicación de prohibiciones absolutas o parciales- e informar a los trabajadores de que va existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos, así como de las medidas que han de adoptarse en su caso para garantizar la efectiva utilización laboral del medio cuando sea preciso, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones.*"

[46] Y, por tanto, de llevarse a cabo tal acceso, no desplegaría eficacia en juicio.

[47] Tales garantías serían respetadas cuando quedara acreditado que los trabajadores conocen que el correo de la organización no debe utilizarse para fines personales y, atendiendo a lo señalado en la sentencia del TSJ de Cataluña, de 22.06.2004, cuando el registro informático se efectúa, ante la falta de representantes de los trabajadores, en presencia de dos compañeros de trabajo, o en presencia de un notario, un representante de los trabajadores y un técnico informático (sentencia del TSJ de Cantabria de 26.08.2004), pero en ningún caso si el registro tiene lugar en ausencia de trabajador, de representantes legales o de compañeros de trabajo (sentencia TSJ de Cantabria de 23.12.2004).

El TSJ de Cataluña, en su sentencia, de 21.09.2004, ha señalado que para que el resultado del control del correo electrónico de que ha hecho uso el trabajador pueda aportarse como medio de prueba válido, se han de dar las siguientes condiciones: la necesidad de un propósito específico, explícito y legítimo; que la supervisión sea una respuesta proporcionada a un cierto riesgo; la mínima repercusión sobre los derechos a la intimidad del trabajador; y la presencia del trabajador y de sus representantes en el momento de apertura del correo.

En todo caso, insiste el TC que **el secreto de comunicaciones no quedará vulnerado si existe una prohibición expresa previa del uso privado o personal de la cuenta de correo electrónico corporativo** y, en consecuencia, no existirá "*una expectativa fundada y razonable de confidencialidad respecto al conocimiento de las comunicaciones mantenidas por el trabajador a través de dicha cuenta de correo*", llevando implícita dicha prohibición "*la facultad de la empresa de controlar su utilización, al objeto de verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales*", al considerarse el canal de comunicación empleado por el trabajador abierto al ejercicio del poder de inspección reconocido al titular de los medios empleados[48].

## 4.4 EL REGISTRO DE ACTIVIDAD EN EL ÁMBITO PENAL

El TS[49] ha restringido el alcance de las medidas de intervención antes citadas al ámbito de la Jurisdicción social o laboral, señalando que no pueden extenderse al enjuiciamiento penal, no contemplando posibilidad o supuesto alguno, ni acerca de la titularidad de la herramienta comunicativa (ordenador, teléfono, etc., propiedad de tercero ajeno al comunicante), ni del carácter del tiempo en el que se utiliza (jornada laboral) ni, tan siquiera, de la naturaleza del cauce empleado ("correo corporativo"), para excepcionar la necesaria e imprescindible **reserva jurisdiccional (autorización judicial).**

Por tanto, según afirma el TS, debe quedar claro que **en el ámbito del procedimiento penal**, para que pueda otorgarse valor y eficacia probatoria al resultado de la prueba consistente en la intervención de las comunicaciones protegidas por el derecho consagrado en el artículo 18.3 de la Constitución, **resultará siempre necesaria la autorización e intervención judicial**, en los términos y con los requisitos y contenidos que tan ampliamente se han venido elaborando en multitud de Resoluciones de la Sala de lo Penal del TS[50], cualquiera que fueren las circunstancias o personas, funcionarios policiales, empresarios, etc., que tales injerencias lleven a cabo.

Añade el TS que esta necesidad de autorización judicial operará tan sólo respecto a lo que estrictamente constituye el "*secreto de las comunicaciones*", es decir, con **exclusión de los denominados "datos de tráfico"** o incluso de la posible utilización del equipo informático para acceder a otros servicios de la red como páginas web, etc., de los mensajes que, una vez recibidos y abiertos por su destinatario, no forman ya parte de la comunicación propiamente dicha, respecto de los que rigen normas diferentes como las relativas a la protección y conservación de datos (art. 18.4 CE) o a la intimidad documental en sentido genérico y sin la exigencia absoluta de la intervención judicial (art. 18.1 CE).

[48] Sentencia TC 170/2013, citada.

[49] Sentencia 2844/2014, de 16 de junio.

[50] Especialmente, a partir del importante Auto, de 18 de junio de 1992 (caso "Naseiro").

## 4.5 EL REGISTRO DE ACTIVIDAD EN EL TRATAMIENTO DE DATOS PERSONALES

Cuando se están tratando datos de carácter personal cualquier acción relativa al *Registro de actividad* de los usuarios (retención de información para su monitorización, análisis, investigación y documentación) deberá respetar la normativa vigente al efecto[51] en lo relativo a las personas habilitadas para acceder a tales datos y los condicionantes para su acceso.

Como se ha mencionado, tal cautela ha sido puesta de manifiesto en el art. 4.2 de la LRJSP, cuando señala: "*Las Administraciones Públicas velarán por el cumplimiento de los requisitos previstos en la legislación que resulte aplicable, para lo cual podrán, en el ámbito de sus respectivas competencias y con los límites establecidos en la legislación de protección de datos de carácter personal, comprobar, verificar, investigar e inspeccionar los hechos, actos, elementos, actividades, estimaciones y demás circunstancias que fueran necesarias*".

Finalmente, es necesario recordar que, en virtud de la legislación vigente:

- El Administrador del sistema (y, en su caso, el Responsable de Seguridad) tiene la obligación de secreto profesional en relación con los datos de los trabajadores a que tenga acceso durante las operaciones de control antedichas.
- La no necesidad de consentimiento de los usuarios para llevar a cabo el registro de la navegación por razones de seguridad, diferenciándose con claridad tal consentimiento del preceptivo deber de informar[52].
- La necesidad de cumplir con los principios de exactitud y conservación, de manera que los datos tratados sean exactos y puestos al día, debiendo ser cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados[53].

[51] El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), que será de plena aplicación el 25 de mayo de 2018. Entretanto, permanecen vigentes la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su Reglamento de Desarrollo, operado por Real Decreto 1720/2007, de 21 de diciembre.

[52] Así lo entiende el Grupo de Trabajo del artículo 29, en su Documento de Trabajo relativo a la vigilancia de las comunicaciones electrónicas en lugar de trabajo, de 29 de mayo de 2002, cuando señala: "La finalidad determinada, explicita y legítima vendrá dada en el presente caso por la necesidad de garantizar la seguridad de los sistemas informáticos, debiendo analizarse en cada caso si el tratamiento de datos que dicha supervisión comporta se ajusta a los requerimientos de proporcionalidad del artículo 4 de la Ley Orgánica 15/1999."

[53] En relación con los principios de exactitud y conservación, el Grupo de Trabajo del artículo 29, en su Documento de Trabajo relativo a la vigilancia de las comunicaciones electrónicas en lugar de trabajo, de 29 de mayo de 2002, señala: ""Este principio requiere que todos los datos legítimamente almacenados por un empleador (después de tener en cuenta todos los demás principios enunciados en este capítulo) que incluyan datos procedentes de una cuenta de correo electrónico de un trabajador, de su utilización de Internet o relativos a las mismas deberán ser precisos y actualizarse y no podrán conservarse más tiempo del necesario. Los empleadores deberían especificar un período de conservación de los mensajes electrónicos en sus servidores centrales en función de las necesidades profesionales. Normalmente, es difícil imaginar que pueda justificarse un período de conservación superior a tres meses." Naturalmente, el establecimiento de los periodos de conservación deberá acompasarse a los tiempos y plazos exigidos por el desenvolvimiento del procedimiento administrativo, cuando ello proceda.

- Es necesario incluir la necesidad de informar a las personas ajenas a la organización de las actividades de vigilancia que pudieran afectarles[54]; insertando, por ejemplo, avisos de la existencia de sistemas de vigilancia en todos los mensajes salientes de la organización.

## 5. CONCLUSIONES

De todo lo anterior, se pueden extraer las siguientes conclusiones:

1. El ***Registro de la actividad*** **de los usuarios** y las acciones que comprende (retención de información para su monitorización, análisis, investigación y documentación) es, en las circunstancias y con las cautelas señaladas, **jurídicamente lícito**.
2. Es necesario que la entidad desarrolle, con anterioridad a la adopción de cualquier medida de control, **un análisis de los riesgos que garantice la proporcionalidad** de tales medidas, contemplando las especiales circunstancias que concurran en cada caso, atendiendo, simultáneamente, a las funciones o competencias de los departamentos o unidades concernidas, los perfiles de los empleados públicos, la naturaleza de la información tratada y los riesgos a los derechos personales involucrados.
3. Que, para garantizar su licitud, es necesario que las medidas que se pretenden adoptar superen el llamado **Juicio de Proporcionalidad** (juicio de idoneidad, juicio de necesidad y juicio de proporcionalidad, en sentido estricto) que, en materia de seguridad de la información, serán directamente proporcionales a la categoría del sistema de información concernido, atendiendo a lo dispuesto en el ENS. En otras palabras: **el control debe ser proporcional**, necesario y lo menos invasivo posible, **evaluando el equilibrio entre el interés de la entidad y la privacidad del empleado**[55].
4. Que la existencia de las antedichas **medidas**, su alcance, tipología e intensidad sean previamente **difundidas, conocidas y aceptadas por los usuarios implicados**, lo que puede lograrse a través de la publicación, puesta a disposición o entrega de la Normativa correspondiente[56] y la exigencia de su

[54] Así se pronuncia el Grupo de Trabajo del artículo 29, en su Documento de Trabajo relativo a la vigilancia de las comunicaciones electrónicas en lugar de trabajo, de 29 de mayo de 2002.

[55] Según el Documento de Trabajo del Grupo del artículo 29, relativo a la vigilancia de las comunicaciones electrónicas en el lugar del trabajo, de 29 de mayo de 2002, "el principio de proporcionalidad excluye por lo tanto el control general de los mensajes electrónicos y de la utilización de Internet de todo el personal, salvo si resulta necesario para garantizar la seguridad del sistema. Si existe una solución que implique una intromisión menor en la vida privada de los trabajadores y que permita lograr el objetivo perseguido, el empleador debería considerar su aplicación (por ejemplo, debería evitar los sistemas que efectúan una vigilancia automática y continua)".

[56] A modo de ejemplo no exhaustivo, tal Normativa podría contemplar los siguientes extremos: la política de la entidad en cuanto a utilización del correo electrónico e Internet, definiendo en qué medida los trabajadores pueden utilizar los sistemas de comunicación de la empresa con fines privados o personales (por ejemplo, períodos y duración de utilización); los motivos y finalidad de la monitorización, en su caso (por ejemplo, estableciendo en qué circunstancias se podrá llevar a cabo, como en el caso de ser necesario para garantizar la seguridad del sistema informático o detección de código dañino), información detallada sobre las medidas de monitorización adoptadas, p. ej. ¿quién? ¿qué? ¿cómo? ¿cuándo?; información detallada sobre los procedimientos de aplicación, precisando cómo y cuándo se informará a los trabajadores en caso de infracción de las directrices internas y de los medios de que disponen para reaccionar en estos casos; información sobre en qué condiciones se autoriza la utilización de Internet con fines privados e indicarles los elementos que no pueden visualizar o copiar; información relativa a los sistemas instalados para impedir el acceso a algunos sitios o para detectar una posible utilización abusiva, precisando el alcance del control, por ejemplo si este control se efectúa de manera individualizada o por departamentos, o si el contenido de los sitios

suscripción por parte del usuario, y, en todo caso, antes de tomar medidas disciplinarias[57].

5. La entidad pública en cuestión debe decidir sobre **si permite a los usuarios o no la utilización de los medios electrónicos corporativos y en qué medida lo hace** (prohibición absoluta, prohibición parcial, etc.), debiendo hacer pública tal decisión en la correspondiente Normativa a la que se ha hecho referencia. En todo caso, se recuerda que la **explícita y absoluta prohibición de los medios electrónicos para uso personal** facilita la adopción de los mecanismos de control adecuados[58]. Esa también constituye nuestra recomendación.
6. Las medidas adoptadas deberán ser objeto de una **evaluación periódica respecto de sus efectos y resultados obtenidos**, al objeto de que no pueda apreciarse que la acción de fiscalización de la entidad haya resultado desmedida respecto a la afectación sufrida por la privacidad del empleado.
7. En el ámbito del procedimiento penal, para que pueda otorgarse valor y eficacia probatoria al resultado de la prueba consistente en la intervención de las **comunicaciones protegidas por el derecho** consagrado en el artículo 18.3 de la Constitución, resultará siempre necesaria la **autorización e intervención judicial**.

Finalmente, se recomienda una lectura detenida de la Guía CCN-STIC 821 y, en concreto, del Apéndice I (Normativa General de Utilización de los Recursos y Sistemas de Información del Organismo); Apéndice II (Normas de Acceso a Internet) y Apéndice III (Normas de Uso del Correo Electrónico) que contienen modelos de la Normativa citada, y que, tomando en consideración lo señalado en la presente Guía, deberán ser convenientemente adaptadas atendiendo a las circunstancias que concurran en cada caso[59].

## 6. REFERENCIAS CITADAS

- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Constitución española.

consultados será visualizado o registrado en determinados casos; especificar, cuando proceda, el uso que se hará de los datos recogidos sobre las personas que visitaron sitios específicos; informar a los trabajadores del papel de sus representantes, tanto en la aplicación de la política como en la investigación de las presuntas infracciones.

[57] En cualquier caso, el proceso disciplinario debe ser rápido y confidencial, salvaguardándose los derechos, reputación, honor y propia imagen del empleado, de conformidad con lo señalado en el art. 23 del ENS. Con la misma pretensión se pronuncia el Grupo de Trabajo del artículo 29, en su Documento de Trabajo relativo a la vigilancia de las comunicaciones electrónicas en lugar de trabajo, de 29 de mayo de 2002, cuando señala que "Al analizar la utilización de Internet por los trabajadores, los empleadores deberían evitar sacar conclusiones precipitadas, dada la facilidad con que pueden visitarse involuntariamente algunos sitios a través de respuestas de motores de búsqueda, vínculos hipertextuales ambiguos, pancartas publicitarias engañosas o errores al pulsar las teclas. En todos los casos, deberán presentarse al trabajador en cuestión todos los hechos de que se le acusa y ofrecerle la posibilidad de refutar la utilización abusiva alegada por el empleador."

[58] Si el medio se utiliza para usos privados en contra de estas prohibiciones y con conocimiento de los controles y medidas aplicables, no puede entenderse que, al realizarse el control, se ha vulnerado "una expectativa razonable de intimidad" en los términos establecidos en los siguientes pronunciamientos: TEDH 25-6-97, caso Halford; 3-4-07, caso Copland para valorar la existencia de una lesión del CEDH art.8.

[59] Lo que podrá comportar un mayor o menor grado de exigencia o rigurosidad en las medidas que finalmente se adopten.

- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.
- Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el Texto Refundido de la Ley del Estatuto de los Trabajadores.
- Sentencias (citadas) del Tribunal Europeo de Derechos Humanos (TEDH), Tribunal Constitucional, Tribunal Supremo e Informes de la Agencia Española de Protección de Datos.
- Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.
- Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.
- Guía CCN-STIC 821 Normas de Seguridad.
- Guía CCN-STIC 830 Ámbito de aplicación del ENS.
- Guía CCN-STIC 827 Gestión y uso de dispositivos móviles.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto 1720/2007, de 21 de diciembre, Reglamento de Desarrollo de la LOPD.
- Dictamen 8/2001, del Grupo de Trabajo del artículo 29, sobre el tratamiento de datos personales en el contexto laboral.
- Documento de Trabajo del Grupo del artículo 29, relativo a la vigilancia de las comunicaciones electrónicas en lugar de trabajo, de 29 de mayo de 2002.