Col·legi de Censors Jurats de Comptes de Catalunya

EL CØL·L3G1

AUDITORES

Instituto de Censores Jurados de Cuentas de España

EL REGISTRE DEL CORREU ELECTRÒNIC D'UN TREBALLADOR PER PART DE L'EMPRESA, CONSEQÜÈNCIES PENALS I LABORALS

29 de març de 2017

Juan Pablo Correa, doctor en dret, advocat i professor UB
Tirso Gracia, advocat i professor EADA

EdA ESCOLA D'AUDITORIA

VENTURA GARCÉS & LÓPEZ-IBOR
ABOGADOS

Control de las nuevas tecnologías puestas a disposición de los empleados, por parte de las empresas

Ponentes
Tirso Gracia
Juan Pablo Correa

Barcelona, 29 de marzo de 2017

I. PARTE LABORAL

¿Pueden las empresas controlar el correo electrónico, el teléfono móvil, el Whats App y las nuevas tecnologías puestas a disposición del empleado?

Ponente
Tirso Gracia
Socio

CORREO ELECTRONICO - INTERNET

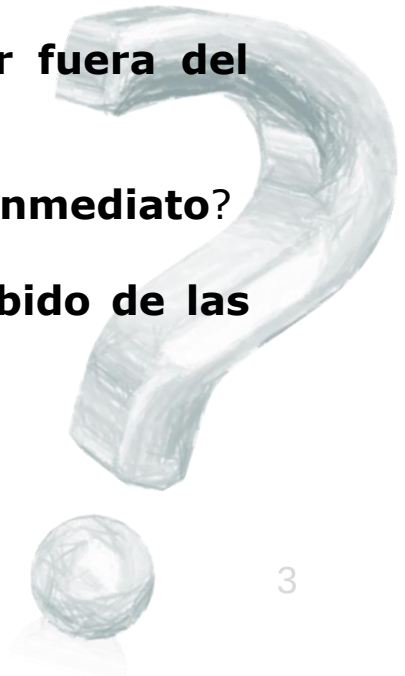
- ¿Conoce el empresario **el buen uso que se hace de las nuevas tecnologías de la empresa** puestas a disposición de los empleados y el contenido de la información trasmitida? ¿Puede controlar y verificar su contenido?

- ¿Conoce el empresario **el tiempo dedicado por los empleados durante la jornada de trabajo a las nuevas tecnologías**? ¿Está relacionado con el contenido del puesto de trabajo?

- ¿Puede el empresario **obligar a los empleados a trabajar fuera del horario de trabajo** mediante las nuevas tecnologías?

- ¿Puede el empresario poner un **programa espía con control inmediato**?

- ¿Puede el empresario **sancionar una falta por el uso indebido de las nuevas tecnologías** sin aplicar un despido?



VERIFICACION DEL CORREO ELECTRONICO

- ✓ Confluencia de Derechos cuando se pretende el control de su contenido

Confidencialidad e Intimidad vs Control Empresarial

- ✓ La falta de legislación comporta inseguridad jurídica para ambas partes

- ✓ La corriente jurisprudencial mayoritaria en España (TC – TS) y en el TEDH:
  - Se trata de un medio de producción
  - Conocimiento previo por parte de los empleados. Información previa de un "protocolo tecnológico de uso de medios informáticos"

- ✓ Otras corrientes:
  - Protección como si se tratara de taquillas personales Art. 18 ET

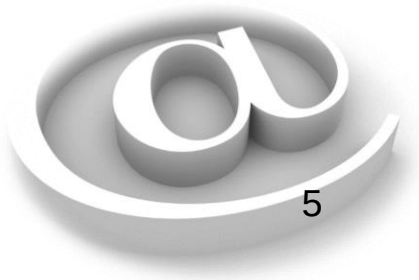
VERIFICACION DEL CORREO ELECTRONICO

- ✓ Contenido de la información a la que se tiene acceso mediante el control realizado

1. Se trata de un medio de producción propiedad de la empresa puesto a disposición de los empleados para realizar su trabajo

2. Se requiere proteger la intimidad del empleado poniendo en conocimiento del mismo los límites de su uso y la posibilidad de controles

3. Por ello se exige respeto a la intimidad en la difusión de los contenidos conocidos, únicamente se requiere su uso para actuar con proporcionalidad



SE RECOMIENDA UN PROTOCOLO TECNOLOGICO o CODIGO DE CONDUCTA

- ✓ Que indique la **titularidad del correo electrónico** como medio de producción y la advertencia de controles
- ✓ Que establezca la **configuración como un medio exclusivo de información profesional**
- ✓ Que determina la **prohibición total o parcial de su uso** para fines no profesionales
- ✓ Que pueda establecer que **su uso se limite a la jornada laboral**
- ✓ Que establezca la **limitación o prohibición de acceso** a determinadas paginas Web
- ✓ Debe reiterarse el **contenido del protocolo de forma continuada y recurrente**, como ponerse el cinturón en el coche al acceder al vehículo

STEDH Caso 12-1/2016 Ingeniero Barbolescu (Rumania)

- ✓ Responsable de ventas de la compañía.
- ✓ La compañía decide abrir cuenta de correo en YAHOO! para atender solicitudes de clientes, que usa el empleado para fines particulares
- ✓ Los Tribunales rumanos determinan la procedencia del despido
- ✓ Existía un código de conducta de prohibía el uso informático para fines particulares
- ✓ STEDH:

"No es abusivo que el empleador quiera verificar el cumplimiento de las obligaciones de los empleados durante su horario de trabajo"

"No existe vulneración del Derecho a la Intimidad ni del artículo 8 del Convenio para la protección de los Derechos Humanos"

RECOMENDACIONES SOBRE EL CONTROL

- ✓ Si no existe "**protocolo tecnológico o código de conducta**", es aconsejable hacerse ante un inminente control, y que se reitere la conducta
- ✓ Que la **verificación sea externa** mediante medios forenses
- ✓ La gravedad vendrá determinada, con "proporcionalidad", por el **contenido** de la información remitida o el tiempo dedicado
- ✓ Hay que tener presente la **prescripción de los hechos** y a la respuesta empresarial en situaciones y antecedentes similares
- ✓ Es recomendable justificar una sospecha con **argumentos de casualidad**
- ✓ La medida sancionadora ha de guardar **proporcionalidad** con la falta
- ✓ Se debe estar a lo tipificado en **Convenio Colectivo** si se quiere sancionar

TELEFONO MOVIL

Diferenciación entre teléfono móvil de empresa y teléfono particular del empleado utilizado para fines profesionales

Teléfono de empresa

- ✓ Su fiscalización es posible si existe un "**protocolo de uso**" con advertencia de su prohibición para fines particulares y advertencia de su control

Teléfono particular

- ✓ **Su fiscalización no sería posible**, pero sí es válido el contenido de una grabación de la conversación mantenida con la empresa, o con un tercero que la pone a disposición de la empresa, pues una conversación telefónica es propiedad de ambos interlocutores

- ✓ El secreto de las comunicaciones no rige entre los propios comunicantes

WHATSAPP – TELEGRAM – MESSENGER

- ✓ Si no existe "protocolo tecnológico" que prohíba total o parcialmente su uso para fines particulares, se encuentra **protegida por el "secreto de las comunicaciones"**, salvo que, el contenido sea puesto a disposición de la empresa por alguno de los interlocutores

- ✓ Transcripción de la conversaciones de WhatsApp es admitida como prueba documental

UTILIZACION DE CAMARAS OCULTAS

- ✓ Se trata de una excepción al derecho de intimidad
- ✓ Solo se pueden utilizar:
  - Ante una inminente falta por parte del trabajador
  - Ante evidencias o denuncias incuestionables
  - Que no exista otro modo de acreditar la deslealtad
  - A ser posible con conocimiento por parte de alguien del comité de empresa, o con declaración notarial del objeto de la instalación
  - Con encargo motivado a profesionales externos
  - Si se trata de averiguar quien puede ser el autor, aunque tengamos sospechas de alguien, las cámaras deben ser colocadas con situación estratégica neutra

UTILIZACION DE CAMARAS DE SEGURIDAD

- ✓ SENTENCIA TS 31-01-2017 Unificación de Doctrina
- ✓ LA UTILIZACION DE LA PRUEBA A TRAVES DE LAS CAMARAS DE VIDEOVIGILANCIA ES VALIDA AUNQUE EL TRABAJADOR NO HAYA SIDO EXPRESAMENTE INFORMADO.
  - Sigue doctrina TC de rebajar exigencias informativas de la empresa cuando instala video vigilancia (STC 39/2016)
  - No es una instalación oculta, y aunque el motivo sea la seguridad, puede servir para el control de la actividad aunque no se hubiera informado de tal finalidad
  - Se exige el control de idoneidad, necesidad, proporcionalidad en el uso de las imágenes y en la instalación. Debe respetarse el derecho de intimidad.
  - En ambos supuestos contemplados en la Unificación de la Doctrina, en uno el trabajador sabía que se estaba grabando y en el segundo esa conducta había sido objeto de sanción, por lo que no lo hace Universal para todos los supuestos.

II. PARTE PENAL

Responsabilidad Penal de empresas e intervinientes

Ponente
Juan Pablo Correa
Socio

II. PARTE PENAL: BIEN JURÍDICO PROTEGIDO

- ✓ El marco normativo se contiene en el art. 197 CP, que se halla regulado en el Título X de su Libro II, dentro de los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio.

- ✓ En concreto, el art. 197.2 regula el tipo básico, junto a determinadas agravantes y supuestos específicos introducidos por la reforma operada por Ley Orgánica 1/2015, que ha añadido los artículos bis a quinquies.

- ✓ Bien jurídico protegido: Derecho fundamental a la intimidad, consagrado en el art. 18 CE.

II. PARTE PENAL: BIEN JURÍDICO PROTEGIDO

- ✓ Aunque el concepto de intimidad pueda ser muy laxo y determinarse caso por caso, como bien sintetiza la AP Madrid (SAP de 7 de diciembre de 2005), lo que tal precepto constitucional garantiza es un derecho al secreto, a ser desconocido.

- ✓ Dicho sea de otro modo, ***"son datos de carácter reservado los que no son susceptibles de ser conocidos por cualquiera"***, quedando excluidos ***"todos aquellos introducidos en el circuito público con el consentimiento de su titular"*** (STS de 30 de diciembre de 2009).

II. PARTE PENAL: BIEN JURÍDICO PROTEGIDO

✓ Sujetos activo y pasivo del delito:

- Perjudicado es la persona que como consecuencia de un delito o falta sufre un daño y/o perjuicio;

- Ofendido es el sujeto pasivo del delito, si bien éste puede ocasionar perjuicios igualmente a terceras personas.

- A los efectos de lo dispuesto en el art. 201 ap. 1 del Código Penal, debe entenderse que sólo el titular de los datos de que se trate está legitimado para denunciar, sin perjuicio de que, si así lo hace, cualquier tercero que pudiera haber sufrido un efectivo perjuicio como consecuencia del delito pueda mostrarse parte en la causa a los efectos de defender sus derechos e intereses legítimos.

II. PARTE PENAL: CONDUCTAS TÍPICAS

- ✓ Se contienen, básicamente, en los apartados primero y segundo del art. 197 CP

- ✓ Observaciones:

No es necesario que efectivamente se conozcan los datos para que el delito quede perfeccionado: basta con la acreditación de la **intención del agente** (cabe, por tanto, la tentativa acabada o inacabada).

II. PARTE PENAL: CONDUCTAS TÍPICAS

- ✓ **El apoderamiento puede ser físico o meramente intelectual** (por ejemplo, la captación mental o intelectual sin desplazamiento físico también llena el tipo).

- ✓ **Incluso si se dispone de autorización para obtener determinados datos, no puede irse más allá de lo establecido en la misma**, so pena de incurrir en actividad delictiva (SAP de Madrid de 9 de junio de 2014, que sanciona un policía por acceder a bases de datos policiales para averiguar si su esposa había frecuentado determinado hotel).

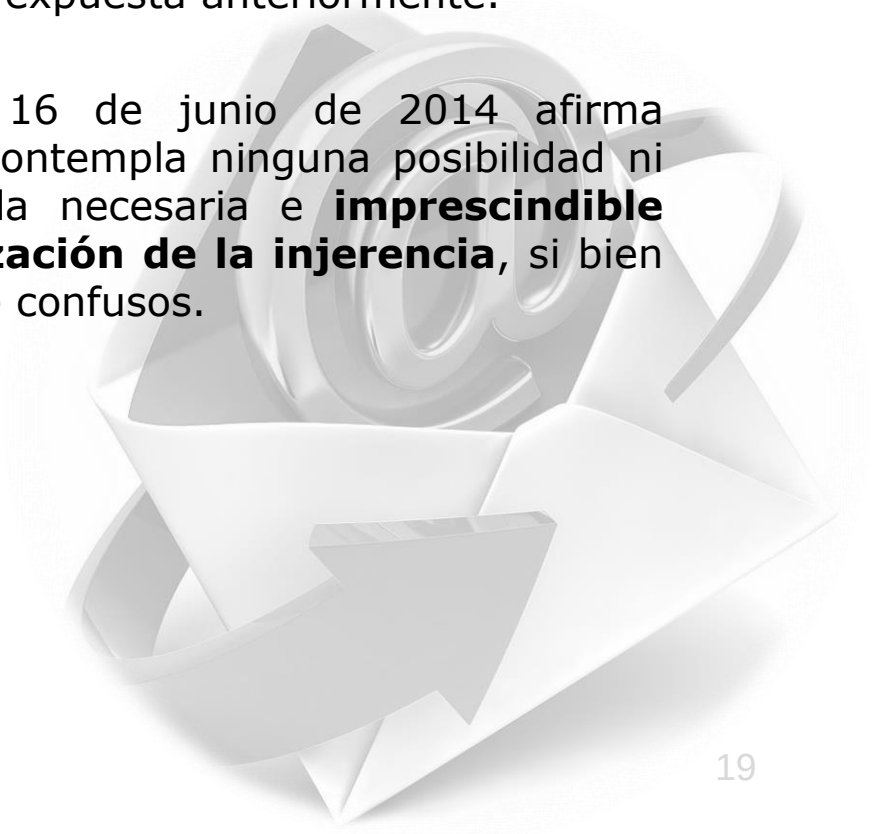
- ✓ **El tipo requiere de dolo y de un elemento subjetivo del injusto: el ánimo de vulnerar la intimidad o descubrir los secretos de otro**, que tiene, por tanto, que demostrar la acusación.

- ✓ **Interesante: ¿puedo recabar datos para denunciar?**

II. PARTE PENAL: ACCESO AL CORREO ELECTRÓNICO

- ✓ El punto de partida es el mismo que en Derecho laboral: la doctrina del TC, del TS y del TEDH que ha quedado expuesta anteriormente.

- ✓ Ahora bien: una reciente STS de 16 de junio de 2014 afirma rotundamente que el art. 18 CE no contempla ninguna posibilidad ni supuesto, que permita excepcionar la necesaria e **imprescindible reserva jurisdiccional en la autorización de la injerencia**, si bien introduce importantes matices, aunque confusos.



II. PARTE PENAL: ACCESO AL CORREO ELECTRÓNICO

- ✓ En cualquier caso, y como requisito previo, **la empresa debe fijar las reglas de uso y las prohibiciones absolutas o parciales de usos personales de los medios tecnológicos** puestos a disposición de los trabajadores.

- ✓ Por ello, cuando la empresa ha prohibido expresamente el uso personal de los medios telemáticos de su propiedad, se admite el control oculto, pues no hay garantía de intimidad.

- ✓ Esta doctrina es aplicable a los medios informáticos, a los correos electrónicos u otras comunicaciones, a la propia navegación por internet, y a los archivos temporales y carpetas que almacenan datos sobre el uso de los medios tecnológicos.

- ✓ El derecho al secreto de las comunicaciones no alcanza a las realizadas en canales abiertos sujetos a la facultad de control e inspección empresarial, quedando limitada la protección constitucional del derecho al secreto de las comunicaciones a las que tienen lugar **por canales cerrados**.

- ✓ Para que pueda otorgarse **valor probatorio** a la intervención de las comunicaciones, es siempre necesaria la autorización e intervención judicial, con las confusas excepciones contenidas en la STS de 16 de junio de 2014.

II. PARTE PENAL: CONSECUENCIAS

- ✓ ¿Y si vulnero estos preceptos, a qué pena me enfrento?

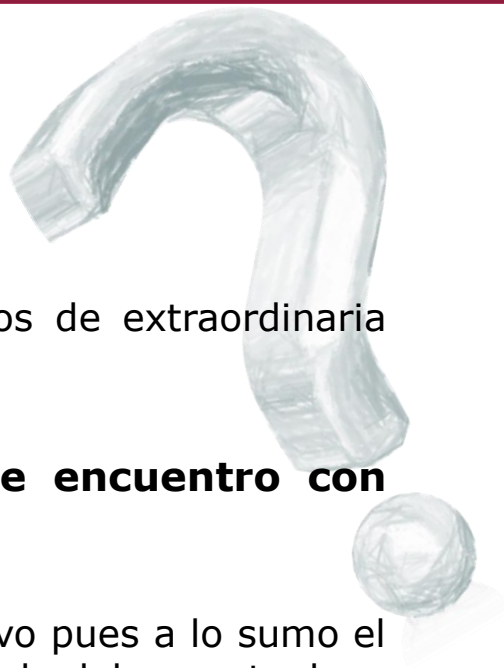
  - Tipo básico: pena de prisión de uno a cuatro años, y multa de doce a veinticuatro meses.

  - Si además me divierto a difundir, revelar o ceder a terceros los datos o hechos descubiertos o las imágenes captadas, pena de prisión de dos a cinco años.

  - La ley contempla, asimismo, otras agravantes en sus apartados 4 a 6 que no comento pues es bastante improbable que los aquí presentes las cometiéramos.

  - Resulta asimismo conveniente examinar los arts. 197 bis, 197 ter, y 197 quater, que contemplan determinados subtipos (como, por ejemplo, para quien facilite a terceros un programa informático con la intención de cometer el delito).

II. PARTE PENAL: CONSECUENCIAS



- ✓ **¿Y si me condenan, me voy a la cárcel?**

En condiciones normales no, a no ser que haya cometido hechos de extraordinaria gravedad (art. 80 CP).

- ✓ **¿Qué pasa si, accediendo al correo corporativo, me encuentro con correos privados? ¿Es punible mi conducta?**

No, puesto que no puede entenderse realizado el elemento subjetivo pues a lo sumo el sujeto, sobre la vulneración de la intimidad, habría actuado a título de dolo eventual.

- ✓ **¿La persona jurídica puede ser condenada por este delito?**

Sí, y le pueden imponer una pena de multa de seis meses a dos años, además de las penas de los apartados b) a g) del art. 33.7 CP. De ahí la necesidad, nuevamente, de hacer un *compliance*.

II. PARTE PENAL: CURIOSIDADES Y HECHOS A TENER EN CUENTA

- ✓ El registro de **conversaciones de las que se toma parte** ha sido tradicionalmente rechazado como conducta subsumible en el tipo, en la medida en que el interlocutor, al participar de la conversación, no estaría ya descubriendo secretos.

- ✓ No acontece lo mismo con **cámaras ocultas**, sobre todo si la filmación afecta al "núcleo duro" de la intimidad, aunque en ocasiones también se obtiene alguna absolución (Caso Antena 3, SAP de Madrid de 15 de abril de 1999).

- ✓ **Bajo ningún concepto pueden utilizarse claves personales para acceder a redes de contactos o Facebook**, de lo contrario la conducta es punible.

II. PARTE PENAL: CURIOSIDADES Y HECHOS A TENER EN CUENTA

- A los efectos del delito, es indiferente que el fin último del autor fuera utilizar el contenido de las conversaciones en un juicio (SAP de Barcelona de 19 de noviembre de 2014, donde se aportan a un proceso matrimonial para obtener la custodia de su hija).

- Los ficheros a los que se accede deben estar previamente registrados, descartándose la tipicidad del acceso a datos que se encuentren en ficheros clandestinos.

- En algunos casos, se autoriza la difusión de datos del investigado para "calmar" a la opinión pública (ATS de 7 de noviembre de 2014, caso del pederasta de Ciudad Lineal).

- En otros, en cambio, se rechaza (se condena a unos periodistas por divulgar el nombre de dos presos con VIH que trabajaban en la cocina de la cárcel).

III. CONCLUSIÓN

- ✓ En todos los casos, se necesita una **política interna** que avise claramente de que el correo electrónico de empresa no es privado + avisos de que la empresa puede controlarlo cuando lo estime oportuno (STS de 6 de octubre de 2011).

- ✓ No obstante, **la prudencia se impone**: investigar el correo de empresa tiene que ser el último recurso y, a ser posible, demostrar que se han implementado otras políticas de prevención.

- ✓ El derecho al secreto de las comunicaciones **no alcanza a las realizadas en canales abiertos** sujetos a la facultad de control e inspección empresarial.

- ✓ **Tampoco alcanza cuando se accede a correos institucionales**, de utilización para fines no estrictamente personales, aunque ocasionalmente pueda hallarse algún correo electrónico privado (Caso del profesor universitario de Alcoy).

III. CONCLUSIÓN

- ✓ Según la última doctrina del TS (controvertida), para que la prueba pueda surtir efectos en el ámbito penal, **se requiere de autorización judicial**, excepto lo que denomina "datos de tráfico" y mensajes que, una vez abiertos por su destinatario, no forman parte de la comunicación propiamente dicha.

- ✓ Como tantas otras veces en Derecho, **no estamos ante una ciencia exacta:** la jurisprudencia es vacilante, y depende mucho del caso por caso (ejemplo, en materia de cámaras ocultas, cuyo uso indebido también se subsume en estos mismos preceptos).

- ✓ **¿A efectos prácticos, si sospecho que puede haber delito, cómo he de actuar?** Preparo querella + precinto ante notario + interpongo querella (588 LECRIM).

Ruegos y preguntas

VENTURA GARCÉS & LÓPEZ-IBOR
ABOGADOS

¡Gracias por vuestra atención!

Tirso Gracia
Socio
tirso.gracia@vg-li.com
T. +34 93 241 97 40

Juan Pablo Correa
Socio
juanpablo.correa@vg-li.com
T. +34 93 241 97 40

www.venturagarceslopezibor.com

VENTURA GARCÉS & LÓPEZ-IBOR

ABOGADOS

BARCELONA

Freixa, 26-28, bajos · 08021 Barcelona
T. (+34) 93 241 97 40 · F. (+34) 93 209 83 91

MADRID

López de Hoyos, 35, 3º A · 28002 Madrid
T. (+34) 91 521 78 18 · F. (+34) 91 524 00 93

www.venturagarceslopezibor.com