JUZGADO DE LO PENAL
NÚMERO SEIS DE BARCELONA

Procedimiento abreviado 117/2016

SENTENCIA Núm.

En Barcelona a treinta de junio dos mil dieciséis.

Vistos por Dª Graziella Moreno Graupera, Magistrada Juez del Juzgado de lo Penal nº 6 de Barcelona los autos de Procedimiento abreviado 117/2016 procedente del Juzgado de Instrucción nº 24 de Barcelona, seguido por un presunto delito continuado de descubrimiento de secretos y un delito de revelación de secretos, siendo acusado **GUSTAVO C. B.,** mayor de edad, con DNI XX, sin antecedentes penales, asistido del letrado Carlos Sánchez Almeida, habiendo intervenido el Ministerio Fiscal como representante de la acción pública y la acusación particular de la Corporació Catalana de Mitjans Audiovisuals SL asistido del letrado en sustitución Enrique Estruch Sellarés.

ANTECEDENTES DE HECHO

PRIMERO.- La presente causa tiene su origen en el atestado 585990/2012 de fecha 2/8/2012 de los Mossos d´Esquadra de Barcelona, por un presunto delito de descubrimiento y revelación de secretos, que dio lugar a las diligencias previas 2484/2012 seguido en el Juzgado de Instrucción nº 24 de Barcelona, frente al acusado indicado en el encabezamiento de esta resolución. En dicha causa se acordó la continuación del procedimiento, y por el Ministerio fiscal se interesó la apertura del juicio oral contra el referido como autor de un delito continuado de descubrimiento de secretos del art. 197,1 y 74 del Código Penal, solicitando la imposición de la pena de 3 años y 6 meses de prisión, inhabilitación especial para el ejercicio del derecho de sufragio pasivo durante el tiempo de la condena y multa de 24 meses a razón de una cuota diaria de 15 euros con la responsabilidad personal subsidiaria en caso de impago del art. 53 del Código Penal y como autor de un delito de revelación de secretos del art. 197,4 del Código Penal, solicitando la pena de 3 años y 6 meses de prisión e inhabilitación especial para el ejercicio del derecho de sufragio pasivo durante el tiempo de la condena y la condena en costas. En igual sentido se pronunció la acusación particular, solicitando que la cuota mensual de la multa sea de 20 euros diarios.

Por la defensa del acusado se ha presentado escrito solicitado su absolución.

Remitidas las actuaciones a este Juzgado, se dictó auto en el que se admitieron las pruebas propuestas por las partes, celebrándose el acto del juicio el 30/6/2016. En la fecha indicada, el acto del juicio se verificó con la asistencia del Ministerio fiscal, la acusación particular y la defensa del acusado, así como los testigos propuestos, con el resultado que consta en autos conforme al acta del juicio grabada en soporte audiovisual.

Como cuestión previa el Ministerio fiscal solicitó la testifical de los agentes de Mossos d´Esquadra 7.957 y 5.329, solicitados también por la acusación particular, lo que fue admitido.

SEGUNDO: El Ministerio fiscal elevó sus conclusiones provisionales que obran en el folio 547 a 550 de las actuaciones a definitivas, interesando la condena del acusado en los términos propuestos en su informe.

La acusación particular elevó sus conclusiones provisionales que obran en el folio 555 a 560 de las actuaciones a definitivas, interesando la condena del acusado en los términos propuestos en su informe.

TERCERO: Por la defensa del acusado se informó en el sentido de entender que no habían quedado probados los hechos que se imputaban a sus representados, solicitando se dictara sentencia absolutoria con todos los pronunciamientos favorables y se declaran las costas de oficio.

Concedida la última palabra al acusado, no efectuó manifestación alguna.

HECHOS PROBADOS

UNICO.- De la prueba practicada en el acto del juicio ha quedado acreditado que el 30 de julio de 2012, Jordi R. G. del Departamento de Recursos Humanos de la Corporació Catalana de Mitjans Audiovisuals (CCMA) remitió a la sra. Teresa F. i L., Directora de Gestió i Recursos de la CCMA, un correo electrónico con tres hojas Excel que contenía información relativa a datos laborales y salariales de trabajadores de la CCMA, de Televisió de Catalunya (TV3) y de Catalunya Ràdio Serveis de Radiodifusió de la Generalitat SA (Catalunya Ràdio). Este correo fue remitido al sr. Brauli D. L.

El 1 de agosto de 2012, el indicado correo fue reenviado a las 16:19 horas por persona desconocida a ochenta buzones de correo de Outlook pertenecientes a la lista global de direcciones de la CCMA. Para realizar dicho reenvío se usó una conexión IP de la red TOR y desde la Web Proxy anónimas. La primera permite ocultar el origen real de las conexiones de sus usuarios y no aparece por tanto la IP real del usuario. Los servicios de la segunda son páginas webs que ofrecen servicios de navegación anónima, y el usuario accede a la página web y navega por Internet sin que su IP real quede registrada en el servidor del servicio de destinación.

Se ha probado que una persona desconocida consiguió el acceso ilícito a cuatro buzones de correo que tenían conexiones IP de la red TOR y de servicios Web Proxy anónimas (Zendproxy, Hidemyass y Anonymouse): DUART_BRA (correspondiente a Brauli D., Presidente del Consejo de Gobierno de la CCMA), PICO_ANT (correspondiente a Antoni P., Jefe del departamento de explotación CEI-Unidades móviles), SALL_EUG (correspondiente a Eugeni S., Director de TV3) y CERD_GUS (correspondiente al acusado **GUSTAVO C. B.,** mayor de edad, con DNI XX, sin antecedentes penales), y ello se produjo de forma continuada entre el 26 de mayo de 2012 y el 1 de agosto de 2012, accediéndose desde fuera de la red de la CCMA mediante la red TOR y desde el interior de la red de la CCMA, mediante el uso de servicios Web Proxy extranjeros. El acceso consistía en la visualización de los correos electrónicos contenidos en los citados

buzones, sin que se realizasen acciones de borrar, reenviar, responder o crear un nuevo correo, salvo el envío de 1/8/2012 ya citado desde el buzón DUAR_BRA.

Tras practicar la entrada y registro en el domicilio del acusado y en la propia CCMA en fecha 11/10/2013, se analizó la actividad de los equipos: IP 192.168.147.33, IP 172.29.111.98 e IP 172. 29.110.194 entre los días 1/4/2012 y 3/8/2012, llegándose a la conclusión de que los accesos ilícitos se llevaron a cabo desde el departamento de Post Producción CEI (Edificio TV3) donde trabajaba el acusado como informático desde las conexiones IP 172.29.111.98 y 172.29.110.194 y siendo el usuario CERD_GUS.

Se ha probado en el acto del juicio que a la fecha de los hechos, podía accederse sin problemas al departamento de Post Producción, instalar programas en los ordenadores sin supervisión y trabajar en los ordenadores abiertos por otro usuario sin introducir ninguna contraseña o clave identificativa.

No se ha probado que desde equipos informáticos propiedad del acusado y que se hallaron en su domicilio se hayan realizado las antedichas conductas delictivas.

No se ha probado que el acusado realizase ninguno de los accesos ilegítimos relatados y en definitiva, que sea autor de ninguno de los dos delitos por los que se ha formulado acusación.

FUNDAMENTOS DE DERECHO

PRIMERO: **Pruebas practicadas**

La prueba de cargo aportada por el Ministerio Fiscal y la acusación particular en el presente procedimiento la constituye, esencialmente, la documental, pericial y la testifical

En el acto del juicio **el acusado** ha contestado únicamente a las preguntas de la defensa y ha expresado que el día anterior a que la policía entrase en su casa, trabajó hasta tarde en el programa “Efectivament” y por la mañana del día siguiente se presentaron los Mossos en su casa con una orden de registro. Les dijo que entraran y que registraran lo que quisieran. Tuvo que vestirse ante un Mosso. Procedieron al registro del despacho. Actuaron en forma agresiva, se subían a las sillas, recogieron cd´s personales y copias de seguridad, fue una actuación contundente. No le comunicaron que estaba detenido. Por la tarde fueron a hacer un registro a TV3 y entonces le detuvieron. Le preguntaron si tenía claves de acceso en el ordenador y les dijo que no. Después del episodio en su casa le dijeron que le tenían que acompañar en un coche y fueron hasta TV3 donde le dijeron que no salieran del coche y luego lo llevaron al departamento de postproducción y recogieron equipos tipo MAC. Él no entendía nada y no sabía qué responder, luego fueron al despacho de marketing. No le habían leído previamente los derechos. Los Mossos iban desalojando las zonas por las que iban. Les pidió para ir al lavabo y le acompañó un agente. Le leyeron los derechos al salir de TV3 a las cinco de la tarde. Le interrogaron sin abogado y le decían que confesara y que dijera quiénes eran sus cómplices, le amenazaron con que no trabajaría en Cataluña. Estuvo dos noches en el calabozo. Declaró con abogado al segundo día, pero no quiso decir nada. No le dejaron dormir en

dos días. No quiso declarar ante el juez. Pidió asistencia médica porque no se encontraba bien. Tiene titulación de ingeniero superior de telecomunicaciones, con altos conocimientos de configuración de redes. Era técnico de postproducción en TV3, administraba y configuraba los sistemas de edición, de video y de audio. En postproducción se utiliza Windows y Mac. Se dejan abiertos para poder trabajar en cualquier momento en postproducción. Las claves eran compartidas, todos tenían conocimiento de las claves. Los ordenadores corporativos no, tenían clave personal. No tenía que pedir autorización para instalar programas, ninguno de los trabajadores informáticos tiene que hacerlo. No ha accedido a la cuenta de correo de nadie, algún trabajador le ha pedido alguna vez que le ayudara con el correo. Niega haber entrado en las cuentas de correo por las que se le acusa. En el ordenador de su casa tiene instalado el programa TOR, lo instaló después de la detención de 2012. Todo lo que dicen los Mossos que se instaló en el ordenador lo hizo después de ser detenido. El TOR lo instaló para dar seguridad al equipo Mac para trabajar. Los documentos que ha presentado a la causa los ha compartido con un perito informático y hay más posibilidades de las que han investigado los Mossos, en las que no se ha entrado. Fuera de la empresa se puede acceder al correo mediante una aplicación. Es posible instalar TOR en los ordenadores de la Corporación y que funcione.

El testigo Ignacio J. V., ha declarado que en agosto de 2012 era el responsable de los Servicios Jurídicos de la Corporación Catalana. Presentó la denuncia al exponérsele los hechos, diciéndole que se envió un correo a la jefa de recursos que a su vez lo reenvió y apareció en los buzones corporativos. No se le dijo en ese momento que había más afectados. Aportó un fichero que le suministró el área de servicios. Todo lo que le expusieron está en la denuncia. No conoce en profundidad las normas de correo corporativo. Denunció la intromisión de correo de Brauli D.. Se puso la denuncia como entidad propietaria de los materiales de la corporación y en nombre de ella. Los Mossos no le suministraron información de la investigación, con él no contactaron.

El **testigo Eugeni S. G.** ha declarado que en el año 2012 era el Director de Televisió de Catalunya y tuvo conocimiento a finales de julio del tema. Entró como director en mayo. Supo que alguien había accedido a su ordenador y a sus cuentas de correo. Se lo comunicó al Presidente de la Corporació. Se produjo un reenvío de su correo. Habló con los Mossos en agosto de 2012. Tenía una dirección de correo corporativo y es a esa cuenta a la que han accedido. No le dijeron explícitamente que esa cuenta sólo era para uso profesional, porque ya se entiende así. Este correo contiene información confidencial de la empresa, sólo puede acceder él. No le dijeron que la cuenta pudiera ser revisada por nadie, ni que iba a ser controlada. Denunció que se había vulnerado el password que únicamente conocía él. No había sucedido nunca y nadie estaba autorizado a acceder a su equipo. No presentó denuncia a título personal. El comité de empresa siempre ha reclamado información sobre los salarios, lo que hasta ese momento era secreto. Ahora ha cambiado en parte, las retribuciones son públicas, según los cargos y categorías, pero no los nombres y apellidos.

El testigo Brauli D. L., ha declarado que como presidente del consejo de gobierno tuvo la primera noticia a través de una llamada que le hicieron explicándole que había un correo que había salido de su cuenta con datos de los trabajadores de la plantilla. Aparentaba como si él hubiese mandado ese correo. El correo estaba en su cuenta porque lo había recibido. Se reunió con la

Directora de Recursos para saber lo que estaba pasando. Por la tarde emitieron un comunicado diciendo que se había producido una comunicación no autorizada. Fueron a denunciar. Esta cuenta la tenía desde enero de 2008. Para acceder a la cuenta tenía un usuario y una contraseña. Las cuentas profesionales solo podían usarse para el trabajo. No había prohibición expresa de usarlas para temas personales pero ya se entendía. Solo el usuario puede ver sus cuentas, no había autorizado a nadie para que entrara en su cuenta. No sabe que esto haya ocurrido nunca. Luego le informaron que su correo ya había sido vulnerado anteriormente. No conoce al acusado. La Corporació no permite un uso personal del correo. Hubo incidencias en el correo y se quejó de que o cargaba su perfil de usuario. Los Mossos no le informaban directamente.

El testigo Antoni P. L. ha declarado que era el jefe del departament d´explotació del CEI, dentro de su departamento había varias secciones entre ellas la de postproducción. El acusado era técnico y estaba en su departamento. Sobre Gustavo había un jefe de servicio. Trabajaba físicamente junto a Gustavo y compartían impresora. No sabe si en postproducción los ordenadores podían compartirse porque él no llevaba el tema. Tenía una cuenta de correo y un nombre de usuario con password. La noticia le llegó por la unidad de investigación de Mossos que le dijeron que habían accedido a su correo. Era un tema de empresa, no suyo. Usaba la cuenta sólo a nivel profesional. No le dijeron que un superior jerárquico controlaría la cuenta de correo o de que podía verlo alguien más. Esto no le había pasado nunca. No le había dado al acusado su password. Le dijeron que habían entrado a su correo desde Alemania. No conoce programas para ocultar su identidad. Se enteró de todo después. La información de esta cuenta es titularidad de la Corporació. No denunció.

El testigo Jordi R. G. ha declarado que trabaja en la Corporació. Supo de los hechos el 31/7 al ver un comunicado en el portal de la empresa que decía que había unos correos publicados y lo envió a Mª Teresa F., David de A. y a Meritxell. Envió un Excel a los Mossos.

La testigo Mª Teresa F. L. ha declarado que es la directora de Dirección de Recursos. El 1 de agosto le llamaron del departamento de comunicación para decirle que había recibido un mail dirigido a buzones de correo. Vio que eran los mismos ficheros y llamó a Brauli D. que vino inmediatamente y habló con informática. Recibió el correo en su buzón corporativo. No tiene conocimiento de que ello hubiera sucedido en otra ocasión. El comité de empresa siempre había pedido los complementos que se pagaban. Declaró lo que le preguntaron.

El testigo David de A. M. ha declarado que es el Director de Recursos Humanos y estaba de vacaciones. Vio que le habían llamado varias veces y le dijeron que se habían hecho públicos los datos de los trabajadores. Supo que se había enviado un mail con datos salariales. A principios de junio, su jefa, la sra. F. le encargó que hiciera un listado con datos salariales, dio traslado de esta petición a Meritxell G. Vinieron los Mossos y colaboró con ellos, pidiendo datos y marcajes de los trabajadores a través del registro informático, él no conoce los horarios.

La testigo Meritxell G. F., ha declarado que en agosto supo del tema, que se había enviado un correo electrónico con un fichero en el que había datos salariales de los trabajadores.

La testigo Roser M., ha declarado ser la presidenta del comité de empresa de TV3. Le avisó por teléfono el presidente de Catalunya Ràdio y le

explicó que a una serie de buzones de correo había llegado un Excel en le que figuraban los salarios de la plantilla, avisó a Nuria A., presidenta en esa época del Comité de Empresa. Todos los buzones eran de la Corporació y todos empezaban con la palabra “BÚSTIA-“. Eran siempre buzones internos. El sindicato no aparecía como destinatario. Esta información la habían solicitado reiteradamente al sospechar que había gente cobrando fuera de convenio. No conocía en aquella época al acusado, lo conoció al salir de los calabozos. Recientemente se advirtió que se había detectado que se podía acceder a contraseñas no encriptadas. Se tomaron medidas, se cambiaron passwords y se hicieron cambios. En 2012 también les hicieron cambiar el password de acceso al entorno corporativo para trabajar. Al correo puede acceder desde su casa. Nadie le ha dicho que en la cuenta del correo corporativo puede entrar alguien a revisar. En la empresa puede trabajar en cualquier ordenador. Cree que la seguridad informática es mejorable. En este caso, al principio pensaron que era un error. Vio la hoja Excel en la que había nombre, DNI, salario, categoría, indemnización en caso de un posible ERO y el sueldo recortado. En 2012 era miembro del comité de empresa.

El testigo Carlos T. C. ha declarado se compañero de trabajo del acusado, compartían los turnos. A primera hora del mañana, el primero que llega se identifica y abre. En los ordenadores corporativos entras con login y password y en los de postproducción no hacía falta password. En éstos se podía acceder a Internet. Desde el ordenador de postproducción no puede accederse sin password a los corporativos, pero a través de Internet sí que puede accederse a las cuentas de correo con la contraseña. Si un trabajador se ausenta, puede hacerse servir el ordenador del otro sin que quede bloqueado. Tardaba mucho en bloquearse. No sospechaba nada del acusado. Eran 8 o 9 personas en el departamento, pero según turnos o vacaciones podía haber más de una persona, se intenta que no haya nadie solo. Podían instalar cualquier programa en 2012 sin supervisión. No conoce cómo funciona TOR. No hay ordenadores personales, están los corporativos y se conecta cualquiera y hay los de dominio.

El testigo Francisco Javier H. Z., ha declarado que es compañero de trabajo del acusado. Para entrar en el despacho usan unas tarjetas y abre el primero que llega, luego queda abierto para todos. Hay ordenadores corporativos con contraseña y de postproducción que no tienen contraseña. En 2012 se dejaba la sesión abierta, ahora no. Cualquiera podía entrar sin usar password. Antes podían instalar programas sin problemas. Usó dos veces el programa TOR. En primavera de 2013, la plantilla hizo una serie de acciones para dar visibilidad al problema de personal que tenían y se creó el “batallón de twister” y para ello se instaló TOR, sólo lo utilizó para cosas concretas. Se sorprendió cuando detuvieron al acusado, cree que le han suplantado a cuenta. Las contraseñas eran débiles. Conoce la web Proxy pero no la ha instalado.

El testigo Mosso d´Esquadra nº 7.957, ha declarado que es el jefe de Subinspectores de la Unidad de Delitos Informáticos y el instructor del atestado. Es ingeniero de telecomunicaciones. Les dijeron que se había mandado un correo corporativo a correos de la Corporació. Actuaron a partir de la denuncia. Estudiaron toda la estructura de la Corporació. El acceso OWA es el servidor electrónico de la Corporació. Alguien instala TOR para acceder al servidor OWA, se accedía al correo pero no al ordenador. TOR es una red paralela a Factbook o Google pero la información está cifrada por lo que no queda la IP de origen, da saltos a cualesquiera otras. TOR supone la realización de actividad ilícita. Las

webs Proxy consiguen desubicar el país y no aparece el lugar desde dónde se está actuando. Para usar TOR hay que descargarlo, la descarga es fácil, la cuestión es hacerlo funcionar. Si no te deja usar TOR puedes acceder con Proxy y obtener estos resultados de acceso. Se ratifica en las conclusiones a las que llegaron. Se analizó la información que les daba el departamento de informática. En la investigación no vieron contenidos, solo la actividad efectuada. Se pidieron todas las conexiones para descartar los accesos lícitos de los ilícitos. Pueden determinar quién ha hecho una llamada a la IP TOR o a la IP Proxy. El juzgado y fiscalía les limitó el acceso a la información para evitar intervenciones agresivas. Empezaron a investigar el grupo de postproducción y vieron indicios contra el acusado. Las máquinas estaban conectadas a postproducción. Identificaron al acusado porque coincidían horas y fechas en las que trabajaba con la de los registros del equipo informático. Los horarios no coincidían con ningún otro trabajador. No vio las periciales derivadas de la entrada y registro. Se trataba de diferentes ordenadores. Participó en la entrada y registro en TV3. 4 de los 5 ordenadores estaban en postproducción y el otro en el departamento de marketing en la habitación de al lado.

Los peritos Albert Hugas Eixarch, Juan Manuel Parra Ríos, Mossos d´Esquadra 146 y 14614, el Mosso d´Esquadra 12.293, y Josep Lluís F. G., se han ratificado en sus respectivos informes y han contestado a las preguntas que les han formulado las partes.

La doctora forense Pérez Bouton se ha ratificado en el informe pericial del acusado y ha contestado a las preguntas de las partes.

Obran en la causa las periciales antedichas y la documental aportada por la defensa.

SEGUNDO: Delitos de descubrimiento y revelación de secretos

Se ha puesto en duda por parte de la defensa de que los hechos objeto de enjuiciamiento sean constitutivos de un delito de descubrimiento y revelación de secretos, puesto que se trata de un acceso a buzones de correo corporativo, sin que se haya acreditado que su contenido sea “secreto”, así como que no obra en la causa copia alguna del correo con los datos personales de trabajadores que se remitió en su día.

El delito de descubrimiento de secretos es un delito de naturaleza tendencial, que requiere la constatación en el obrar el autor de un dolo específico de conocer los secretos o de vulnerar la intimidad de otro. Así, el art. 197,1 del Código Penal establece: "El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación…”

Este delito se configura sobre la acción de adquirir de forma ilícita una información reservada con la finalidad de perjudicar a su titular. Esa información

tiene que ser conseguida al margen de cauces lícitos, casuales o derivados de una relación o situación normal (STS de 10 de diciembre de 2010), en perjuicio de su titular (STS de 30 de diciembre de 2009), sin autorización o de forma ajena a vías normales o socialmente aceptadas (STS de 27 de mayo de 2008), lograda en uso de un dolo específico finalista de descubrir y vulnerar la esfera de intimidad o comúnmente aceptada como reservada del conocimiento común (STS de 21 de marzo de 2007) y a través del quebrantamiento de un sistema de custodia o comunicación cuyo empleo esté directamente conectado con ese ámbito de privacidad (STS de 19 de junio de 2006).

Sobre el bien jurídico protegido, la naturaleza y estructura típica la sentencia del Tribunal Supremo de 21 de marzo de 2007 señala: *"El delito de descubrimiento de secretos del artículo 197.1º del Código Penal se orienta a la protección de la intimidad, reconocida como derecho fundamental en el artículo 18 CE , que garantiza el derecho a la intimidad personal y familiar, derecho que "es propio de la dignidad de la persona reconocida en el art. 10.1 CE e implica «la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura para mantener una calidad mínima de la vida humana»" (* STC 89/2006 *).*

El tipo requiere del dolo, es decir, del conocimiento por el autor de los elementos del tipo objetivo, y además de un especial elemento subjetivo consistente en que la acción se ejecuta con la finalidad ("para") de descubrir los secretos o vulnerar la intimidad de otro. No solo, pues, dolo genérico. Es indiferente a los efectos de este primer apartado la finalidad ulterior del autor, aunque la existencia de un propósito lucrativo tiene su reflejo en el apartado sexto del mismo precepto."

La STS 358/2007, de 30 de abril de 2007 , en sentido similar, razona: *"El artículo 197 del Código Penal contiene varias conductas en una compleja redacción y sanciona en primer lugar al que se apodere de los papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales de otra persona, al quien interceptare las comunicaciones de otro y al que utilizare artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o la imagen o de cualquier otra señal de comunicación, en todos los casos sin su consentimiento y con la finalidad de descubrir sus secretos o vulnerar su intimidad. Se trata de conductas distintas que no precisan que el autor llegue a alcanzar la finalidad perseguida. En los dos primeros casos requiere sin embargo un acto de apoderamiento o de interceptación efectivos, mientras que en el supuesto de utilización de artificios basta con la creación del peligro que supone su empleo con las finalidades expresadas para la consumación de la infracción penal.*

También sanciona a quien, sin estar autorizado, se apodere, en perjuicio de tercero, de datos reservados de carácter personal o familiar de otro, que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Así como a quien simplemente acceda a ellos por cualquier medio sin estar autorizado."

Y específicamente sobre el elemento subjetivo del injusto, la STS de 20 de junio de 2003 significa que la conducta típica *"...ha de ser dolosa, pues no se recoge expresamente la incriminación imprudente, exigida conforme al artículo 12*

del texto legal, que ha de llevarse a cabo con la finalidad de descubrir secretos o vulnerar la intimidad, ya que la dicción literal del precepto emplea la preposición "para"."

Este dolo o voluntad específica de invadir la intimidad ajena supone que la mera intrusión, es decir sin particular finalidad, haya de considerarse impune. Las intromisiones accidentales, como cuando se accede a una comunicación ajena, por un fallo técnico, así al descolgar el teléfono para llamar a otra persona, se escucha la conversación que mantienen dos personas, supone un caso fortuito; y lo mismo cabe entender cuando se deja una información de tipo privado a la vista, por descuido, pues la intencionalidad que exige el tipo penal, requiere un esfuerzo tendente a invadir la intimidad ajena.

Consecuencia de este dolo específico es que, por ejemplo, la sentencia de la Audiencia Provincial de Madrid, secc. 7ª, de siete de diciembre de 2005 , asumida por la *sentencia de la y* Secc. 16ª, de 12 de diciembre de 2012 , razone: *"Debe recordarse que los tipos del art. 197 del C.P requieren el dolo de apoderamiento y el dolo de divulgación; o lo que es lo mismo: el propósito de descubrir secretos y de vulnerar la intimidad de su entonces esposo. Ningún ánimo de conocer o de descubrir secretos se aprecia en la conducta de la acusada cuando, en su propio domicilio y a través de su propio ordenador, encuentra la información de carácter privado, afectante a las relaciones fuera del matrimonio que mantenía su esposo, que él mismo ha introducido en la casa común y en el ordenador común, dejando tal información a la libre disposición de la esposa,..."*

En el caso de autos, la conducta analizada consiste como se ha indicado en los hechos probados, en utilizar sistemas ilegítimos para conseguir entrar en los buzones analizados y acceder a la información allí contenida. Ha quedado claro y manifiesto de la prueba practicada que en los citados buzones se remitía y recibía correo de la Corporación, sin que se haya acreditado que se usaran para asuntos personales. Los testigos han declarado que se remite información confidencial de la empresa y que sólo podía acceder cada uno con su clave.

Sobre el concepto de "secreto de empresa " (aplicable aquí a la información confidencial de una empresa), que ha sido y es objeto de controversia doctrinal, se pronuncia el TS en su sentencia 285/2008 de 12 de mayo que expresa que no define el CP qué debemos entender por tal, seguramente por tratarse de un concepto lábil, dinámico, no constreñible en un "numerus clausus". Por ello, habremos de ir a una concepción funcional-práctica, debiendo considerar secretos de empresa los propios de la actividad empresarial, que de ser conocidos contra la voluntad de la empresa, pueden afectar a su capacidad competitiva. Así serán notas características: la confidencialidad (pues se quiere mantener bajo reserva), la exclusividad (en cuanto propio de una empresa), el valor económico (ventaja o rentabilidad económica) y la licitud (la actividad ha de ser legal para su protección).

Estas notas pueden predicarse de la información o contenido de los correos que se remitiesen entre los afectados y más aún en cuanto al correo que fue detectado, en el que aparecían datos, categorías y salarios de trabajadores de la Corporación. Es cierto que no obra en la causa dicho correo, pero no existen dudas de su existencia, ya que incluso los propios testigos de la defensa, en particular, la testigo Roser M. ha expresado su contenido.

Por todo ello, debe concluirse que los hechos objeto de enjuiciamiento son

constitutivos de un delito continuado de descubrimiento de secretos en cuanto al acceso ilegítimo a los buzones de correo en el periodo indicado y de un delito de revelación de secretos en cuanto a la remisión a ochenta cuentas de correo de los documentos que contenían datos laborales y salariales de trabajadores de la CCMA, TV3 y Catalunya Ràdio.

TERCERO: Prueba sobre la autoría.

Las acusaciones consideran que Gustavo C. es el autor de los hechos y ello en virtud de los indicios obrantes en la causa y especialmente de las periciales practicadas por los Mossos d´Esquadra.

El acusado ha contestado únicamente a las preguntas de su letrado y ha negado la autoría de los hechos que se le imputan. Los testigos, tanto de la acusación como de la defensa, no han efectuado ninguna manifestación relativa a la autoría del acusado. Se ha probado que en la fecha de los hechos desarrollaba sus funciones en el departamento de Post Producción y los testigos que trabajan en el mismo han declarado que accedían mediante el uso de una tarjeta y que el primero que llega, abre y a partir de ahí la entrada es libre. Asimismo, han manifestado que en la actualidad existen controles en cuanto a la instalación de programas en los ordenadores, que en el año 2012 no existían, (todos los testigos han afirmado que tras los hechos se tomaron medidas y se cambiaron passwords). En cuanto al acceso a los equipos, han expresado que en el año 2012, se podía entrar en un ordenador precisamente del departamento de Post Producción, aprovechando la ausencia del usuario, sin necesidad de introducir password. En los ordenadores corporativos había que introducir el usuario y el password, pero hasta que no se bloqueaba por falta de uso, transcurría un cierto tiempo y era muy fácil utilizarlos sin tener que introducir clave alguna. Ello también ha sido corregido en la actualidad. En la fecha de los hechos trabajaban allí unas 8 o 9 personas, han declarado los testigos de la defensa, según los turnos y se intentaba que no hubiera una persona sola.

Es evidente que la seguridad informática en el año 2012 era bastante deficiente y que no existía un control de acceso a los equipos o al propio departamento. Las acusaciones basan su tesis en la existencia de múltiples indicios: la conducta ilícita tiene lugar con los ordenadores del departamento donde trabajaba el acusado, en las horas en las que prestaba servicio e incluso, en equipos informáticos en su domicilio tenía instalado el citado sistema TOR. El instructor de las diligencias, el Mosso d´Esquadra 7.957 ha declarado que tanto el juzgado de instrucción como la fiscalía les limitaron el acceso a la información para evitar las intervenciones agresivas y empezaron a investigar el grupo de Post Producción. Llegaron a la conclusión (folio 493), que en los momentos en los que se detectó la actividad ilícita, el único que trabajaba en el departamento de Post Producción era el acusado. Debe reseñarse aquí que dicha afirmación no ha sido acreditada en forma alguna ya que en el folio 185 se indica los horarios de los titulares de los buzones afectados, pero no los de los trabajadores que pudieran hallarse en el departamento de Post Producción.

Todos esos indicios no dejan de ser puramente circunstanciales, cualquiera pudo entrar en ese departamento y usar los ordenadores como se ha dicho y no se ha probado que la instalación del sistema TOR por parte del acusado en el ordenador Apple Macbook Pro de su propiedad fuese realizada en

la fecha de los hechos (2012), ni que tuviese los requisitos necesarios para funcionar como lo hizo. Debe recordarse que la entrada y registro en casa del acusado se produce en octubre de 2013 y a preguntas de esta juez, los peritos han informado que no han podido saber en qué fecha se instaló dicho programa, ya que los registros que obran en el ordenador no son fiables en este sentido. La pericial de la defensa introduce dudas sobre el origen y la utilización de la red TOR y afirma que el software encontrado en el equipo Apple del domicilio del acusado no pudo utilizarse para obtener las contraseñas de las cuentas de usuario vulneradas, así como que no posee el sistema operativo del que parten las conexiones TOR. Dichas dudas no han sido aclaradas por los informes periciales de las acusaciones.

Finalmente, en cuanto al propio acusado, debe ponerse de manifiesto que los usuarios de los buzones afectados han manifestado que ni siquiera le conocían y su propio jefe, indica que trabajaba junto a él y nunca sospechó nada. Los testigos aportados por la defensa, también compañeros, han expresado su sorpresa por los hechos. No se ha efectuado ninguna investigación sobre el acusado más allá de hacer constar dónde trabajaba y los equipos que usaba en la empresa y en su domicilio. Se ha dado a entender en el acto del juicio que en la época de los hechos existía tensión con los trabajadores ante la amenaza de un ERE, siendo precisamente uno de los contenidos del correo que se reenvía, la indemnización que correspondería a cada uno de los trabajadores que allí se indicaban si dicho expediente se realizaba. Es evidente que una información de este calibre tenía interés para todos los trabajadores, pero en ningún momento se ha puesto de manifiesto el perfil del acusado dentro de la empresa, ni que tuviese interés en perjudicarla. Aparece como un trabajador anodino al que únicamente conocen sus compañeros de trabajo más directos.

Tal y como expresa la sentencia de la Sala 2ª del Tribunal Supremo de fecha 28/9/2010, ROJ 4840/2010, a falta de prueba directa, también la prueba indiciaria puede sustentar un pronunciamiento de condena, sin menoscabo del derecho a la presunción de inocencia (*STS. 870/2008 de 16.12)*, siempre que:

a) Los indicios se basen en hechos plenamente probados y no en meras sospechas, rumores o conjeturas.

b) Que los hechos constitutivos del delito o la participación del acusado en el mismo, se deduzcan de los indicios a través de un proceso mental razonado y acorde con las reglas del criterio humano, detallado en la sentencia condenatoria.

Como se dijo en las *SSTC. 135/2003 de 30.6 y 263/2005 de 24.10*, el control constitucional, de la racionalidad y solidez de la inferencia en que se sustenta la prueba indiciaria puede efectuarse tanto desde el canon de la **lógica o coherencia** (de modo que será irrazonable si los indicios acreditados descartan el hecho de que se hace desprender de ellos o no conduzcan naturalmente a él), como desde el de su **suficiencia o carácter concluyente** , (no siendo pues, razonable, cuando la inferencia es excesivamente abierta, débil o imprecisa),si bien en este último caso se debe ser especialmente prudente, puesto, que son los órganos judiciales quienes, en virtud del principio de inmediación, tienen un conocimiento cabal, completo y obtenido con todas las garantías del acervo probatorio.

En este sentido la *sentencia del Tribunal Constitucional 189/1998* expresa que “partiendo en que además de los supuestos de inferencias ilógicas o inconsecuentes, deben considerarse asimismo insuficientes las inferencias no concluyentes, incapaces también de convencer objetivamente de la razonabilidad de la plena convicción judicial, ha señalado que un mayor riesgo de una debilidad de este tipo en el razonamiento judicial se produce en el ámbito de la denominada prueba de indicios que es la caracterizada por el hecho de que su objeto no es directamente el objeto final de la prueba, sino otro intermedio que permite llegar a éste a través de una regla de experiencia fundada en que usualmente la realización del hecho base comporta la de la consecuencia. En el análisis de la razonabilidad de esa regla que relaciona los indicios y el hecho probados hemos de precisar ahora que solo podemos considerarla insuficiente desde las exigencias del derecho a la presunción de inocencia, si a la vista de la motivación judicial de la valoración del conjunto de la prueba, cabe apreciar de un modo indubitado o desde una perspectiva externa y objetiva que la versión judicial de los hechos es más improbable que probable. En tales casos... no cabrá estimar como razonable bien que el órgano judicial actuó con una convicción suficiente ("más allá de toda duda razonable"), bien la convicción en si”*(SSTC. 145/2003 de 6.6, 70/2007 de 16.4*).

Ante esta situación de incertidumbre probatoria y ante la inexistencia de indicios, necesariamente ha de acudirse al auxilio del principio *in dubio pro reo* y al mandato absolutorio que el mismo impone.

CUARTO.- Costas

Las costas procesales, dado el carácter absolutorio de la sentencia, conforme a lo dispuesto en el artículo 123 del Código Penal y en los artículos 239 y 240 de la LECrim, se declaran de oficio.

FALLO

ABSUELVO a **GUSTAVO C. B.,** mayor de edad, con DNI nº XX, sin antecedentes penales, del delito continuado de descubrimiento de secretos y delito de revelación de secretos por los que venía acusado por el Ministerio fiscal y por la acusación particular, **declarando de oficio las costas causadas**.

Notifíquese esta resolución al Ministerio Fiscal y demás partes personadas, conforme dispone el artículo 248.4 de la Ley Orgánica del Poder Judicial.

Expídase testimonio literal de la presente resolución, que se unirá a los autos de su razón, y el original intégrese en el libro de sentencias a que se refiere el artículo 265 de la Ley Orgánica del Poder Judicial.

Así por esta mi Sentencia, por el poder que me confiere la Constitución Española, en nombre de S. M. El Rey, lo pronuncio, mando y firmo.

PUBLICACIÓN.- Leída, dada y publicada la anterior sentencia por el Ilmo. Sr. Magistrado que la dictó, estando celebrando audiencia pública. Doy fe.-