

Castigo laboral "versus" crimen empresarial. Control empresarial de dispositivos electrónicos para uso laboral y su repercusión en los delitos contra la intimidad.

Magdalena Nogueira Guastavino

Catedrática de Derecho del Trabajo y de la Seguridad Social. Universidad Autónoma de Madrid.

Resumen: No se incurre en delito de descubrimiento y revelación de secretos por parte del empresario que accede a los correos electrónicos (incluso personales) de los trabajadores cuando han sido debidamente informados del exclusivo uso profesional de los correos en reiteradas ocasiones y el acceso se produce de modo casual al realizar una copia de seguridad del servidor de correo electrónico corporativo de la empresa, propiciada por un problema en su funcionamiento motivado por el hecho de que el buzón del citado correo estaba lleno.

Palabras clave: Intimidad. Correo corporativo. Dispositivos digitales en el trabajo. Alcance de la injerencia a efectos penales.

Abstract: There is no offense of discovery and disclosure of secrets committed by the employer who accesses the employees' emails (including personal ones) when they have been duly informed of the exclusive professional use of the emails on repeated occasions and the access occurs incidentally while making a backup of the company's corporate email server, caused by a malfunction due to the email inbox being full.

Keywords: Privacy. Corporate email. Digital devices at work. Scope of interference for criminal purposes.

I. Introducción

Se plantean querellas contra la empresa por parte de extrabajadores que fueron despedidos por realizar un uso personal del correo exclusivamente corporativo. Los despidos fueron considerados nulos en la jurisdicción social por ilícita obtención de los correos electrónicos por vulneración de derechos fundamentales. En el ámbito penal se rechaza que el comportamiento empresarial incurra en el tipo delictivo de revelación o descubrimiento de secretos del art. 197 CP.

II. Identificación de la resolución judicial comentada

Tipo de resolución judicial: sentencia.

Órgano judicial: Tribunal Supremo, Sala de lo Penal.

Número de resolución judicial y fecha: sentencia núm. 889/2024, de 23 de octubre.

Tipo y número recurso o procedimiento: recurso de casación por infracción de ley núm. 3302/2022.

ECLI:ES:TS:2024:5200

Ponente: Excmo. Sr. D. Andrés Martínez Arrieta.

Votos Particulares: carece.

III. Problema suscitado. Hechos y antecedentes

Durante años tres trabajadores prestaron servicios para una misma mercantil (CONASA Consultores, cuya administradora y socia mayoritaria es María Rosa). La empresa proporcionaba a los trabajadores equipos informáticos con una cuenta de correo electrónico corporativo asignada a cada uno de ellos, encendiéndose cada uno de los ordenadores con una clave genérica conocida por todos los trabajadores de la empresa, y sin que el acceso al correo electrónico de cada uno de ellos requiriese de clave alguna. El artículo 26 del Convenio de Oficinas y Despachos, norma aplicable al trabajo desarrollado, establece como constitutiva de falta grave la realización "sin el oportuno permiso, trabajos particulares durante la jornada, así como emplear para uso propio, herramientas o materiales de la empresa". En el presente caso ninguno de los tres trabajadores tenía autorización para emplear el correo electrónico corporativo para fines propios. En la empresa CONASA se celebraban periódicamente reuniones entre la directiva y los ocho empleados con los que contaba, constando que, al menos hasta 8 ocasiones, se dieron a los empleados órdenes reiteradas en relación con que el uso de los medios informáticos de la empresa (incluidos ordenadores, programas informáticos, Internet, etc.) insistiéndose en que sólo debían ser utilizados para el desarrollo de la actividad laboral y no para uso personal. El 13 de marzo de 2015 los tres empleados afectados firmaron, sin reserva alguna, un documento confeccionado por doña María Rosa, en el que se les reiteraba la obligación ineludible de respetar la absoluta confidencialidad de la información relativa a la actividad laboral, así como que el uso de los sistemas propios, sistemas y programas informáticos y aparatos electrónicos propiedad de la empresa se hallaba restringido exclusivamente al desempeño del trabajo profesional de los empleados de la misma, al igual que el acceso a Internet, redes sociales, etcétera que la empresa ponía a disposición de sus empleados.

Con ocasión de la recuperación en tales fechas (marzo de 2015) de una copia de seguridad del servidor de correo electrónico corporativo de la empresa, propiciada por un problema en su funcionamiento motivado por el hecho de que el buzón del citado correo estaba lleno, doña María Rosa tuvo acceso al contenido de gran número de correos electrónicos remitidos por sus trabajadores empleando el correo corporativo de la empresa, entre los cuales se encontraban cientos de correos enviados a lo largo del tiempo, muchos de ellos con un contenido ajeno a la actividad laboral de la empresa y relativos a la esfera personal de estos tres empleados (atinentes a sus relaciones conyugales y familiares, e incluso reveladores de la existencia de una relación personal de carácter íntimo entre dos de estas personas). En algunos de los citados mensajes de correo electrónico remitidos o intercambiados por doña Valle, doña Virtudes y don Carlos Alberto son varias las ocasiones en las que se instaban a borrarlos, así como a emplear otros medios de comunicación como los SMS, lo que resulta muestra de que percibían el correo electrónico corporativo como un medio de comunicación abierto al acceso por parte de terceros. Sobre la base de dichos correos la empresa procede a despedir a los trabajadores quienes impugnaron los mismos obteniendo sentencia del Juzgado de lo Social de Donostia declarado los despidos disciplinarios nulos por vulneración de los derechos fundamentales de estas tres personas, declarándose la ilicitud en la obtención de los correos electrónicos.

Los trabajadores instaron, como querellantes, acciones penales contra la dirección de la empresa, representada por Doña María Rosa. El Juzgado de lo Penal n.º 5 dictó resolución absolviendo a Doña María Rosa de los delitos contra la intimidad del art. 197 CP de los que era acusada en la causa. La representación de los extrabajadores

interpuso recurso de apelación ante Audiencia Provincial de Guipúzcoa, que confirmó la absolución, contra la que se interponen recurso de casación. La Sentencia del Tribunal Supremo, Sala de lo Penal, confirma las sentencias anteriores y condena en costas a los recurrentes.

La STS sintetiza los ocho motivos esenciales del recurso de los querellantes y comienza delimitando el ámbito del recurso de casación respecto resoluciones de las Audiencias provinciales en apelación de sentencias de los Juzgados de lo Penal, recordando la doctrina contenida en su STS 626/2024, de 19 de junio, interpretando el art. 847.1 b) LECrim, así como el criterio contenido en el Acuerdo del Pleno No Jurisdiccional de 9 de junio de 2016, interpretando dicho precepto y avalado por ATC 40/2018. En resumen, se recuerda que el recurso de casación solo es admisible por la vía del artículo 849.1º LECrim, que permite la casación por infracción de un precepto penal de carácter sustantivo (error iuris) que deba ser observado en la aplicación de la Ley Penal (normas determinantes de subsunción), sin que proceda por ninguno de los motivos de quebrantamiento de forma, ni los previstos por el art. 850 LECrim, ni frente a las sentencias dictadas en segunda instancia por las Audiencias la infracción de ley prevista en el art. 849.2º LECrim fundada en error en la apreciación de la prueba, basado en documentos que obren en autos, que demuestren la equivocación del juzgador, pero sin resultar contradichos por otros elementos probatorios. Proyectando dicha doctrina a los motivos del recurso, el TS rechaza conocer de la mayor parte de las quejas. En concreto, considera que los motivos en los que la casación se sustenta en la denuncia de un error de derecho sobre preceptos no sustantivos penales, como las leyes procesales, las leyes de protección de datos o los Convenios colectivos, carecen de virtualidad para formular una queja casacional, siendo tampoco atendibles las quejas fundadas en vulneraciones de derechos fundamentales. En ambos supuestos, porque “los errores por denuncias de aplicación indebida de preceptos no sustantivos, o de derechos fundamentales, han sido objeto de dos instancias, la del enjuiciamiento y la de la revisión, y ese pronunciamiento ha sido resuelto en los términos previstos en la legislación procesal, con arreglo al proceso debido”.

El debate se centra, así pues, en el motivo en el que se denuncia el error de derecho por la inaplicación, al hecho probado, del art. 197 del Código penal^[1] sobre el delito de descubrimiento y relevación de secretos de otro, cuya tipicidad se vertebraba sobre el apoderamiento ilícito realizado para descubrir los secretos de otro o vulnerar su intimidad, y sobre la interceptación de las comunicaciones. Comienza el Tribunal recordando que los derechos a la intimidad personal y a la propia imagen, garantizados por el artículo 18.1 de la Constitución Española (CE), son considerados bienes de la personalidad y están protegidos bajo el Código Penal en el título de “Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio”. No se interpreta en el sentido de confidencialidad, sino que se trata de derechos que protegen un espacio de intimidad personal y familiar contra intromisiones externas, especialmente frente al desarrollo de medios de captación, divulgación y difusión de información. Asimismo, recuerda que en el art. 197.1 CP la idea de secreto resulta conceptualmente indisociable al concepto de intimidad (con cita de la STS nº 666/2006, de 19 de junio), como se extrae de la ubicación del precepto en el Título, dedicado a los delitos contra la intimidad, y de modo coherente con su propia redacción, pues en el primer apartado del art. 197 relaciona los papeles, cartas o mensajes de correo electrónico con otros documentos o efectos personales, y su segundo apartado (197.2 CP) se refiere a datos reservados de carácter personal o familiar.

En relación con la conducta enjuiciada, resalta el Tribunal que el *tipo objetivo* requiere solamente un “acto de apoderamiento”, sin necesidad de que el autor llegue a descubrir los secretos o vulnerar la intimidad en el primer caso, y el “mero acceso” de los datos protegidos en el segundo. El *tipo subjetivo* exige, sin embargo, la finalidad de descubrir secretos o vulnerar la intimidad junto con el dolo en el acto de apoderamiento o de acceso.

Comienza la Sala de lo Penal examinando el término “apoderarse de datos” poniendo de manifiesto la existencia de una interpretación estricta (como apoderamiento en los delitos patrimoniales), pero también otra más amplia que incluiría copiar datos dejando intactos los originales o simplemente el hecho de captar información. Por otro lado, en cuanto al supuesto de hecho del segundo párrafo relativo a “apoderarse, utilizar o modificar datos reservados de carácter personal o familiar”, el TS afirma que “utilizar” es usar sin apoderarse de ellos y “modificar” es alterarlos, tanto si se trata de mejorar como de perjudicar la situación del sujeto al que afectan. En todo caso, las conductas tienen que producirse sin estar autorizado para acceder, manipular o modificar el banco de datos y realizarse en perjuicio de tercero, tercero que puede ser distinto al titular de los datos, en cuyo caso se produce una triple implicación de sujetos (sujeto activo, titular de los datos y eventual perjudicado) que responde, a la idea de que el titular de los datos no puede ser sujeto activo del delito porque él es el sujeto pasivo, dado que lo tutelado es su intimidad (con cita de la STS 1461/2001, de 11 de julio).

En el caso examinado las sentencias recurridas hacen referencia al “hallazgo de correos” cuando se realiza una copia de seguridad al constatar que el buzón estaba al completo, momento en el que se localizaron “cuentas de correos” entre los querellantes, ajenas al trabajo y que, por incumplir la reserva impuesta por el convenio y las directrices empresariales, sirvieron a la empresa para extinguir la relación laboral, extremo que fue impugnado por los empleados quienes vieron estimada su reclamación en la jurisdicción social.

Para la Sala, el núcleo de la cuestión desde la perspectiva penal es el de decidir el carácter de apoderamiento que requiere la tipicidad del delito objeto de la acusación y para ello considera que debe examinar la jurisprudencia de la Sala de lo penal, del Tribunal Constitucional y del Europeo de Derechos Humanos a fin de conformar el carácter indebido de la conducta del empleador. Tras aludir al art. 20 bis ET y el art. 87 LOPDyGDD, la Sentencia pone de relieve que las “situaciones conflictivas surgen en el ejercicio de los respectivos derechos, a la intimidad, y al control de los medios de producción, en los que las decisiones del orden social de la jurisdicción, observante de las relaciones laborales, y de la penal, pueden abordar las situaciones conflictivas desde distintas perspectivas, la relación laboral y la agresión a bienes jurídicos de naturaleza fundamental”.

El Tribunal hace un repaso de las sentencias claves a la hora de dar solución a la situación conflictiva que puede producirse cuando el empleo de medios informáticos suministrados por el empleador es utilizado por el trabajador para su uso personal, poniendo de relieve que en su mayor parte se refieren a “información obtenida en aparatos de uso corporativo en los cuales el trabajador ha introducido datos de carácter personal y se pretende su utilización como hecho de prueba”. En concreto, hace referencia a la STS Penal nº 528/2014 de 16 de junio, STS Penal 489/2018 de 23 de octubre, STS Penal (Pleno) nº 328/2021, de 22 de abril, STS Penal 56/2022 de 24 de enero, STS Penal 817/2022, de 14 de octubre, Sentencia 89/2023 (asunto Pescanova), de 10 de febrero.

La doctrina de dichas sentencias, aun no uniforme y basada en la casuística, parte del examen de la ilegitimidad de la intromisión y de que se produce cuando se vulnera la expectativa de intimidad por parte del trabajador. Se insiste en que la clave reside en si el trabajador ha consentido anticipadamente reconociendo esa capacidad de supervisión al, empresario y, por tanto, cuenta con ello y está advertido, ya que en tal caso se trata de una limitación conocida y contractualmente asumida, posible en las relaciones privadas, pero que no es trasladable al ámbito de las relaciones con los Poderes Públicos, donde no cabe esa “cesión” anticipada o renuncia previa a ese espacio de intimidad virtual. En palabras del TS (STS Pleno [328/2021]): “El reconocimiento previo, explícito o implícito, de esa facultad del empresario constituye el *punctum dolens* la clave, en el ámbito de las relaciones laborales. En una investigación penal lo será la autorización judicial o el consentimiento actual”.

Proyectada la doctrina penal al caso concreto, la sentencia desestima los recursos porque desde la perspectiva del error de derecho, al no constatarse un apoderamiento ilícito y observarse las reglas de valoración de la protección de la intimidad de los empleados, no ha existido un quebrantamiento de sus expectativas de intimidad, la sentencia impugnada no ha incurrido en ningún error al declarar la absolución de la acusada. En concreto, la sentencia subraya que los querellantes habían sido advertidos y habían tomado conocimiento de las prohibiciones de hacer un uso particular del material informático puesto a su disposición por el empleador para el desarrollo de la actividad laboral. Tampoco sus correos estaban protegidos por una contraseña propia y personal. Habían sido informados, sin reserva alguna, y se reiteraba la obligación ineludible de respetar la absoluta confidencialidad de la información relativa a la actividad laboral, así como del uso de los sistemas propios, sistemas y programas informáticos que se hallaban restringidos, exclusivamente, al desempeño del trabajo profesional, habiendo sido requeridos, al menos en ocho ocasiones, y se ha probado que ellos mismos se advertían en sus mensajes sobre la necesidad de borrarlos y de emplear otros medios de comunicación. Por ello concluye que eran conscientes de la limitación de uso y de los límites a su utilización. Asimismo, resalta que se ha probado que “no hubo un acto de intromisión, sino que, al realizar una copia de seguridad y constatar que el buzón de correo se acumulaba al límite de su capacidad, se constató su utilización para cuestiones ajenas a su autorización para a ser utilizado como instrumento de trabajo. Consecuentemente, desde la perspectiva del error de derecho, ningún error cabe declarar en la absolución de los acusados, cuando el relato fáctico no refiere un apoderamiento ilícito y se declara la observancia de las reglas de valoración de la protección de la intimidad con pleno conocimiento de la obligación de los empleados de los límites de utilización, sin que quepa afirmar, desde el hecho probado, un quebrantamiento de las expectativas de intimidad que hayan sido vulneradas”.

IV. Normativa aplicable al caso

- Arts. 18 1 y 3 CE; art. 197 del Código Penal; art. 20 bis ET; art. 87 LOPDyGDD

V. Doctrina básica

La parte empleadora no incurre en delito de apoderamiento y descubrimiento de secretos de los que fueron sus trabajadores cuando habían sido advertidos del uso exclusivamente personal del material informático puesto a su disposición por el empleador para el desarrollo de la actividad laboral, el canal de comunicación era abierto al no existir clave en ningún ordenador, usarse una genérica conocida por todos, y reconocer los trabajadores en sus correos privados entre ellos que debían borrar los mensajes y comunicarse por otra vía. Sin que exista acto de intromisión cuando, al realizar una copia de seguridad y constatar que el buzón de correo se acumulaba al límite de su capacidad, se constató su utilización para cuestiones ajenas a su autorización estrictamente laboral.

VI. Parte dispositiva

Desestima el recurso y condena a los recurrentes al pago de costas.

VII. Pasajes decisivos

- “Los derechos a la intimidad personal y a la propia imagen garantizados por el art. 18.1 CE, forman parte de los bienes de la personalidad que pertenecen Código Penal que se rotula como “Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio”. STS al ámbito de la vida privada. Salvaguardan estos derechos un espacio de intimidad personal y familiar que queda sustraído a intromisiones extrañas, destacando la necesaria protección frente al creciente desarrollo de los medios y procedimiento de captación, divulgación y difusión de la misma y de datos y circunstancias que pertenecen a la intimidad”

- “En relación con la conducta enjuiciada, interesa resaltar que el tipo objetivo requiere solamente un acto de apoderamiento, sin necesidad de que el autor llegue a

descubrir los secretos o vulnerar la intimidad en el primer caso, y en el mero acceso de los datos protegidos en el segundo. El tipo subjetivo exige, sin embargo, aquella finalidad, junto con el dolo en el acto de apoderamiento o de acceso”.

- “Las conductas tienen que producirse sin estar autorizado para acceder, manipular o modificar el banco de datos y realizarse en perjuicio de tercero, tercero que puede ser distinto al titular de los datos produciéndose una triple implicación de sujetos (sujeto activo, titular de los datos y eventual perjudicado) que responde, a la idea de que el titular de los datos no puede ser sujeto activo del delito porque él es el sujeto pasivo, dado que lo tutelado es su intimidad, tal como preciso la STS 1461/2001, de 11 de julio”.

- “Las situaciones conflictivas surgen en el ejercicio de los respectivos derechos, a la intimidad, y al control de los medios de producción, en los que las decisiones del orden social de la jurisdicción, observante de las relaciones laborales, y de la penal, pueden abordar las situaciones conflictivas desde distintas perspectivas, la relación laboral y la agresión a bienes jurídicos de naturaleza fundamental”.

VIII. Comentario

De nuevo se plantea un conflicto entre dos importantes derechos confrontados y dos perspectivas de análisis no necesariamente concurrentes al depender su solución de dos jurisdicciones distintas que atienden a bienes y tutelas propias. La paradoja que puede darse en este cruce de jurisdicciones es que la empresa, haciendo uso de su poder de vigilancia y control de los dispositivos informáticos puestos a disposición de los trabajadores para el exclusivo desarrollo de su prestación laboral, pueda despedir precedentemente a quienes, incumpliendo, los usan para actividades no laborales, pero que a continuación se enfrente en el ámbito penal a una condena por un delito de descubrimiento de secretos. Ello es especialmente sensible en relación con una posible vulneración del art. 18.3 CE, muy flexiblemente interpretado en el ámbito laboral y constitucional laboral, pero de modo muy estricto en el ámbito penal. Prueba de ello sería la STS penal 528/2014, de 16 de junio donde se clarificaba la necesidad de autorización judicial, en todo caso, cuando el empresario monitorice correos privados del trabajador. En dicha sentencia el art. 18.3 CE es tajante garantizando el secreto de comunicaciones “salvo resolución judicial” y “no contempla por tanto, ninguna posibilidad ni supuesto, 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 en la autorización de la injerencia”. La sentencia, además, rechazaba también la posibilidad de una tácita renuncia al derecho al secreto a las comunicaciones, porque, “a diferencia de lo que ocurre con la protección del derecho a la inviolabilidad domiciliaria (art. 18.2 CE) nuestra Carta Magna no prevé, por la lógica imposibilidad para ello, la autorización del propio interesado como argumento habilitante para la injerencia”. En dicha sentencia se afirmaba que ello “no impedía la utilización de medios de investigación tan útiles para el descubrimiento de conductas gravemente reprochables sino, tan sólo, de dar cumplimiento a las previsiones constitucionales rectoras de un procedimiento tan invasivo en derecho de semejante trascendencia para los ciudadanos, resultando, a tal efecto, imprescindible, como decimos, la autorización y el control que sólo el Juez puede dispensar en nuestro ordenamiento, incluso según la legislación laboral, que al menos aparentemente sigue el mismo criterio de clara vocación judicial” (con cita del art. 76.4, 90.2 y 4 de la LRJS). A partir de esta sentencia se abrían numerosos interrogantes y cautelas laborales, obligando a repasar el contenido constitucional del ámbito del derecho reconocido en el art. 18.3 sobre el secreto de las comunicaciones (y no así del tráfico de datos que estaría excluido), qué comunicaciones, qué sujetos están vinculados por dicho secreto, cuál es su diferencia con el derecho a la intimidad, y la posibilidad de monitorizar los correos cuando hubiera finalizado el proceso de comunicación, en caso de canales abiertos, o una vez hubieran sido abiertos los correos que podría considerarse que fenecía el secreto.

La Sala de lo Penal ha ido perfilando y precisando tan contundente afirmación, así como matizando algunos de sus criterios a la vista de la evolución tecnológica (que permitirá poner en duda la certeza de que todo correo cerrado deba tenerse por no leído, restando relevancia a este indicio). De momento se ha clarificado que la exigencia de autorización judicial para cualquier intromisión en el secreto de las comunicaciones del art. 18.3 CE queda limitada a la preservación de tal derecho. (STS Penal caso Pescanova nº 89/2023). La presente sentencia lo confirma. Exigencia nacional que se ha considerado mucho más rígida que la contemplada por el TEDH en tanto en su Sentencia *Barbulescu* II sólo impone un exhaustivo cumplimiento del principio de información, transparencia y proporcionalidad, y que no debiera generar fricciones cuando en el ámbito nacional se exige un estándar de protección más alto del derecho fundamental al secreto de las comunicaciones pues el CEDH se limita a establecer los niveles de protección mínimos en sociedades democráticas (Albert Estrada i Cuadras^[2]). En puridad en el asunto *Barbulescu* no parece que se entre a valorar el derecho al secreto de la correspondencia del art. 8 CEDH porque en el ámbito interno el recurrente no había impugnado el informe de la fiscalía que dictaminaba que no había vulneración -porque era la empresa la propietaria del sistema informativo y de la conexión de internet y podía revisar la actividad y la información almacenada al estar prohibido el uso personal de los sistemas informáticos-, y solo en las observaciones ante la Gran Sala se alegó la vulneración del secreto de la correspondencia lo que, por tal motivo, expresamente quedó fuera del ámbito del caso examinado (párrafos 64 y 94). Al margen de ello, en las últimas sentencias de la Sala de lo Penal, ya queda claro que la exigencia de autorización judicial no es exigible cuando el derecho que está en juego es el de la intimidad o el de la autodeterminación informativa.

En la sentencia que se comenta, sin embargo, el único motivo de examen es el error de derecho por la inaplicación, del art. 197 del Código penal, en relación con el delito de apoderamiento de los secretos de otro, como delito relativo a la intimidad personal y vinculado con el art. 18.1 CE. Y, como en las sentencias penales que la anteceden y a las que se remite, se centra en examinar si en la conducta empresarial concurre un acto de intromisión, lo que niega al ser resultado de un hallazgo casual derivado de la copia de seguridad de un disco provocado por el elevado número de correos que lo había saturado. Vamos, que en la medida en que el descubrimiento del secreto personal no se ha producido como consecuencia de una conducta encaminada a su averiguación, no se cumpliría un elemento del tipo. Considera además que no hay apoderamiento pues el acceso no es ilegal, en tanto lo prohibido es el acceso no autorizado, carente de consentimiento, y en el caso concreto, se parte en los hechos probados de un claro supuesto de incumplimiento de la normativa aplicable y de las instrucciones y reservas sistemáticamente realizadas. Cumplida la transparencia informativa, considera que no hay expectativa de intimidad y el acceso, casual, no puede subsumirse en el tipo penal. Se ratifica con esta sentencia el criterio de la Sala de lo Penal (STS 89/2023) reforzando la importancia del consentimiento expreso y explícito de los trabajadores para la intervención de sus correos electrónicos y de que, sin dicho consentimiento las intervenciones pueden ser consideradas vulneración de la privacidad. Sólo a partir del conocimiento, consentimiento y negociación contractual sobre el uso de los dispositivos empresariales, se admite la reducción de la expectativa de privacidad y se legitiman las medidas de control por el empleador.

A mi juicio, las sentencias de lo Penal (las citadas por la comentada y ella misma) aluden siempre a *Barbulescu* II y al art. 87 LOPDyGDD, pero minimizan en su proyección al caso concreto la importancia de la “ventana de privacidad” que claramente impone dicha sentencia y que se recoge en el art. 87 LOPDyGDD. Me refiero a la relativa al “uso social” como límite a las prohibiciones totales de uso personal de los dispositivos o herramientas laborales informáticas. A mi juicio un planteamiento (laboral o penal) adecuado a la doctrina europea mencionada, así como a la nueva regulación de derechos digitales contenida en el art. 87 de la LOPDyGDD (cuyo objeto expreso, por cierto, es proteger la intimidad) debe partir de que, incluso cuando el correo es corporativo, se ha comunicado e informado del uso exclusivo

profesional, debe concurrir otro elemento para considerar la licitud de la intromisión consistente en explicar e informar no solo del “uso”, sino expresamente proyectar la transparencia informativa sobre un segundo elemento que es del “control” (qué tipo, donde, cuando, extensión), pues sólo en tal caso verdaderamente la expectativa de privacidad se reduce. Además debiera permitir, incluso en casos de prohibición total y exclusivo uso del correo corporativo, un uso esporádico, no reiterado ni abusivo de la herramienta laboral, siempre que no se afecte al buen funcionamiento de dichos dispositivos. Si nos referimos al correo para uso mixto o personal, en tal caso, entiendo que las prevenciones deben ser mayores y el aumento de expectativa de privacidad del trabajador se incrementa en la misma proporción que se reduce la facultad de injerencia del empresario. De momento, la sentencia comentada no aporta claves en exceso y su mayor virtualidad es la de listar las sentencias penales existentes en la materia.

Referencias:

1. [^] Se reproducen los dos primeros párrafos del precepto: Artículo 197: “1. 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, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses. 2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, 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. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero. (...)”.
2. [^] Silva Sanchez, Jesus-María & Vallès, Ramon & Robles, Ricardo & Pastor Muñoz, Nuria & Fernández, Raquel & Coca Vila, Ivó & Cuadras, Albert. (2023). El «caso Pescanova». Comentario a la STS 89/2023, de 10 de febrero. 678-724. InDret 3/2023, Revista Crítica de Jurisprudencia Penal.