CONTROL DEL CORREO ELECTRÓNICO DEL EMPLEADO PARA PREVENIR Y REPRIMIR EL FRAUDE CORPORATIVO

Gabriel ADRIASOLA*

1. EL PROBLEMA GLOBAL

Cada día más se profundiza un debate fruto de las denominadas NTIC (Nuevas Tecnologías de la Información y Comunicación). En ese debate se confronta el derecho a la privacidad del trabajador en el ámbito laboral y el derecho del empleador a controlar el uso de esas tecnologías (Internet, correo electrónico) por parte del empleado.

En esta contribución no pretendo abordar el problema en su globalidad, que abarca cuestiones relacionadas tanto al derecho laboral como al derecho penal, sino que me ceñiré a la posibilidad de control y acceso al correo electrónico corporativo por parte del empleador con la finalidad de probar la comisión de delitos por parte de un empelado infiel. En efecto, se ha dicho que "el uso del correo electrónico e Internet en el ámbito laboral, significa un importante avance para la productividad del trabajo. Pero su utilización indebida puede traer consecuencias dañosas a la empresa. Esta nueva realidad determina que la empresa se vea obligada a generar mecanismos de control eficaces, que detecten el uso improductivo de estas herramientas de trabajo".[1]

Sin embargo, no se trata solo de detectar un "uso improductivo" del correo electrónico corporativo (entendiendo por tal el proporcionado por la empresa). Esta perspectiva resulta válida y parte del supuesto de que el empleador cede a sus empelados las herramientas informáticas para que desarrollen su trabajo[2], pero el mal uso del correo electrónico (p.e. utilización con fines personales[3]) no solo puede generar improductividad, sino que también puede ser utilizado para cometer fraudes contra la propia empresa. En efecto, el correo electrónico se puede utilizar, o mal utilizar, no solo con fines personales, sino también como un instrumento más para cometer fraudes contra la empresa, tipo desviación de clientela o competencia desleal.[4]

Desde esta perspectiva cabe el planteo de dos preguntas: a) ¿puede el empleador acceder al correo electrónico corporativo del empleado?; y b) ¿puede utilizar esa información, obtenida sin autorización judicial ni del empleado,

---

* Profesor titular de Derecho Penal de la Facultad de Derecho del CLAEH (Uruguay). Ex Profesor titular de Derecho Penal General y Especial de la Universidad Católica del Uruguay. Profesor de los Cursos de Certificación para Oficiales de Cumplimiento en prevención de lavado de dinero de la Universidad Católica del Uruguay-ISEDE. Profesor Invitado a los Cursos de Especialización en Derecho Penal Empresario y Tributario de la Universidad Austral de Buenos Aires.

1 RAFFO, Verónica/ LARRAÑAGA ZENI, Nelson. "Control del uso de correo electrónico e Internet en la empresa", en Revista de Derecho y Tribunales, N° 11, Montevideo, octubre de 2009, p. 57.

2 Ibídem, p. 57.

3 Un ejemplo de improductividad puede ser el caso Deutsche Bank, en el que un empleado fue despedido al constatarse que envió 140 correos electrónicos privados desde el ordenador del Banco en un período de 42 días. Una reseña del caso puede verse en: MUÑOZ LORENTE, José. "Los Límites penales en el uso del correo electrónico e Internet en la empresa", en El uso laboral y sindical del correo electrónico e internet en la empresa". ROIG BATALLA, Antonio (Coordinador). Tirant Lo Blanch, Valencia 2007, ps. 159-163.

4 ROIG, ANTONIO. "El uso de Internet en la empresa: aspectos constitucionales", en El uso laboral y sindical del correo electrónico e internet…, cit., p. 74.

como prueba lícita en una causa penal contra ese empleado?

2. PRIVACIDAD DEL TRABAJADOR VS. DEBERES DE CONTROL

No es posible abordar el derecho de acceso del empleador al correo electrónico del empleado desde la única perspectiva de que, al ceder la empresa las herramientas informáticas con el único fin de que el empleado realice su trabajo en beneficio de la empresa, ello implica necesariamente un derecho irrestricto de acceso, que incluso puede estar contenido en un reglamento o protocolo en el que se aclara que no podrán ser utilizados para fines personales, o que incluso el empleado renuncia a su derecho a la privacidad de las comunicaciones realizadas mediante el correo corporativo.[5]

La jurisprudencia comparada ha reconocido que el derecho a la intimidad del trabajador se extiende también al ámbito laboral, y que además, aún en ese ámbito, el trabajador goza de la protección al secreto de las comunicaciones[6]. La doctrina que se ha ocupado de este tema se encuentra dividida. Ya se vio que para algunos el hecho de que la empresa provea los medios (en este caso el correo electrónico), hace que el empleado tenga sobre ellos no derechos personales sino solo los delegados por la empresa[7].

Sin embargo, otros autores estiman que la mera titularidad del medio empleado no justifica el acceso a las comunicaciones realizadas desde el servidor de la empresa,, ya que el contrato de trabajo no transforma al empresario en un "tercero cualificado" para vulnerar el secreto de las comunicaciones[8]. Para esta posición el empresario es un tercero, pese a ser quién provee los medios, porque la comunicación no se entabla con el empleador, sino entre el empleado y el destinatario de la comunicación. En este sentido, alguna jurisprudencia comparada ha establecido que se vulnera el derecho al secreto de las comunicaciones no solo interceptando el mensaje, sino también cuando este es aprehendido desde el disco duro[9].

Sin embargo, entre estas dos posiciones extremas, es necesario ubicar un punto de equilibrio. No es posible sostener que el empleador es un tercero ajeno a la comunicación en todos los casos, porque en definitiva el hecho de proveer el medio con un uso determinado (en beneficio del empelado y de la empresa) debe tener su peso a la hora de proponer una solución a esta aparente colisión de intereses.

Se ha señalado que hay que distinguir entre datos o comunicaciones profesionales de aquellas catalogadas como personales o privadas[10]. Sin embargo, esta distinción muchas

---

5 HAIZENREDER JÚNIOR, Eugenio. "O poder direitivo do empregador frente a intimidade e a vida privada do empregado na relacao de emprego: conflitos decorrentes da utilizacao dos meios informáticos no trabalho", en "Questoes controvertidas de Direito do Trabalho e outros estudos", Brasil, 2006, ps. 74-75. Cit. por RAFFO, Verónica. LARRAÑAGA ZENI, Nelson. Control del uso de correo electrónico e Internet…, cit. p. 57.

6 STC 70/2002.

7 En esta línea también FERNÁNDEZ HUMBLE, Jua. "Aspectos laborales en la utilización de los medios informáticos", en "Revista Trabajo y Seguridad Social". Argentina, septiembre 2001, ps. 730-731.

8 MARÍN ALONSO, Inmaculada. "El poder de control empresarial sobre el uso del correo electrónico en la empresa. Su limitación en base al secreto de las comunicaciones", Tirant Lo Blanch, Valencia, 2004, ps. 159-160.

9 STC 114/1984.

10 ROIG, ANTONIO. "El uso de Internet en la empresa: aspectos constitucionales", en El uso laboral y sindical del correo electrónico e internet…, cit., p. 74.

veces no es posible en la práctica. En efecto, muchas veces se tiene la sospecha de que el empleado está cometiendo o ha cometido un fraude contra la empresa, y la distinción entre correos profesionales y privados solo puede hacerse luego de un acceso global. Incluso, el correo que sirve de evidencia del fraude no puede ser considerado ni como profesional ni como privado.

En esta dirección no es posible negar a la empresa el derecho de "acceso y copiado" del correo electrónico, aunque ese derecho no puede ser indiscriminado. El criterio para definir la legitimidad de ese derecho de acceso reside en la razonabilidad de la decisión.

3. LOS ESTÁNDARES PARA UN ACCESO LEGÍTIMO AL CORREO ELECTRÓNICO DEL EMPLEADO

Parecería que el derecho anglosajón proporciona mayor protección al empleador que accede al correo electrónico del empleado. La respuesta al conflicto en ese sistema se estructura bajo el derecho de daños, y el empleado debe probar que tenía una expectativa de privacidad y acreditar además que existió una intrusión en la privacidad ("intrusión upon seclusion") y/o una causación intencional de angustia emocional ("intentional infliction of emotional distress")[11]. Así, una pretensión de ilegitimidad de la conducta del empleador debe probar que el acceso al e mail del demandante supuso una intrusión altamente ofensiva para una persona razonable, lo que es muy difícil de demostrar cuando el ordenador pertenece a la empresa, o que el empleador desplegó una conducta intencional, extrema e indignante ("extreme and outrageus conduct")[12]. Asimismo, bajo este sistema, "el empresario puede blindarse frente a las posibles acciones por vulneración de la privacidad mediante la comunicación oportuna del programa de monitorización que se vaya a llevar a cabo[13].

El derecho continental parece ser un poco más exigente que el anglosajón. En el ya citado caso Deutsche Bank, ventilado ante los tribunales españoles (ver nota 3), el empleado despedido (que enviaba e mails jocosos o de contenido sexual a compañeros de trabajo y a terceros desde el correo corporativo), denunció penalmente al banco el delito de descubrimiento y revelación de secretos. Si bien las autoridades del banco fueron sobreseídas, se llegó a conocer que "la ausencia de condena penal se debió a un acuerdo económico entre la empresa y el trabajador, en tanto que los delitos contra la intimidad admiten el perdón del ofendido como causa de extinción de la acción penal"[14].

En un sentido opuesto al derecho anglosajón, la Corte de Casación francesa ha establecido que la expresa prohibición del uso del correo electrónico con fines no profesionales no autoriza el acceso al contenido de los mensajes personales[15].

Para la doctrina española el principio general es que el empleador no puede acceder al contenido del correo electrónico del empleado sin que medie orden judicial, pero esta regla admite excepciones[16]. Excluyendo los llamados

---

11 AGUSTINA SANLEHÍ, José Ramón, "Privacidad del trabajador versus Deberes de prevención del delito en la empresa", BdeF, Montevideo-Buenos Aires, 2009, p. 114.

12 Ibídem, p. 114. También KESAN, J. P., "A first principles examinatios of electronic privacy in the workplace", en Blanpain, R (ed.), "On line rights for employees in the Information Society", 2002, p. 259.

13 AGUSTINA SANLEHÍ, José Ramón, Privacidad del trabajador versus Deberes de prevención del delito…, cit., p. 114.

14 Ibídem, ps. 115-116.

15 Cass. Soc, 12 de octubre de 2004, No. 02-40.932.

16 ROIG, ANTONIO. "El uso de Internet en la empresa: aspectos constitucionales", en El uso laboral y sindical del correo electrónico e internet…, cit., p. 78.

datos personales, para los que siempre se requeriría orden judicial, dice ROIG que "desde el punto de vista constitucional, las facultades empresariales cubrirían una fiscalización residual de contenidos, siempre bajo circunstancias muy excepcionales. La finalidad de la medida debe ser lícita, como por ejemplo, tener la sospecha de que se están realizando actividades ilegales o competencia desleal; debería tratarse, además, del único recurso para poder constatar la infracción y la medida debería ser la mínima en cuanto a sus efectos y su duración para obtener el resultado deseado"[17]. Y agrega este autor, como garantía adicional para el empleador: "Sería deseable que el trabajador conociera la posibilidad de este control, aunque la falta de transparencia podría no ser decisiva si la infracción fuera particularmente grave"[18]. Y concluye: "¿Quiere ello decir que el empresario no puede en ningún caso aprehender el contenido de los mensajes electrónicos enviados o recibidos por el trabajador, si no es mediante autorización judicial? Como regla general, es así. Sin embargo, desde un punto de vista constitucional, las facultades contractuales de dirección del empresario facultan a este a un control, excepcional, también sobre los contenidos. Pero hay que insistir en su carácter excepcional, pues de otro modo se vulneraría la proporcionalidad de la medida: debe tener justificación explícita, en un contexto de circunstancias excepcionales y imperativos de seguridad, respetando el contradictorio y ser proporcionada, adecuada, necesaria (no hay alternativa menos gravosa) y ponderada (no causa más perjuicios que beneficios)"[19] .

Creo que esta posición restringe en demasía dos factores. Por un lado, el hecho incuestionable de que el correo electrónico es una herramienta que la empresa pone en manos del trabajador para que la utilice con un fin lícito y en un marco de lealtad con la empresa.

Es necesario que existan reglas claras en esta materia, y que el empresario no se vea enfrentado siempre el riesgo de una denuncia penal y a los vaivenes de la jurisprudencia. Traigo nuevamente a colación el caso Deutsche Bank. Si bien, como se dijo, la fiscalía pidió el sobreseimiento y el mismo culminó con un acuerdo económico en beneficio del demandante, la Magistrado encargada de la Instrucción sentó criterios, a mi juicio alarmantes, y que refuerzan esa necesidad de dotar de seguridad jurídica a la empresa a la hora de ejercitar las que considero ineludibles y necesaria tareas de control y vigilancia. Así, el referido auto destacó los aspectos para sustentar que en principio la conducta del banco, al ordenar el "el acceso, bloqueo y copiado" de los correos electrónicos del empleado, podría encuadrar en el artículo 197 del Código Penal Español (delito de descubrimiento y revelación de secretos). En síntesis, dijo la Magistrado Instructora: a) se agregaron a la causa copia de los correos electrónicos, el texto íntegro de los mismos; b) el artículo 197 CPE requiere el elemento subjetivo consistente en la finalidad de "descubrir los secretos o vulnerar la intimidad del remitente"; c) desde que la orden fue de "acceso, bloqueo y copiado", ello revela la existencia de ese elemento subjetivo, ya que hubiera bastado con bloquear el servicio de correo sin acceder al contenido del mismo y pedir explicaciones al trabajador; d) solo con una orden judicial se puede acceder al contenido de las comunicaciones[20].

Se trata de un caso paradigmático que demuestra que, sin una regulación legal clara, la empresa se ve en muchas ocasiones expuestas a una coacción penal por parte de empleados

---

17 Ibídem, p. 74.
18 Ibídem, p. 74.
19 Ibídem, p. 78.
20 MUÑOZ LORENTE, José. Los Límites penales en el uso del correo electrónico e Internet…, cit., ps. 160-162.

infieles. Y aún en ausencia de legislación –como es el caso uruguayo- es necesario construir estándares de actuación claros y precisos. Esos estándares deben partir de que, a diferencia de lo que se sostuvo en el caso Deutsch Bank, no es posible desconocer las siguientes circunstancias: a) el empleador es quién provee las herramientas informáticas; b) la existencia de reglamentos o protocolos de actuación que permiten al empleado conocer que sus comunicaciones a través de esas herramientas en determinadas circunstancias no son confidenciales y que, por consiguiente, el empleador no es un tercero respecto a las mismas; y c) la finalidad de defensa de la empresa nunca puede ser una finalidad de violación del derecho a la intimidad dentro de un marco reglado.

El hecho de que sea el empleador quién provee las herramientas informáticas (en concreto el servidor y el correo electrónico) es una circunstancia que necesariamente debe tener un peso específico a la hora de fijar una postura en esta materia. Si el empresario es quién proporciona los medios y es el propietario de ellos, no puede ser considerado un "tercero no qualificado" para ejercer un control y un derecho de acceso sobre el uso de esos medios. No es posible parificar la creación de una dirección electrónica a través de un servidor de acceso público a el uso de un correo electrónico corporativo. A vía de ejemplo, en el año 2000 se dictó en el Reino Unido el "Regulatory of Investigation Power Act", que permite a la empresa el acceso rutinario al correo electrónico del empleado. Se fundamenta precisamente en que el empleado nvía mensajes utilizando los medios de propiedad de la empresa, y por esa razón ni siquiera se exige su consentimiento para que se verifique el control. El control puede realizarse tanto por una sospecha de conducta criminal como para garantizar el cumplimiento de las políticas internas de la empresa[21].

La denominada "expectativa de privacidad" debe ser eliminada mediante el conocimiento del empleado de que la empresa puede acceder al contenido de sus mensajes enviados a través de los medios proporcionados por ella. En este sentido, en jurisdicciones no reguladas, es conveniente que exista un consentimiento –que es algo más que conocimiento- del trabajador. Sin embargo, para algunos autores como MARTÍNEZ FONS, "el consentimiento del trabajador constituye requisito necesario pero no suficiente para proceder a la fiscalización del contenido de los correos electrónicos laborales"[22]. Este tipo de afirmaciones se basan en la afirmación de que no se puede renunciar a los derechos fundamentales. No comparto esta tesitura, pero aún admitiéndola, se verá que el conocimiento o consentimiento a la facultad de acceso (transparencia del control) por parte del empleado, junto a la finalidad del acceso, tornan lícita la actuación del empresario. Al respecto señala ROIG que "la vigencia del derecho fundamental no queda excluida con la renuncia"[23], pero atempera su afirmación agregando que "aún con el consentimiento, la fiscalización debe tener una justificación legítima, ser razonable y proporcional"[24]. De este modo, se pone el acento en la finalidad del empleador, de modo de justificar el acceso cuando la finalidad, en términos del derecho anglosajón, no se basa en una arbitraria intención de violar la privacidad o d causar una angustia innecesaria al empleado. Sin embargo, no puede ponerse el

[21] Cfr. RAFFO, Verónica, LARRAÑAGA ZENI, Nelson. Control del uso de correo electrónico e Internet…, cit. p. 64.

[22] MARTÍNEZ FONS, Daniel. "El control de la correspondencia electrónica personal en el lugar de trabajo. (Comentario a la SJS No. 32 de Barcelona, de 16 de septiembre de 2002)", en "Relaciones Laborales, I (2003) 797-813.

[23] ROIG, ANTONIO. "El uso de Internet en la empresa: aspectos constitucionales", en El uso laboral y sindical del correo electrónico e internet…, cit., p. 81.

[24] Ibídem, p. 81.

acento final en ese elemento, que sin duda es necesario, pero que también es subjetivo.

Con respecto a la teoría de la renuncia a derechos fundamentales, no hay que confundir la renuncia a la intimidad o privacidad con la renuncia a parcelas de la intimidad. Existen muchos ejemplos donde cuando las personas se colocan en el marco de una relación laboral o profesional se deben someter a un marco estatutario por el cual renuncian no a su derecho a la intimidad, sino a parcelas de ese derecho. Así, en numerosas legislaciones determinados funcionarios públicos deben renunciar a su intimidad patrimonial declarando sus bienes e ingresos, sea que esa declaración sea reservada y solo pueda accederse a ella en caso de sospecha, o puede tratarse de una declaración pública. En materia tributaria existen previsiones en que el acceso a determinados beneficios fiscales se condiciona, por ejemplo, al levantamiento voluntario del secreto bancario[25]. En materia laboral existen empresas que –consentimiento mediante- realizan a sus empleados controles de orina para detectar si consumen estupefacientes[26].

Desde esta perspectiva, quién acepta colocarse en una relación laboral que implica el uso de un correo electrónico proporcionado por el empleador, no ve vulnerado su derecho fundamental a la intimidad si, conociendo la existencia de facultades de control del contenido, el empleador las ejerce, porque en ese caso lo que existe es una renuncia a una parcela de la intimidad, no al derecho fundamental en toda su dimensión.

Esta argumentación no excluye, como se verá, la exigencia de que el acceso sea razonablemente justificado y proporcional. Pero esa exigencia no significa poner el epicentro del derecho de acceso a la evaluación de la finalidad por un tribunal, sino que se trata de un corolario natural de todo poder o facultad de control: que el mismo no se utilice de manera desviada por parte del empleador. En otras palabras, y traspolando una terminología propia del derecho administrativo, la propiedad de las herramientas informáticas y la transparencia del control (renuncia del empleado a una parcela de su intimidad) le confieren al empleador el derecho de acceso, que bajo esas premisas será siempre legítimo, salvo que se ejecute con desviación de poder, esto es, con una finalidad espuria.

El tercer elemento para tratar de construir un estándar lo más objetivo posible es el ejercicio legítimo de esa facultad de control. La sospecha de delito contra la empresa o contra terceros es un justificativo suficiente. Ahora bien, ello conduce a preguntarse cual es el estándar con que el empleador debe medir esa sospecha.

En primer lugar la facultad de acceso es una forma de buscar evidencia, por lo que no se puede exigir al empleador una convicción de que el empleado está cometiendo un fraude a

---

[25] Así, el artículo 50 de la Ley uruguaya No. 18.083 que creó el IRPF, IRAE e IRNR, denominada de "Reforma Tributaria", dispone: "Levantamiento voluntario del secreto bancario.- La Dirección General Impositiva podrá celebrar acuerdos con los contribuyentes en los que éstos autoricen, para un período determinado, la revelación de operaciones e informaciones amparadas en el secreto profesional a que refiere el artículo 25 del Decreto-Ley Nº 15.322, de 17 de setiembre de 1982. La autorización conferida por los contribuyentes en los términos del inciso anterior tendrá carácter irrevocable y se entenderá dirigida a todas las empresas comprendidas en los artículos 1º y 2º del Decreto - Ley Nº 15.322 de 17 de setiembre de 1982.Para quienes otorguen la autorización referida en el inciso anterior, la Dirección General Impositiva podrá reducir el término de prescripción de sus obligaciones tributarias. En tal caso, los términos de cinco y diez años establecidos por el artículo 38 del Código Tributario, podrán reducirse a dos y cuatro años respectivamente".

[26] Ese tipo de controles ha sido considerado legítimo en tanto exista consentimiento del empleado aún cuando puedan considerarse invasiones a la privacidad. Ver STC 196/2004, de 14 de noviembre.

la empresa basada en pruebas objetivas. Basta con que el empleador tenga una sospecha legítima y esa sospecha puede basarse incluso en informaciones no confirmadas. Un ejemplo posible es la denuncia formulada por medio de una "Hot Line". La "Hot Line "Se encuentra entre las herramientas de mayor difusión en los últimos tiempos entre las empresas preocupadas por reforzar su política de ética y lucha contra el fraude. Se trata de una línea anónima que llega directamente a los directivos, destinada a recoger denuncias de fraude. Para que esto sea efectivo, debe garantizarse que aquellos que tengan conocimiento o sospechas acerca de actos indebidos, puedan comunicarlo a los interesados sin temer represalias. Estos empleados son los que, en investigación del fraude, se denominan whistleblowers (informantes). El aporte crítico de estas personas en el descubrimiento de grandes esquemas de defraudación ha hecho que el uso de líneas directas y gratuitas (0800) para denuncias anónimas de fraude se impusiera, en los Estados Unidos, como un estándar obligatorio"[27].

De este modo, cualquier estándar similar bastará para fundamentar la sospecha y, en consecuencia, proceder al acceso del correo electrónico corporativo por parte de la empresa.
En suma, se construye de este modo un estándar básico de legitimidad de ese acceso basado en tres supuestos: a) la empresa es la propietaria del correo electrónico y por lo tanto esta es una herramienta de trabajo que se le confiere al trabajador para que la use con fines profesionales y legítimos; b) el conocimiento por parte del empleado que la empresa tiene facultad de acceso (transparencia de control), con lo que se elimina cualquier expectativa de privacidad, y el consentimiento (aceptando el reglamento o protocolo) constituye una dispensa estatutaria a una parcela de la intimidad y no al derecho fundamental de manera absoluta; y c) el control de acceso debe estar motivado en la simple sospecha de fraude o uso indebido del correo electrónico, con los estándares analizados para definir el "nivel de sospecha".

Bajo estas premisas el acceso al contenido del correo electrónico no sería ilegítimo, sin embargo, a efectos de contribuir a una mayor seguridad jurídica es necesario excluir la posibilidad de tipicidad de la conducta.

4. LA ATIPICIDAD PENAL DEL ACCESO AL CONTENIDO DEL CORREO ELECTRÓNICO DEL EMPLEADO

Desde la perspectiva de la tipicidad objetiva no es posible sostener que el acceso del empleador al correo electrónico del empleado pueda configurar un delito de intrusión en secretos. La existencia de un consentimiento del empelado con base en la transparencia del control excluye la tipicidad. Así, si "los bienes jurídicos sirven para el libre desarrollo del individuo…no puede existir lesión alguna del bien jurídico cuando una acción se basa en una disposición del portador del bien jurídico que no menoscaba su desarrollo, sino que, por el contrario, constituye su expresión"[28]. Así, con el consentimiento eficaz se desvanece el disvalor de resultado, y con él el disvalor de acción y el tipo penal[29].

El valor del consentimiento como factor que elimina la tipicidad –o la antijuridicidad para otros- está contenido en muchos códigos penales. En el caso de Uruguay esa previsión está

27 CANO, Diego. "Master en Negocios 2009", Tomo No. 9, en http://www.fraudinvestigationsargentina.com/MasterennegociosPrevencionydetecciondefraudes.pdf, (consultado el 3 de mayo de 2013).

28 ROXIN, Claus. "Derecho Penal. Parte General", T. I, Traducción de la 2ª edición alemana por Diego-Manuel Luzón Peña, Miguel Díaz y García Conlledo y Javier de Vicente Remesal, Civitas, Madrid, 1997, p. 517.

29 Ibídem, p. 519.

recogida por el artículo 44 del Código Penal[30]. Desde esta perspectiva, la intimidad no es de aquellos bienes jurídicos de "nula o limitada posibilidad de consentimiento" ya que no es un bien de la comunidad ni involucra la vida humana[31]. Podría sí cuestionarse que el consentimiento, en el caso del empleado, es un consentimiento "no libre", como se postula a menudo desde el derecho del trabajo. Pero como señala ROXIN, "unánimemente se reconoce que no pueden ser aplicables las normas jurídicociviles sobre el significado de los vicios de la voluntad…Pues, jurídicocivilmente, las manifestaciones que adolecen de vicios de voluntad son, por de pronto, válidas y solo posteriormente pueden ser impugnadas a libre elección del manifestante; por el contrario, en el Derecho penal debe constar en el momento de la intervención si el hecho es punible, es decir, si el consentimiento es eficaz o no"[32]. Por lo tanto, el consentimiento será ineficaz solo en casos de engaño, error o coacción en el sentido de violencias o amenazas[33].

Tampoco es posible fundar una tipicidad subjetiva pues no existe en estos casos una acción del empleador dirigida a lesionar gratuitamente un bien jurídico. Ya se indicó que este tipo de conductas están justificadas cuando se obra ante la sospecha de un delito. El razonamiento de la Magistrado instructora en el caso Deutsch Bank en el sentido de que la orden de "acceso, bloqueo y copiado" revela el elemento subjetivo del tipo porque el empleador no se detuvo en el bloqueo, no es un argumento compartible. En verdad, en los delitos de descubrimiento y revelación de secretos debe existir un dolo de violentar la intimidad. En el supuesto que se analiza, la empresa tiene una sospecha de que se está cometiendo o se ha cometido un fraude por parte del empelado, pero no tiene todavía la evidencia suficiente para requerir una orden judicial y por eso procede al "acceso, bloqueo y copiado". La conducta se realiza a sabiendas que el derecho a la intimidad del empleado ha sido restringido por el consentimiento de este, y es sabido que todo derecho fundamental admite restricciones. Lo que sí no es posible es un acceso sin causa alegable o con finalidad meramente aflictiva.

No obstante este desarrollo teórico, creo que este verdadero conflicto de intereses, junto a otros que se plantean a diario en el ejercicio de la fiscalización del fraude corporativo, como las videograbaciones o las investigaciones internas mediante detectives, deberían ser objeto de una regulación legal. Ello dará las seguridades necesarias tanto a empleador como al empleado.

30 Artículo 44: No es punible la lesión causada con el consentimiento del paciente, salvo que ella tuviera por objeto sustraerlo al cumplimiento de una ley, o inferir un daño a otros.

31 ROXIN, Claus. Derecho Penal…, cit, p. 526-529.

32 Ibídem, p. 544.

33 Ibídem, 544-552.