Tratamiento de datos en los canales de denuncias

Personal data processing in whistleblowing

Carlos Franco Blanco

Abogado ICA LEÓN

Resumen

El presente trabajo analiza la gestión de datos personales en los canales de denuncias, enfocándose en la protección de datos y la confidencialidad de los informantes. A su vez, se aborda la integración de canales de denuncias en programas de Compliance, el papel del Delegado de Protección de Datos, y la necesidad de equilibrar los derechos de defensa con la confidencialidad de las personas intervinientes. Por último, se indaga sobre la problemática en el tratamiento de las categorías especiales de datos proporcionando recomendaciones prácticas para la gestión de estas categorías de datos en las investigaciones internas.

Abstract

This work examines the management of personal data in whistleblowing channels, focusing on data protection and the confidentiality of whistleblowers. It addresses the integration of whistleblowing channels into Compliance programs, the role of the Data Protection Officer, and the need to balance the rights of defense with the confidentiality of the involved parties. As a final point, it explores the challenges in handling special categories of data, providing practical recommendations for managing these categories in internal investigations.

Palabras clave

Protección de datos, categorías especiales de datos, *compliance*, canal de denuncias

Key Words

Privacy, special categories of personal data, compliance, whistleblowing

Índice

1.- Conceptualización

En un mundo en constante evolución, donde la información se disemina con una velocidad vertiginosa y la demanda por la transparencia nunca ha sido mayor, las herramientas y sistemas destinados a detectar, reportar y responder a actos inapropiados o ilegales son cruciales.

En este contexto, el canal de denuncias emerge como una herramienta clave para la detección y prevención de conductas inapropiadas, permitiendo que cualquier individuo, de forma anónima o no, pueda reportar situaciones irregulares, garantizando así un mecanismo de control y seguimiento.[1]

ENSEÑAT DE CARLOS define el canal de denuncias como un canal de comunicación directo para que los empleados, clientes o proveedores puedan denunciar el incumplimiento tanto de normas internas como de otras regulaciones que rigen la actividad de la organización constituyéndose en la mejor forma de hacer efectivo su gobierno corporativo.[2]

Por lo tanto, la denuncia de irregularidades se diseña como un mecanismo adicional al resto de medidas del programa de Compliance para que los empleados informen de malas conductas de manera interna a través de un canal específico, basada en el principio de la delación o puesta en conocimiento del empresario de conductas presuntamente irregulares cometidas por personas sujetas al modelo de cumplimiento.

Los programas de denuncia de irregularidades internos generalmente se establecen con vistas a poner en marcha unos principios de gobierno corporativo adecuados en el funcionamiento diario de las organizaciones.

Como ya hemos adelantado, el Canal de Denuncias se establece de manera complementaria a otras vías de comunicación que son habituales en cualquier empresa u organización, como pueden ser las llevadas a cabo a través de los representantes de los empleados, de los mandos o directivos, del personal de control de calidad, o, de los auditores internos, cuya función es precisamente informar acerca de conductas.[3]

---

[1] *Cfr*. PUYOL MONTERO, J. y FRANCO BLANCO, C., *Las Evidencias y Garantías en las Investigaciones en el Canal de Denuncias*, Tirant lo Blanch, Valencia, 2023, p. 22.

[2] *Cfr*. ENSEÑAT DE CARLOS, S., *Manual del Compliance Officer. Guía Práctica para los responsables de Compliance de habla hispana*, Thomson Reuters Aranzadi, Navarra, 2016, p. 49.

[3] *Cfr*. PUYOL MONTERO, J., "Algunas consideraciones sobre los datos personales y el canal de denuncias", *Confilegal*, 26 de agosto de 2021. Disponible en: https://confilegal.com/20210826-opinion-algunas-consideraciones-sobre-los-datos-personales-y-el-canal-de-denuncias/

En el ámbito del Compliance, se concede un especial valor al descubrimiento y la investigación de ilícitos por la propia persona jurídica, puesto que no solo evidencia la eficacia del modelo de Compliance, sino su consonancia con la cultura de cumplimiento corporativo. De ahí la necesidad, tal como señala la Ley 2/2023, del fortalecimiento de la cultura de la información, de las estructuras de integridad de las organizaciones y el fomento de la cultura de la información o comunicación como mecanismo para prevenir y detectar amenazas al interés público.[4]

Finalmente, cabe destacar que VELASCO NÚÑEZ afirma con rotundidad que el canal de denuncias interno, y sus eventuales investigaciones internas corporativas, constituyen *"El más importante requisito legal (art. 31 bis 5.4.º CP) de los que necesariamente ha de contener el Compliance para poder eximir delitos realizados por la empresa*.[5]

Por lo que respecta a la protección de datos, hemos de recordar que se trata de un derecho de construcción jurisprudencial consolidado como derecho fundamental a finales del siglo pasado, gracias a la doctrina del Tribunal Constitucional (STC 292/2000, de 30 de noviembre), implícitamente reconocido en el artículo 18.4 de nuestra Carta Magna y consagrado en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea y en el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea.[6]

Por supuesto todo tratamiento de datos realizado en el canal de denuncias deberá respetar los principios propugnados por el artículo 5 RGPD[7]. Por lo que respecta a las bases legítimas, el artículo 30.2 de la Ley 2/2023 establece que es entenderá lícito debido a que el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento mientras que si no fuere obligatorio, por incorporar en el ámbito objetivo de la política interna del canal tipos adicionales previstos en el artículo 2

---

[4] *Cfr*. PUYOL MONTERO, J. y FRANCO BLANCO, C., *Formularios habituales de Compliance*, Tirant lo Blanch, Valencia, 2023, pp. 23 - 25

[5] VELASCO NÚÑEZ, E., *10 años de responsabilidad penal de la persona jurídica (análisis de su jurisprudencia)*, Thomson Reuters Aranzadi, Cizur Menor, 2020, pp. 140 – 141.

[6] *Cfr.* SIMÓN CASTELLANO, P., *El ejercicio de las funciones del delegado de protección de datos en la supervisión y gestión de procesos críticos*, en SIMÓN CASTELLANO, P. y BACARIA MARTURS, J., (Coords.), *Las funciones del delegado de protección de datos en los distintos sectores de actividad*, Wolters Kluwer, Madrid, 2020, p. 27.

[7] Nos referimos a los principios de licitud, lealtad y transparencia; limitación de la finalidad; minimización de datos; exactitud; limitación del plazo de conservación; integridad y confidencialidad y; responsabilidad proactiva.

de la referida Ley, el tratamiento se presumirá necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

2.- Medidas reforzadas en materia de protección de datos en los tratamientos llevados a cabo en el canal de denuncias

Debido al modelo de cumplimiento del RGPD –responsabilidad proactiva y rendición de cuentas- será necesario documentar los procesos y las decisiones adoptadas para dar cumplimiento a las obligaciones y principios previstos por la normativa. Es decir, cada actuación con relación al cumplimiento del RGPD deberá estar documentada y, cuando proceda, la citada documentación deberá estar convenientemente actualizada.

En este marco, el Delegado de Protección de Datos, que deberá participar de forma adecuada y en tiempo oportuno de todas las cuestiones relativas a la protección de datos personales, de acuerdo con el artículo 38 RGPD, intervendrá también en el proceso de documentación de forma directa, elaborando informes, actas y recomendaciones del seguimiento del cumplimiento de la normativa por parte del responsable, así como asesoramiento, procesos de identificación, tratamiento y evolución del riesgo, políticas de protección de datos, etc. Todos estos documentos le permitirán al responsable del tratamiento y también al encargado del tratamiento demostrar ante los interesados, autoridades de control y terceros su voluntad de cumplimiento y diligencia en el cumplimiento de lo previsto por la normativa.[8]

El Delegado de Protección de Datos es una figura independiente que está en contacto permanente con el responsable del tratamiento, con terceros encargados de tratamientos, con los interesados o afectados por el mismo y con la autoridad pública de control. Se define como la persona, física o jurídica, encargada de garantizar el cumplimiento de la normativa de protección de datos en la organización. Puede ser interno o externo a la misma y debe contar con conocimientos especializados en Derecho en la práctica de la protección de datos.[9]

---

[8] *Cfr*. BACARIA MARTURS, J., *El DPD en el ejercicio de las funciones de información y medición*, en SIMÓN CASTELLANO, P. y BACARIA MARTURS, J., (Coords.), *Las funciones del delegado de protección de datos… Op. Cit.*, Wolters Kluwer, Madrid, 2020, p. 76.

[9] *Cfr*. SIMÓN CASTELLANO, *El desempeño de las funciones de Delegado de Protección de Datos. Gestión de procesos críticos y casos prácticos*. Wolters Kluwer, Madrid, 2018, p. 71.

Cabe destacar que, en aplicación de los principios de responsabilidad proactiva y gestión de riesgos, algunos autores han establecido similitudes entre la figura del Delegado de Protección de Datos y el Compliance Officer, ya que ambos se caracterizan por su función de asegurar el cumplimiento normativo, de supervisar, informar, formar y asesorar a la organización, así como funciones relacionadas con la intervención en las eventuales reclamaciones ante las autoridades competentes.[10]

En este sentido, nos posicionamos a favor de CAMPOS ACUÑA cuando afirma que es posible compatibilizar las funciones de Delegado de Protección de Datos con las de Compliance Officer, garantizando en todo caso que sus funciones y cometidos no den lugar a conflicto de intereses.[11] Para ello, desde nuestro punto de vista, deberá establecerse nítidamente las acciones de abstención y recusación del responsable del sistema interno en la política interna del canal de denuncias de la organización en cuestión.

A su vez, y de forma acertada, el artículo 31.4 de la Ley 2/2023 prevalece la investigación de las infracciones limitando el derecho de oposición por el denunciado toda vez que ocasionaría una impunidad *de facto* sobre la figura del afectado por la comunicación.

Por otro lado, el artículo 32.1 de la antedicha Ley limita el acceso a los datos personales del canal de denuncias a responsable del sistema, responsable de recursos humanos[12], responsable de servicios jurídicos[13], eventuales encargados de tratamiento y Delegado de Protección de Datos.

Por último, y de posterior desarrollo, respecto de las categorías especiales de datos se procederá a la inmediata supresión sin que se proceda al registro y tratamiento de los mismos.

3.- Problemática respecto a la confidencialidad de los intervinientes

[10] *Cfr*. MORO CORDERO, M.A., *Protección de datos personales: una nueva cultura de gestión de la información*, en SUBIRANA DE LA CRUZ, S. y FORTUNY CENDRA, M., *Compliance en el Sector Público*, Thomson Reuters Aranzadi, Cizur Menor, 2020, p. 484.

[11] *Cfr*. CAMPOS ACUÑA, C., "Puede el DPD ser también Compliance Officer (adaptado a la nueva LOPD)?", *Masqleyes*, 2018. Disponible en: https://concepcioncampos.org/puede-el-delegado-de-proteccion-de-datos-ser-tambien-compliance-officer/

[12] Solamente cuando proceda la adopción de medidas disciplinarias contra un trabajador.

[13] Solamente en lo necesario para la adopción de medidas legales en relación con los hechos relatados en la comunicación.

La confidencialidad, en contraposición de la anonimidad donde la identidad de la persona informante no es conocida por nadie, es la garantía de que la información personal será protegida para que no sea divulgada[14] o conocida por ninguna persona que carezca de autorización para ello.

El Considerando 82 de la Directiva *whistleblower* considera una medida ex ante esencial para evitar represalias consiste en salvaguardar la confidencialidad de la identidad del denunciante durante el proceso de denuncia y las investigaciones desencadenadas por la denuncia. Solo ha de poder divulgarse la identidad del denunciante en caso de que exista una obligación necesaria y proporcionada en virtud del Derecho de la Unión o nacional en el contexto de investigaciones llevadas a cabo por autoridades o de procesos judiciales, en particular para salvaguardar el derecho de defensa de las personas afectadas. (…). La protección de la confidencialidad no debe aplicarse cuando el denunciante haya revelado intencionadamente su identidad en el contexto de una revelación pública.

La normativa de transposición al Ordenamiento Jurídico interno de la citada Directiva 2019/1937, consiste en la Ley 2/2023 que en su artículo 31.2 establece la prohibición de comunicar al afectado la identidad del informante. En el mismo sentido, el artículo 33.1 de dicha Ley indica que quien presente una comunicación tiene derecho a que su identidad no sea revelada a terceras personas[15].

Asimismo, puede tener la consideración de infracción grave o muy grave la vulneración de las garantías de confidencialidad y de grave el incumplimiento de la obligación de adoptar las medidas para garantizar la confidencialidad y secreto de las informaciones.

Sin embargo, en la práctica del responsable del sistema interno de información instructor de investigaciones internas, se encontrará, entre otras, con las siguientes coyunturas:

---

[14] *Cfr.* ÁVILA FUNES, J.A., "Confidencialidad de la información", *Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán*, 2013. Disponible en: https://www.incmnsz.mx/opencms/contenido/investigacion/comiteEtica/confidencialidadInformacion.html

[15] Aunque podrá ser comunicada a la Autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora en aplicación del artículo 33.3 de la Ley 2/2023.

a) Confidencialidad vs Derecho de Defensa: La confidencialidad debe abarcar a todos los intervinientes en el expediente de investigación de modo que ninguna persona ajena al mismo tenga conocimiento de los hechos o personas involucradas.

Sin embargo, respecto a las personas que tengan la condición de interesados o legitimados en el procedimiento, existen dos posturas:

- Por un lado, la posición de mantener la confidencialidad de todas las personas, incluidos los testigos, de modo que la única persona que puede conocer la identidad y, por lo tanto, realizar la práctica de la prueba será el responsable del sistema interno de información.

Esta metodología favorece la estricta confidencialidad del informante puesto que en aquellos supuestos donde participen varias personas y algunas de ellas tengan la condición de testigos a excepción de una de ellas, la persona afectada podría eventualmente llegar a conocer la identidad del informante.

- Por otro lado, la posición de mantener únicamente la confidencialidad de la persona informante de modo que su declaración será en la sola presencia del responsable del sistema interno de información mientras que para la práctica del resto de pruebas se debe permitir la participación de la persona afectada por la comunicación.

Desde nuestro punto de vista, debe prevalecer en todo caso el derecho de defensa de la persona afectada por la comunicación en tanto que si no puede participar en la práctica de pruebas, a excepción de su propia declaración y eventual documental, podría suponer una nulidad de la investigación en sede judicial por una manifiesta indefensión.

b) Confidencialidad del informante

Durante la práctica de la prueba, principalmente relativa a las testificales y declaración del afectado, resulta extremadamente complejo mantener la confidencialidad del informante sin vulnerar el derecho de defensa del afectado toda vez que el instructor de la investigación debe realizar preguntas tendentes al averiguamiento de la verdad donde han participado una o varias personas.

Asimismo, en aquellas investigaciones donde coincide en la persona del informante la condición de perjudicado o víctima de los hechos, habrá que preguntar sobre los acontecimientos nombrando a dicha persona. Sin embargo, la Ley 2/2023 requiere mantener la confidencialidad de la persona informante. Por lo tanto, habrá que

separar en todo caso la vinculación de la víctima y el informante, en tanto que es posible que se trate de personas distintas.

4.- Particularidades de los tratamientos de categorías especiales de datos

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD, en adelante), regula en su artículo 9 las categorías especiales de datos personales.

Este tipo de datos personales son aquéllos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.

En este sentido, el apartado 1 del ya citado artículo 9 RGPD prohíbe su tratamiento. Sin embargo, el apartado 2 de dicho artículo prevé una serie de excepciones a dicha prohibición de tratamiento de categorías especiales de datos. En este contexto, se permite el procesamiento si el interesado ha dado su consentimiento explícito. Además, se autoriza el tratamiento para cumplir obligaciones y derechos laborales, proteger intereses vitales cuando el interesado no puede consentir, y cuando organizaciones sin ánimo de lucro lo realizan con garantías específicas. También se contempla el tratamiento de datos manifiestamente públicos, en la formulación y defensa legal de reclamaciones, por razones de interés público esencial, para fines médicos y de salud pública, así como para archivos de interés público, investigación científica o histórica, y fines estadísticos, siempre bajo medidas proporcionadas y específicas para resguardar los derechos fundamentales del interesado.

Respecto a esta cuestión, en el Ordenamiento Jurídico interno, es importante destacar que el artículo 9 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales establece que, a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o

étnico. Esto no impedirá el tratamiento de dichos datos al amparo de los restantes supuestos contemplados en el artículo 9.2 del RGPD.[16]

En aplicación de la normativa específica del canal de denuncias, la ya citada Ley 2/2023, en el tercer párrafo del artículo 36.2 prevé que "*si la información recibida contuviera datos personales incluidos dentro de las categorías especiales de datos, se procederá a su inmediata supresión, sin que se proceda al registro y tratamiento de los mismos*".

En este sentido, en atención al principio general del Derecho de especialidad normativa (*Lex specialis derogat generali*)[17] entendemos debe resultar de aplicación la Ley especial sobre los canales de denuncias, es decir la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

Sin embargo, en la práctica observamos con cierta asiduidad cómo tanto en las denuncias como en las declaraciones de los intervinientes son utilizados estas categorías especiales de datos personales por ejemplo para comunicar comentarios de naturaleza racista o los motivos de una incapacidad temporal[18] provocada por los hechos denunciados.

---

[16] *Cfr.* YEBRA SERRRANO, I., "Categorías especiales de datos personales para proteger la información más sensible", *INEAF*, 28 de octubre de 2021. Disponible en: https://www.ineaf.es/tribuna/categorias-especiales-de-datos-personales/

[17] Adoptamos la definición de TARDÍO PATO del principio de especialidad normativa como *la preferencia aplicativa de la norma reguladora de una especie de cierto género sobre la norma reguladora de tal género en su totalidad.* TARDÍO PATO, J.A., "El principio de Especialidad Normativa (Lex Specialis) y sus Aplicaciones Jurisprudenciales", *Revista de Administración Pública*, núm. 162, 2003, p. 191.

[18] Mención específica merecen los datos relativos a la salud. El RGPD, en su artículo 4.15, define datos relativos a la salud como «datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud». La única aportación que hace el RGPD en la definición de dato de salud es la consideración como dato de salud de la información referida a la «prestación de servicios de atención sanitaria», como puede ser, por ejemplo, el pago de la prestación sanitaria -aunque ésta no contenga referencia a ninguna enfermedad- o la gestión administrativa de la asistencia prestada, siempre que revelen información sobre su estado de salud. El Considerando 35 del RGPD precisa más esta cuestión considerando dato relativo a la salud «todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro». *Cfr.* TRONCOSO REIGADA, A., "Las categorías especiales de datos personales en el Reglamento General de Protección de Datos de la Unión Europea", *ElDerecho.com*, 10 de julio de 2019. Disponible en: https://elderecho.com/las-categorias-especiales-de-datos-personales-en-el-reglamento-general-de-proteccion-de-datos-de-union-europea

Por lo tanto, eventualmente encontraremos situaciones donde, por el propio fondo de los hechos denunciados, será requerido el tratamiento de categorías especiales de datos en aplicación de las excepciones previstas en el artículo 9.2.b) RGPD.

5.- Recomendaciones prácticas

Con el objeto de realizar tratamientos de datos en los expedientes del canal de denuncias que merezcan una especial atención, particularmente útil resulta realizar una justificación y motivación completa de los siguientes principios establecidos por la STEDH de 5 de septiembre de 2017 Caso Barbulescu contra Rumanía:

- Principio de necesidad: la supervisión debe ser necesaria para alcanzar un objetivo determinado.

- Principio de finalidad: los datos deben recopilarse con fines específicos, explícitos y legítimos.

- Principio de transparencia: el empresario debe proporcionar a los empleados información completa sobre las operaciones de supervisión.

- Principio de legitimidad: las operaciones de tratamiento de datos sólo pueden tener lugar con un fin legítimo.

- Principio de proporcionalidad: Este principio destaca la importancia de equilibrar los derechos y libertades de los individuos con los intereses legítimos de los empleadores.

- Principio de seguridad: el empresario está obligado a adoptar todas las medidas de seguridad posibles para garantizar que los datos recogidos no sean accesibles a terceros.[19]

En el ámbito interno resulta imprescindible recordar la STC 96/2012 que, en su Fundamento Jurídico Décimo recoge que "*para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si,*

[19] *Cfr*. PUYOL MONTERO, J., "El test Barbulescu como elemento de «Compliance», *Confilegal*, 5 de octubre de 2023. Disponible en: https://confilegal.com/20231005-el-test-barbulescu-como-elemento-de-compliance/#_ednref1

además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto).”

En conexidad con lo anterior, en el procedimiento interno de investigación deber realizarse una aplicación por analogía de lo previsto en el artículo 11.1 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (LOPJ) que establece que “*En todo tipo de procedimiento se respetarán las reglas de la buena fe. No surtirán efecto las pruebas obtenidas directa o indirectamente, violentando los derechos o libertades fundamentales.”* [20]

Todo ello con el último propósito de evitar la aplicación de la conocida teoría de los frutos del árbol envenenado en virtud de la cual, *cualquier prueba que directa o indirectamente y por cualquier nexo se le pudiera relacionar con la prueba nula, debía ser igualmente estimada nula*.[21]

La doctrina del «fruto del árbol envenenado” se consagró en España en el año 1984, tras la STC 114/1984, de 29 de noviembre[22], al afirmar:

Aun careciendo de regla legal expresa que establezca la interdicción procesal de la prueba ilícitamente adquirida, hay que reconocer que deriva de la posición preferente de los derechos fundamentales en el ordenamiento y de su afirmada condición de «inviolables» (art. 10.1 de la Constitución) la imposibilidad de admitir en el proceso una prueba obtenida violentando un derecho fundamental o una libertad fundamental. Para nosotros, en este caso, no se trata de decidir en general la problemática procesal de la prueba con causa ilícita, sino, más limitadamente, de constatar la «resistencia» frente a la misma de los derechos fundamentales, que presentan la doble dimensión de derechos subjetivos de los ciudadanos y de «elementos esenciales de un ordenamiento objetivo de la comunidad nacional, en cuanto ésta se configura como marco de una convivencia

[20] *Cfr*. FRANCO BLANCO, C., “Problemática en el tratamiento de categorías especiales de datos en el procedimiento del canal interno de información”, *Confilegal*, 9 de julio de 2023. Disponible en: https://confilegal.com/20230709-problematica-en-el-tratamiento-de-categorias-especiales-de-datos-en-el-procedimiento-del-canal-interno-de-informacion/

[21] *Cfr*. URIARTE VALIENTE, L.M. y FARTO PIAY, T., *El proceso penal español: jurisprudencia sistematizada*, La Ley, Madrid, 2007, pp. 714 – 715.

[22] ECLI:ES:TC:1984:114.

humana, justa y pacífica...» (…). Esta garantía deriva, pues, de la nulidad radical de todo acto -público o, en su caso, privado- violatorio de las situaciones jurídicas reconocidas en la sección primera del capítulo segundo del Título I de la Constitución y de la necesidad institucional por no confirmar, reconociéndolas efectivas, las contravenciones de los mismos derechos fundamentales (el deterrent effect propugnado por la jurisprudencia de la Corte Suprema de los Estados Unidos).[23]

6.- Conclusiones

Los canales de denuncias son un elemento imprescindible de todo modelo de Compliance así como para lograr la exención de la responsabilidad penal de la persona jurídica.

Es posible compatibilizar la figura del Delegado de Protección de Datos con el Responsable del Sistema Interno de Información, o Compliance Officer, salvaguardando en todo caso las acciones de abstención y recusación en aquellas investigaciones internas donde pueda existir un conflicto de intereses.

Debe prevalecer el derecho de defensa de la persona afectada por la comunicación sobre la confidencialidad de los intervinientes en la investigación interna, a excepción del informante.

El test Barbulescu resulta una herramienta idónea para justificar el tratamiento de categorías especiales de datos en los canales de denuncias.

7.- Bibliografía

ÁVILA FUNES, J.A., "Confidencialidad de la información", *Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán*, 2013. Disponible en: https://www.incmnsz.mx/opencms/contenido/investigacion/comiteEtica/confidencialidadInformacion.html

BACARIA MARTURS, J., *El DPD en el ejercicio de las funciones de información y medición*, en SIMÓN CASTELLANO, P. y BACARIA MARTURS, J.,

[23] STC 114/1984, de 29 de noviembre. ECLI:ES:TC:1984:114

(Coords.), *Las funciones del delegado de protección de datos en los distintos sectores de actividad*, Wolters Kluwer, Madrid, 2020.

CAMPOS ACUÑA, C., "¿Puede el DPD ser también Compliance Officer (adaptado a la nueva LOPD)?", *Masqleyes*, 2018. Disponible en: https://concepcioncampos.org/puede-el-delegado-de-proteccion-de-datos-ser-tambien-compliance-officer/

ENSEÑAT DE CARLOS, S., *Manual del Compliance Officer. Guía Práctica para los responsables de Compliance de habla hispana*, Thomson Reuters Aranzadi, Navarra, 2016.

FRANCO BLANCO, C., "Problemática en el tratamiento de categorías especiales de datos en el procedimiento del canal interno de información", *Confilegal*, 9 de julio de 2023. Disponible en: https://confilegal.com/20230709-problematica-en-el-tratamiento-de-categorias-especiales-de-datos-en-el-procedimiento-del-canal-interno-de-informacion/

MORO CORDERO, M.A., *Protección de datos personales: una nueva cultura de gestión de la información*, en SUBIRANA DE LA CRUZ, S. y FORTUNY CENDRA, M., *Compliance en el Sector Público*, Thomson Reuters Aranzadi, Cizur Menor, 2020.

PUYOL MONTERO, J., "Algunas consideraciones sobre los datos personales y el canal de denuncias", *Confilegal*, 26 de agosto de 2021. Disponible en: https://confilegal.com/20210826-opinion-algunas-consideraciones-sobre-los-datos-personales-y-el-canal-de-denuncias/

PUYOL MONTERO, J., "El test Barbulescu como elemento de «Compliance», *Confilegal*, 5 de octubre de 2023. Disponible en: https://confilegal.com/20231005-el-test-barbulescu-como-elemento-de-compliance/#_ednref1

PUYOL MONTERO, J. y FRANCO BLANCO, C., *Formularios habituales de Compliance*, Tirant lo Blanch, Valencia, 2023.

PUYOL MONTERO, J. y FRANCO BLANCO, C., *Las Evidencias y Garantías en las Investigaciones en el Canal de Denuncias*, Tirant lo Blanch, Valencia, 2023.

SIMÓN CASTELLANO, *El desempeño de las funciones de Delegado de Protección de Datos. Gestión de procesos críticos y casos prácticos*. Wolters Kluwer, Madrid, 2018.

SIMÓN CASTELLANO, P., *El ejercicio de las funciones del delegado de protección de datos en la supervisión y gestión de procesos críticos*, en SIMÓN CASTELLANO, P. y BACARIA MARTURS, J., (Coords.), *Las funciones del delegado de protección de datos en los distintos sectores de actividad*, Wolters Kluwer, Madrid, 2020.

TARDÍO PATO, J.A., "El principio de Especialidad Normativa (Lex Specialis) y sus Aplicaciones Jurisprudenciales", *Revista de Administración Pública*, núm. 162, 2003.

TRONCOSO REIGADA, A., "Las categorías especiales de datos personales en el Reglamento General de Protección de Datos de la Unión Europea", *ElDerecho.com*, 10 de julio de 2019. Disponible en: https://elderecho.com/las-categorias-especiales-de-datos-personales-en-el-reglamento-general-de-proteccion-de-datos-de-union-europea

URIARTE VALIENTE, L.M. y FARTO PIAY, T., *El proceso penal español: jurisprudencia sistematizada*, La Ley, Madrid, 2007.

VELASCO NÚÑEZ, E., *10 años de responsabilidad penal de la persona jurídica (análisis de su jurisprudencia)*, Thomson Reuters Aranzadi, Cizur Menor, 2020.

YEBRA SERRRANO, I., "Categorías especiales de datos personales para proteger la información más sensible", *INEAF*, 28 de octubre de 2021. Disponible en: https://www.ineaf.es/tribuna/categorias-especiales-de-datos-personales/