Creación de un canal de denuncias y cumplimiento de la normativa vigente en materia de protección de datos

Autora: **Sandra Pérez Bastardo**, Abogada TIC y Protección de Datos. Consultora de Prodat Castilla y León

El canal de denuncias o **"whistleblowing channel"** tiene su origen en la administración pública norteamericana. Asimismo, si atendemos a su origen etimológico se remonta a la práctica de los oficiales de policía británicos que hacían sonar sus **silbatos (whistle) soplando (blow)**, cuando presenciaban la comisión de un delito.

Con esta breve referencia histórica **podemos pasar a la definición actual del canal de denuncias:** canal que pretende facilitar la comunicación entre la **dirección de la empresa y personas vinculadas a ella que**, por una causa u otra, sienten inquietud o dudas sobre alguna actuación en el seno de la empresa que pueda ser susceptible de implicar un delito o de conductas que simplemente incumplen los principios de la compañía o alguna normativa interna (por ejemplo, el código ético).

Por lo tanto, nos encontramos ante una herramienta que permite a los empleados y a otras personas **alertar confidencialmente a una organización sobre sospechas de mala conducta.** Siendo un mecanismo necesario y cada vez más importante para reducir los riesgos y crear confianza, ya que permite a los directores detectar la mala conducta en una etapa temprana.

En cuanto a la normativa de la que deriva el canal de denuncias nos encontramos con la Directiva 2019/1937 que obliga a una serie de entidades a contar con dicha herramienta, debiendo de cumplir estas con un plazo de implementación que finaliza en diciembre del 2021, ***¿Qué entidades se ven afectadas?***

- Empresas del sector privado con más de 50 trabajadores.
- Todas las entidades pertenecientes al sector público.
- Entidades que no cumplan los requisitos anteriores, pero les sean de aplicación leyes específicas como por ejemplo la Ley de Prevención de Blanqueo de Capitales (LPBC).

Asimismo, en aras de cumplir con la normativa de aplicación indicada y facilitar la utilidad del propio canal de denuncias, el canal deberá de contar con una serie de características:

- **Seguridad**: La entidad ha de asegurarse de que este cumpla con las certificaciones en la materia y comprobar las posibles vulnerabilidades de forma regular.
- **Facilidad**: Ha de ser un mecanismo fácil y rápido de usar, de tal manera se incentivará mucho más su utilización por parte de los interesados.
- **Confianza**: Al igual que el punto anterior, el hecho de que se salvaguarde la identidad del "whistleblower" o denunciante ante posibles represalias conseguirá que el canal se utilice por mayor parte de interesados.
- **Legal**: Ha de adecuarse a las exigencias normativas tanto de la Directiva 2019/1937 como de la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

De todas las características indicadas, a continuación, nos centraremos en el análisis de la relación que tiene la implementación del canal de denuncias en materia de protección de datos:

Artículo 24 LOPDGDD. Sistemas de información de denuncias internas.

"1. Será lícita la creación y mantenimiento de sistemas de información a través de los cuales pueda ponerse en conocimiento de una entidad de Derecho privado, incluso anónimamente, la comisión en el seno de la misma o en la actuación de terceros que contratasen con ella, de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial que le fuera aplicable. Los empleados y terceros deberán ser informados acerca de la existencia de estos sistemas de información.

2. El acceso a los datos contenidos en estos sistemas quedará limitado exclusivamente a quienes, incardinados o no en el seno de la entidad, desarrollen las funciones de control interno y de cumplimiento, o a los encargados del tratamiento que eventualmente se designen a tal efecto. No obstante, será lícito su acceso por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan. Sin perjuicio de la notificación a la autoridad competente de hechos constitutivos de ilícito penal o administrativo, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador, dicho acceso se permitirá al personal con funciones de gestión y control de recursos humanos.

3. Deberán adoptarse las medidas necesarias para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas por la información suministrada, especialmente la de la persona que hubiera puesto los hechos en conocimiento de la entidad, en caso de que se hubiera identificado.

4. Los datos de quien formule la comunicación y de los empleados y terceros deberán conservarse en el sistema de denuncias únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados. En todo caso, transcurridos tres meses desde la introducción de los datos, deberá procederse a su supresión del sistema de denuncias, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica. Las denuncias a las que no se haya dado curso solamente podrán constar de forma anonimizada, sin que sea de aplicación la obligación de bloqueo prevista en el artículo 32 de esta ley orgánica. Transcurrido el plazo mencionado en el párrafo anterior, los datos podrán seguir siendo tratados, por el órgano al que corresponda, conforme al apartado 2 de este artículo, la investigación de los hechos denunciados, no conservándose en el propio sistema de información de denuncias internas.

5. Los principios de los apartados anteriores serán aplicables a los sistemas de denuncias internas que pudieran crearse en las Administraciones Públicas."

En efecto, el hecho de gestionar e investigar las denuncias que se reciben a través del canal de denuncias implica **el tratamiento de datos de carácter personal**, pudiendo ser estos solamente identificativos o llegando incluso a ser datos sensibles como los casos de sospecha sobre la comisión de un delito. Por lo tanto, al igual que ocurre en cualquier otro tratamiento de datos que lleve a cabo la entidad se deben respetar los principios de la normativa en materia de protección de datos, eso sí teniendo en cuenta en este caso una serie de particularidades;

Ø Dictamen 1/2006 del Grupo de Trabajo del Artículo 29, **el órgano sostiene que la aplicación de la normativa en materia de protección de datos en este ámbito es de utilidad para la protección del denunciado, a mayor abundamiento el WG29 se postula hacia canales de denuncia abiertos, es decir, de manera identificada**, fundamentándolo hasta en seis razones diferentes, pero a pesar de su preferencia, **no rechaza** de forma categórica la posibilidad de que **se puedan dar denuncias de forma anónima.**

Ø Informe 128/2007 de la Agencia Española de Protección de Datos (AEPD), en el cual se fijaron los requisitos para la implantación de un canal de denuncias, los cuales a pesar de determinarse en base a la antigua LOPD 15/1999 pueden extrapolarse a la normativa en vigor actualmente, LOPDGDD y RGPD, siendo los siguientes:

- En el indicado informe se aconsejaba evitar la existencia de denuncias anónimas, garantizándose así la exactitud e integridad de la información contenida en dichos sistemas. Pero como hemos visto en párrafos anteriores actualmente este informe ha quedado superado por el Art. 24.1 LOPDGDD, que si permite la denuncia anónima.
- Todo tratamiento de datos que se realice a través del canal de denuncias ha de contar con una base legitimadora, siendo en este caso una relación contractual (Art. 6.1.b RGPD). Este extremo deja abierto el hecho de que la relación contractual sea laboral, civil o mercantil, por lo cual el uso del canal de denuncias no se limita solamente a los empleados de la entidad, sino que también puede ser utilizado por clientes o proveedores, etc.
- La entidad debe de establecer un plazo máximo para la conservación de los datos de carácter personal relacionados con las denuncias, siendo esto un reflejo del principio de limitación del plazo de conservación (Art. 5.1.e. RGPD), el cual tiene por objetivo principal cesar en el tratamiento de los datos de carácter personal cuando dejen de ser necesarios para la finalidad perseguida. En el caso concreto de los canales de denuncia la AEPD indica que esta conservación debería limitarse a la tramitación de las investigaciones internas y, como máximo, a la tramitación de los procedimientos judiciales que, en su caso, puedan derivarse de la denuncia.
- Todas las personas de las que se traten datos de carácter personal a través del canal de denuncias han de ser debidamente informadas de los extremos necesarios en materia de protección de datos (Arts. 13 y 14 RGPD) (Art. 11 LOPDGDD), de esta manera la entidad estará cumpliendo con su deber de información.
- Las medidas de seguridad implementadas para el tratamiento de los datos de carácter personal recabados a través del canal de denuncias han de ser reforzadas, tal y como indica la AEPD, dado que no es posible conocer a priori que tipos de datos se van a registrar, siendo muy posible el tratamiento de datos especialmente protegidos como puede ser lo relacionado con afiliación sindical o salud de una persona.

Para finalizar, no podemos dejar de hacer referencia a la Circular de la Fiscalía 1/2016, en la cual se indica la prohibición expresa de cualquier tipo de represalia contra los "whistleblowers" por parte de la entidad, lo cual crea una mayor seguridad jurídica en este ámbito. Asimismo, se debe garantizar que los denunciantes tengan acceso a información y asesoramiento completo, independiente y gratuita sobre los procedimientos y recursos disponibles, así como a asistencia jurídica durante los procedimientos.

Como conclusión, tal y como se ha ido evidenciando a lo largo del presente artículo el hecho de que el canal de denuncias sea una parte del cumplimiento del sistema de Compliance (Art.31 Bis C.Penal) no exime de que este tenga que cumplir con la normativa en materia de protección de datos, al igual que ocurre con todo tratamiento de datos de carácter personal realizado en nuestro país y dentro de la UE.

Fuente: Legal Today