Protección al denunciante de infracciones del derecho comunitario

El pasado 17 de diciembre de 2019 entró en vigor la Directiva del Parlamento Europeo y del Consejo, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión, Directiva (UE) 2019/1937, de 23 de octubre de 2019.

Las denuncias y revelaciones públicas sobre infracciones del derecho comunitario permiten detectar, investigar y enjuiciar de manera efectiva las mismas, mejorando así la transparencia y la rendición de cuentas. Es por ello que se ha considerado especialmente importante prestar una adecuada y efectiva protección a los denunciantes (en inglés conocidos como *"whistleblowers"*) ya que muchos renuncian a informar por temor a represalias.

Dado que, hasta la fecha, en la Unión Europea (UE) la protección de los denunciantes se encontraba fragmentada en los diferentes Estado miembros y era desigual en los distintos ámbitos, se decidió que debían existir y aplicarse unas mínimas normas comunes que se han plasmado en la presente Directiva.

Infracciones

Se prevé la protección de los denunciantes que informen sobre las infracciones relativas a los siguientes ámbitos: contratación pública, servicios financieros, prevención del blanqueo de capitales y financiación del terrorismo, seguridad del transporte, protección ambiental, seguridad nuclear, seguridad alimentaria, sanidad animal, salud pública, protección de los consumidores, protección y la seguridad de los datos y sistemas de información, y las regulaciones tributarias e intereses financieros de la UE.

Denunciantes

La presente Directiva se aplicará a los denunciantes que trabajen en el sector privado o público y que hayan conocido la infracción en un contexto laboral, incluyendo si ha sido obtenida en el marco de una relación laboral ya finalizada o durante un proceso de selección o de negociación precontractual.

Canal de denuncias

Toda empresa del sector público, y las empresas del sector privado con más de 50 empleados, están obligadas a implementar un procedimiento interno para poder recibir y gestionar las denuncias. Si bien la Directiva prevé la posibilidad de que, en su transposición, cada Estado miembro decida si exime de tal obligación a los municipios de menos de 10.000 habitantes o con menos de 50 trabajadores, u otras entidades públicas con menos de 50 trabajadores

La Directiva recoge la obligación de establecer canales de denuncias, tanto internos como externos a las organizaciones que garanticen la confidencialidad de los denunciantes, debiendo aprobar procedimientos internos donde se regule el proceso de recepción y tramitación de las denuncias:

La obligación de enviar un acuse de recibo de la denuncia al denunciante en el plazo máximo de 7 días
Designación de la persona o el órgano que se encargará de tramitar las denuncias
El plazo para dar una respuesta al denunciante, que no podrá ser superior a 3 meses desde el acuse

de recibo
Información clara y fácilmente accesible sobre los procedimientos de denuncias en los canales externos existentes

Apoyo y protección

En todo caso, los Estados miembros adoptarán las medidas de apoyo necesarias para prohibir cualquier forma de represalia contra los denunciantes, tales como:

Facilitarles información y asesoramiento independientes, accesibles y gratuitos sobre los procedimientos y recursos disponibles
Asistencia efectiva por parte de las autoridades competentes ante cualquier autoridad implicada en su protección frente a represalias
Asistencia jurídica en los procesos penales y en los procesos civiles transfronterizos, así como asistencia jurídica en otros procesos y asesoramiento jurídico o cualquier otro tipo de asistencia jurídica
Asistencia financiera y medidas de apoyo a los denunciantes, incluido apoyo psicológico, en el marco de un proceso judicial

Y en cuanto a las medidas para su protección, los Estados miembros velarán por que las mismas gocen de su derecho a la tutela judicial efectiva y a un juez imparcial, así como a la presunción de inocencia y al derecho de defensa, incluido el derecho a ser oídos y el derecho a acceder a su expediente.

Transposición

Los Estados miembros tendrán hasta el 17 de diciembre de 2021 para transponer la Directiva. No obstante, las entidades jurídicas del sector privado que tengan de 50 a 249 trabajadores, no estarán obligadas a establecer canales de denuncia interna hasta el 17 de diciembre de 2023.

Actualización de las medidas europeas sobre ciberseguridad

El 27 de junio entró en vigor el Reglamento de la Unión Europea del Parlamento Europeo relativo a la Agencia de la Unión Europea para la Ciberseguridad y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación.

La norma, que deroga el anterior Reglamento sobre la Ciberseguridad del 2013, tiene como aspiración alcanzar un nivel elevado de ciberseguridad, ciberresiliencia y confianza dentro de la Unión Europea.

A continuación destacamos los dos bloques fundamentales del documento:

Agencia Europea para la Ciberseguridad

En primer lugar, el Reglamento establece los objetivos y aspectos organizativos de la nueva Agencia Europea para la Ciberseguridad (ENISA), y le asigna las siguientes tareas:

Contribuir a la elaboración y ejecución de la política y del derecho de la Unión en el ámbito de la ciberseguridad
Asistir a los Estados en la creación de capacidades de ciberseguridad
Apoyar la cooperación entre los países miembros, las instituciones, órganos y organismos de la Unión y entre las partes interesadas
Promover el desarrollo y la aplicación de la política de la UE en materia de certificación de la ciberseguridad de productos, servicios y procesos TIC
Analizar las tecnologías emergentes y preparar evaluaciones sobre los efectos esperados, de tipo social, jurídico, económico y reglamentario, de las innovaciones tecnológicas
Sensibilizar al público sobre los riesgos relacionados con la ciberseguridad y facilitar orientaciones sobre buenas prácticas
Asesorar a las instituciones, órganos y organismos de la Unión y a los Estados miembros sobre las necesidades y prioridades de la investigación en el ámbito de la ciberseguridad y las tecnologías de la información, y a utilizar eficazmente las tecnologías de prevención del riesgo
Promover la cooperación internacional en relación con los problemas que se refieren a la ciberseguridad

Certificación de la ciberseguridad

Por otra parte, aborda la definición de un marco para la creación de esquemas europeos de certificación de la ciberseguridad, a efectos de garantizar un nivel adecuado de ciberseguridad de los productos, servicios y procesos de las tecnologías de la información y la comunicación (TIC) y de crear un mercado único digital para estos productos, servicios y procesos.

Este marco define un mecanismo destinado a instaurar esquemas europeos de certificación de la ciberseguridad y a confirmar que los productos, servicios y procesos de TIC que hayan sido evaluados con arreglo a dichos esquemas, cumplen los requisitos de seguridad especificados. De esta manera se trata de proteger la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o procesados o las funciones o servicios que ofrecen.

La Comisión Europea publicará un programa de trabajo evolutivo para los esquemas europeos de certificación que definirá las prioridades estratégicas para los futuros esquemas e incluirá una lista de productos, servicios y procesos de TIC, o de categorías de los mismos, que pudieran beneficiarse de su inclusión en el ámbito de aplicación de un esquema europeo de certificación de la ciberseguridad.

Procesos digitales en el ámbito del Derecho de sociedades

Una vez más, la UE ha revisado sus normas en materia de Derecho de sociedades para adaptarlas a la revolución digital. En este sentido, el día 31 de julio entró en vigor la Directiva (UE) 2019/1151 del Parlamento Europeo y del Consejo que modifica la regulación actual[1] relativa a los procesos digitales en el ámbito del Derecho de sociedades.

Según cifras proporcionadas por la Comisión, existen unos 24 millones de sociedades en la UE y de éstas, el 80 % son sociedades de responsabilidad limitada. Unos datos que justifican el objetivo de estas medidas: lograr una mayor eficiencia, transparencia y seguridad jurídica mediante el uso de herramientas digitales a lo largo del ciclo de vida de las sociedades.

Los principales beneficiados de estas medidas serán las micro, pequeñas y medianas empresas,

quienes podrán constituir sociedades y registrar sucursales de manera íntegramente electrónica. De esta manera, se reducirán los costes, el tiempo y las cargas administrativas asociados a estos procesos.

En concreto, las principales novedades contenidas en la Directiva permiten y garantizan:

La presentación electrónica de todos los documentos e información societarios, como la escritura de constitución y sus estatutos, el nombramiento y cese de funciones de los miembros que representan a la sociedad o los documentos contables, entre otros
La constitución de sociedades de capital electrónicamente o en línea. En concreto, se garantiza la constitución de sociedades de responsabilidad limitada mediante modelos disponibles electrónicamente. No obstante lo anterior, los Estados miembros podrán restringir esta constitución en línea a determinados tipos de sociedades de capital
La opción de efectuar los pagos electrónicamente para realizar los procedimientos regulados en la norma; esto es: registro de sucursales y constitución de sociedades
El registro electrónico de una sucursal en un plazo máximo de 10 días sin necesidad de que los solicitantes comparezcan en persona ante cualquier autoridad
Una información concisa, de fácil consulta, gratuita y, al menos, en una lengua ampliamente comprendida por el mayor número posible de usuarios transfronterizos, en los portales o sitios web de registro accesibles.

La Directiva deberá ser transpuesta por los Estados Miembros antes del 1 de agosto de 2021, sin perjuicio de que algunas disposiciones deban ser aplicadas antes del 1 de agosto de 2023 y de la previsión de una prórroga máxima de un año en supuestos de especiales dificultades para su transposición.

[1] Directiva (UE) 2017/1132

5ª Directiva sobre prevención del blanqueo de capitales y financiación del terrorismo

El Parlamento Europeo y el Consejo de la Unión Europea aprobaron el pasado mes de mayo la 5ª Directiva en materia de prevención del blanqueo de capitales y la financiación del terrorismo, que modifica la anterior Directiva UE 2015/849, publicada en septiembre de 2015 y que analizamos en uno de los primeros números de Progreso.

A pesar de considerar la 4ª Directiva como el "*principal instrumento jurídico de prevención de la utilización del sistema financiero de la Unión para el blanqueo de capitales y la financiación del terrorismo*", los organismos europeos han visto preciso completar sus disposiciones para perfeccionar el marco preventivo vigente y promover la lucha eficaz contra la financiación del terrorismo.

La 5ª Directiva refleja la necesidad de incrementar la transparencia a nivel global del entorno económico y financiero de la Unión Europea y de asegurar su integridad, a fin de prevenir, detectar e investigar el blanqueo de capitales, en el convencimiento de que una mayor transparencia es un potente factor disuasorio.

A continuación presentamos las principales modificaciones:

Ámbito de aplicación

Amplía el ámbito de aplicación a los siguientes sujetos:

Además de los auditores, contables externos y asesores fiscales, a toda aquella persona que preste asistencia o asesoramiento en cuestiones fiscales como actividad empresarial o profesional principal, ya sea directamente o a través de terceros con los que esté relacionada
A los agentes inmobiliarios que actúen como intermediarios en el arrendamiento de bienes inmuebles, en relación a transacciones para las que el alquiler mensual sea igual o superior a 10.000 euros
A las personas que comercien con obras de arte o actúen como intermediarios en ese sector, o bien cuando lleven a cabo galerías de arte y casas de subastas, o puertos francos, y siempre que el importe de una transacción o de varias transacciones relacionadas sea igual o superior a 10.000 euros
A los proveedores de servicios de custodia de monederos electrónicos
A los proveedores de servicios de cambio de monedas virtuales por monedas fiduciarias

Respecto a las monedas virtuales (como *bitcoins)*, recoge que las autoridades competentes deberán estar facultadas para vigilar el uso de las monedas virtuales, a fin de asegurar un enfoque equilibrado y proporcionado que ampare los avances técnicos y el alto grado de transparencia en el ámbito de la financiación colectiva y el emprendimiento social.

Además, dado que el anonimato de las monedas virtuales puede ser una causa de su posible uso indebido, concluye que las Unidades de Inteligencia Financiera (UIF) nacionales deberán poder obtener todas aquellas informaciones que les permitan asociar las direcciones de las monedas virtuales a la identidad de su propietario.

Titularidad real

La norma recoge que los Estados miembros deben velar por que las sociedades y entidades jurídicas obtengan y mantengan información precisa y actualizada sobre su titularidad real, y defiende, además, que esta información sea de acceso público para mantener la confianza en la integridad de las transacciones empresariales y del sistema financiero.

En línea con lo anterior, establece que los Estados miembros deberán permitir el acceso a dicha información de forma suficientemente coherente y coordinada, estableciendo normas claras de acceso para que cualquier tercero que pueda demostrar un interés legítimo pueda conocer quiénes son los titulares reales de las sociedades y entidades jurídicas así como de los fideicomisos e instrumentos jurídicos análogos.

No obstante, recoge que se podrán incluir exenciones a la divulgación de la información en circunstancias excepcionales, cuando el titular real pudiera ser expuesto a algún riesgo desproporcionado de fraude, secuestro, chantaje, extorsión, acoso, violencia o intimidación; así como exigir la inscripción en línea, para identificar a todo aquel que solicite información del registro, y el pago de una tasa para acceder a información registrada.

Además, los Estados miembros deberán garantizar que los fiduciarios o personas con cargos

equivalentes en instrumentos jurídicos análogos, comuniquen tal condición y transmitan la información precisa a las entidades obligadas cuando realicen negocios o transacciones que superen los umbrales determinados en el artículo 11 (letras b, c y d) de la Directiva. Así mismo, en relación a la información relativa a su titularidad real, exigirán que se conserve en un registro central de titularidad real creado por el Estado miembro en el que esté establecido o resida el fiduciario o quien ostente posición equivalente y deberán presumir que esta información es adecuada, exacta y actualizada y establecerán mecanismos para tal fin.

Medidas de debida diligencia

Los Estados miembros deben aplicar medidas de debida diligencia en relación a los clientes, entre las que se incluye la identificación del cliente y su identidad sobre la base de documentos, informaciones o datos obtenidos de fuentes fiables e independientes. La nueva Directiva amplía la forma de verificar dicha información a través de medios de identificación electrónica, servicios de confianza o cualquier otro proceso de identificación remota o electrónica segura que haya sido reconocida o aceptada por las autoridades nacionales competentes.

Además, incluye que cuando el titular real identificado sea una persona que ejerce un cargo de alta dirección de alto nivel, las entidades obligadas deberán tomar las medidas razonables necesarias para verificar su identidad, consignando en los registros las medidas tomadas y las eventuales dificultades durante el proceso de verificación.

También regula que los Estados miembros deberán proteger y asegurar el derecho al anonimato de todas aquellas personas que revelen información sobre cuestiones relativa a blanqueo de capitales.

Excepciones

A la obligación de aplicación de medidas de debida diligencia se incorpora una excepción, de tal forma que no deberán adoptarse las mismas cuando se trate de dinero electrónico, siempre y cuando se cumplan ciertas circunstancias atenuantes, entre las que destaca: i) que el instrumento de pago no sea recargable o tenga un límite máximo mensual para transacciones de pago de 150 euros (frente a los anteriores 250 euros), y que ii) el importe máximo almacenado electrónicamente no sea superior a 150 euros (frente a los anteriores 250 euros).

Terceros países de alto riesgo

Contempla que todas aquellas transacciones o negocios con terceros países de alto riesgo deberán limitarse si se detectan insuficiencias significativas en el sistema de lucha contra el blanqueo de capitales y la financiación del terrorismo.

Así, cuando se dé esta situación de alto riesgo, los Estados miembros deberán exigir medidas de debida diligencia reforzadas respecto del cliente (información adicional sobre el cliente, el propósito del negocio, la procedencia de los fondos, etc.) para así poder gestionar y atenuar los riesgos. También podrán exigir medidas atenuantes adicionales complementarias a las anteriores (mecanismos reforzados de notificación, limitación de las transacciones, etc.), con un enfoque basado en riesgo y teniendo en cuenta las características concretas del negocio o transacción en cuestión.

Evaluación de riesgos

Incluye que el informe de la Comisión Europea en el que se evalúen los riesgos de blanqueo de capitales y de financiación del terrorismo, deberá abarcar, además:

El valor estimado de los volúmenes monetarios de blanqueo de capitales facilitados por Eurostat* respecto de cada uno de los sectores analizados

Los medios utilizados en las transacciones entre los Estados miembros y terceros países, con independencia de que sean identificados como de alto riesgo

Este informe deberá publicarse, como máximo, a los 6 meses de haber sido puestos a disposición de los Estados miembros, salvo aquellas partes del documento que contengan información clasificada.

Añade, además, que cada Estado miembro deberá: i) comunicar la estructura institucional y los procedimientos generales de su sistema de lucha contra el blanqueo de capitales y la financiación del terrorismo, incluyendo las UIF, las autoridades tributarias y fiscales, así como los recursos humanos y financieros asignados; e ii) informar sobre el capital humano y presupuesto utilizados. Deberán también informar a la Comisión sobre los resultados de sus evaluaciones de riesgos y sus actualizaciones, poniendo a disposición del público un resumen de las mismas.

Unidades de Información Financiera

La Directiva destaca el papel relevante de las UIF nacionales en la detección de delitos de terrorismo y de sistemas y redes de organizaciones terroristas, por lo que defiende que debe aumentarse su eficacia y eficiencia, especificando sus competencias y modalidades de cooperación entre cada organización de cada Estado miembro, a fin de abordar de forma eficaz y eficiente las distintas investigaciones relacionadas con el terrorismo y, en especial, con el uso indebido de monedas virtuales.

En ese sentido, recoge que deberán poder recabar toda la información necesaria relativa a sus funciones. También estarán obligadas a garantizar, de forma rápida, constructiva y eficaz, la cooperación internacional más amplia posible con las UIF de terceros países en relación con el blanqueo de capitales, los delitos subyacentes y la financiación del terrorismo, y todo ello en consideración de las Recomendaciones del GAFI.

Entrada en vigor

Los Estados miembros tendrán un periodo de 18 meses para transponer las disposiciones contenidas en la Directiva.

*Oficina Europea de Estadística