08/08/2023

La Ley de Informantes llega a España: "Es imposible cumplirla sin el uso de la tecnología"

Los Papeles de Panamá o en la Lista Falciani todavía tienen consecuencias en suelo europeo y, una de las últimas, se ha materializado en forma de normativa en España a principios de este ejercicio. Se trata de la**Ley de Protección de Informantes**, la trasposición española de la conocida como Whistleblower Protection Directive.

Hay que remontarse cinco años atrás, hasta abril de 2018, cuando comienza a fraguarse en el seno de la Comisión Europea**una legislación que busca proteger a los informantes**. Esta ley nace después de que saliesen a la luz los mencionados escándalos, que fueron conocidos por las autoridades gracias a la comunicación efectuada por los denunciantes.

Todo ello inició un debate relativo a los límites y las garantías en relación a la libertad de expresión e información que se vio reforzado por diferentes estudios realizados por la Comisión Europea, tal y como recuerda junto a D+I Jeannell Alfau, manager de Compliance y PBC de ECIJA. En ellos, los miembros de organizaciones consultadas trasladaban su creencia de que reportar cualquier infracción "resultaría inútil" y manifestaban el miedo que tenían a las represalias en caso de hacerlo; también, admitían que tenían un**"total desconocimiento" de los procedimientos de denuncia**.

Este caldo de cultivo dio como resultado la mencionada directiva europea de protección de informantes que, sobre el papel, se adoptó en 2019, pero, realmente, empezó a operar a finales de 2019 de forma efectiva.

A pesar de ello, no ha sido hasta 2023 cuando esta ley ha llegado a España y no lo ha hecho sin polémica, ya que la Comisión tuvo que darle varios "tirones de orejas" a este país y a otros para que avanzasen en su incorporación. De hecho, la CE tuvo que referir a ocho de estas regiones, incluida la española, a la Corte de Justicia por "fallar en la transposición y notificación de las medidas" al aplicarla.

"Un momento idóneo"

No obstante, y a pesar de todos los percances, desde el pasado 21 de febrero, España ya cuenta con una normativa adaptada a la legislación europea que busca doblar la protección de los usuarios que denuncien irregularidades sobre conductas indebidas o malas prácticas.

"Llega en un momento idóneo", cuenta a D+I María Dolores Pescador, presidenta ejecutiva de Grupo Logalty, que precisa que el país se encuentra "estancado en la prevención y lucha contra la corrupción", de acuerdo con el índice de Percepción de la Corrupción de 2022.

Además, señala que esta normativa permitirá establecer un marco adecuado para denuncias por acoso laboral o sexual que, actualmente, se encuentran silenciadas por temor a las represalias.

"Esta ley promete ser una herramienta clave en la lucha contra ambas prácticas, lo que, sin duda, mejorará el entorno laboral de los trabajadores y el crecimiento empresarial en nuestro país", afirma la presidenta ejecutiva de Grupo Logalty.

En concreto, la legislación española afecta a aquellas empresas u organizaciones que tengan más de 50 trabajadores en plantilla y les obliga a disponer de un canal oral para emitir estas denuncias (ya sea por teléfono o por un sistema de mensajes de voz como un contestador), en persona (mediante reuniones disponibles a petición del denunciante) o por escrito (donde se incluye el correo postal, el correo electrónico o un canal de denuncias digital).

Todas las metodologías deben garantizar la confidencialidad de los datos de la persona que recurre a ellas. En caso de que las empresas no introduzcan estos mecanismos, la normativa contempla multas que van desde los mil hasta el millón de euros.

Dos fechas relevantes

De momento, los reguladores han puesto sobre la mesa dos fechas relevantes, siendo la primera el próximo 13 de junio, antes de la cual deben incorporar las demandas recogidas en la ley las entidades del sector público en municipios más de 10.000 habitantes, las empresas privadas con más de 250 empleados y los partidos políticos, sindicatos o fundaciones que reciban o gestionen fondos públicos. Mientras, el 1 de diciembre deberán hacerlo las firmas entre 50 y 250 empleados y los municipios de menos de 10.000 habitantes.

Ante este escenario, las firmas españolas afectadas se han puesto "manos a la obra" para cumplir con los requerimientos dispuestos en este mecanismo.

Pescador cuenta que, desde su compañía, están observando "un creciente interés" de las empresas por conocer los pormenores de la normativa y cumplir con sus exigencias, aunque aún existen muchas dudas a su alrededor, entre ellas, cuál va a ser el papel efectivo de la Autoridad de Supervisión de los Denunciantes.

Por su parte, Alfau pone el foco en las problemáticas que están afrontando las compañías e instituciones a la hora de incorporar esta ley a su estructura, entre las que se encuentra**la dificultad de integrar las exigencias de dicha legislación** junto a sus sistemas internos y el resto de cumplimientos de normativas sectoriales y específicas.

Además, la experta precisa que**la norma 'peca' de falta de concreción** a la hora de aterrizar algunas medidas de protección y garantías a las personas que participen en calidad de perjudicados o de denunciantes.

"Esto sumado a la obligación de extender estas las garantías y mecanismos de protección no únicamente sobre los empleados de la organización, sino sobre aquellos terceros o stakeholders que vienen delimitados en su ámbito subjetivo", añade.

El reto tecnológico

No obstante, entre todos ellas, destaca el**"reto tecnológico"**, en palabras de Pescador.

Según explica, las empresas deben incorporar los requisitos recogidos en la normativa, entre ellos la confidencialidad, de forma eficaz, cumpliendo con los plazos definidos, "y a un precio razonable",**algo que es "imposible de cumplir sin el uso de la tecnología".**

"Las empresas deben dar un paso más en su proceso de transformación digital y aplicar también la digitalización en los procesos y departamentos de Recursos Humanos, Legal o Compliance si quieren adaptarse rápidamente, tanto a esta nueva ley como a las próximas", precisa la presidenta ejecutiva de Grupo Logalty.

En este sentido, la manager de Compliance y PBC de ECIJA destaca que "uno de los momentos más críticos" es la elección de un **"partner tecnológico"** que configure el sistema de información interno y permita que la organización cumpla los requisitos de la normativa en materia de anonimización y confidencialidad de las comunicaciones.

"La necesidad de adecuarse a la norma por parte de sujetos obligados con una casuística tan variada y con necesidades tan dispares **ha generado una atomización de la oferta en las herramientas tecnológicas** que permiten la comunicación a través de estos canales", explica.

Así, señala que hay plataformas que permiten que se genere un usuario anónimo con el que el informante podrá acceder para emitir una comunicación, seguir su estado y recibir requerimientos de documentación efectuados por el responsable del expediente de investigación. Asimismo, en el caso del canal verbal, existen sistemas de distorsión de voz que faciliten la disociación de la comunicación con cualquier elemento identificativo de la persona informante.

De esta forma, Alfau apunta que son **"múltiples" las herramientas tecnológicas** que existen, actualmente, en el mercado enfocadas a cubrir las necesidades derivadas de las exigencias normativas en relación a la confidencialidad y en base a los requerimientos propios de cada entidad, pública o privada.

"El marco normativo de aplicación a estos sistemas de información es amplio y, por tanto, su cumplimiento y adaptación a los requerimientos y exigencias es esencial para que las entidades puedan garantizar a través de la tecnología la confidencialidad del denunciante", puntualiza.

Entre las medidas más importantes a tener en cuenta se encuentran **el cifrado, el control de accesos físico y logístico a la información, la anonimización o pseudoanonimización de los datos**. Todo ello en línea con marcos normativos básicos como el Reglamento General de Protección de Datos (RGPD) o la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).

Alfau puntualiza que estas garantías no deben ser sólo adoptadas por las plataformas tecnológicas que sirvan de base a los sistemas de información, sino en el entorno y sistemas de las propias entidades obligadas, ya que los datos "pueden encontrarse en otras ubicaciones que deberán **tener el mismo nivel de seguridad y garantías de confidencialidad".**

Fuente: elespanol.com

LINK DE LA NOTICIA