

Cómo proteger mejor a los alertadores:

Guía práctica para transponer la Directiva europea

Autores:
Naomi Colvin, Bruno Galizzi y Veronika Nad



Agradecimientos

Blueprint for Free Speech agradece el apoyo de Open Society Initiative for Europe, que forma parte de Open Society Foundations. El proyecto Expanding Anonymous Tipping (E.A.T.) también agradece el apoyo de del Internal Security Fund de la Unión Europea.

Agradecemos al profesor David Lewis de la Universidad de Middlesex, así como a Tom Devine y Samantha Feinstein de la organización Government Accountability Project (GAP) y a Katharina Beck, Robert Benditz, Isabelle Brams, Adrien Giraud, Peter Neuboeck, y Sven Voelcker de Latham & Watkins LLP por sus valiosos conocimientos y aportaciones.

Co-funded by the
Internal Security Fund
of the European Union



Este informe ha sido financiado en parte con el Fondo de Seguridad Interior - Policía de la Unión Europea. Su contenido es responsabilidad de sus autores y representa sus puntos de vista. La Comisión Europea no se hace responsable del uso que se pueda dar a la información que contiene.

Índice de contenidos

Introducción	1
EU Whistleblowing Compliance Checker	2
Capítulo 1 - Lo que contempla la Directiva	3
Revelaciones en seguridad nacional	4
Lost in translation – Por qué las palabras importan cuando se está definiendo al alertador	6
Capítulo 2 ¿A quién ampara la Directiva?	7
Capítulo 3 - ¿A quién ampara la Directiva? (II)	8
Delitos informáticos	9
Capítulo 4 ¿A quién ampara? (III)	10
El papel de la sociedad civil	11
Capítulo 5 - ¿A quién dirige el alertador su denuncia?	12
Capítulo 6 - ¿Quién necesita establecer un canal interno?	13
Capítulo 7 – Cómo deberían ser los canales internos	14
Buzones digitales seguros	15
Capítulo 8 – Cómo deberían configurarse los canales externos	16
La autoridad independiente del denunciante: cómo funciona	18
Capítulo 9 – Revelaciones a los medios	19
Proteger la fuente en la era digital	20
Capítulo 10 – Confidencialidad y anonimato	21
Denuncias Anónimas y buzones online seguros	21
Capítulo 11 – La protección legal al denunciante	23
Capítulo 12 – Apoyo y medidas provisionales	24
Capítulo 13 - La otra parte: la protección de las personas afectadas	26
Capítulo 14 - ¿Funciona? Disposiciones para la presentación de informes, la supervisión y evaluación	27
Capítulo 15 La denuncia de irregularidades en la era de COVID-19	28

Introducción

En muchas de las grandes noticias de la última década ha participado en algún momento un alertador o denunciante^I. Tanto si se habla de influencia antidemocrática en determinada publicidad política online, de fraude fiscal internacional a gran escala o de negligencia en las pruebas medioambientales y de salud pública expuestas en el escándalo *dieselgate*, nuestro debate público sería mucho más pobre sin la contribución de los denunciantes.

Es probable que se necesiten décadas para determinar el verdadero alcance de los daños que se consiguieron mitigar o que se evitaron al salir a la luz estas cuestiones. Pero de lo que no se puede dudar es de que sin la contribución de los que tomaron la decisión de hablar, los costes para la sociedad habrían sido mucho mayores.

A los alertadores o *whistleblowers* se les puede considerar sistemas humanos de alerta temprana, ya que detectan desde simples errores y encubrimientos conexos hasta abusos y fraudes sistemáticos que afectan a sociedades enteras. Sus acciones no solo ayudan a prevenir daños graves, sino que también contribuyen a mejorar la ética en el comercio mundial y la cultura de transparencia, cuyo valor se ha hecho aún más evidente en el contexto de la lucha contra la pandemia mundial de COVID-19.

Sin embargo, revelar información resulta arriesgado y sigue siendo así tanto si los denunciantes o alertadores intentan informar a sus empleadores (como hace más del 90% de ellos), como si van directamente a un regulador o, con menos frecuencia, a los medios de comunicación. Que se tomen represalias contra ellos puede significar que su carrera profesional sufra daños o incluso la pérdida del trabajo y los significativos costes económicos que ello conlleva.

Luchar para ser reconocido como un denunciante o alertador y ser compensado por ello puede llegar a ser un trabajo a tiempo completo. Muchos alertadores terminan afrontando largas y costosas batallas judiciales, incluso cuando están intentando hacer valer derechos que en teoría les tendrían que proteger.

Son conscientes de los riesgos que asumen. Las encuestas muestran una y otra vez que las personas que son testigos de malas prácticas no suelen denunciarlas por temor a represalias o porque no creen que existan sistemas efectivos para impedir que eso ocurra^I.

Si queremos que los denunciantes den un paso al frente, actúen como un sistema de alerta temprana en las organizaciones que conocen y que hagan sonar la alarma sobre los casos realmente graves de malas prácticas, entonces tenemos que asegurarnos que informar sobre ello no acaba trastocándoles la vida.

Introducir una serie de medidas legales de protección es una forma de hacerlo. Las leyes para proteger a los alertadores buscan regularizar esa compleja situación. Su objetivo es asegurar que se investiga lo denunciado y que se limitan los riesgos para todas las partes involucradas. En los últimos años se ha avanzado mucho en este sentido, sobre todo en Europa.

En 2018, 19 de los 28 países que conformaban entonces la Unión Europea (UE), habían introducido medidas para proteger a los alertadores (los países mejor posicionados en la encuesta que se realizó fueron Francia, Irlanda, Malta y Reino Unido). Sin embargo, ninguno de ellos llegaba a cumplir con los estándares internacionales^I.

En abril de 2019, la Unión Europea dio un paso significativo para la protección de *whistleblowers* al aprobar una nueva Directiva que convirtió la protección de los alertadores en una obligación legal. La Directiva de protección del denunciante, cuyo título oficial es Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión o Directiva 2019/1937, detalla una base estándar de protección que se aplicará en los 27 miembros de la Unión Europea^{II}.

La Directiva establece las disposiciones sobre quién puede estar amparado como *whistleblower* y los temas sobre los que puede informar. Define cómo la idea de proteger a los alertadores está interconectada con otras obligaciones éticas y legales. Prevé protección a familiares, colegas u otras personas que podrían verse afectadas por las represalias.

Uno de los asuntos más difíciles que un informante debe afrontar es ante quién tiene que informar una actividad ilícita o una mala práctica.

I. El uso del término alertador para definir a la persona que comunica una infracción es una cuestión relevante para evitar connotaciones negativas (véase la sección Lost in translation en la pág. 6)
II. Para una evaluación reciente de los costes de las denuncias de irregularidades véase la publicación Post Disclosure Survival Strategies: <https://whistleblowingimpact.org>

La Directiva establece disposiciones sobre cómo deberían funcionar los canales de denuncia internos (dentro de una empresa), externos (organismos reguladores o agencias externas), su deber de confidencialidad con el alertador y los procedimientos para la investigación. Establece además el deber de hacer públicos esos detalles para que potenciales alertadores, habiéndose informado, puedan tomar una decisión sobre a quién dirigirse para realizar la denuncia.

La Directiva también establece protección legal para el alertador, pero también para los individuos o entidades que han sido denunciados o se han visto implicados en la denuncia. Por último, existen procedimientos para mantener registros y una supervisión a fin de poder comprobar que las normas funcionan. La Directiva de la Unión Europea no tiene la última palabra en la protección del denunciante, pero sí supone un importante avance en esa dirección. Su buena puesta en práctica es importante y con una implicación significativa mucho más allá del bloque de los 27 países de la UE.

Sobre este informe

La Directiva no es de aplicación inmediata. Los países miembros de la Unión Europea tienen de plazo hasta fines de 2021 para transponerla y convertirla en una ley nacional en consonancia con los estándares que se disponen^{III}. Si bien la Directiva establece algunas obligaciones llamativas, entre ellas la de que toda empresa privada con 50 empleados o más tendrá que establecer o proporcionar un canal interno de denuncias, es mucho lo que queda a discreción de los legisladores nacionales.

El texto de la Directiva es también claro acerca de qué debería considerarse como una base para establecer el nivel de protección y de que los países miembros deberían considerarla como un punto de partida sobre la que construir sus leyes nacionales. La sociedad civil estuvo muy implicada en el proceso que desembocó en esta Directiva, de forma inusual según las normas de la Unión Europea, y hemos evaluado que la Directiva cumple con las mejores prácticas en muchos, pero no en todos los aspectos^{IV}.

Este informe es para aquellos que quieren asesoramiento sobre si la actual ley o el proyecto de ley en sus respectivos países cumple con las demandas de la Directiva. Además, proporciona orientación sobre la forma en que los Estados miembro pueden resolver mejor algunas de las cuestiones más difíciles del texto de la Directiva y elevar el listón en las áreas sobre las que la Directiva no dice nada.

Esperamos que este informe también sea útil para los que podrían encargarse de aplicar la transposición.

EU Whistleblowing Compliance Checker

Esta herramienta interactiva online permite evaluar un nuevo proyecto de ley o la propuesta para la transposición nacional de la Directiva:

<https://tool.blueprintforfreespeech.net>

La herramienta está diseñada para hacer tres cosas. En primer lugar, proporciona una base para evaluar si una ley, o una propuesta legislativa, cumple con la Directiva. En segundo lugar, califica la ley o el proyecto de ley según las normas internacionales más allá de la Directiva, y muestra las áreas de mejora. Por último, la herramienta propone una serie de escenarios de denuncia basados en ejemplos reales de la actual pandemia de COVID-19. La intención de esta sección es destacar cuán bien funcionan en la práctica los marcos legales, en particular durante una pandemia.

La herramienta online tiene la forma de una checklist. Un recorrido por la puntuación de checklist está disponible aquí:

<https://www.blueprintforfreespeech.net/en/compliance-checker-example>

La herramienta propone una serie de preguntas a las que se responde con un sí o un no. Debería ser posible responder a casi todas las preguntas guiándose tan solo por la referencia al texto legislativo. No se asume como referencia ninguna ley de protección de alertadores en particular.

Cuando se ha contestado a todas las preguntas, la herramienta proporciona una puntuación que indica el cumplimiento de la Directiva, de las normas internacionales más amplias y situaciones prácticas. Además, también proporciona un detallado comentario

III. Los avances en la transposición de la Directiva en los 27 países de la Unión Europea están siendo seguidos en el *EU Whistleblowing Meter*: <https://euwhistleblowingmeter.polimeter.org/>
IV. De las 23 normas de mejores prácticas que examinamos, encontramos que la Directiva cumplía plenamente con 11 de ellas y parcialmente con otras ocho. Las cuatro restantes quedaron fuera del texto por completo o han quedado a discreción de los países miembros.

y un análisis de las fortalezas y debilidades de la propuesta, así como sugerencias acerca de cómo reaccionar.

La Directiva de la UE demandará cambios más amplios en algunos Estados miembros que en otros. Pero todos los países del bloque estarán obligados a modificar su legislación para cumplir con la Directiva. Nuestra esperanza es que este informe y nuestra checklist ayude a proporcionar coherencia en toda la Unión Europea y sirva para orientar a otros grupos en otros países que quieran mejorar su normativa de protección.

Capítulo 1 - Lo que contempla la Directiva

Existe más de una manera de abordar la protección de los alertadores. Si bien el fenómeno de los individuos que dan un paso al frente y se atreven a hablar de cuestiones importantes tiene una larga historia, el término "*whistleblower*" cobró relevancia por primera vez en Estados Unidos a finales de la década de los 60 y principios de los 70.

Como resultado de ello, surgieron en Estados Unidos algunas de las primeras leyes destinadas a proteger a los denunciantes de irregularidades. Esas primeras leyes establecieron regímenes por sectores, creando normas especiales para determinados grupos de empleados públicos y, más tarde, para la industria financiera y otros del sector privado.

En la actualidad, la protección de alertadores en Estados Unidos es un entramado complejo de diferentes esquemas legislativos que abarca diversas áreas de trabajo. Las leyes posteriores, incluyendo la propia Directiva de la UE, han adoptado un enfoque horizontal diferente, que intenta establecer un conjunto de normas para los denunciantes de manera general.

La ventaja de este enfoque horizontal es que facilita a los posibles alertadores de irregularidades comprender primero sus derechos y recursos, así como la reducción de los costes que ese conocimiento conlleva.

En la práctica, bajo el sistema estadounidense, las normas y su aplicación son hasta cierto punto opacas y es esencial para las personas que están pensando en sacar algo a la luz contactar con un abogado privado o una organización sin ánimo de lucro para que les oriente durante todo el proceso.

La Directiva de la Unión Europea vincula la protección del "*whistleblower*" al trabajo del mercado interno, un criterio que abarca todo, desde el etiquetado de la comida para animales hasta la seguridad de las redes informáticas. A diferencia de muchos planes de protección, cubre tanto el sector público como el privado. De hecho, la Directiva viene a abarcar todo lo que la Unión Europea podría legislar, pero eso deja mucho fuera.

La Directiva contempla denuncias sobre las infracciones de las normas de la Unión. En algunas áreas, como el sistema de educación nacional y el sistema de salud, la Unión Europea solo tiene competencias de apoyo. Eso significa que la UE no legisla directamente en esas áreas, que se deja en manos de los gobiernos nacionales. Las denuncias de infracciones en esas áreas encajan más bien en la ley nacional y no tanto en la del derecho de la Unión y, como tales, no están cubiertas de forma específica por la Directiva.

Esta es una de las carencias que los gobiernos nacionales deberían considerar cubrir para asegurarse que las mismas normas se aplican a todos los alertadores. No es realista en términos prácticos esperar que un alertador juzgue si lo que preocupa en su denuncia es una infracción de la ley nacional o del derecho de la Unión. La mejor forma de trasladar el amplio enfoque de la Directiva a la ley nacional es con la introducción de medidas *horizontales* para proteger al denunciante, que también se puedan aplicar en las áreas gobernadas por leyes nacionales o regionales. El derecho internacional que no sea originario de la UE tampoco estará dentro del alcance de las protecciones, a menos que los Estados miembros tomen la decisión proactiva de incluirlo.

Además de las limitaciones impuestas por el mandato de la UE, la Directiva también especifica algunas áreas que quedan exentas de cobertura. Un terreno siempre especialmente sensible y que se rige por la ley nacional es seguridad nacional, defensa y divulgación de información clasificada. A pesar de que las divulgaciones en esta esfera han sido objeto de algunas de las revelaciones de interés público más importantes de los últimos años, la transmisión, recepción o publicación no autorizada de material clasificado está prohibida y tipificada en el derecho penal en muchos países.

La Directiva no modifica esta situación, lo que constituye una de las deficiencias más evidentes de la legislación. Si bien algunos aspectos de la contratación pública en materia de defensa entran en el ámbito de aplicación de la Directiva, la seguridad nacional y la defensa son áreas reservadas

explícitamente a los Estados miembros.

Aunque la Directiva no establece nuevas obligaciones en esas áreas, la denuncia de infracciones en materia de seguridad nacional no es un ámbito que deba ser ignorado. Tras las divulgaciones de Chelsea Manning y Edward Snowden, entre otras, la denuncia de irregularidades en materia de seguridad nacional ha sido objeto de recomendaciones sobre mejores prácticas internacionales y de jurisprudencia del Consejo de Europa. En ellas se sugiere que los Estados deberían proporcionar algunas vías a la que puedan recurrir los alertadores en materia de seguridad nacional y defensa, incluso si esas vías difieren de las previstas para la presentación de denuncias en otros ámbitos.

Revelaciones en seguridad nacional

La Directiva deja en manos de los países miembros la decisión de cómo tratar las revelaciones en materia de seguridad nacional y de defensa. Hay una serie de normas europeas e internacionales en estos ámbitos sobre los que basarse.

Los Principios de Tshwane sobre seguridad nacional y el derecho a la información (2013)³

Estas directrices detalladas para equilibrar los intereses en seguridad nacional de los Estados con el derecho de sus ciudadanos a saber fueron compilados por una serie amplia de actores de la sociedad civil. En ellas se recalca que existe un interés público primordial en determinado tipo de información como, por ejemplo, las pruebas de abusos de derechos humanos (Principio 10) y que los alertadores en esos ámbitos tienen que tener un marco de protección legal similar al desarrollado en la Directiva de la Unión Europea (Principios 40-43).

Recomendación del Consejo de Ministros del Consejo de Europa (CM Rec 2014/7)⁴

Esta recomendación del Consejo de Europa sobre la protección de los alertadores refleja muchas de las normas que se acabaron incluyendo en Directiva y también incluye denuncias en el ámbito de la seguridad nacional. Establece que los miembros puedan conformar “un régimen especial o normas” para los denunciantes de temas de seguridad, pero que haya también para ello algún tipo de canal para poder hacer las denuncias. La Asamblea Parlamentaria del Consejo de Europa ha respaldado los Principios de Tshwane en una serie de ocasiones.

Bucur y Toma contra Rumanía - 40238/02 (Tribunal Europeo de Derechos Humanos)

El caso se refiere a un programa de escuchas telefónicas que reveló Constantin Bucur, un miembro del Servicio de Inteligencia de Rumanía, durante una rueda de prensa. Rumanía juzgó a Bucur por ello en un Tribunal Militar. El Tribunal consideró que el juicio al que fue sometido Bucur constituyó una obstrucción injustificada en su libertad de expresión considerando el interés público de la información revelada⁵.

¿Qué es una infracción?

La Directiva tiene por objeto proteger a quienes denuncien infracciones del derecho de la Unión Europea en una serie de ámbitos. Tan importante como las áreas que cubre la Directiva son los tipos de acciones que cumplen con el umbral de comportamiento denunciabile.

Es importante comprender que una “infracción” en los términos de la Directiva es más amplia que las violaciones de la ley. La Directiva

define una infracción como un acto ilícito u omisión. La omisión es este caso abarca no hacer cumplir la normativa, ya sea a propósito o por negligencia. También se consideran protegidas las divulgaciones de información sobre posibles infracciones o los esfuerzos por encubrirlas.

La amplitud de esta definición ayuda a mejorar la previsibilidad de la ley para los alertadores, a los que no se les requiere analizar si un acto concreto constituye una violación de la ley antes de informar sobre él. Por esa misma lógica, los Estados miembros tal vez deseen considerar si la cobertura de la Directiva es lo suficientemente amplia.

El despilfarro y las ineficiencias no son necesariamente resultado de la negligencia y son un ejemplo de temas que bien pueden ser objeto de valiosos reportes que no están explícitamente cubiertos por la Directiva. Otros marcos legales de protección de denunciantes difieren del enfoque adoptado por la Unión Europea. La Ley de Protección de Alertadores de Estados Unidos, que se aplica a los funcionarios federales, protege las revelaciones sobre la mala gestión cuando esta socava el propósito de una organización. Esta podría ser un área en la que los Estados miembro o las organizaciones que operan los canales de denuncia tal vez quieran ampliar yendo más allá de los estándares propuestos en la Directiva y acepten renuncias que abarquen una gama más amplia de cuestiones^V.

La Directiva reconoce esta cuestión de la previsibilidad en su tratamiento del estado mental del denunciante.

Un alertador tiene derecho a protección si tiene motivos razonables para creer que su denuncia está dentro del ámbito de aplicación de la Directiva, aunque luego resulte que no es así.

Uno de los fundamentos para vincular la protección de los denunciantes con el funcionamiento del mercado interior ha sido el reconocimiento de que los grandes problemas suelen tener una dimensión transfronteriza. El escándalo de la carne de caballo en 2013 puso sobre la mesa la cuestión de la complejidad de las cadenas de suministro. Detectado por primera vez en Irlanda, la comercialización de carne de caballo bajo etiquetas engañosas acabó destapando una situación que afectaba a 16 Estados de la UE.

Tal vez pueda sorprender un poco que la Directiva no contenga un lenguaje explícito sobre las denuncias con dimensión transfronteriza. No obstante, lo que queda claro por la implicación que tienen es que esos casos tienen que estar cubiertos, al menos en aquellos casos en los que otro país o países involucrados también son miembros de la Unión Europea.

La Directiva permite que las infracciones se comuniquen a los órganos de la UE, prevé la asistencia jurídica en los procedimientos civiles transfronterizos y cita la capacidad de los Estados miembros de cooperar en la investigación de denuncias con repercusiones transfronterizas con un tema específico para evaluar si la legislación funciona.

V. Los canales internos de denuncia de irregularidades también pueden utilizarse para plantear otros tipos de quejas en lugar de trabajo, como los conflictos personales, que según la Directiva, los empleadores tal vez deseen canalizar a través de otros procedimientos. Considerando 22

Lost in translation – Por qué las palabras importan cuando se está definiendo al alertador

El término denunciante (*whistleblower*) se usa desde hace unos 50 años y generalmente se entiende bien en los países de habla inglesa. En otros lugares, sin embargo, es diferente. Términos nuevos como el *lanceur d'alerte* en francés o *klokkenluider* en holandés han sido acuñados en una serie de países europeos para desprenderse de las connotaciones negativas asociadas a otros vocablos y se acercan más al sentido de “informante” (informant) en inglés. Como se traduce la palabra “informante” en otros idiomas también puede tener un impacto legal, algo que varios países están teniendo que enfrentar a la hora de transponer la Directiva.

España es uno de los países que carece de una ley nacional de protección de denunciantes en la actualidad y tendrá que hacer cambios significativos como resultado de la Directiva. La terminología a emplear es en sí mismo objeto de debate. El término más utilizado en la legislación vigente es “denunciante”, pero está lejos de ajustarse perfectamente a los términos de la Directiva.

El término “denunciante”, tal como se define en el Código Penal español, es alguien que hace una denuncia ante las fuerzas del orden, cuando esta vía puede no ser la mejor opción para un alertador debido al asunto del que se trate su denuncia o el contexto en el que se hace. El concepto también obliga a que la persona informante sea identificada por su nombre, lo que entra en conflicto con la idea de permitir denuncias anónimas, una opción que sí contempla la Directiva. Además, el “denunciante” en la legislación española reporta delitos penales. Y como se ha visto, el concepto de “infracciones” en la Directiva es mucho más amplio.

Aun cuando alzar la voz sobre estas infracciones es un acto de justicia y verdad en defensa del interés público, los denunciantes pueden estar mal vistos y el término puede tener connotaciones negativas. En muchos idiomas la terminología en sí no ayuda. “Denunciante” conlleva una connotación extremadamente negativa en español y está asociado a otros significados peyorativos como “chivato” o “soplón”. Por el contrario, el término “alertador” permite definir el concepto de denunciante en un lenguaje más neutro y evita los problemas jurídicos relacionados con una terminología concreta.

Esta situación también se plantea actualmente en otros países europeos. El concepto griego de Μάρτυρας δημοσίου συμφέροντος, que se traduce como “testigo de interés público” también podría tener implicaciones similares en el proceso de transposición. Es por ello que las organizaciones de la sociedad civil están abogando por un término más positivo como “πρόσωπο που αναφέρει παράνομα ή παράτυπα περιστατικά”, persona que reporta incidentes ilegales o irregulares.

Capítulo 2 ¿A quién ampara la Directiva?

Uno de los aspectos más progresistas de la Directiva es la forma en la que define quién tiene derecho a la protección por revelar una irregularidad, lo que llevará a que más alertadores sean reconocidos y apoyados en la mayoría de los países miembros de la UE.

La Directiva abarca a toda persona que tenga información sobre infracciones en un contexto laboral y por lo tanto trata de asegurar que el tipo de trabajo amparado por la legislación nacional sea lo más amplio posible. Al incorporar en la legislación un amplio abanico de relaciones laborales actuales, la Directiva busca de nuevo asegurarse de que haya cierta previsibilidad para los alertadores.

Esto es algo que muchos marcos legislativos no han logrado conseguir. Muchas leyes de protección del denunciante, como por ejemplo la Ley de Divulgaciones Públicas de Australia de 2013, se aplica solo en el sector público. Otras no se han actualizado con los cambios en la composición de la fuerza de trabajo, tal como ocurre con la Ley de Divulgación de Interés Público de Reino Unido, que data de 1998.

Esta ley utiliza una definición de “trabajador” que no cubre a la mayoría de las personas que trabajan por cuenta propia y que en 2017 suponían más del 15% de la fuerza laboral en Reino Unido.

Los Estados miembros que buscan transponer la Directiva tienen que asegurarse de que su legislación nacional abarque al máximo posible toda la gama de posibles relaciones laborales que se registran actualmente.

Dado que la Directiva está vinculada al funcionamiento del mercado interior, establece que cualquier persona que encuentre pruebas de un asunto en el curso de su vida laboral debería tener derecho a protección. Dentro de esa limitación de “un contexto de trabajo”, el ámbito personal que abarca la Directiva es amplio: incluye empleados, autónomos y contratistas, así como sus subcontratistas y sus empleados, voluntarios y accionistas. También están cubiertos los exempleados y otros cuya relación laboral con el asunto en cuestión sea algo del pasado. Por último, protege a los solicitantes de empleo y a otros cuya relación laboral aún no ha comenzado.

Sin embargo, es importante reconocer que la Directiva no protege a todos los ciudadanos en todas las circunstancias. Por un lado, la Directiva crea una categoría separada de “facilitador” para los terceros que ayudan o asisten a un informante. Esta disposición se debate abiertamente en el capítulo 4, pero los periodistas, sindicalistas y las ONG podrían sufrir represalias por divulgar información protegida y, por lo tanto, merecen protección directa.

El requisito de que la información se haya adquirido en el contexto de una actividad laboral excluye a otro grupo. Tal vez haya personas que estén en posesión de información sobre infracciones fuera de su entorno laboral y pueden querer denunciarlo para enmendarlo. Esas personas por supuesto que también podrían sufrir represalias por ello, pero no están amparadas por la Directiva.

Ejemplos de personas que no estarían acogidas por el lenguaje de la Directiva es el paciente de un hospital o sus familiares a los que les preocupa la mala praxis. O cuando alguien es testigo de un arresto ilegal en un lugar público o siente que ella misma ha sido víctima de una entidad pública. En ninguno de estos casos contaría con protección.

Esta es otra laguna que los países miembros de la UE tienen la oportunidad de enmendar, entre otros, porque hay ejemplos a los que recurrir. Algunos países europeos ya han adoptado marcos legales para que se puedan hacer denuncias que van más allá de la Directiva y están abiertos a todas las personas, como es el caso de la *Loi Sapin II* en Francia, que identifica como alertador a cualquier persona que haga una revelación de la manera que se pide. También en algunas regiones de España, sobre todo en la Comunidad Valenciana, se ha incluido una legislación que protege a toda persona física o jurídica que emplee uno de los canales de denuncia digitales seguros para denunciar actividades corruptas. En base a ello, la propuesta de transposición para la Directiva en España que propuso la organización X-Net incluye la protección de todos los posibles denunciantes⁶.

Un área de posible ambigüedad es la diferencia entre un alertador que ha encontrado pruebas de infracciones en un contexto laboral y aquella que haya tenido una relación con la persona o la institución que sería objeto de la denuncia. Lo primero no implica necesariamente lo segundo. La Directiva exige que alguien que denuncie haya adquirido esa información en el contexto de una relación de trabajo y que la información se refiera a una organización con la que está en contacto o lo estuvo en el pasado.

No es necesario para un denunciante tener una relación directa de trabajo con el asunto que se denuncia o que lo haya estado en el pasado. De hecho, la Directiva de la UE sugiere que las empresas tengan sus propios canales internos abiertos a un rango mayor de personas que han estado en contacto con ellas (véase el capítulo 7 sobre la configuración de los canales internos de denuncias).

Capítulo 3 - ¿A quién ampara la Directiva? (II)

La estructura básica de las leyes de protección de alertadores es establecer ciertas pautas para protegerlos. La Directiva de la UE no es una excepción.

La Directiva se elaboró con una importante aportación de la sociedad civil. Y como resultado de ello, el texto de la Directiva refleja muchas de las lecciones aprendidas de la forma en que la legislación previa ha funcionado en la práctica. Esto es evidente sobre todo en esta sección de la legislación, en la que pone la atención en los criterios para determinar los umbrales. ¿Cuál era el estado mental del alertador cuando hizo la denuncia? Hasta qué punto podemos evaluar lo que estamos intentando lograr y ¿eso importa realmente? ¿Existe un límite de tipos de acciones que los denunciantes tienen derecho a realizar? ¿Cuál es la mejor manera de evitar que se abuse de las protecciones legales?

En el presente capítulo se examinan tres cuestiones consideradas fundamentales en la Directiva en lo referente a los límites de protección: los requerimientos de buena fe, las denuncias malintencionadas o abusivas y los límites a la inmunidad jurídica.

Buena fe

Cuando se informa de denuncias, los medios de comunicación suelen centrar su atención en los individuos que dicen la verdad a pesar de los obstáculos y ponen el énfasis en su civismo e intención moral, a menudo con alguna justificación. Por lo tanto, resulta tentador ver como uno de los rasgos definitorios de un denunciante es que tenga un motivo.

En la práctica, sin embargo, las ONG y otras instituciones que trabajan en esta área suelen estar de acuerdo al afirmar que las intenciones de buena fe pueden llegar a ser contraproducentes en la práctica e incluso dificultar que se cumpla con la protección de las personas⁷.

La experiencia de Reino Unido muestra que la buena fe y otros requisitos de tipos de motivaciones pueden permitir a los empleadores poner en marcha un tipo amplio de ataques en los tribunales a esos individuos, lo que hace más difícil que los alertadores obtengan la protección de la ley y se aleje del foco la esencia de la denuncia⁸.

La motivación también puede usarse como un factor para reducir el monto de la compensación económica a los alertadores, aun cuando ganen el caso, como sucede en Reino Unido e Irlanda.

Es por ello que, en los intentos de la Directiva de definir los criterios para garantizar la protección, no se exige una evaluación de la motivación personal. No es preciso especular sobre el estado emocional o psicológico de un informante para decidir si tuvo una *creencia razonable de que el contenido de su denuncia era cierto*. Solo se necesita preguntar si, en su posición, sabiendo lo que la persona denunciada hizo, sería razonable para cualquier persona creer que la información era verdad.

Del mismo modo, el estándar en la legislación estadounidense de protección de alertadores (US Whistleblower Protection Act) es que el denunciante cree razonablemente que está desvelando pruebas de una supuesta conducta errónea^{VI}.

Los requisitos de buena fe son onerosos para los denunciantes y su ausencia de la Directiva es deliberada. Tampoco se requiere que los alertadores hagan sus denuncias en línea con los requerimientos procesales de la prueba. En lugar de ello, al alertador se le exige tan sólo tener motivos razonables para creer que su denuncia es verdadera. Si cuando se investigue el asunto se determina que la denuncia carece de base, la persona que hizo la denuncia no pierde su derecho a estar protegida.

En otras palabras, la Directiva también protege a quien cometió un error sin intencionalidad alguna. Sin embargo, las denuncias o revelaciones públicas deliberadamente falsas no están protegidas por la Directiva, y pueden estar sujetas a sanciones penales.

VI. Una diferencia entre la normativa de EEUU y la de la UE es que la Directiva explícitamente apoya a aquellos que expresen dudas razonables, pero "no tengan pruebas positivas" (Considerando 43).

Denuncias maliciosas

Una de las razones por las que la motivación del denunciante puede ser cuestionada es debido a que preocupa que se pueda abusar del sistema de denuncias con reportes vejatorios o acusaciones maliciosas que buscan acosar a otras personas o hablar mal de ellas.

A pesar de que es posible que se haga una denuncia válida con intenciones dudosas, la Directiva incluye disposiciones para disuadir de abusos. Por lo tanto, aquellos que lo hagan, se arriesgan a una acción disciplinaria por parte del empleador o incluso a que se emprendan medidas legales en su contra.

La Directiva exige que haya sanciones "efectivas y disuasorias" por abusar del sistema con información que el denunciante sabe que es falsa. Las sanciones para denuncias que se sabe que son falsas se debaten en el capítulo 13.

Límites a la inmunidad

Otro de los criterios que pueden establecer límites a quiénes pueden gozar de protección, se refiere a la inmunidad jurídica y a la interacción de las medidas de protección de los denunciantes con diferentes partes de la legislación. Los alertadores se pueden ver sometidos a una serie de disposiciones legales como la difamación, la protección de datos, el secreto comercial, la confidencialidad y las leyes de delitos informáticos.

El grado en el que las medidas existentes para proteger a los denunciantes mejoran esta situación varía dependiendo de las jurisdicciones. La ley de Divulgación de Interés Público en Reino Unido, por ejemplo, siempre ha excluido a los informantes que "cometiesen un delito" durante el curso de la denuncia. En cambio, la ley de Divulgación Protegida de Irlanda contempla que se pueda hacer una revelación presentándose como defensa "de cualquier delito que prohíba o restrinja la divulgación de la información".

Delitos informáticos

La legislación sobre delitos informáticos se enmarca de manera similar en todas las jurisdicciones, utilizando las definiciones del Convenio sobre Ciberdelincuencia. Esas leyes tipifican como delito el acceso a un sistema informático sin permiso, la interferencia con y para restringir el acceso a un sistema informático. Las leyes de delitos informáticos normalmente carecen de exenciones por interés público o por defensa.

En tanto, siguen creciendo las disposiciones sobre delitos informáticos, en particular las que prohíben el acceso no autorizado, contra los periodistas y sus fuentes. El denunciante de "Football Leaks", Rui Pinto, se enfrenta a un gran número de esos cargos. A los casos de Julian Assange y Glenn Greenwald conviene prestar una atención especial precisamente porque el uso de estas leyes parece restringir las libertades periodísticas⁹.

Además, existe un problema de larga data por el que la notificación de los problemas de seguridad informática, que pueden ser entendidos como un tipo de denuncia, suelen constituir una infracción técnica del derecho penal. Algunos países, como los Países Bajos, han tratado de hacer frente a este problema mediante el asesoramiento a los fiscales. Muchos argumentan que se necesita una reforma¹⁰.

Los denunciantes que tengan derecho a protección en virtud de las disposiciones de la Directiva pueden solicitar la desestimación de los procedimientos judiciales en base a una serie de motivos, entre los que se incluyen la difamación, la violación de los derechos de autor, la protección de datos y la divulgación de secretos comerciales.

Cuando se trata de la responsabilidad penal, la situación es un poco más complicada. La exclusión de la seguridad nacional del ámbito de aplicación de la Directiva (véase el capítulo 1) significa que las restricciones legales a la transmisión de información clasificada se mantienen. Además, la Directiva establece que hay una excepción para inmunidad general de procesamiento penal si la adquisición o el acceso a la información no constituye una ofensa

criminal en sí misma. Esta cláusula genera cierta incertidumbre. No es raro que la adquisición de la información en la que un alertador basa en su denuncia sea clasificada como un robo. Prevenir este tipo de procedimientos legales vejatorios -que fueron característicos del caso LuxLeaks - fue, de hecho, uno de los factores que impulsaron esta Directiva. De alguna manera, las disposiciones de la Directiva aclaran esta situación especificando que "el ataque físico o la piratería informática" sean tratados como casos en los que se debe aplicar la legislación nacional. Sin embargo, también se debería ser cuidadoso en este punto. El hackeo es un término que evoca inventiva, creatividad e indagación, pero a menudo se entiende, tal como se utiliza aquí, como una forma alternativa al uso no autorizado de un sistema informático, pero el acceso no autorizado en sí mismo es un concepto muy resbaladizo.

La naturaleza de los puestos de trabajo en 2020 supone que la mayoría de los casos de denuncia se refieren a información digital almacenada en un dispositivo o red. Lo que se califica como "robo" para socavar la reclamación de protección de un alertador podría igualmente enmarcarse en lo que se denomina "acceso no autorizado"^{vii}. Además, es probable que muchas divulgaciones relacionadas con la protección de datos o la red de seguridad, áreas que explícitamente abarca la Directiva, también puedan constituir infracciones de la legislación de delitos informáticos. Si la inmunidad no se extiende a estas áreas, los tribunales nacionales deberían poder considerar la necesidad y proporcionalidad de tales acciones en relación con la denuncia o la revelación pública en cuestión.

A fin de evitar la inseguridad jurídica, los países miembros deberían asegurarse al transponer la Directiva de que la noción de "un acto que constituye una ofensa criminal en sí mismo" se entienda y se defina como totalmente ajena a la capacidad de hacer una legítima divulgación de interés público.

Capítulo 4 ¿A quién ampara? (III)

La imagen más reconocible de un alertador es la de un individuo cuyas acciones le convierten en alguien diferente. Algunos lo admiran, otros lo critican, pero su decisión de dar un paso al frente lo hace diferente, de modo que su carácter y motivación son tan importantes como la información que saca a la luz.

Como los observadores habrán notado hay algo de autoperpetuación en esta imagen. Muchos de los que se deciden a denunciar se ven ante todo como profesionales que cumplen con su trabajo. Los individuos que trabajan en labores de auditorías o de supervisión del cumplimiento de las normas son ejemplos de los que tienen la obligación profesional de señalar las irregularidades con las que se topan.

A menudo, se asume el papel de objetor de conciencia que recibe una reacción negativa de compañeros y empleados, aunque irónicamente cuenta con el apoyo de personas ajenas¹¹.

En realidad, la denuncia de irregularidades no tiene por qué ser un esfuerzo en solitario. Los empleados que hacen los informes pueden tener aliados en su lugar de trabajo, que podrían proporcionar un oído atento, apoyar su interpretación de lo que está pasando o incluso haber hecho denuncias similares ellos mismos. Un posible alertador podría querer hablar con sus colegas antes de hacer su denuncia para confirmar información u obtener pruebas. La experiencia con los alertadores muestra que los colegas de trabajo, o los parientes cercanos son a menudo los primeros a los que acuden cuando tienen preocupaciones. Los que siguen adelante con la denuncia puede que incluso compartan lugar de trabajo con su cónyuge o pareja. En ese tipo de situaciones, cualquier represalia que se tome contra el denunciante podría tener efecto en las carreras profesionales de sus más cercanos. Resulta fácil ver cómo podría desalentar a algunos a denunciar.

La Directiva de la UE reconoce este tipo de situaciones y extiende las protecciones a ciertas categorías de terceros, ya sea porque están conectados con el alertador o porque están involucrados en el proceso de denuncia.

La protección que se ofrece a los individuos que denuncia se extiende a colegas y parientes, que pueden sufrir consecuencias negativas de esa denuncia. El abanico de grupos e individuos que se involucran en los casos de denuncia de irregularidades

VII. Para subrayar este punto, esto es exactamente lo que sucedió en el caso "LuxLeaks", donde los informantes Antoine Deltour y Raphael Halet fueron acusados de "fraude informativo", así como de "robo".

puede ser mucho más amplio, ya que puede alcanzar a sindicatos, periodistas y las organizaciones para las que trabajan, organizaciones profesionales, ONG, asociaciones comunitarias y otros grupos. La Directiva también establece algunas disposiciones para estos grupos, aunque de manera que cada Estado miembro de la UE tenga una gran influencia sobre cómo aplicar en la práctica estas protecciones en el proceso de transposición.

La Directiva se refiere explícitamente a los derechos de los trabajadores a consultar con representantes y sindicatos. Más allá de eso, hay una cláusula que otorga protección a los "facilitadores", definidos como "una persona física que asiste a un informante en el proceso de presentación de informes en un contexto laboral". Los análisis jurídicos de esta parte de la Directiva han expresado la preocupación de que esta cláusula restrinja la protección al facilitador al individuo que hace ese trabajo y deje fuera a la organización o la persona jurídica para la que trabajan o quién le ha contratado¹².

Si se adopta tal como está, esto podría significar que un individuo que trabaja para una ONG está protegido frente a las repercusiones jurídicas que pueda tener el haber aconsejado a un alertador, sin embargo, la propia ONG para la que trabaja no lo está. A un periodista se le puede conceder protección (además de las ya existentes en la legislación nacional, véase el capítulo 9 sobre la información pública), pero no al medio para el que trabaja. Los Estados miembro tal vez deseen considerar la posibilidad de incluir expresamente a los colaboradores o testigos en la definición de facilitadores.

Dado que los denunciantes a menudo discuten las preocupaciones con colegas de confianza en el trabajo antes de hacer una revelación, puede ser que como resultado de ello enfrenten algún tipo de represalia. Es por ello, que debería haber una garantía de que se dispone también de medidas de protección para ellos.

Como hemos visto, el idioma es una preocupación clave en la promoción de una cultura de transparencia y apoyo a los que hacen revelaciones (para más detalles, véase la sección *Lost in translation* del capítulo 1). Dado que el término "facilitador" es nuevo en este contexto, debe ser traducido cuidadosamente para evitar una connotación peyorativa.

El papel de la sociedad civil

Los facilitadores son una parte cada vez más importante del proceso de denuncia de irregularidades. Gran parte de la labor práctica de apoyo y asesoramiento a los alertadores de irregularidades en toda la UE la realizan organizaciones de la sociedad civil, que a su vez han presionado para conseguir esta legislación y han proporcionado la base informativa para apoyar esos esfuerzos.

Uno de los mejores ejemplos es la *Maison des lanceurs d'alerte* (MLA) de Francia, una organización sin fines de lucro, creada a través de una alianza de diferentes grupos activos en el campo de la transparencia y los derechos cívicos. La MLA comenzó su andadura tras la aprobación de la ley Sapin II, que ofrece protección legal a los denunciantes, pero adolece de marcos integrales de apoyo y asesoramiento. El MLA viene a llenar ese vacío.

En Irlanda Transparency International cumple un papel similar al proporcionar asesoramiento jurídico gratuito a los posibles denunciantes a través de su Transparency Legal Advice Centre (TCLA)

Capítulo 5 - ¿A quién dirige el alertador su denuncia?

La capacidad de los alertadores para elegir dónde hacer una denuncia, ya sea a su empleador, a un regulador externo o, en circunstancias más limitadas, a los medios de comunicación es un elemento clave de la Directiva.

Estos tres tipos diferentes de cauces de denuncia deben presentarse como una serie de opciones que un alertador puede elegir, más que como una jerarquía que fija un camino a seguir. Una característica esencial en cualquier implementación exitosa de la Directiva contemplará que los alertadores no estén obligados a hacer sus denuncias ante su empleador en primer lugar, sino que puedan recurrir a cualquier otro cauce.

Durante el proceso legislativo de aprobación de la Directiva, este tipo de restricción fue un tema particularmente polémico. Solo se consiguió descartar tras ingentes esfuerzos. Como resultado de ello, la Directiva deja a la libre elección de los alertadores dónde realizar la primera denuncia, ya sea en un canal regulador interno o en uno externo. También es posible hacer una primera denuncia ante la opinión pública o en un medio de comunicación, aunque con algunas restricciones (véase el capítulo 9).

Gran parte de las preocupaciones acerca de permitir a los denunciantes la elección de dónde hacer su reporte carecen de fundamento. La mayoría de los alertadores (muchos estudios indican que son un 90%¹³) hacen su primera denuncia a través de los cauces internos.

Si la capacidad de recurrir inicialmente a un regulador u otro organismo externo se vuelve crítica, son pocos los casos en los que un empleador probablemente no haga caso de una denuncia o, peor aún, penalice al alertador y destruya las pruebas tras ser avisado de una mala conducta.

Se puede llegar a incurrir en la obstrucción a la justicia¹⁴ si se concentran todas las comunicaciones e información relevante sobre las infracciones en manos de aquellos con capacidad para descartar la denuncia, ocultarla o modificarla y se insiste en la obligatoriedad de presentar una denuncia primero a nivel interno.

Un segundo problema potencial con los canales internos es que un gran número de casos de denuncia de irregularidades involucran a individuos que son penalizados por comunicar determinada información como parte de sus deberes laborales normales.

Aquellos que desempeñan labores de cumplimiento de normas, auditoría, salud y funciones de seguridad a menudo tienen que someterse a una serie de requisitos legales para poder informar de los problemas con los que se encuentran y entre sus funciones pueden que incluyan responsabilidades similares. La creación de un canal protegido específico para las revelaciones de los alertadores no debe crear una expectativa diferente a otros canales de valor similar en otros lugares.

Lo que las organizaciones de incidencia política llaman “duty speech”^{viii} debe estar explícitamente protegido, como así ha sido para los funcionarios del Gobierno de Estados Unidos desde que se aprobó una mejora de la Ley de Protección del Denunciante en 2012. Si bien el Considerando 62 de la Directiva contempla la protección del deber de reportar, ello no queda explicitado en los artículos principales de la legislación. Los Estados miembros deberían considerar la posibilidad de aclarar este aspecto en la transposición a fin de evitar incertidumbre jurídica.

La Directiva permite a los países miembros fomentar la presentación de denuncias internas, pero no a expensas de que se proporcione información completa al denunciante sobre cómo podría hacer la denuncia por otra vía. La Directiva también regula la creación y el funcionamiento de canales externos, que estarán operados por autoridades competentes.

Los Estados miembros tienen la facultad discrecional de decidir cuáles son esas autoridades competentes y ya hay varios modelos diferentes que se están utilizando en toda la Unión Europea. Esto se analiza con más detalle en el capítulo 8.

VIII. En la presente publicación, traducido como el “deber de reportar”

Aun cuando no es obligatoria, la Directiva da a los Estados miembros la opción de establecer una autoridad nacional dedicada a proteger a los alertadores. Este organismo podría constituirse en un canal externo básico para recibir, investigar y hacer seguimiento de divulgaciones (véase el capítulo 8) o como órgano de evaluación del funcionamiento práctico de la legislación (véase capítulo 14), así como una fuente de información para potenciales denunciadores.

Independientemente de la forma en que se constituyan esos canales, un requisito fundamental de la Directiva es que se facilite información sobre cómo los alertadores pueden hacer una denuncia y los diferentes lugares en los que podrían hacerlo. Los canales internos están obligados a proporcionar información sobre las alternativas externas. Las autoridades competentes que gestionan los canales externos están obligadas a ofrecer información completa sobre los procedimientos de denuncia y lo que las personas que alertan deberían poder tener a su disposición: “una sección independiente y de fácil acceso” de un sitio web público.

Capítulo 6 - ¿Quién necesita establecer un canal interno?

Una de las principales características proactivas de la Directiva es la obligación de los empleadores de implantar canales de denuncia internos (o, en determinadas circunstancias, contratar a un tercero para que lo haga). Esta disposición de la Directiva es probable que sea uno de los factores de mayor impacto y tiene el potencial de influir significativamente en la cultura corporativa y la ética del trabajo en toda la Unión Europea.

Los próximos dos capítulos se centran en quién necesita implantar un canal de denuncias y cómo debería hacerlo. En general, la Directiva estipula que cualquier entidad legal o del sector privado que cuente con 50 empleados o más tendrá que establecer mecanismos internos de recepción y seguimiento de denuncias.

Se aplican normas especiales a las empresas o entidades con una plantilla de entre 50 y 249 empleados. Podrán compartir los recursos y las configuraciones de los canales de denuncia con otras empresas a fin de mantener los costos internos a un nivel razonable.

Además, teniendo en cuenta que puede haber motivos para exigir medidas especiales en los sectores de alto riesgo, el texto de la Directiva permite a los Estados miembros introducir obligaciones más estrictas cuando sea necesario, por ejemplo, para organizaciones en los sectores del medio ambiente o la salud.

Cuando los Estados miembros deseen ampliar las obligaciones de sus canales internos están obligados a notificarlo a la Comisión Europea con un escrito en el que se razone la medida y los criterios en los que basan su evaluación. En los casos en los que las empresas y entidades privadas ya tengan la obligación legal de establecer canales internos de denuncias bajo otras regulaciones legales a las de la Unión Europea o por la legislación nacional, la Directiva no introduce un estándar más bajo.

Con la intención de reflejar el amplio alcance de las relaciones de trabajo que contempla la Directiva (véase capítulo 2), la legislación prevé que el canal de denuncias interno de una organización también esté abierto a un grupo más amplio que a los propios empleados. Los trabajadores de una entidad legal deben poder hacer una denuncia a través de un cauce interno, pero también los empleados de sus filiales, proveedores y cualquier otra persona que haya adquirido información en el contexto de su trabajo o sus actividades laborales relacionadas con la entidad jurídica en cuestión^X.

Las entidades jurídicas del sector público tienen la responsabilidad de crear e instalar mecanismos internos de denuncia de irregularidades para sus empleados; se hace una consideración especial de las organizaciones del sector público en los municipios con menos de 10.000 habitantes, que pueden estar exentos de esta responsabilidad.

La Directiva permite que terceros gestionen la recepción e investigación de las denuncias. Es probable que aumente la oferta de este tipo de servicios de terceros a medida que las disposiciones de la Directiva se vayan introduciendo en la legislación nacional. La participación de terceros genera inquietud en varios frentes. Uno de los temas que preocupa es si la subcontratación de canales de

X. Las ONG no han sido mencionadas explícitamente en la directiva, pero sería mejor considerarlas como un subconjunto de entidades jurídicas del sector privado.

denuncia va a significar que los empleadores puedan evitar comprometerse de manera significativa con las denuncias y si ello tendrá como consecuencia un cambio cultural limitado precisamente en las industrias donde más se necesita.

Otra de las preocupaciones que ha surgido es si el servicio comercial de canales de denuncia podría sufrir un conflicto de interés y no ser capaz de manera imparcial, lo que conduciría a una falta de confianza y a un posible perjuicio de los alertadores.

Según contempla la directiva, los proveedores de fuera de la entidad o la empresa están obligados a cumplir con la misma protección de datos y normas de confidencialidad como los cauces equivalentes operados directamente. Se debería considerar, además, si conviene establecer una serie de normas mínimas a fin de evitar conflictos de intereses.

Capítulo 7 – Cómo deberían ser los canales internos

La Directiva abre nuevos caminos al establecer procedimientos para la denuncia de irregularidades dentro de las organizaciones y normas básicas sobre cómo deben realizarse las investigaciones. La legislación también reconoce la importancia de los mecanismos de comunicación que permiten un seguimiento con los informantes. Este extremo refuerza la confianza del público en los esquemas de denuncia de irregularidades en general, lo cual es crucial para la aplicación efectiva de la Directiva.

De las disposiciones de la Directiva se desprende claramente que los alertadores de irregularidades deben poder presentar una denuncia por diferentes vías. La Directiva exige que las entidades jurídicas públicas y privadas con más de 50 empleados creen canales internos y mecanismos que permiten presentar una denuncia “mediante contacto personal, por correo, a través de un buzón físico destinado a recoger denuncias, por teléfono o a través de una plataforma en línea (intranet o internet)”.

Las organizaciones están obligadas a designar personas o departamentos imparciales para recibir y gestionar las denuncias, y se espera que las personas que estén al frente de la gestión de estos canales mantengan el registro correspondiente y la comunicación con el alertador. Una persona que presenta una denuncia tiene derecho a que se acuse recibo de su reporte en un plazo de siete días y a recibir respuesta en un plazo de tres meses. Los Estados miembros pueden optar por acortar el plazo para la denuncia en casos seleccionados o de forma general.

Además, estos cauces internos deberían permitir a los informantes comunicar sus preocupaciones de manera segura. Asimismo, deberían configurarse de forma que mantengan la confidencialidad tanto de la identidad de los alertadores como de otras personas que presenten denuncias. Las normas básicas de confidencialidad están en consonancia con otros reglamentos de la UE sobre el tratamiento de la información personal, en particular la RGPD. Los canales internos deben reflejar esas regulaciones.

Una de las principales deficiencias de la Directiva en general, y que es contraria a las recomendaciones internacionales, es que los canales internos no están obligados a permitir que las denuncias se hagan de forma anónima. El papel de la divulgación anónima se ha convertido en un tema destacado, particularmente en la última década debido a la irrupción de buzones digitales seguros. Esta importante cuestión se examina más a fondo en el capítulo 10.

Otros requisitos que la Directiva hace opcionales para los canales internos operativos podrían marcar la diferencia en cuanto a la efectividad. Aunque se reconoce la necesidad de que los responsables de gestionar las denuncias tengan una formación adecuada, la Unión Europea no ha esbozado en detalle ninguna norma mínima al respecto. En todo caso esto sí es obligatorio para los que operan canales externos.

Los Estados miembros deben asegurarse de que la legislación aprobada en la transposición de la Directiva establezca unas normas mínimas para que los técnicos de integridad procesen las revelaciones de los denunciadores de manera correcta y eficiente. Al mismo tiempo, esas leyes deben asegurar que estos empleados cuenten con un estatuto organizativo que les impida convertirse ellos mismos en un objetivo, y que todas las acciones lícitas llevadas a cabo por los técnicos de integridad estén protegidas.

De manera similar, si bien existe el requisito de que quienes operan los canales internos mantengan registros con fines académicos, no hay obligación alguna de mantener o publicar estadísticas sobre el número de denuncias recibidas ni el resultado de las

investigaciones. Los empleadores tal vez deseen considerar la posibilidad de hacerlo como un medio de demostrar que sus medidas están funcionando como se pretendía.

Además, la directiva prevé que la información sobre la disponibilidad y funcionalidad de los cauces internos de denuncias se comunique de manera eficaz y que los empleados tengan acceso a la información necesaria para utilizarlos correctamente.

Como ejemplo de cómo han funcionado en la práctica los canales internos de presentación de denuncias, los Estados miembro pueden mirar a Italia. La Ley italiana del 30 de noviembre de 2017, n. 179 requiere que las administraciones públicas pongan en marcha mecanismos internos de información. Actualmente hay más de 600 administraciones públicas que utilizan buzones digitales seguros en sus sistemas internos para denuncias y estos se basan en tecnología de fuente abierta, que es fácil de usar y de reproducir.

Los buzones facilitan las revelaciones anónimas y los operadores han adquirido experiencia en cómo estructurar las interfaces de usuario para obtener información procesable. La experiencia italiana pone de relieve el valor de establecer mecanismos digitales que proporcionen una mejor seguridad no sólo para los empleados que podrían querer hacer una denuncia, sino también para los gestores involucrados y la información en sí misma.

Buzones digitales seguros

La implantación del buzón digital seguro es uno de los avances más importantes en el contexto de las denuncias de la última década. La expansión del uso de estos buzones digitales seguros ha ido aparejada con el desarrollo de las protecciones legales. En la actualidad, el proyecto *GlobaLeaks* -desarrollado por el Centro Hermes para la Transparencia y los Derechos Humanos- y el sistema *SecureDrop* de la Fundación para la Libertad de Prensa, son los dos sistemas de buzones digitales seguros más conocidos y más ampliamente utilizados.

Aunque los primeros en adoptar estos sistemas de buzones fueron medios de comunicación, un número creciente de entidades del sector público y privado están optando por instalar este tipo de mecanismos, que se basan en una tecnología segura, encriptada, de código abierto y que permite el anonimato. Esta tecnología ofrece varias ventajas, entre ellas la posibilidad de una comunicación bidireccional entre los informantes y los gestores del sistema, así como el almacenamiento de documentos.

Los buzones digitales se han adaptado y desarrollado para satisfacer los requisitos, tanto de medios de comunicación diferentes como *Il Sole 24 ore* en Italia o *Mexicoleaks* en México, como de entidades como la Corte Penal Internacional y la Oficina Antifraude del Ayuntamiento de Barcelona en España. Grandes empresas como Edison o GruppoFalk también están utilizando mecanismos digitales seguros de denuncia.

Cuando se informa y publicita adecuadamente, los buzones seguros parecen ser el cauce preferido para comunicar infracciones. En su memoria de 2019¹⁵, la Agencia Antifraude valenciana señala que una abrumadora mayoría del 76% de las denuncias fueron recibidas a través de su buzón digital seguro. Sólo el 15% se efectuó por el Registro General y el 10% a través del correo electrónico. A su vez, el 51% de las 168 denuncias presentadas en 2019 se hizo de forma anónima.

Capítulo 8 – Cómo deberían configurarse los canales externos

Además de establecer el requisito de introducir canales internos de denuncia de irregularidades, la Directiva obliga a los Estados miembros a establecer mecanismos que permitan a los alertadores plantear sus preocupaciones directamente a los organismos reguladores o a las autoridades competentes.

La Directiva concede a los países miembros un margen importante para decidir qué constituye una autoridad competente. Los Estados Miembros pueden designar como competente a cualquier autoridad nacional, siempre que esté equipada para cumplir con las disposiciones de la Directiva sobre la recepción, el seguimiento y la respuesta a los denunciadores. Algunas naciones de la Unión Europea ya adoptaron diferentes estructuras para sus canales externos, y éstas se examinan con más detalle a continuación.

A pesar de la amplia discreción en este ámbito, los reguladores de la UE han incluido específicamente "instituciones pertinentes, órganos, oficinas u organismos de la Unión" como receptores elegibles para las denuncias externas. Dado que se puede recurrir a instituciones de la Unión Europea, inclusive organismos como la Comisión Europea y la Oficina Europea de Lucha contra el Fraude (OLAF), puede ser conveniente crear una situación similar para las instituciones nacionales cuando se transponga la Directiva a la legislación nacional.

Los denunciadores son libres de elegir si hacen sus revelaciones por la vía interna o externa, y los países tienen que garantizar que los denunciadores tengan acceso a medidas de protección y apoyo iguales en ambos procedimientos. Esto significa que haya similitudes en cuanto a los requisitos de presentación de denuncias en canales internos y externos, sobre todo en lo referente a la seguridad de los datos, la gestión de las denuncias y la comunicación con los alertadores. Tanto los canales internos como los externos deben garantizar la confidencialidad de la identidad de la persona informante, y los funcionarios tienen obligaciones similares: las de proporcionar a los denunciadores información sobre las investigaciones en curso.

Además, las autoridades competentes que operan canales externos deben proporcionar información online sobre las formas de denunciar, los procedimientos, los derechos y los límites de la protección. El personal que admite y maneja las denuncias debe recibir una formación específica, y los canales tienen que estar diseñados de forma que sean fáciles y seguros de usar y permitan asimismo el almacenamiento de información.

Al mismo tiempo, las leyes de transposición deben tener en cuenta la función particular de técnicos e investigadores que denuncien la existencia de un delito, e incluir derechos que les protejan de las represalias, así como una definición precisa de funciones y responsabilidades.

Las normas adicionales que se aplican a los mecanismos de presentación de denuncias externas sólo se refieren al mantenimiento de registros y la supervisión de medidas.

Las autoridades competentes tienen que revisar sus mecanismos de presentación de denuncias cada tres años y, si es necesario, adaptarlos. Los Estados miembros tienen que informar regularmente a la Comisión Europea sobre ello (véase el capítulo 14).

Teniendo en cuenta que los canales externos podrían recibir un volumen significativo de denuncias, la Directiva incluye disposiciones sobre el tratamiento de las denuncias repetitivas o triviales, así como sobre los procedimientos de selección para tratar las denuncias más graves primero. Los reglamentos nacionales basados en las disposiciones de la Directiva deben diseñarse de manera que se evite el abuso de estas exenciones.

En este contexto son importantes definiciones claras sobre qué infracciones pueden considerarse menores y por tanto ser ignoradas por las autoridades, una regulación de lo que sucede cuando se retrasa una investigación, así como normas para priorizar las denuncias si el volumen recibido es alto.

Se debe prestar más atención a las normas relativas al establecimiento de canales y procedimientos de presentación de denuncias a fin de garantizar que se respete la confidencialidad en todo momento, y que las sanciones por violación y negligencia sean creíbles y disuasivas. Las disposiciones acertadas en esta área refuerzan considerablemente la confianza de la población en las medidas de protección que se ofrecen, lo cual es importante a su vez para asegurar el objetivo general de la Directiva.

Definir autoridades competentes

Los requisitos de la Directiva permiten a los países miembros cierta flexibilidad a la hora de decidir cómo se van a estructurar los canales de denuncias. Una opción sería asignar a los distintos organismos nacionales responsabilidades para recibir y gestionar denuncias en sus respectivas áreas.

Siguiendo los ejemplos de Reino Unido e Irlanda, esto podría incluir el nombramiento de “personas designadas” de entre las oficinas de regulación existentes. Los alertadores podrían recurrir a los servicios de personal capacitado dentro de los organismos más adecuados para tratar su preocupación.

Los sistemas de “personas designadas” pueden indicar muchas organizaciones que pueden recibir las denuncias y puede no quedar claro cuál es la autoridad especializada es la apropiada en cada caso. Las experiencias del Reino Unido e Irlanda han demostrado que la capacidad de responder eficazmente a las denuncias puede variar enormemente entre los organismos reguladores.

Otros esquemas de protección de los denunciantes existentes utilizan un enfoque más centralizado: En los Países Bajos, los denunciantes pueden dirigirse a la Autoridad Holandesa de Denunciantes (Huis voor Klokkenluiders). Esta autoridad pública fue fundada en 2016 no solo con el fin de publicar información sobre los derechos de los denunciantes, sino también para recibir e investigar denuncias en coordinación con otras autoridades pertinentes. También tiene una función de supervisión general que fomenta las mejores prácticas en otras organizaciones.

Las evaluaciones iniciales de la actuación de esta entidad holandesa en sus primeros años de existencia han constatado en general que sus objetivos eran demasiado ambiciosos, especialmente en lo que respecta a su función de investigación.

Existe la alternativa de que los Estados miembros puedan decidir fusionar las disposiciones sobre denuncias externas de irregularidades con las estructuras existentes, como las oficinas anticorrupción o antidiscriminación, muchas de las cuales ya tienen en marcha ciertos mecanismos para defender los derechos de los ciudadanos.

Francia ha designado la oficina del *défenseur des droits*, una autoridad constitucional independiente que defiende los derechos y las libertades individuales en diferentes áreas, como una de las instituciones públicas en las que los alertadores pueden hacer llegar sus denuncias. Este planteamiento reduce significativamente el umbral para potenciales alertadores que busquen consejo.

En Italia, el Organismo Nacional Anticorrupción ANAC constituye una de las autoridades públicas a la que los denunciantes pueden recurrir directamente. Además, la institución también proporciona orientación y apoyo a la ética de funcionarios encargados de recibir las denuncias en otras instituciones, lo que contribuye en la práctica a garantizar una cierta coherencia en todas las organizaciones. Las operaciones del organismo italiano se financian en su mayor parte con los ingresos procedentes de las tasas que las entidades privadas pagan cada vez que solicitan una licitación pública.

Puede obtenerse más información sobre los aspectos prácticos de la protección institucionalizada de los denunciantes de irregularidades en la recién formada Red de Autoridades Europeas de Integridad y Denuncia (NEIWA). Establecida en 2019, NEIWA tiene el objetivo de intercambiar conocimientos prácticos sobre la protección institucionalizada de denunciantes de irregularidades y la promoción de la integridad.

En esta etapa, la red cuenta con 15 organizaciones contribuyentes de 13 países europeos diferentes, entre ellas la Agencia Italiana Anticorrupción (ANAC), la Autoridad Holandesa de Denuncias y la francesa *Défenseur des Droits*. Para determinar su misión, los miembros de NEIWA firmaron la Declaración de París¹⁶ en diciembre de 2019.

La autoridad independiente del denunciante: cómo funciona

Las buenas prácticas internacionales respaldan firmemente que las medidas de protección de los alertadores vayan acompañadas por el establecimiento de una autoridad que se dedique a ello. La directiva sugiere que tal institución podría funcionar como primer punto de referencia para los denunciantes y como centro de información.

Una opción es también convertirla en la receptora principal de las denuncias y dotarla de la capacidad para realizar las investigaciones iniciales y que las pueda remitir a otras autoridades si es necesario. La idea de albergarlo “todo bajo el mismo techo” asegura que todos los alertadores tengan acceso a la misma información pública y que puedan confiar en que los procedimientos y los conocimientos técnicos serán iguales cuando hagan consultas. Asimismo, se proporciona una mayor certeza jurídica, ya que los denunciantes se ven liberados de la carga de evaluar cuál sería la autoridad competente para su preocupación.

A todo ello se suma que un enfoque centralizado facilita considerablemente la supervisión y evaluación de las medidas adoptadas y garantiza la igualdad de tratamiento mediante la coherencia de los procedimientos, la capacitación del personal y la gestión de los conocimientos.

Los Países Bajos se convirtieron en el primer país de la UE en introducir una autoridad nacional de denuncia de irregularidades 2016¹⁷. Y lo hizo en un plazo de tres meses a partir de la aprobación de la ley. Las tareas de la institución son tres: promover medidas preventivas en las instituciones gubernamentales y empresas, apoyándolos con la introducción de medidas para la protección e integridad de las personas que señalen infracciones; asesorar y consultar a los posibles alertadores y recibir sus denuncias; y poner en marcha investigaciones tanto de las actividades irregulares como de las represalias, centrándose sobre todo en estas últimas. Entre los poderes formales de que dispone figura una variedad de medidas para permitir el acceso a la documentación pertinente y a los edificios relacionados con las investigaciones, así como a tomar testimonio bajo juramento a las personas involucradas.

En 2018, las operaciones de la Autoridad Holandesa de Denunciantes funcionaron con un presupuesto de 3 millones de euros, empleando a una plantilla de 15 funcionarios públicos que atendieron un total de 365 solicitudes de asesoramiento. Menos del 10% de estos casos se referían a infracciones actuales, y entre su establecimiento en junio de 2016 y diciembre de 2018, se han iniciado un total de 19 investigaciones¹⁸.

La autoridad holandesa reporta anualmente al Parlamento. Tres años después de su puesta en marcha, la experiencia ha demostrado que vale la pena tomarse un tiempo para instalar una institución de este tipo. Según la propia evaluación de la Autoridad, el rápido lanzamiento en apenas tres meses dio lugar a algunos problemas, ya que las estructuras y los procedimientos se resintieron por la falta de claridad. Es por ello que recomienda emplear el tiempo suficiente para establecer los procedimientos de denuncia de infracciones y adoptar un enfoque holístico e integral. Además, es importante proporcionar una financiación adecuada, así como capacitación.

Capítulo 9 – Revelaciones a los medios

Para muchos, denunciar es sinónimo de periodismo. Es cierto que, sin la confidencialidad de las fuentes, mucho periodismo, y especialmente el periodismo de investigación, sería imposible. El Consejo de Europa reconoce que los alertadores de infracciones tienen su derecho a la libertad de expresión y su contribución es necesaria para que los periodistas cumplan su "papel de guardianes" en las sociedades democráticas.

En la actualidad, que la denuncia de irregularidades sea vista como un problema se debe a que los alertadores actúan como fuentes de periodistas. El reconocimiento de la importancia de la denuncia por su interés público ha sido enormemente valioso, aunque las principales divulgaciones del tipo "Panama Papers" representan sólo una pequeña parte de los casos de denuncias.

La importancia de la relación periodista-fuente también puede oscurecer determinados tipos de revelaciones públicas que no son mediadas por periodistas. En la era de las redes sociales cada vez es más frecuente que se hagan públicas directamente en estos medios informaciones que han sido ocultadas.

La Directiva no define qué constituye una divulgación pública. Aunque gran parte del debate sobre las revelaciones se centra en la relación entre los denunciadores y los periodistas, no hay nada que diga que los periodistas tienen que estar necesariamente involucrados en tales divulgaciones. La publicación directa, la publicación de un artículo de opinión, la entrada en un blog o en una red social, también deben ser entendidas como formas de hacer públicas revelaciones.

Revelaciones directas

La pandemia de COVID 19 ha puesto de relieve la información que se publica directamente en las redes sociales.

Los denunciadores del sector de la salud de muchos países se han enfrentado a medidas disciplinarias y otras sanciones por hablar de la escasez de medios y de los peligros que enfrentaban en sus puestos de trabajo¹⁹.

Las leyes de protección de alertadores en vigor no siempre han demostrado ser las adecuadas para proteger a las personas en esta posición, ya que expresar preocupaciones u observaciones en redes sociales no suele estar considerado como una divulgación pública protegida.

La legislación postcoronavirus debería prestar atención especial a este ámbito y asegurarse de que los profesionales interesados no sufran represalias por expresar su opinión o sus preocupaciones sobre amenazas inmediatas a la salud y la seguridad públicas.

La Directiva ofrece un margen considerable para establecer disposiciones equilibradas. Si la transposición no es adecuada en esta área, es probable que tenga un efecto disuasorio en posibles alertadores.

Proteger la fuente en la era digital

La importancia de los alertadores en el proceso periodístico se contraponen a la reiterada falta de protección dentro de ese proceso. Tradicionalmente, los denunciantes se han visto obligados a confiar en la capacidad de los periodistas de proteger sus fuentes, con poca seguridad si eso fallara.

En algunas jurisdicciones, los periodistas están protegidos por ley contra la revelación de sus fuentes. Sin embargo, la protección de las fuentes es una cuestión tanto práctica como jurídica. Y eso es así cada vez más, sobre todo en una época en la que las comunicaciones electrónicas y los poderes de control hacen más vulnerable la seguridad de las conversaciones entre los periodistas y sus fuentes.

Si bien la vigilancia gubernamental ha recibido una enorme atención, el aumento de la vigilancia en el puesto de trabajo da lugar a planteamientos similares. Los periodistas deben ser capaces de comprender estos riesgos y ayudar a sus fuentes a hacer sus propias evaluaciones^X. Precisamente teniendo en cuenta el riesgo que se corre en este entorno, es importante la protección del denunciante.

Protecciones de revelaciones públicas

La Directiva de protección del denunciante de la UE prevé que la mayoría de los casos no se hagan públicos en primera instancia, pero sí contempla la posibilidad de informar a la población, aunque de manera más restringida que yendo a un empleador o a un regulador.

Debe decirse que los términos de la Directiva no son particularmente permisivos en lo que se refiere a hacer públicas las denuncias. Las revelaciones públicas de infracciones se harán "en casos de urgencia y peligro manifiesto para el interés público o cuando exista un riesgo de daños irreversibles, incluidos, entre otros, peligro para la integridad física".

La Unión Europea considera que la denuncia de irregularidades está vinculada en primer lugar a un contexto laboral. Sin embargo, en otros países, como por ejemplo Estados Unidos, este tipo de denuncias están más ligadas con los derechos esenciales de la libertad de expresión.

Las infracciones que se deciden hacer públicas también están protegidas en situaciones en las que han intentado otros canales de denuncia y no se han tomado las medidas adecuadas en el plazo establecido. En los considerandos de la Directiva se aclara que esto abarca situaciones en las que se han realizado investigaciones, pero no se han adoptado medidas correctivas adecuadas.

Si una denuncia se ha evaluado erróneamente como de menor importancia y se ha cerrado una investigación sobre esa base, los considerandos sugieren que esto puede ser una razón para hacerla pública. Allí donde las leyes nacionales ya ofrecen una mayor protección, estos casos no se ven afectados por la directiva. Así es, por ejemplo, en Suecia, donde la protección de la fuente está garantizada constitucionalmente.

Términos como "peligro inminente o manifiesto" ponen relativamente alto el listón para hacer divulgaciones públicas y la Federación de Periodistas ha criticado estas cláusulas de la Directiva por considerarlas "gravosas y laberínticas"²⁰. Al igual que con otros aspectos de la Directiva, los Estados miembros tienen la libertad de introducir normas más permisivas. Pueden atribuirse el mérito de revisar los límites que pone la Directiva a las revelaciones públicas a la luz de las cuestiones prácticas planteadas por el COVID-19.

X. Para saber más sobre cómo los periodistas deberían trabajar con whistleblowers en la era digital, véase Blueprint's Perugia Principles (2019)

Capítulo 10 – Confidencialidad y anonimato

La confidencialidad y el anonimato son aspectos clave de la protección de los denunciantes. Son conceptos distintos y diferentes. Los requisitos de confidencialidad anticipan una situación en la que la identidad de un alertador es conocida por individuos específicos que tienen el deber de no permitir que se conozca más ampliamente.

El anonimato es diferente. Si la identidad de un alertador es anónima, no se conoce en absoluto. Esto ofrece protección a la persona que denuncia contra cualquier incumplimiento del deber de confidencialidad y no fuerza a los alertadores a depositar excesiva confianza en el sistema.

Denuncias Anónimas y buzones online seguros

La tecnología ha supuesto un punto de inflexión en la denuncia anónima. La introducción de los buzones anónimos online, que utilizan la encriptación y otras tecnologías de mejora de la privacidad para ocultar la identidad de la persona que hace la revelación, ha dado lugar a una serie de revelaciones en los medios de comunicación.

Hoy en día, los buzones anónimos están siendo empleados por los reguladores, el Gobierno y los medios de comunicación.

A diferencia de otros métodos anónimos, los buzones permiten continuar la comunicación con la persona que presenta la denuncia, tal como requiere la Directiva. Cuando hay preocupaciones sobre la seguridad o la falta de fe en el procedimiento, el anonimato es una buena manera de animar a la gente a reportar infracciones.

Según una encuesta realizada en 2019 a empresas de Alemania, Suiza, Reino Unido y Francia, en las empresas donde se aceptaban denuncias anónimas, un 58 por ciento de las denuncias optaron por hacerlo de esa vía. Sin embargo, en alrededor de un tercio de estos casos, las personas que hicieron la denuncia no permanecieron en el anonimato, sino que revelaron voluntariamente su identidad en el curso de una investigación.

En todos los casos, la tasa de denuncias falsas o malintencionadas se mantuvo baja, entre el 3% y el 12%²¹.

La Directiva contiene un compromiso firme sobre el anonimato, para garantizar que a los alertadores que hacen los señalamientos de forma anónima no se les prive de protección. Si la identidad de alguien que ha hecho una denuncia anónima se conoce, esta persona tiene derecho a la misma obligación de confidencialidad y protección contra represalias que los alertadores que han empleado otros cauces.

Más allá de este compromiso, la Directiva sugiere que los Estados miembros consideren la posibilidad de exigir a los canales externos que tramiten e investiguen las denuncias anónimas que reciban. Esta obligación ya existe en Italia y Australia. Además, el 75% de las empresas holandesas encuestadas por Transparencia Internacional en 2019 dijeron que los empleados podían hacer denuncias internas de forma anónima²².

Las buenas prácticas internacionales recomiendan siempre que se ofrezca la opción de la notificación anónima, a fin de fortalecer a los denunciantes y la confianza del público. Los Estados miembros deberían evitar la introducción de estructuras de denuncia de irregularidades que permiten ignorar los reportes anónimos, ya que esto puede conducir a escenarios en los que al final no se aborde información importante sobre brechas particularmente peligrosas.

El deber de la confidencialidad

El deber de la confidencialidad es una parte clave de la Directiva, que establece normas sobre cómo debe funcionar y un muy limitado número de excepciones. La experiencia demuestra que los canales de información que no cumplen con este deber de confidencialidad hacen más daño que otra cosa y a menudo hacen a los denunciantes aún más vulnerables a las represalias de lo que podrían ser de otra manera.

Hay muchos ejemplos de canales externos que fallan en este sentido. La incapacidad de garantizar la confidencialidad puede ser sintomático de un problema más amplio, como que los reguladores están demasiado cerca de las industrias que deben supervisar y carecen de la suficiente independencia.

La Directiva establece normas detalladas sobre el tratamiento de los datos personales y la necesidad de que éste se limite a personas autorizadas. Quienes operan los canales de denuncias tienen la responsabilidad de cumplir las normas de protección de datos de la UE, con el propósito de la recopilación de información en este contexto y a fin de asegurar que una investigación pueda llevarse a cabo adecuadamente.

La confidencialidad se aplica no solo a los datos personales, sino también a otra información a partir de la cual la identidad del informante se podría deducir. Esta es una categoría más amplia que el concepto estadounidense de Información de identificación personal, que se limita esencialmente a la información que identifica directamente a un individuo, como su número de la seguridad social o sus detalles bancarios. Las disposiciones de confidencialidad de la Directiva se extienden a otras personas involucradas, como las personas implicadas por un denunciante, así como facilitadores y partidarios.

La Directiva estipula sanciones para quienes incumplan este deber de confidencialidad. Esa sanción debería ser "eficaz, proporcionada y disuasoria" pero, como el resto de las cláusulas de penalización de la Directiva, se deja en manos de los Estados miembros determinar exactamente lo que ello implica.

Ya existen diferentes enfoques dentro de la UE. La Ley de Divulgación Pública de Irlanda da lugar a que se tomen medidas legales si los alertadores sufren un perjuicio debido a que se ha revelado su identidad.

La ley Sapin II de Francia tipifica la violación de la confidencialidad como un delito penal que se castiga con una multa o una pena de hasta dos años de prisión.

Hay excepciones limitadas del deber general de confidencialidad, como consecuencia de la investigación de un reporte o de la aplicación de medidas judiciales en procedimientos relacionados con una denuncia. La identidad de un alertador puede ser revelada si éste da su consentimiento explícito o si se evalúa que sea "necesaria y proporcionada" a efectos de la investigación, en el contexto de la legislación nacional.

En este caso, el denunciante debe recibir una notificación y una explicación por escrito. Aunque no está explícitamente previsto en la Directiva, los Estados miembros tal vez deseen considerar la posibilidad de dar a los alertadores la capacidad de impugnar esas decisiones, con suficiente antelación para que se les permita hacerlo.

El funcionamiento de estas exenciones depende en gran medida de los marcos jurídicos nacionales y de los derechos de cualquier persona o entidad que es objeto de una denuncia, por ejemplo, el derecho a ver su propio expediente. Los Estados miembros deben referir las obligaciones jurídicas pertinentes al incorporar esas disposiciones a la legislación nacional.

Capítulo 11 – La protección legal al denunciante

Como en cualquier marco legal de protección a los alertadores, las disposiciones reales para proteger a los denunciantes del sufrimiento de perjuicio por hacer una divulgación constituyen una piedra angular de la Directiva. En general, la ley estipula que se prohíben todas las formas de represalia, así como los intentos de represalia, siempre que los denunciantes hayan hecho su divulgación en la forma prescrita.

En el artículo 19 de la Directiva se incluye una amplia lista de los tipos de represalias que pueden sufrir los denunciantes. Se incluyen las formas más comunes de acciones de represalia a las que se enfrentan a menudo las personas que señalan infracciones, como la suspensión del empleo, la modificación o eliminación de sus funciones o el cambio de las condiciones de trabajo, el acoso y la discriminación, pero también medidas que reflejan diferentes relaciones de trabajo amparadas por la Directiva, como los boicots del sector que dificultan encontrar un nuevo empleo, daño a la reputación y no renovación de contratos o permisos. Esta lista no es exhaustiva.

Los Estados Miembros deben asegurarse de que las variedades informales y sociales de represalias estén incluidas en su definición. A pesar de que la lista de ejemplos de la Directiva no es exhaustiva, es posible que algunas medidas de represalias no puedan ser reconocidas como tales. Debido a su naturaleza interjurisdiccional, la extradición no siempre se entiende como una forma de represalia, a pesar del aumento de su uso tanto contra alertadores como contra los periodistas²³.

Otras formas comunes de represalia no incluidas en la Directiva se refieren a la negativa a proporcionar capacitación, asignación de funciones que no se ajustan a las calificaciones del candidato, o traslado a lugares que no puede aceptar. Dado que la lista de medidas de represalia sólo está limitada por la imaginación, los Estados miembros tal vez deseen considerar la transposición de la Directiva de tal manera que se considere explícitamente cualquier forma de discriminación contra los alertadores como sancionables.

Además de la prohibición de las represalias, la Directiva incluye otras disposiciones destinadas a reforzar la posición legal de los denunciantes. En primer lugar, incluye una exención de responsabilidad respecto de la presentación de denuncias o la adquisición de información, lo que significa que los alertadores no pueden ser procesados por incumplimiento de las obligaciones profesionales de secreto o acuerdos similares, incluidas las políticas del lugar de trabajo, al hacer un informe de acuerdo con la Directiva.

Además, los derechos y recursos previstos en la Directiva no pueden ser objeto de renuncia o derogación en ningún tipo de acuerdo, incluyendo acuerdos de conciliación y de no divulgación. Si bien los acuerdos de confidencialidad son herramientas indudablemente importantes para crear un ambiente profesional confiable, las experiencias del Reino Unido subrayan la importancia de considerarlos de tal manera que no contradigan las medidas de protección de los alertadores²⁴.

En segundo lugar, de acuerdo con las mejores prácticas internacionales, la ley incluye una inversión de la carga de la prueba: el perjuicio que sufren los denunciantes se supone a priori que es en represalia por un reporte o una revelación pública realizada. Esto significa que si un caso que involucra a un denunciante termina en un proceso legal, es el empleador quien debe mostrar que cualquier acción tomada contra un alertador no fue consecuencia de su denuncia.

Esta carga invertida de la prueba es una cláusula importante en la Directiva, que marca una diferencia significativa en la capacidad de los denunciantes para recibir las protecciones a las que tienen derecho por ley.

Por último, se penalizan tanto las represalias como el incumplimiento de ciertos deberes respecto de un alertador. La Directiva requiere que los Estados miembros introduzcan sanciones por tomar represalias contra un denunciante u obstaculizar su actuación, así como intentos de hacerlo, violando la confidencialidad debida o entablando procedimientos vejatorios contra ellos. Las sanciones se refieren a las medidas adoptadas por la entidad que recibe una denuncia, que está implicada por ese reporte o que implica a un tercero. La naturaleza de estas sanciones se deja a la discreción de los Estados miembros, de los que se espera que adopten un enfoque "eficaz, proporcionado y disuasorio".

La cuestión de las sanciones para los empleadores (y otros) que tratan mal a los alertadores es importante. A menudo, los denunciantes que sienten que los sistemas existentes les han fallado mencionan la posibilidad de que haya repercusiones legales por represalias como una prueba de credibilidad clave.

Hay ejemplos de sanciones penales por infringir las normas sobre la protección de los denunciadores. El PIDA (Public Interest Disclosure Act) de Australia hace que la represalia contra un denunciante sea un delito penal con un máximo de dos años de prisión. La ley Sapin II de Francia crea una pena similar por no cumplir con la confidencialidad de la identidad de un informante. Un sistema ejemplar de sanciones o multas también podría formar parte de un sistema "disuasorio" de penas.

Dado que un objetivo clave de la Directiva no es sólo proteger a los denunciadores, sino garantizar que sus denuncias sean investigadas adecuadamente, puede haber un argumento para introducir penalizaciones por fallos que no sean específicamente citados en la Directiva. Una propuesta de reforma del PIDA del Reino Unido incluye un régimen de multas civiles para cuando el gestor de un canal de información interno o externo no investiga o cumple las normas establecidas para el tratamiento de las divulgaciones protegidas²⁵.

Los planes de sanciones son ya un elemento eficaz en muchos de los esquemas existentes para la protección de los denunciadores existentes. El PDA irlandés permite a los alertadores que sufren represalias iniciar una acción de agravio por experimentar un perjuicio, solicitando sanción disciplinaria a los que ejecutan las represalias. La primera demanda de penalización en virtud de la ley se concedió a una mujer que informa de problemas de salud y seguridad en un asilo de ancianos. Después de juzgar su queja, el Tribunal Laboral confirmó que sufrió un período de suspensión relacionado con su divulgación, concediéndole una indemnización de 17.500 euros²⁶.

Las sanciones pueden aplicarse no sólo en los casos de represalias, sino también en los casos de infracción del derecho a la intimidad. La Ley coreana sobre la protección de los alertadores de interés público hace que la divulgación indebida de información sensible relacionada con una denuncia, como su contenido o la identidad de un informante, sea castigada con 2 años de prisión o una multa de unos 18.000 dólares. Las represalias o la discriminación contra un denunciante de interés público pueden ser castigada con hasta 1 año de prisión²⁷.

Capítulo 12 – Apoyo y medidas provisionales

Más allá de proporcionar una lista de acciones de represalia de las que se debe proteger a los alertadores, la Directiva obliga a los Estados Miembros a introducir medidas de apoyo y medidas provisionales. Como mínimo, éstas tienen que incluir el acceso libre y fácil a la información sobre los derechos y procedimientos, así como la asistencia efectiva y el apoyo legal si fuese necesario.

Además, los Estados miembros pueden considerar explícitamente la posibilidad de proporcionar apoyo económico. La Directiva guarda silencio sobre la cuestión de recompensar económicamente a los alertadores por sus acciones en el contexto de un sistema coordinado de recompensas.

En los considerandos del texto de la UE se reconoce el alto potencial de desaliento de los alertadores cuando los procedimientos no están claros o los medios de vida se ven amenazados y destaca la importancia de explicar el panorama al que se enfrentan los denunciadores de la forma más inequívoca posible.

También sugiere el establecimiento de un órgano gubernamental independiente que supervise los procedimientos de denuncia, que funcione como un centro de información y apoyo público.

Generalmente, los mecanismos de apoyo deben reflejar la amplia gama de situaciones en las que pueden encontrarse los alertadores cuando necesiten medidas provisionales, y los mecanismos de indemnización deben ser "reales y efectivos" para no desalentar a futuros informantes.

Los marcos existentes para la denuncia de infracciones prevén una variedad de medidas diferentes para apoyar a los alertadores de irregularidades antes, durante y después de hacer una revelación de una infracción. El asesoramiento y el apoyo jurídico gratuito es una de las medidas más comunes disponible para los denunciadores en muchos países europeos, como Irlanda, Francia, Italia, España, entre otros. Y se trata de una medida vital. Las investigaciones en este campo subrayan los importantes costos legales de los alertadores que van a los tribunales, incluso en los países donde desde hace años se protege a los alertadores²⁸.

Los Estados Miembros tal vez deseen considerar si el requisito de asistencia jurídica obligatoria de la Directiva es lo suficientemente amplio como para cubrir todos los tipos de acciones a las que un informante se pueda ver sometido. En particular, deben tenerse en cuenta los costes que el alertador podría afrontar por la pérdida de su empleo y otros procedimientos civiles.

Además, la denuncia de irregularidades a menudo tiene un costo psicológico importante. Muchos alertadores experimentan respuestas negativas de sus compañeros de trabajo o superiores, lo que puede poner en tensión los lazos familiares o la salud mental en general²⁹.

Los estudios también sugieren que las experiencias negativas en esos contextos también pueden impedir que en el futuro otros informantes decidan dar un paso al frente, lo que en última instancia derrotaría el propósito de la Directiva.

Las mejores prácticas internacionales recomiendan incluir medidas de apoyo psicológico en todo plan de protección del denunciante contundente³⁰, por ejemplo, en forma de puntos de contacto dedicados a este tema. Lo ideal sería que se pudiera acceder a ellos en todas las etapas del proceso de divulgación.

Los Estados miembros también pueden considerar la posibilidad de introducir mecanismos para apoyar financieramente a los informantes de infracciones, de ser necesario.

El apoyo financiero puede revestir distintas formas. En Estados Unidos, los sistemas de gratificaciones crean incentivos para que los alertadores hagan sus denuncias recompensándolos con una parte de los bienes salvados o recuperados como resultado de su denuncia.

Aunque este enfoque puede facilitar la promoción de una cultura de divulgación de las malas acciones, algunas voces críticas sostienen que la perspectiva de las ganancias financieras choca con la cuestión del interés público a la hora de hacer una denuncia.

La alternativa sería crear planes de apoyo diseñados de forma que las ganancias económicas compensen tan solo las pérdidas que sufren los alertadores como resultado de hacer una revelación. Diferentes organizaciones de la sociedad civil en toda Europa, como Transparencia Internacional Alemania, abogan por la introducción de un "fondo de ayuda a los denunciantes", diseñado como apoyo financiero de emergencia. De manera similar a los sistemas de recompensas establecidos, los medios financieros para proporcionar dicho fondo de ayuda podrían provenir de los activos recuperados a través de las declaraciones de los alertadores. En Irlanda, los denunciantes que hayan sido despedidos injustamente como resultado de una divulgación protegida tienen derecho a una compensación de hasta 5 años de salario.

Teniendo en cuenta las mejores prácticas internacionales, se aconseja a los Estados miembros de la UE que vinculen las medidas de apoyo a los órganos de supervisión, ya que ese enfoque facilitará enormemente la situación de los alertadores. Si los Estados miembros optan por introducir una autoridad de supervisión independiente dedicada a la denuncia de irregularidades (véase el capítulo 8), la disposición y la gestión de las medidas de apoyo debería ser uno de sus mandatos clave.

En Bosnia, la introducción de un "estatuto de denunciante" ha demostrado ser una medida provisional eficaz. En virtud de la ley sobre la denuncia de irregularidades en las instituciones de Bosnia y Herzegovina, los empleados del sector público que denuncien irregularidades en su institución no podrán ser sancionados hasta que se hayan concluido las investigaciones sobre sus reclamaciones.

Las represalias contra esas personas son consideradas un delito y se castiga con una multa³¹. Este mecanismo ha llevado a investigaciones rápidas de las denuncias de los informantes e incluso la reincorporación de los alertadores a sus puestos de trabajo.

Así pues, los Estados miembros pueden considerar la posibilidad de introducir un sistema de certificación en el que un alertador pueda demostrar el estado de una investigación en curso. Esto podría aumentar sustancialmente la certeza jurídica en caso de represalias mientras se realizan las investigaciones, y facilitar el proceso de ser reconocido como denunciante en caso de que experimente represalias a pesar de todo.

Los empleados cuyas denuncias se descubran más tarde como insustanciales o incluso maliciosas, y que abusaron abusar conscientemente del sistema de certificación de alertadores deben ser sancionados de acuerdo con la ley nacional de empleo.

Capítulo 13 - La otra parte: la protección de las personas afectadas

La Directiva de la UE abre nuevos caminos al establecer la obligación para quienes reciben las denuncias, no sólo de abstenerse de represalias contra el alertador, sino también de investigar el contenido de esos reportes.

Tras mirar ese aspecto de las obligaciones, tanto para los empleadores del sector público y privado como para los reguladores y otras organizaciones designadas para recibir denuncias de segundo nivel o "externas", el deber de investigar una denuncia conlleva obligaciones recíprocas con los individuos o entidades que son objeto de esa denuncia.

Es necesario asegurarse de que ellos también sean tratados de manera justa y que sus derechos se respeten, incluyendo la presunción de inocencia y un juicio justo.

La Directiva vela por los intereses de las personas objeto de los informes ("personas afectadas") principalmente de dos maneras. En primer lugar, incluye disposiciones destinadas a impedir que los canales de denuncia se utilicen de manera maliciosa y disuadir a los individuos de abusar del sistema.

En segundo lugar, la Directiva afirma los principios básicos de justicia natural que deben observarse en relación con las personas que son señaladas en las denuncias. Casi por definición, estos principios ya deberían ser observados en los Estados miembros de la UE.

No obstante, las investigaciones de denuncias plantean cuestiones particulares en las que los derechos de la denuncia y la persona sobre la que informa deben ser consideradas cuidadosamente.

Si nos fijamos en primer lugar en las cláusulas contra el abuso de la Directiva, hemos visto que si bien para el requisito de la protección no se pide demostrar buena fe, sí que se excluye específicamente de esa protección las denuncias "deliberadamente falsas". De hecho, los Estados miembros están obligados a introducir sanciones "disuasorias" para los que presentan tales informes. Irlanda, por ejemplo, ha introducido sanciones por declaraciones deliberadamente erróneas de hasta 12 meses de prisión.

Todas las pruebas muestran que este tipo de uso malicioso de las reglas de denuncia es extremadamente raro. Es importante que

las sanciones por las denuncias de abusos se elaboren de manera lo suficientemente estricta como para que no supongan un desincentivo para aquellos que no están tratando de abusar del sistema. Si las sanciones por abuso disuaden de legislar sobre la presentación de denuncias, socavan todo el propósito de la legislación.

Es posible que la legislación nacional ya prevea sanciones apropiadas. El caso particular de la divulgación pública de información falsa y perjudicial sobre un individuo o una persona jurídica suele estar cubierto por la ley de difamación.

El riesgo de abuso no es la única situación en la que hay que considerar los intereses del sujeto de una denuncia. Cuando se investiga una denuncia, el sujeto de ese reporte tiene derecho a saber cuáles son las acusaciones en su contra y tienen derecho a dar su versión de la historia. Si bien ninguno de esos principios se contradice, la experiencia práctica sugiere que los procedimientos de la investigación deben ser cuidadosamente diseñados para asegurarse de que se respetan esos derechos.

En el caso de Irlanda, algunos de los encargados de aplicar la Ley de Divulgación Protegida de 2014 han expresado su preocupación por el hecho de que la obligación de mantener confidencial la identidad del informante pueda entrar en conflicto con el derecho del interesado a acceder a su expediente y a los detalles de la alegación planteada. Los códigos de práctica han tratado de lidiar con el tema³².

Como se sugiere en el capítulo 10, se han planteado preocupaciones similares acerca de la compatibilidad del anonimato con los derechos de las personas investigadas. Dado que la Directiva permite excepciones a la norma de confidencialidad cuando la ley lo exige, se trata de una cuestión en la que la claridad de procedimiento es importante. Esos procedimientos deben resolver en qué momento del proceso de la investigación la persona afectada debe ser informada y cómo puede cumplirse con su derecho a entregar su versión sin comprometer el deber de confidencialidad con el alertador.

Otros marcos jurídicos nacionales pueden dar lugar a sus propias y diferentes cuestiones de procedimiento.

Por último, la Directiva establece ciertos tipos de medidas cautelares para la persona señalada durante la investigación. Si bien gran parte de esto se deja a la discreción de los Estados miembros, las obligaciones recíprocas de confidencialidad para la persona sobre la que se informa, al menos en lo que respecta al dominio público, se mencionan específicamente. Como tal, los Estados Miembros deben asegurarse de que no se revele la identidad de un afectado hasta que la investigación haya concluido.

Capítulo 14 - ¿Funciona? Disposiciones para la presentación de informes, la supervisión y evaluación

La Directiva exige a los Estados miembros que complementen los procedimientos de denuncia de irregularidades con mecanismos que supervisen su eficacia. Esto incluye la obligación de que las entidades públicas y privadas mantengan registros de cada informe recibido de conformidad con los requisitos de confidencialidad necesarios que se describen tanto en la Directiva como en otras regulaciones de la UE como la RGPD.

Las normas sobre los canales de información externa prevén que las autoridades competentes revisen sus mecanismos de denuncias al menos cada tres años y adaptar sus procedimientos según su eficacia. De los gestores de los canales externos se espera que mantengan registros de cada denuncia, que pueden ser inspeccionados por el alertador si así lo solicitara. Asimismo, se espera que mantenga un registro del número total de denuncias recibidas, el resultado de las investigaciones y los fondos recuperados.

Los Estados Miembros están obligados a presentar anualmente información a la Comisión sobre el número de denuncias presentadas, investigaciones resultantes y, de ser posible, una estimación de los daños financieros y los bienes recuperados. Estas estadísticas servirán, a su vez, de base para revisar la legislación europea actual y proporcionarán una visión útil de la eficacia de las medidas de protección de los denunciantes.

Al mismo tiempo, la cuantificación del impacto de las medidas de denuncia de irregularidades únicamente en términos financieros no

tiene en cuenta otros acontecimientos positivos, tales como prevención del delito en general o un aumento de la confianza de población.

El establecimiento de mecanismos exhaustivos de supervisión y examen es una debilidad en muchos mecanismos de denuncias. En el Reino Unido, una convocatoria de 2013 encontró que los denunciantes no confiaban en que sus denuncias se estuviesen investigando, lo que condujo a una reforma de las obligaciones de presentación de denuncias de las personas designadas para recibir los reportes de los alertadores.

Según un reglamento introducido en 2017, las personas designadas tienen que presentar informes sobre el número de denuncias recibidas, casos investigados, así como información sobre las medidas adoptadas anualmente. Este enfoque tiene en cuenta que la coherencia de los procedimientos, así como la demostración de transparencia son factores importantes para aumentar la confianza de los denunciantes en que sus revelaciones se toman en serio³³.

Recomendaciones sobre prácticas óptimas internacionales^{XI} también, enfatizan la necesidad de un uso y aplicación transparentes de la legislación relativa a los denunciantes a fin de reforzar la confianza de la población en las medidas adoptadas. Esto incluye informar sobre el número de casos, los resultados de las investigaciones y los bienes recuperados.

Los gestores de los canales internos tal vez deseen considerar la posibilidad de mantener estadísticas agregadas y publicarlas periódicamente, ya que de esa forma la reputación gana en valor, además de crear confianza en el sistema.

La Directiva no estipula qué procesos de revisión deben tener lugar a nivel nacional, aparte un registro de que ciertas estadísticas y que es necesario revisar los canales externos por lo menos cada tres años. Para facilitar el examen de las medidas establecidas, sugerimos que además de mantener registros de resultados de las investigaciones, y que los operadores de los canales externos registren las razones para no iniciar investigaciones.

Además, puede ser valioso agregar los datos sobre el resultado de las denuncias y los procedimientos judiciales iniciados en relación con los reportes. Esto debe incluir cualquier procedimiento por represalias o por hacer un señalamiento a sabiendas de que es falso.

Como resultado de la falta de supervisión de los actores estatales, las organizaciones de la sociedad civil de toda Europa han establecido marcos para examinar la forma en que los sistemas nacionales y las disposiciones jurídicas protegen a los denunciantes en la práctica. Un ejemplo es la *Maison des lanceurs d'alerte*, una organización de la sociedad civil francesa que supervisa la aplicación de la *Loi Sapin II* y ofrece apoyo a los denunciantes³⁴. Se prevé que esta tendencia continúe; los Estados miembros tal vez deseen considerar la posibilidad de aprovechar los conocimientos especializados reunidos por las organizaciones, algunas de las cuales han trabajado activamente durante décadas.

Para facilitar el examen del funcionamiento de las medidas de protección de los alertadores, se aconseja a los Estados miembros que vinculen procesos de supervisión y evaluación al órgano de supervisión respectivo, idealmente una autoridad centralizada de denuncias (véase el capítulo 8).

Capítulo 15 La denuncia de irregularidades en la era de COVID-19

Las protecciones legales para los alertadores de irregularidades sólo son valiosas en la medida en que se enfrentan al desafío de los escenarios del mundo real. La COVID-19 presenta una importante serie de casos de prueba, ya que los denunciantes han desempeñado un papel fundamental en la comprensión de la pandemia desde su comienzo.

El Dr. Li Wenliang fue uno de los médicos que fueron reprendidos por las autoridades locales chinas por compartir información sobre el primer grupo de pacientes con síntomas similares al SARS admitidos en los hospitales de Wuhan en diciembre de 2019. El 30 de diciembre, Li y otros publicaron información sobre los primeros casos en grupos privados que compartían con colegas. Esa información se difundió más ampliamente en un momento en que no había información oficial sobre el brote.

XI. Realizado por Blueprint for Free Speech, Government Accountability Project, Consejo de Europa, Transparencia Internacional y otros

Las noticias sobre el "SARS de Wuhan" fue una tendencia en la red social Weibo antes de ser censuradas. Al menos ocho médicos fueron convocados a comisarías locales en los primeros días de 2020 y obligados a firmar documentos renunciando a sus declaraciones. Otros parecen haber recibido reprimendas verbales de las autoridades hospitalarias por compartir "información falsa". El Dr. Li contrajo COVID-19 poco después de volver a trabajar a principios de enero y su muerte menos de un mes después tuvo un enorme eco en las redes sociales.

Poco antes de la muerte del Dr. Li, la Corte Suprema de China amonestó a las autoridades locales por reprender a los ocho médicos y comentó que la distribución de información en este caso podría haber cumplido una función social útil³⁵. Este reconocimiento de un alertador de irregularidades que plantea información en interés público, en contraposición a ayudar a mejorar la aplicación de la ley marca un hito importante en el pensamiento jurídico chino.

A mediados de marzo de 2020, la exoneración póstuma de Li fue noticia en todo el mundo³⁶.

La pandemia ha llevado a que el papel de la denuncia de infracciones se comprenda mejor en China; las organizaciones internacionales y la sociedad civil se apresuraron a afirmar la importancia de los denunciantes para la crisis en otros lugares.

El conjunto de herramientas del Consejo de Europa para los Estados miembros afirma que la pandemia no debe ser utilizada como una excusa para silenciar denunciantes³⁷. Más de 100 organizaciones de la sociedad civil se unieron a la Coalición para hacer que la denuncia de irregularidades sea segura durante la COVID-19 y después³⁸.

No obstante, en la práctica se han dado distintos problemas

El intercambio de información entre médicos en las redes sociales se ha convertido en un tema recurrente de la pandemia. Los médicos italianos que se ocuparon del primer gran brote en Europa emitieron advertencias en los medios digitales sobre la gravedad de la situación, que se tradujeron a otros idiomas y fueron ampliamente compartidos a principios de marzo de 2020³⁹.

En otros lugares, los profesionales de la salud y otros trabajadores expusieron en Facebook alertas sobre la escasez de equipos de protección personal (EPI), que les obligaban a trabajar en condiciones inseguras.

La posición legal de los que hacen denuncias en redes sociales no siempre ha sido clara. Las restricciones en denuncias que se hacen públicas son demasiado limitadas para proteger a los que se encuentran en una situación de verdadera amenaza para la vida. El hecho que la organización Protect recomiende a los trabajadores de la salud en Reino Unido utilizar diferentes canales de información o informar de manera anónima a través de un periodista, da una idea del tipo de obstáculos a los que se enfrentan estos trabajadores⁴⁰.

En la práctica, ha habido numerosos ejemplos de represalias. Las denuncias sobre la falta de EPIs, ya sea en redes sociales o a través de otros canales, han llevado a la suspensión o el despido de personal médico en India, Estados Unidos y Polonia, a pesar de la extraordinaria demanda de personal calificado durante la pandemia⁴¹. En el Reino Unido, se han publicado información en los medios de comunicación sobre las amenazas de medidas disciplinarias y la vigilancia de las redes⁴² y trabajadores de la salud en el sector privado fueron despedidos por plantear inquietudes⁴³.

Según los informes de los medios de comunicación, los académicos y los médicos de Bangladesh han sufrido represalias en el lugar de trabajo y han sido arrestados por informar sobre la propagación del virus y la escasez de equipos de protección personal⁴⁴. Los médicos en Turquía han sido arrestados y obligados a pedir disculpas públicamente por lo que han publicado en sus redes sociales⁴⁵. Se ha informado de agresiones físicas en Rusia y Pakistán⁴⁶ y de la detención de varios médicos de Egipto, donde se ha visto que manifestar preocupación por la pandemia formaba parte de una campaña más amplia de represión de disidencia política⁴⁷.

Los temas no se han limitado, por supuesto, a los médicos. En EEUU, se ha informado de despidos por plantear problemas de salud y seguridad en lugares de trabajo tan diversos como los portaaviones de la Marina a los almacenes de Amazon⁴⁸. Las

preocupaciones sobre la precisión y la disponibilidad de información estadística sobre la pandemia también ha sido objeto de divulgaciones de información en varios países⁴⁹.

La denuncia de irregularidades se identifica por lo general como la forma más eficaz de detectar el fraude y es probable que demuestre su importancia dada las cantidades sin precedentes de dinero público invertidas en mantener a flote las economías nacionales. Los planes del gobierno para mantener a los trabajadores mediante la subvención de los salarios es probable que se conviertan en un importante foco de reclamaciones fraudulentas, en particular cuando esos planes se han iniciado desde cero⁵⁰. Los operadores de líneas telefónicas de denuncia en el Reino Unido han dicho que las preocupaciones sobre fraude representan hasta un tercio de las llamadas que han recibido, y se han hecho más denuncias directamente ante las autoridades fiscales⁵¹.

La pandemia también ha puesto de relieve la capacidad de informar sobre las preocupaciones relativas al uso de la tecnología. Muchos países buscaron soluciones tecnológicas para aumentar la frecuencia y la eficacia del rastreo de los contactos, con la esperanza de que las infecciones por coronavirus pudiesen detectarse rápidamente y se pudiesen aplicar medidas de cuarentena.

A pesar de que la eficacia de enfoques que usan datos de localización o mediciones de proximidad bluetooth para identificar a los individuos que pueden haber contraído el coronavirus no ha sido probado, estas tecnologías tienen importantes implicaciones de privacidad, sobre todo para los alertadores.

Esto es aún más cierto cuando la participación en un esquema de rastreo de contactos es obligatoria. Uno de esos planes obligatorios lo impuso Qatar, donde no descargar la aplicación nacional de rastreo de contactos es un delito penal. Poco después de que la aplicación fuera lanzada, Amnistía Internacional encontró una debilidad crítica que significaba que los datos personales eran ampliamente accesibles⁵². Es importante que este tipo de cuestiones se saquen a la luz y es probable que ningún sistema sea inmune a los problemas.

Por último, los estudios han demostrado que los esquemas de gobierno democráticos y transparentes han demostrado ser más exitosos a la hora de abordar los desafíos de las pandemias mundiales y han conseguido minimizar las muertes en todo el mundo a diferencia de las sociedades autocráticas que se basan en el secreto⁵³.

Las políticas de información transparente tienden a fortalecer la confianza de la población, lo que contribuye de manera decisiva a una eficaz aplicación de estrategias de emergencia que dependen de la cooperación de la población en general. La pandemia mundial de COVID-19 destaca la importancia de apoyar la denuncia de infracciones en el establecimiento de democracias sanas que funcionen en interés de todos los ciudadanos. Los gobiernos de toda la Unión Europea deberían tenerlo en cuenta al transponer la Directiva europea a la legislación nacional.

1. Blueprint for Free Speech, Gaps in the System (2018), pp.18-19, <https://www.blueprintforreespeech.net/s/BUEPRINT-Gaps-in-the-System-Whistleblowers-Laws-in-the-EU-s7pm.pdf>
2. Blueprint for Free Speech, Gaps in the System (2018), <https://www.blueprintforreespeech.net/s/BUEPRINT-Gaps-in-the-System-Whistleblowers-Laws-in-the-EU-s7pm.pdf>
3. The Tshwane Principles on National Security and the Right to Information (2013), <https://www.justiceinitiative.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles>
4. Consejo de Europa, Recomendación para la Protección de los denunciantes CM/Rec(2014)7 y memorando explicativo (2014), <https://rm.coe.int/16807096c7>
5. Tribunal Europeo de Derechos Humanos, Bucur y Toma vs Rumanía (2013), <https://www.right2info.org/cases/21-bucur-and-toma-v-romania>
6. XNet, Propuso un proyecto de ley para la protección del denunciante en 2019, <https://xnet-x.net/en/template-law-full-protection-whistleblowers/>
7. International Bar Association, Whistleblower Protections: A Guide (2018), p.23, <https://www.ibanet.org/LPRU/Whistleblowing.aspx>
8. Blueprint for Free Speech, Protecting Whistleblowers in the UK: A New Blueprint (2016), <https://www.blueprintforreespeech.net/s/Report-Protecting-Whistleblowers-In-The-UK.pdf>
9. James Goodale, The Dumbwaiter Defense (2020), <https://www.cjr.org/opinion/greenwald-intercept-assange-manning-wikileaks.php>; Rainey Reitman, When Computer Crimes Are Used To Silence Journalists: Why EFF Stands Against the Prosecution of Glenn Greenwald (2020), <https://www.eff.org/deeplinks/2020/01/when-computer-crimes-are-used-to-silence-journalists-why-eff-stands-against>
10. Criminal Law Reform Now Network (CLRNN), Reforming the Computer Misuse Act 1990 (2020), <http://www.clmn.co.uk/publications-reports>
11. Kate Kenny, Whistleblowing: Toward a New Theory (2019)
12. European Federation of Journalists, Implementing the new EU Whistleblower Directive: A Transposition Guide for Journalists (2020), <https://europeanjournalists.org/wp-content/uploads/2020/02/Implementing-Finalpages.pdf>
13. Ethics Resource Center (ERC), Inside the Mind of a Whistleblower (2012), <https://www.corporatecomplianceinsights.com/wp-content/uploads/2012/05/Inside-the-mind-of-a-whistleblower-NBES.pdf>
14. Whistleblowing International Network (WIN), WIN Legal Brief – Mandatory Internal & External Disclosures (2018), <https://whistleblowingnetwork.org/WIN/media/files/win-legal-brief-focus-on-mandatory-internal-wb-12-08-181.pdf>
15. Agencia Valenciana Antifraude, Memoria 2019 (2019), p. 59, https://www.antifraucv.es/wp-content/uploads/2020/03/MEMORIA_2019_CAS.pdf
16. Network of European Integrity and Whistleblowing Authorities (NEIWA), Paris Declaration (2019), http://www.federaalombudsman.be/sites/default/files/explorer/Paris_declaration_-_NEIWA.pdf
17. Dutch Whistleblowing Authority, <https://www.huisvoorkloekenluiders.nl/english>
18. Dutch Whistleblowing Authority, Annual Report (2018), <https://www.huisvoorkloekenluiders.nl/Publicaties/jaarsverslagen/2019/03/14/annual-report-2018---dutch-whistleblowers-authority>
19. Protect, Covid-19, Social Media and Whistleblowing (2020), <https://protect-advice.org.uk/covid-19-social-media-and-whistleblowing/>
20. European Federation of Journalists, Implementing the new EU Whistleblower Directive: A Transposition Guide for Journalists (2020), p2, <https://europeanjournalists.org/wp-content/uploads/2020/02/Implementing-Finalpages.pdf>
21. HTW Chur & EQS Group, Whistleblowing Report 2019 (2019), <https://whistleblowingreport.eqs.com/en/home>
22. Transparency International, Dutch Companies Falling Short of Compliance with New EU Whistleblower Directive (2020), <https://www.transparency.org/en/blog/companies-in-the-netherlands-are-falling-short-of-compliance-with-new-eu-directive-for-whistleblower-protection>
23. Blueprint for Free Speech, Blueprint Principles for Whistleblower Protection, pp.6-7, <https://static1.squarespace.com/static/5e249291de6f0056c7b1099b/t/5ea0704123f49c36460b8a9a/1587572801985/Blueprint-Principles-for-Whistleblower-Protection4.pdf>
24. UK Department for Business, Energy and Industrial Strategy, Confidentiality Clauses (2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/783011/confidentiality-clauses-consultation.pdf
25. Protect, A Bill to Strengthen Whistleblower Protection, <https://s3-eu-west-1.amazonaws.com/public-concern-at-work/wp-content/uploads/images/2019/11/06160222/Protect-Whistleblowing-Bill-Nov-2019.pdf>
26. Ireland Department of Public Expenditure and Reform, Statutory Review of the Protected Disclosures Act 2014 (2018), p. 23, <https://assets.gov.ie/8765/7e112c66e7c04062a25561a848e17943.pdf>
27. Greece-OECD Project: Technical Support on Anti-Corruption, Whistleblower Protection in the Private Sector: Developing the Legal Framework (2018), p.21, <http://www.oecd.org/corruption/anti-bribery/OECD-Greece-Whistleblower-Protection-Legislative-Proposal-ENG.pdf>
28. Blueprint for Free Speech, Protecting Whistleblowers in the UK: A New Blueprint (2016), <https://www.blueprintforreespeech.net/s/Report-Protecting-Whistleblowers-In-The-UK.pdf>
29. Government Accountability Project, Whistleblower Trauma, Recovery and Renewal (2015), <https://whistleblower.org/uncategorized/whistleblower-trauma-recovery-and-renewal/>
30. Blueprint for Free Speech, Blueprint Principles for Whistleblower Protection, <https://static1.squarespace.com/static/5e249291de6f0056c7b1099b/t/5ea0704123f49c36460b8a9a/1587572801985/Blueprint-Principles-for-Whistleblower-Protection4.pdf>
31. Law on whistleblowing in the institutions of Bosnia-Herzegovina (2015), <http://rai-see.org/wp-content/uploads/2015/08/LAW-ON-WHISTLEBLOWER-PROTECTION-IN-THE-INSTITUTIONS-OF-BIH-en.pdf>
32. Lauren Kierans, An empirical study of the purpose of the Irish Protected Disclosures Act 2014 (2019), Chapter 5, <https://eprints.mdx.ac.uk/26851/1/LKierans%20thesis%20volume%20L.pdf>
33. UK Department for Business, Energy & Industrial Strategy, Whistleblowing Prescribed Persons Annual Reports 2018/19, http://data.parliament.uk/DepositedPapers/Files/DEP2020-0013/PP_Annual_Reports_2018-19_-_Part_2.pdf
34. Maison des Lanceurs d'Alerte, <https://malerte.org/>
35. Financial Times, Coronavirus whistleblower doctor dies in Wuhan hospital (2020), <https://www.ft.com/content/a82d1cac-4909-11ea-aeb3-9f55839e06441>
36. The Irish Times, China exonerates coronavirus whistleblower who died (2020), <https://www.irishtimes.com/news/world/asia-pacific/china-exonerates-coronavirus-whistleblower-doctor-who-died-1.4207837>
37. Council of Europe, Respecting democracy, rule of law and human rights in the framework of the COVID-19 sanitary crisisA toolkit for member states (2020), <https://rm.coe.int/sg-inf-2020-11-respecting-democracy-rule-of-law-and-human-rights-in-th/16809e1f40>
38. International Coalition Calls for COVID-19 Whistleblower Protection (2020), <https://www.blueprintforreespeech.net/en/news/en/international-coalition-calls-for-covid-19-whistleblower-protection>
39. World Economic Forum, 'Every ventilator becomes like gold' - doctors give emotional warnings from Italy's Coronavirus outbreak (2020), <https://www.weforum.org/agenda/2020/03/suddenly-the-er-is-collapsing-a-doctors-stark-warning-from-italys-coronavirus-epicentre/>
40. Protect, Covid-19, Social Media and Whistleblowing (2020), <https://protect-advice.org.uk/covid-19-social-media-and-whistleblowing/>
41. BBC, Doctor who raised concerns over PPE shortage admitted to mental hospital (2020), <https://www.bbc.com/news/world-asia-india-52719110>; The Atlantic, Hospitals Must Let Doctors and Nurses Speak Out (2020), <https://www.theatlantic.com/ideas/archive/2020/04/why-are-hospitals-censoring-doctors-and-nurses/609766/>; Wybocza.pl, Dyrektor szpitala zwolnił położną, bo alarmowała na Facebooku, że brakuje maseczek i sprzętu (2020), <https://krakow.wyborcza.pl/krakow/7,44425,25814624,dyrektor-zwolnil-polozna-z-pracy-powod-alarmowala-ze-w-szpitalu.html>

42. The Times, Coronavirus: Medics 'threatened with sack' if they speak of PPE shortages (2020), <https://www.thetimes.co.uk/article/coronavirus-medics-threatened-with-sack-if-they-speak-of-ppe-shortages-qt66gbj3v>
43. The Guardian, 170 care workers call UK whistleblower helpline during Covid-19 crisis (2020), <https://www.theguardian.com/society/2020/may/06/over-170-carers-call-uk-whistleblower-helpline-during-coronavirus-crisis>
44. Liberation, Coronavirus : le Bangladesh censure les lanceurs d'alerte (2020), https://www.liberation.fr/planete/2020/04/02/coronavirus-le-bangladesh-censure-les-lanceurs-d-alerte_1783942
45. Ahval, Turkish doctors issue apologies for coronavirus statements (2020), <https://ahvalnews.com/turkey-coronavirus/turkish-doctors-issue-apologies-coronavirus-statements>
46. Amnesty International, Russia: doctor who called for protective equipment detained (2020), <https://www.amnesty.org.uk/press-releases/russia-doctor-who-called-protective-equipment-detained>
47. Reuters, Some medics say they are muzzled in Egypt's coronavirus response (2020), <https://www.reuters.com/article/us-health-coronavirus-egypt-medics/some-medics-say-they-are-muzzled-in-egypts-coronavirus-response-idUSKBN2352JX>
48. NPR, Navy Seeks 'Deeper Review' In Probe Of Pandemic-Struck Warship Captain's Firing (2020), <https://www.npr.org/sections/coronavirus-live-updates/2020/04/29/847842205/navy-seeks-deeper-review-in-probe-of-pandemic-struck-warship-captain-s-firing>; Time, Amazon Vice President Quits in Protest Over Company's Alleged Firings of Coronavirus 'Whistleblowers' (2020) <https://time.com/5831674/amazon-engineer-quits-coronavirus-whistleblowers/>
49. Florida Today, Fired DOH official to speak out, reveals new details of alleged COVID-19 data 'manipulation' attempt (2020), <https://www.floridatoday.com/story/news/2020/05/22/rebekah-jones-fired-florida-department-health-manager-make-public-announcement/5247836002/>; Channel 4 News, Can we rely on Covid-19 death figures? (2020), <https://www.channel4.com/news/can-we-rely-on-covid-19-death-figures>
50. Financial Times, Furlough fraud plagues Europe's drive to save jobs from pandemic (2020), <https://www.ft.com/content/164ca0f9-3101-4825-b9b8-37c6549a4d4b>
51. Personnel Today, Almost 1,900 reports of furlough fraud to HMRC (2020), <https://www.personneltoday.com/hr/almost-1900-reports-of-furlough-fraud-to-hmrc/>
52. Amnesty International, Qatar: 'huge' security weakness in COVID-19 contact-tracing app (2020), <https://www.amnesty.org.uk/press-releases/qatar-huge-security-weakness-covid-19-contact-tracing-app>
53. The Economist, Democracies contain epidemics most effectively (2020), <https://www.economist.com/graphic-detail/2020/06/06/democracies-contain-epidemics-most-effectively>

Créditos

Autores:

Naomi Colvin, Bruno Galizzi y Veronika Nad

Diseño:

Garreth Hanley

© 2020 Blueprint for Free Speech. Todos los derechos reservados.

Nos gustaría que se hiciera llegar este informe a quien pueda utilizarlo. Si así lo hace, le agradecemos que atribuya el crédito a Blueprint for Free Speech y sus autores.