Análisis y propuestas para las necesarias modificaciones del borrador de Directiva de la CE para la Protección de los Alertadores/ Whistleblowers

Por XNET - EDRi (European Digital Rights)
En colaboración con Courage Foundation
Con el apoyo (in progress) de Expose Facts, Institut de Drets Humans (IDHC) y Loïc Dachary

La Directiva es sí una buena noticia, fruto de los esfuerzos de los grupos activistas que hemos trabajado el tema en los últimos años y del grupo de los Verdes en el Parlamento Europeo que lo han defendido, pero tiene varias lagunas graves que se deben corregir antes de su aprobación ya que pueden perjudicar los objetivos propios de la Directiva y los derechos de acceso a la información entre otros.

1 - AMPLIAR LA DEFINICIÓN DE ALERTADOR (Y LA IMPORTANCIA DE LAS JUSTIFICACIONES DE "INTERÉS PÚBLICO")
2 - GARANTIZAR EL ANONIMATO DE LA FUENTE
3 - LIBERTAD PARA DETERMINAR EL CANAL DE DENUNCIA MÁS APROPIADO
4 - PROTECCIÓN DE INTERMEDIARIOS Y FACILITADORES
5 - USO INDEBIDO DE LA PROTECCIÓN DE DATOS (Y OTROS DERECHOS Y LIBERTADES)

1 - AMPLIAR LA DEFINICIÓN DE ALERTADOR (Y LA IMPORTANCIA DE LAS JUSTIFICACIONES DE "INTERÉS PÚBLICO")

El primer problema lo encontramos en la propia definición de quién se considera alertador y en el hecho de que, aunque la definición sea muy amplia, se limita a las personas que alerten sobre ilícito que de algún modo están relacionados con su ámbito laboral.

Si bien en la gran mayoría de los casos de alertadores se dan estas circunstancias, es también cierto que también se dan las circunstancias en las que los ilícitos sean descubiertos por una persona que no tienen ningún tipo de relación laboral con la entidad/personas que los comete.

En nuestra dilatada experiencia trabajando con alertadores sabemos que en al menos un 15% de los casos no se da ningún tipo de relación laboral. En estos caso, por ejemplo, quien denuncia puede ser alguien afectado por el ilícito, un investigador/periodista o un activista que consiga descubrir pruebas, como Ramsay Orta HYPERLINK "https://www.aljazeera.com/indepth/features/2016/10/ny-man-filmed-eric-garner-death-heading-jail-161001074627241.html"https://www.aljazeera.com/indepth/features/2016/10/ny-man-filmed-eric-garner-death-heading-jail-161001074627241.html o Flexispy whistle-blowers HYPERLINK "https://www.theregister.co.uk/2017/04/25/hackers_attack_stalkerware_flexispy/"https://www.theregister.co.uk/2017/04/25/hackers_attack_stalkerware_flexispy/. También son

frecuentes los casos en los que es alguien que tiene relaciones personales con quienes participan en una trama (ejemplo caso Pujol in Spain HYPERLINK "https://es.wikipedia.org/wiki/Jordi_Pujol_Ferrusola"*https://es.wikipedia.org/wiki/Jordi_Pujol_Ferrusola.*).

Se debería extender a toda la ciudadanía lo que dice la propia Directiva para ampliar el concepto de "trabajadores": “no es deseable dejar desprotegidos otros tipos de alertadores” (“leaving unprotected other types of potential whistleblowers”) (…)y “el alcance limitado constituiría una gran laguna en la protección de denunciantes a nivel de la UE al excluir de la protección categorías fundamentales de informantes potenciales, la iniciativa vería limitada su efectividad” (“The limited scope would constitute a main gap in whistleblower protection at EU level while, by excluding from protection crucial categories of potential whistleblowers such an initiative would also have limited effectiveness”). *(Context pag.8)*

Consideramos que en la armonización conjunta y legalmente explícita de las competencias compartidas del espacio de libertad, seguridad y justicia entre la UE y los Estados miembros, cabe absolutamente incluir a toda la ciudadanía (“all citizens”) en la protección que merecen cuando denuncian ilícitos y esto todavía más habiendo observado que la protección de los periodistas y demás facilitadores de que la información llegue a la opinión pública (disclosure) es más laxa de lo deseable (ver punto 4 sobre intermediarios y facilitadores).

Nuestra experiencia desmiente absolutamente la siguiente afirmación: “Cuando no existe tal desequilibrio de poder relacionado con el trabajo, no hay necesidad de protección contra represalias” (“When there is no such work-related power imbalance (for instance in the case of ordinary complainants or citizen bystanders) there is no need for protection against retaliation”) (Recital 23).

Si bien en el ámbito del trabajo las represalias típicas son la” terminación anticipada del contrato de servicios o la pérdida del negocio”, “la coacción, intimidación u hostigamiento, el boicot empresarial o los daños a su reputación” los sufren absolutamente todos los ciudadanos que denuncian ilícitos contra el interés general (“are typically subject to retaliation in the form of early termination or cancellation of contract of services, licence or permit, loss of business, loss of income, coercion, intimidation or harassment, blacklisting/business boycotting or damage to their reputation”).

Si es cierto que “las personas que informan sobre amenazas o daños al interés público (…) hacen uso de su derecho a la libertad de expresión. El derecho a la libertad de expresión está consagrado en el artículo 11 de la Carta de los Derechos Fundamentales de la Unión Europea y en el artículo 10 de la Convención Europea de Derechos Humanos (CEDH) y abarca la libertad y el pluralismo de los medios” (“Persons who report information about threats or harm to the public interest (…) make use of their right to freedom of expression. The right to freedom of expression, enshrined in Article 11 of the Charter of Fundamental Rights of the European Union (‘the Charter’) and in Article 10 of the

European Convention on Human Rights (ECHR), encompasses media freedom and pluralism" (párr. 21)), creemos firmemente que toda la ciudadanía se merece el mismo trato y protección porque si no, se contradiría el enunciado anterior y los tratados europeos que garantizan los derechos y libertades de la población. El artículo 11 de la Carta de los Derechos Fundamentales de la Unión Europea dice expresamente "Todos tienen derecho a la libertad de expresión. Este derecho incluirá la libertad de mantener opiniones y de recibir e impartir información e ideas sin interferencia de la autoridad pública e independientemente de las fronteras".

Consideramos un problema recurrente querer vincular la efectividad de las pruebas obtenidas para atacar un ilícito a cuestiones morales. Consideramos que el objetivo de esta Directiva debe ser el de facilitar el descubrimiento de actos graves contra el interés general. A la luz de este objetivo es irrelevante si la persona que los destapa lo hace con buena o mala intención siempre y cuando correspondan a la verdad. El juicio moral sobre su conducta no debería ser objeto de la Directiva aunque sí su eventual implicación en hechos delictivos. Por esto consideramos que pedir que se proteja al alertador "siempre que el demandado haya actuado con el fin de proteger el interés general" ("provided that the respondent acted for the purpose of protecting the general public interest") entorpece y va en contra del objetivo de la Directiva.

Por último y en general el artículo 14 habla solo de "coerción, intimidación, acoso u ostracismo en el lugar de trabajo" ("coercion, intimidation, harassment or ostracism at the workplace") cuando estos - para trabajadores y no trabajadores-, ocurren en el ambiente de trabajo pero sobre todo fuera del mismo, en el ámbito privado, por la cual cosa la limitación al "ambiente de trabajo" ("workplace") se ha de eliminar de todas formas.

En conclusión, consideramos que cualquier persona que se enfrenta a un riesgo de represalias por denunciar abusos debería disfrutar de una protección. La gama de escenarios es amplia: empleados con sus empleadores (o personal superior), civiles con las autoridades y niños con adultos. Además, cualquier parte que facilite este diálogo también debería disfrutar de protección (véase el punto 4).

Entendemos la intención de acotar el alcance de la Directiva para no invadir ámbitos de luchas contra los ilícitos ya cubiertos por otras competencias o legislaciones específicas, pero entendemos que donde se debe acotar es afirmando con mayor claridad que la Directiva cubre únicamente ilícitos que afectan al interés general – no los ilícitos en sí -, no dejando desprotegidos una parte considerable de los potenciales alertadores.

Para un articulado en este sentido, nos remitimos al artículo 3 de nuestra Plan tilla de Proposición de Ley para la Protección de los Alertadores donde se indica:

a) Alertador o alertadora: cualquier persona que teniendo una convicción razonable sobre la fiabilidad de una información constitutiva de alerta a la que

haya tenido acceso, la pone en conocimiento de terceros mediante denuncia administrativa o jurisdiccional o a través de un canal de recepción de alertas.

b) Información constitutiva de alerta: cualquier información que, acompañada de elementos probatorios o indicios consistentes, permita sospechar fundadamente sobre la posible perpetración de hechos ilícitos cuyas consecuencias **no sólo afecten a la administración o entidad privada en las que sean llevados a cabo sino que trasciendan y sean susceptibles de perjudicar el interés general.**

HYPERLINK "https://xnet-x.net/proposicion-ley-proteccion-integral-alertadores/"https://xnet-x.net/proposicion-ley-proteccion-integral-alertadores/

2 – GARANTIZAR EL ANONIMATO DE LA FUENTE

La "confidencialidad" no es suficiente. Se ha de garantizar explícitamente la posibilidad de denunciar de forma anónima tal y como pedía la *Resolución del Parlamento Europeo, de 24 de octubre de 2017, sobre las medidas legítimas para la protección de los denunciantes (* HYPERLINK "http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0402+0+DOC+XML+V0//ES"***http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0402+0+DOC+XML+V0//ES***) que ha originado el borrador de Directiva.
En el posicionamiento 49 dice: "Considera que la posibilidad de efectuar denuncias anónimas puede animar a los denunciantes a transmitir informaciones que en otras circunstancias no se habrían comunicado; (…) destaca que la identidad del denunciante, así como cualquier otra información que permita su identificación, no deben poder ser reveladas sin su consentimiento; considera que cualquier violación de este carácter confidencial debe estar sujeta a sanciones".

Tal y como indicamos en nuestra Proposición (HYPERLINK "https://xnet-x.net/proposicion-ley-proteccion-integral-alertadores/"https://xnet-x.net/proposicion-ley-proteccion-integral-alertadores/), "existe una situación de asimetría de fuerzas entre los ciudadanos y las instituciones o las corporaciones que imposibilita de facto que las personas puedan cumplir con el deber ciudadano de denunciar los delitos de los que tengan conocimiento, así como denunciar comportamientos impropios, irregularidades o actividades ilícitas.
(…)
El uso de herramientas tecnológicas ahora permite ser más eficientes en la protección de la confidencialidad y anonimato de quien aporta información relevante. Esto permite corregir la mencionada asimetría. Debemos preservar el anonimato de las personas privadas porque son vulnerables cuando se exponen para proteger el bien común.

La diferencia entre anonimato y confidencialidad es que el anonimato es el único

que permite a la fuente de la información controlar en su totalidad su propia protección y el uso que se hace de la información. Ha quedada ampliamente demostrada la vulnerabilidad y porosidad de los sistemas de denuncia que se basan en la mera confidencialidad. Conlleva además peligros inherentes a que se centralice todo el poder (la información) en manos de unas pocas personas (directivos de corporaciones o superiores jerárquicos en las administraciones públicas), llevando a gravísimos abusos masivos, como ya ha pasado en otros momentos de la historia.

Es evidente que las corporaciones e instituciones deben cumplir sus deberes de transparencia e implementar sistemas de vigilancia de irregularidades. Aún así no es posible evitar abusos confiando en una suerte de autorregulación ya que el fraude y la corrupción se dan en posiciones privilegiadas respecto a tales sistemas internos. Por esto debemos aprovechar las oportunidades que nos ofrece ahora la tecnología y trazar cauces que nos permitan una vigilancia ciudadana distribuida.

El anonimato es la única protección real que se le puede ofrecer a un ciudadano alertador y ya ha sido reconocido como cauce justo y necesario en España por la Fiscalía en sus recomendaciones desde 1993, así como por diferentes disposiciones legales de nuestro ordenamiento y por organizaciones como la ONU en su Report on Encryption, Anonymity, and The Human Rights Framework de 2015".

HYPERLINK "http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx"http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx

HYPERLINK "http://www.europarl.europa.eu/stoa/webdav/site/cms/shared/0_home/STOA Study Mass Surveillance Part 1.pdf"http://www.europarl.europa.eu/stoa/webdav/site/cms/shared/0_home/STOA%20Study%20Mass%20Surveillance%20Part%201.pdf

HYPERLINK "https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/instruccion03_1993.pdf?idFile=12794dc6-9acc-4da0-bbc1-daf779e2f084"https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/instruccion03_1993.pdf?idFile=12794dc6-9acc-4da0-bbc1-daf779e2f084

Las innovaciones tecnológicas, disminuyendo considerablemente el riesgo de comprometer la identidad de quien denuncia, contribuyen, con toda seguridad, al objetivo de esta directiva y a una mayor eficacia en la lucha contra el fraude. Las hemos de integrar de forma explícita y positiva aunque sin ingenuidades – siempre que hay humanos pueden haber abusos.

En esta misma perspectiva y debido a que ya existen legislaciones contra las denuncias falsas, el artículo 17.2 de la propuesta de Directiva debe reformularse

de acuerdo con la Recomendación del Consejo de Europa (10) https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805c5ea5: " Los Estados miembros establecerán sanciones efectivas, proporcionadas y disuasorias aplicables a las personas que hagan revelaciones falsas, manteniendo la protección y aplicando las normas de la legislación general ".

3 - LIBERTAD PARA DETERMINAR EL CANAL DE DENUNCIA MÁS APROPIADO

El tercer problema puede por si solo desactivar gran parte de la utilidad de la Directiva.
En nuestra dilatada experiencia, la mayoría de los alertadores que han usado canales internos de la entidad que querían denunciar para denunciar abusos, solo han conseguido la destrucción de pruebas y mucho sufrimientos para ellos y sus familias.

La extensa obligación en el borrador de Directiva en pedir que primero se denuncie internamente, obligando al alertador a tener que demostrar que tiene muy buenos motivos para no hacerlo, en buena parte desactiva los objetivos de esta Directiva.
Estos “buenos motivos” no son definidos y son por eso dejado a la arbitrariedad, desincentivando absolutamente la denuncia.

Una la gran mayoría de los casos, el alertador no estaría amparado: piensen en Snowden o en el caso Luxleaks entre infinidad de otros.

Entendemos que el motivo es el de evitar inútiles efectos negativos para la reputación de una empresa, pero, por ejemplo en los casos anteriormente mencionados, no hubiera sido una solución.

No podemos aceptar esta restricción si no es acotada de forma extremadamente razonable, ya que **un solo caso** de ineficiencia de un canal interno debería ser suficiente motivo por no usarlo. Ser tajantes con esto tendría el efecto de obligar a las entidades a tener canales internos realmente eficaces y seria la única manera para legitimar que se deba usarlos en primera instancia.

Los dice la propia Directiva, pero luego es demasiado vaga la posibilidad de denuncia externa en primera instancia: “En otros casos, no se puede esperar razonablemente que los canales internos funcionen adecuadamente, por ejemplo, cuando las personas que presentan los informes tienen razones válidas para creer que sufrirían represalias en relación con la presentación de informes; que su confidencialidad no estaría protegida; que el titular de la responsabilidad final en el contexto laboral está involucrado en la violación; que la brecha podría ocultarse; esa evidencia puede ocultarse o destruirse; que la eficacia de las acciones de investigación por parte de las autoridades competentes podría verse

comprometida o que se requieren medidas urgentes" ("In other cases, internal channels could not reasonably be expected to function properly, for instance, where the reporting persons have valid reasons to believe that they would suffer retaliation in connection with the reporting; that their confidentiality would not be protected; that the ultimate responsibility holder within the work-related context is involved in the breach; that the breach might be concealed; that evidence may be concealed or destroyed; that the effectiveness of investigative actions by competent authorities might be jeopardised or that urgent action is required").

El art.13.e sobre la posibilidad de utilizar un canal externo en primer debería modificarse. de la siguiente manera: "se debe poder utilizar un canal externo cuando se tenga la creencia razonables de que el uso de canales internos de denuncia podría implicar represalias o poner en peligro la efectividad de las acciones de investigación por parte de las autoridades competentes o cuando el canal interno ha demostrado al menos una vez que su uso puede causar represalias y poner en peligro la efectividad de las acciones de investigación por parte de las autoridades competentes".

En estados muy corruptos, no hay otro modo que hacer publica la información para que personas poderosas no aplasten la verdad cuando operan contra el interés general.

Además en estos casos de uso de canales no internos que erróneamente la Directiva considera excepcionales, la misma no permite acudir a canales externos independientes, que no dependan de ninguna institución, como son los canales de ONG o medios de comunicación, cuando notoriamente en muchos casos son los más efectivos a la hora de que se preste atención a una denuncia.

En cuanto a este tema de la libertad de determinar el canal de denuncia, queremos llamar la atención sobre la declaración muy detallada de los expertos que participan en el Whistleblowing International Network (WIN):

"En realidad, la obligación de una denuncia previa por canales internos no es necesaria. Los estudios informan consistentemente que el 90-96% de los alertadores en empresas hacen sus revelaciones únicamente dentro de la institución. Hay muchos factores que inhiben fuertemente buscar otras opciones: miedo a represalias; una confianza y una identidad arraigadas con la organización del empleador; y consecuencias indirectas en relación con colegas y amigos, solo para nombrar algunos. Los alertadores solo informan al gobierno o a los medios en casos extremos de todos modos".

Y "El problema [en el borrador] es que dado que las excepciones a la obligación de informar internamente son subjetivas, los denunciantes deben adivinar si tienen derechos a la libertad de expresión yendo al gobierno o a los medios. No lo sabrán hasta que termine el juicio, después de un fallo sobre si su decisión fue segura o si se trata de un acto de suicidio profesional ".
Y "[esta medida] socavará la aplicación de la civil / penal y de la justicia: el

alertador pondrá sobre alerta quienes presuntamente cumplan los abusos antes de que las autoridades competentes lleguen a saberlo, dando un tiempo de tres a seis meses para el encubrimiento".

Todo esto nos lleva al cuarto punto.

4 – PROTECCIÓN DE INTERMEDIARIOS Y FACILITADORES

Según nuestra Plantilla de Proposición de Ley de Protección de los Alertadores https://xnet-x.net/proposicion-ley-proteccion-integral-alertadores/, el facilitador "es la persona física o jurídica que contribuye, facilita o ayuda al alertador a revelar o hacer pública la información constitutiva de una alerta."
En la gran mayoría de los casos, plataformas ciudadanas, ONGs, periodistas, sindicalistas son indispensable para ayudar el alertador y sufren también terribles represalias. El caso de Luxleaks HYPERLINK "https://en.wikipedia.org/wiki/Luxembourg_Leaks"https://en.wikipedia.org/wiki/Luxembourg_Leaks , en el que el periodistas ha sufrido la misma condena que el alertador, es solo un ejemplo.

A pesar de que los intermediarios y facilitadores son alabadas en la introducción de la Directiva [1], en el articulado desaparecen.
Es indispensable que reciban la misma protección de forma consistente en todo el articulado, tal y como proponemos en nuestra proposición HYPERLINK "https://xnet-x.net/proposicion-ley-proteccion-integral-alertadores/"https://xnet-x.net/proposicion-ley-proteccion-integral-alertadores/ ("es común que los facilitadores - la persona física o jurídica que contribuye, facilita o ayuda al alertador a revelar o hacer pública la información constitutiva de una alerta - incluyendo personas físicas y entidades legales tales como ONG y medios de comunicación, ayuden a los alertadores (...). Por lo tanto, el objetivo principal de la Ley, de conformidad con el sistema de garantías para denunciantes, es ofrecer protección para los divulgadores y facilitadores involucrados en el caso").

Concretamente y no exhaustivamente, el artículo 15.7 del borrador de Directiva solo cubre al "trabajador" no a quien publica y en la definición de "report" y "reporting person" *(Art.3 "Definition)* se ha de añadir quién facilita o publica si no se quiere poner en peligro la libertad de prensa y de información.

[1] Par. 31: "La protección contra las represalias como un medio de salvaguardar la libertad de expresión y la libertad de información debe ser proporcionada tanto a las personas que reportan información sobre actos u omisiones dentro de una organización (reporte interno) como a una autoridad externa (informes externos) y a las personas que divulgan dicha información al dominio público (por ejemplo, directamente al público a través de plataformas web o redes sociales, o a los medios, funcionarios electos, organizaciones de la sociedad civil, sindicatos u organizaciones profesionales / empresariales)" ("Protection from retaliation as a means of safeguarding freedom of expression and media freedom should be

provided both to persons who report information about acts or omissions within an organisation (internal reporting) or to an outside authority
(external reporting) and to persons who disclose such information to the public domain (for instance, directly to the public via web platforms or social media, or to the media, elected officials, civil society organisations, trade unions or professional/business organisations)").

5 - USO INDEBIDO DE LA PROTECCIÓN DE DATOS (Y OTROS DERECHOS Y LIBERTADES)

Este mal uso podría acarear graves perjuicios al derecho a la información y a la labor de los periodistas, entre otros.

Como se ha comentado, de lo que trata en general la protección de los alertadores es de corregir la asimetría entre los poderes fácticos y la gente de a pie.

No es baladí que cuando un alertador saca a la luz unos abusos, la respuesta de quien los perpetra no suele ser discutir o solucionar el abuso en cuestión, sino atacar al alertador sobre temas inherentes a la ofensa íntima y el orgullo personal y arrollarlo con juicios de este tipo.

En nuestra larga experiencia, mientras hace unos años los poderosos respondían prácticamente siempre abriendo demandas sobre delitos contra el honor o delitos contra la propiedad intelectual o los secretos comerciales (de ahí la larga batalla durante la aprobación del a Directiva de Secretos Comerciales de 2016 - HYPERLINK "http://blogs.publico.es/el-blog-de-xnet/secretos-comerciales/"http://blogs.publico.es/el-blog-de-xnet/secretos-comerciales/) – es necesario también un mejor articulado sobre estos extremos - , ahora está de moda acusar de revelación de datos personales.

Naturalmente nosotros somos activos defensores de los derechos a la privacidad de las personas de a pie. Pero también somos activos defensores de la importancia de la transparencia de las instituciones públicas y grandes corporaciones de sus miembros, justamente para rectificar la asimetría de la que hablamos (HYPERLINK "https://xnet-x.net/transparencia-y-privacidad/"https://xnet-x.net/transparencia-y-privacidad/), objetivo de la Directiva que nos ocupa.

La protección de datos no puede ni debe usarse como excusa para no denunciar ilegalidades (se indica en el Reglamento Europeo de Protección de Datos art. 85-86). Del mismo modo, en este ámbito no se puede usar el mismo baremo que se usa con un ciudadano corriente cuando se trata de servidores públicos o de directivos de empresas que repercuten sobre la gran mayoría de la población – a esos se limita el alcance de esta directiva.

Como hemos dicho anteriormente, muchas veces los abusos no son tratados con

efectividad si no se hacen públicos. Y no se pueden hacer públicos si no se indican las personas supuestamente responsables de los mismos.

Por esta razón, en aras de garantizar el pleno respeto de la libertad de expresión y de información que enuncia la Directiva, solo los datos personales relacionados con el ámbito privado y que no aportan ningún valor informativo – datos tales como números de teléfono, dirección de correo electrónico, dirección del domicilio, así bien como los de privados y personas no responsables del ilícito, deben permanecer ocultos en todo momento y prevalecer sobre la libertad de información.
En este sentido ya se ha expresado la sentencia del Tribunal Europeo de Derechos Humanos sobre el caso del Comité húngaro de Helsinki HYPERLINK "https://www.helsinki.hu/en/magyar-helsinki-bizottsag-v-hungary/"*https://www.helsinki.hu/en/magyar-helsinki-bizottsag-v-hungary/*.

Se ha –entonces- de recalcar que la carga de la prueba debe favorecer al alertador y, como ya hemos dicho, su objetivo y razones no deben reducir la utilidad objetiva de sus revelaciones - no olvidemos que el objetivo último de la Directiva no es moral sino el de eliminar los abusos de las instituciones.

Consideramos indispensable que esta precisión sobre el alcance de la protección de datos personales sea más explicita en el articulado y que se ha de modificar el párrafo 73 de la directiva que dice "...en caso de la supuesta adquisición, uso o la divulgación del secreto comercial se llevó a cabo para revelar la mala conducta ... " (..in case the alleged acquisition, use or disclosure of the trade secret was carried out for revealing misconduct...), porque significaría que el alertador debería probar cuales son sus razones, mientras que el único requisito debería ser el de que las pruebas sean objetivamente indicios de un abuso.

Los alertadores no son santos ni diablos, sus razones personales son...personales. El aura romántica alrededor de los alertadores debe cesar, para que la práctica de denunciar abusos sea una normalidad en una sociedad democrática. Esto debería ser el objetivo último de la Directiva.

XNET - EDRi (European Digital Rights)
En colaboración con Courage Foundation
Con el apoyo (in progress) de Expose Facts, Institut de Drets Humans (IDHC), Electronic Frontier Norway y Loïc Dachary