FIBGAR

blueprint for FREE SPEECH

EXPANDIENDO TECNOLOGIA DE ANONIMIZACION EN EUROPA

Autores: Naomi Colvin, Veronika Nad, Chris Culnane, Bruno Galizzi, Dr. Suelette Dreyfus

Diseño: Ilva Letoja

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

Co-financiado por el Fondo de Seguridad Interna de la Unión Europea. Este informe ha sido posible en parte gracias a las subvenciones del Fondo de Seguridad Interior de la Unión Europea - Policial, y por la Open Society Initiative for Europe dentro de la Open Society Foundations. Su contenido representa únicamente la opinión de los autores y es de su exclusiva responsabilidad. La Comisión Europea no acepta ninguna responsabilidad por el uso que pueda hacerse de la información que contiene.

Tabla de Contenido

Capítulos

1. Resumen Ejecutivo

El proyecto *Expandiendo Tecnología de Anonimización* (en inglés *Expanding Anonymous Tipping*, EAT) se creó con el objetivo de ampliar la base de usuarios de buzones digitales seguros, especialmente en empresas privadas e instituciones públicas, en 11 Estados miembros del sur y el este de Europa. Nueve organizaciones asociadas participaron en el proyecto, que se desarrolló entre enero de 2018 y enero de 2021.

El trabajo sobre el terreno en esos 11 Estados miembros de la UE arroja valiosos conocimientos sobre los factores que llevan a las organizaciones a adoptar los buzones digitales seguros como una vía para realizar comunicaciones en entidades públicas o como parte de sus propios mecanismos de cumplimiento interno. Un segundo elemento clave del proyecto fue ampliar la base de conocimientos sobre este tipo de buzones y su uso en la práctica. En este informe final se explican los antecedentes del proyecto y los logros alcanzados a lo largo de esos dos años.

A la luz de nuestros hallazgos, proponemos un conjunto de herramientas para la presentación de informes coherentes y que preserven la privacidad de las métricas clave, con el fin de evaluar los resultados de los buzones. Anticipamos que esto será útil tanto para futuros investigadores como para las organizaciones que estén considerando adoptar una solución segura de buzón digital como parte de sus requisitos en virtud de la Directiva de la UE 2019/1937 sobre la protección de las personas que alertan sobre infracciones de la legislación de la Unión ("la Directiva de la UE sobre alertadores").

Las nueve organizaciones asociadas al proyecto son ONG con actividades en los ámbitos de la lucha contra la corrupción, la investigación y la promoción de políticas, la transparencia y el derecho a saber, el desarrollo de los medios de comunicación, el desarrollo de tecnologías seguras, el periodismo y los derechos humanos. A través de sus comunidades locales, buscaron organizaciones de los sectores público y privado que estuvieran dispuestas a participar en la instalación de buzones digitales seguros para realizar divulgaciones. Para ello fue necesario desarrollar un proceso de integración de los buzones en distintos tipos de instituciones, que tenían culturas institucionales y de gobernanza diferentes.

Entre los países de la UE que han participado figuran Hungría (*Atlatszo*, periodismo), Rumanía (*Centru Pentru Journalism*), España (*FIBGAR*, derechos humanos), Italia y Malta (*The Good Lobby*, incidencia política), Bulgaria y Croacia (*Media Development Center*), la República Checa y Eslovaquia (*Oživení*, derecho a saber) y Grecia (*Transparency International*, anticorrupción). Además de estos territorios clave de EAT, la ONG internacional *Blueprint for Free Speech* también ha trabajado como asociada en la investigación sobre la adopción y difusión de estos buzones digitales en Chipre, y la *Fundación Hermes* de Italia proporcionó la plataforma técnica de divulgación GlobaLeaks.

Es la primera vez que un proyecto como éste se ha probado a escala con buzones digitales seguros en cualquier parte del mundo. El carácter audaz del proyecto puso a prueba los límites, descubrió obstáculos sorprendentes e hizo descubrimientos aplicando tecnologías innovadoras de encriptación y anonimización con el fin de hacer más seguras las sociedades. Las lecciones aprendidas se recogen en nuestras recomendaciones. El despliegue de leyes nacionales de protección de los denunciantes en 27 países durante un período de dos años, que se completará a finales de 2021, es también una audaz primicia mundial. En última instancia, transformará los sistemas de integridad que sustentan el funcionamiento cotidiano de estas sociedades. Esperamos que las ideas de este informe sirvan para informar y apoyar esa transición.

1. Resumen Ejecutivo

Conclusiones

El valor de los buzones

Los buzones digitales seguros generan más comunicaciones o denuncias de alertadores en general. La promoción, el seguimiento de la respuesta a los alertadores y el compromiso demostrado por parte del operador del buzón contribuyen a aumentar la confianza en el sistema. (Capítulo 2)

La adopción de estos buzones se está extendiendo más allá de los primeros que comenzaron a usarlos: los medios de comunicación y organizaciones afines. Hay importantes lecciones que aprender de la experiencia de los pioneros en instituciones públicas y privadas para garantizar una mayor difusión. (Capítulo 2)

Las autoridades públicas que han implantado este sistema de buzón digital han comprobado que son un instrumento de gran valor. (Capítulo 4)

La posibilidad de mantener una comunicación continua con el denunciante es una característica especialmente valorada de los sistemas de buzones digitales seguros. (Capítulo 3)

Obligaciones legales

Las obligaciones legales marcan la diferencia en la adopción en el momento en que se convierten en legislación nacional. Este es el caso concreto de los países en los que aún no existen marcos de denuncia de irregularidades. (Capítulo 2)

La transposición nacional de la Directiva 2019/1937 de la UE sobre la protección de alertadores debe apoyar la introducción de métodos de denuncia anónimos. (Capítulo 4)

Gobernanza

Las cuestiones de gobernanza son una de las principales preocupaciones de las organizaciones que se plantean implementar este tipo de buzones digitales. (Capítulo 2)

La falta de claridad sobre la relación de los procedimientos de denuncia o alerta de irregularidades con otros ámbitos normativos, por ejemplo, en la protección de datos, inhibe la adopción de buzones digitales seguros. (Capítulo 4)

Las autoridades deberían considerar la posibilidad de proporcionar una guía para ayudar a las organizaciones a implementar canales internos. (Capítulo 4)

Los procedimientos de libertad de información pueden ser un ejemplo a seguir. La próxima norma ISO 37002 también puede servir de orientación. (Capítulo 4)

1. Resumen Ejecutivo

Usabilidad y seguridad

Los buzones por sí solos no son una garantía de anonimato. Para garantizar la confidencialidad es importante que una correcta configuración desde los administradores. (Capítulo 3)

Los gestores del buzón deben estar preparados para que los usuarios hagan hasta el uso menos seguro del canal, incluso si tienen la intención de permanecer en el anonimato. (Capítulo 5)

Cuando es probable que la garantía de anonimato sea el aliciente principal de las denuncias, los gestores deberían considerar dar advertencias explícitas a los usuarios o imponer el uso del navegador Tor para acceder a un canal de denuncia. (Capítulo 5)

Puede ser que finalmente se necesiten un conjunto de tecnologías, más allá del buzón seguro. Los ejemplos incluyen un chat en vivo bidireccional que proporcione un verdadero anonimato y recurrir a las capas que ofrecen navegadores como Tor. (Capítulo 5)

Normas de información segura

Las métricas del buzón para los alertadores deben ser reportadas usando privacidad diferencial para proteger la identidad de las personas que reportan. (Capítulo 5)

Se debe tener especial cuidado cuando el número absoluto de envíos es pequeño. Es preferible informar de las tendencias que de las cifras absolutas. (Capítulo 3)

Apoyo adicional a la investigación

La nueva funcionalidad añadida a la plataforma GlobaLeaks debería facilitar la investigación cuantitativa. (Capítulo 5)

Hemos propuesto un conjunto de herramientas para informar de las métricas del buzón digital basadas en la privacidad diferencial. (Capítulo 5)

Facilitar el acceso a un mensajero anónimo seguro desde la interfaz del buzón probablemente mejoraría la calidad de los informes que se generan. (Capítulo 5)

Se necesita seguir investigando para determinar las mejores prácticas y evaluar qué enfoques educativos funcionan mejor a fin de guiar a los usuarios hacia el uso de Tor. (Capítulo 5)

1. Resumen Ejecutivo

Recomendaciones:

- Deben destinarse recursos a la concienciación de la ciudadanía de los Estados miembros de la UE sobre:
  - alertar sobre irregularidades,
  - las opciones de anonimato y confidencialidad que ofrece la tecnología y los buzones digitales

- Tales recursos mejoran la seguridad al combatir la corrupción, pero también mejoran la conciencia pública de la ciberseguridad en general. Tienen un doble uso.

- Desarrollar estándares sobre una acción voluntaria y un etiquetado de garantía de calidad que las acompañe, que ayude a los consumidores a elegir con conocimiento de causa las opciones que tienen para comunicar la alerta.
  - Los consumidores en este caso pueden ser organizaciones que eligen un servicio para cumplir con la nueva Directiva, pero también los propios alertadores
  - Usar tecnología de **código abierto** tiene que formar parte de ese proceso para infundir confianza y seguridad

- Crear modelos reutilizables para que las organizaciones adopten en términos de estructuras de gobernanza humana detrás de la tecnología de los propios buzones, con el fin de gestionar y responder a las revelaciones
  - La falta de estructuras de gobierno es un **déficit importante**, y **una barrera para la implementación**.
  - Asimismo es una cuestión urgente, ya que las nuevas leyes nacionales entrarán en vigor en 2021
  - **Ni el sector empresarial y ni el público están preparados** y, en muchos casos, ni siquiera son **conscientes** de ello. Los socios de nuestro proyecto se encontraron con esta situación **de forma reiterada en 11 países**.
  - Esta falta de preparación no solo se refiere a los buzones digitales, sino también a requisitos más básicos que introducirá la Directiva.

- Construir un repositorio central de metadatos anonimizados de dichos buzones en toda Europa, para permitir un estudio y una medición precisa del impacto.
  - Es probable que esto requiera un apoyo visible de la Comisión Europea para tener éxito. Las agencias necesitan "permiso" e incentivos para compartir los datos.
  - El diseño debe basarse en la experiencia técnica en la reidentificación de datos para proteger a los alertadores.
  - Las estadísticas anuales de resultados deben ser de fuente abierta en beneficio de los organismos reguladores, de la aplicación de la ley, del cumplimiento y de la investigación, así como de los grupos de la sociedad civil de responsabilidad pública

- Apoyar el desarrollo y la difusión del software de código abierto y de uso gratuito que apoya la aplicación de la Directiva de la UE.
  - Esto incluye emplear el software del buzón digital como ejemplo, los servicios de *onion routing* (enrutamiento cebolla), un chat seguro integrado y otros programas similares
  - Reunir todo esto en un solo lugar como recurso para el sector empresarial y el sector público en todos los Estados miembros puede ser útil y rentable, especialmente para las empresas más pequeñas que tendrán que afrontar nuevos costes a fin de cumplir con la Directiva y una curva de aprendizaje empinada.

2. Introducción

La corrupción es un impuesto sobre la actividad económica de la sociedad. Si queremos hacer un intento serio de combatir la corrupción, la alerta anónima es una de las mejores herramientas a nuestra disposición, un medio tanto para detectar las prácticas corruptas como para evitar que se produzcan. (Johanssen & Carey 2015). Los alertadores suelen desempeñar un papel fundamental a la hora de descubrir el fraude, la mala gestión y el despilfarro, al revelar información que de otro modo pasaría desapercibida y no se denunciaría.

Diferentes estudios confirman que las revelaciones internas tienden a ser más eficaces para detectar el fraude que las auditorías externas. En su Estudio Global sobre el Fraude de 2016, la *Association of Certified Fraud Examiners* (Asociación de Examinadores de Fraude Certificados, con sede en Estados Unidos) identificó las delaciones anónimas como el método de detección más eficaz, al tiempo que determinó que el impacto anual del fraude en los casos que examinaron superaba los 6.000 millones de euros. También los directivos de empresas señalan a las alertas como el medio "más eficaz" para detectar el fraude. (Association of Certified Fraud Examiners 2016, Bausa 2016)

Hacer una revelación puede ser una empresa arriesgada para el alertador. Los ejemplos del mundo real de alertadores que se enfrentan a represalias, despidos o sanciones legales por hablar son demasiado frecuentes, incluso cuando los alertadores utilizan los canales y procedimientos de denuncia designados. No es de extrañar que los estudios de investigación muestren que los alertadores, y en particular aquellos que se perciben a sí mismos en riesgo de sufrir consecuencias negativas, son más propensos a presentarse, si pueden hacerlo, sin revelar su identidad. (Kenny 2019, Johanssen & Carey 2015, Agers & Kaplan 2005)

Por lo tanto, la combinación de estos dos elementos (facilitar las revelaciones protegidas, así como proteger a los alertadores) es fundamental para los esfuerzos anticorrupción. Como reconoció el G20 en sus Principios de Alto Nivel para la Protección Eficaz de los Alertadores, "el riesgo de corrupción aumenta en los entornos en los que no se facilitan y protegen las denuncias". (G20 2019)

La Directiva de la UE sobre protección de alertadores, que se aprobó cuando se estaba desarrollando el Proyecto EAT, proporcionó un antecedente esencial para nuestras actividades. La forma en que las nuevas obligaciones legales interactúan con la voluntad de las organizaciones de adoptar los mecanismos del buzón digital es un tema clave de este informe.

La Directiva reconoce la importancia de la comunicación de irregularidades en la lucha contra la corrupción y el fraude, aunque el ámbito de aplicación de la legislación es más amplio, ya que incluye todas las violaciones de la legislación de la Unión. Aunque la Directiva no impone directamente la provisión de canales de denuncia anónimos, se indica explícitamente como una opción que los Estados miembros puede legislar en ese punto. Blueprint for Free Speech ha elaborado una herramienta online para evaluar los proyectos de legislación nacional a medida que van apareciendo. (Directiva de la UE 2019; Blueprint for Free Speech 2020)

La evolución de la práctica de la alerta anónima

La tecnología permite que la alerta anónima sea más accesible que en el pasado. La llegada del buzón digital seguro permite a las personas que alertan hacer una revelación online, que puede incluir la presentación de documentos que son la fuente de la investigación, con la confianza razonable de que su identidad no será

2. Introducción

revelada cuando esos documentos salgan a la luz. Hay, por supuesto, factores independientes de la forma en que se transmite la información que podrían traicionar la identidad de un alertador. Algunos de ellos se resumen en el Apéndice G.

Los sistemas de buzón digital seguro suelen utilizar la red *Tor* para ocultar el origen digital de cualquier material enviado. Algunos sistemas están configurados para ser accesibles únicamente a través de la red Tor, lo que requiere que el alertador descargue el *Tor Browser Bundle* para acceder al buzón[1]. En este caso hay un equilibrio entre la accesibilidad y la seguridad. Una vez que se recibe un envío, se encripta y se transmite a los destinatarios designados.

Los sistemas seguros de buzón en línea también suelen permitir a los que hacen las revelaciones continuar una conversación con la persona que recibe el envío, normalmente proporcionando una contraseña que permite volver a consultar un informe en una fecha posterior. Se trata de una poderosa combinación de características que es difícil de replicar de forma tan segura con otras formas más antiguas de comunicación anónima, como el correo o el teléfono.

El buzón seguro en línea como tecnología tiene menos de 15 años. Inicialmente se desarrollaron para que los alertadores pudieran revelar información sensible a los medios de comunicación y al público directamente[2]. En este sentido, tuvieron un enorme éxito. No es una coincidencia que la visibilidad pública de la alerta de irregularidades y el apoyo a la protección de los alertadores haya aumentado drásticamente desde la primera aparición de noticias importantes facilitadas por la tecnología del buzón.

También en este sentido, los buzones digitales seguros han contribuido de forma significativa a la lucha contra la corrupción. Muchas de las principales revelaciones de interés público de los últimos 15 años han transformado la comprensión de cuestiones complejas como el blanqueo de dinero y la evasión fiscal por parte de la opinión pública. En varios casos, las autoridades han podido utilizar la información aparecida en las noticias para iniciar investigaciones y tomar medidas al respecto. Un ejemplo de ello son algunas de las importantes investigaciones periodísticas llevadas a cabo por el *Consorcio Internacional de Periodismo de Investigación* (ICIJ) y del *Proyecto de Información sobre Crimen Organizado y Corrupción* (OCCRP).

En la actualidad existen dos sistemas de código abierto establecidos: GlobaLeaks, financiado por *Hermes* (Italia), socio de EAT, y SecureDrop (EE.UU.), mantenido por *Freedom of the Press Foundation* (Fundación para la Libertad de Prensa), con sede en Estados Unidos. Un gran número de medios de comunicación emplean estos sistemas y cada vez más organizaciones y organismos públicos los están adoptando como canales de información. También existen sistemas comerciales operados o vendidos por diferentes entidades. Un ejemplo de ello es el sistema Business Keeper (BKMS), desarrollado por un proveedor alemán.

Entre ellos, GlobaLeaks y SecureDrop representan la abrumadora mayoría de las instancias periodísticas de buzones digitales seguros, así como muchas otras. Hacer un seguimiento de cuántos buzones online están activos

_____

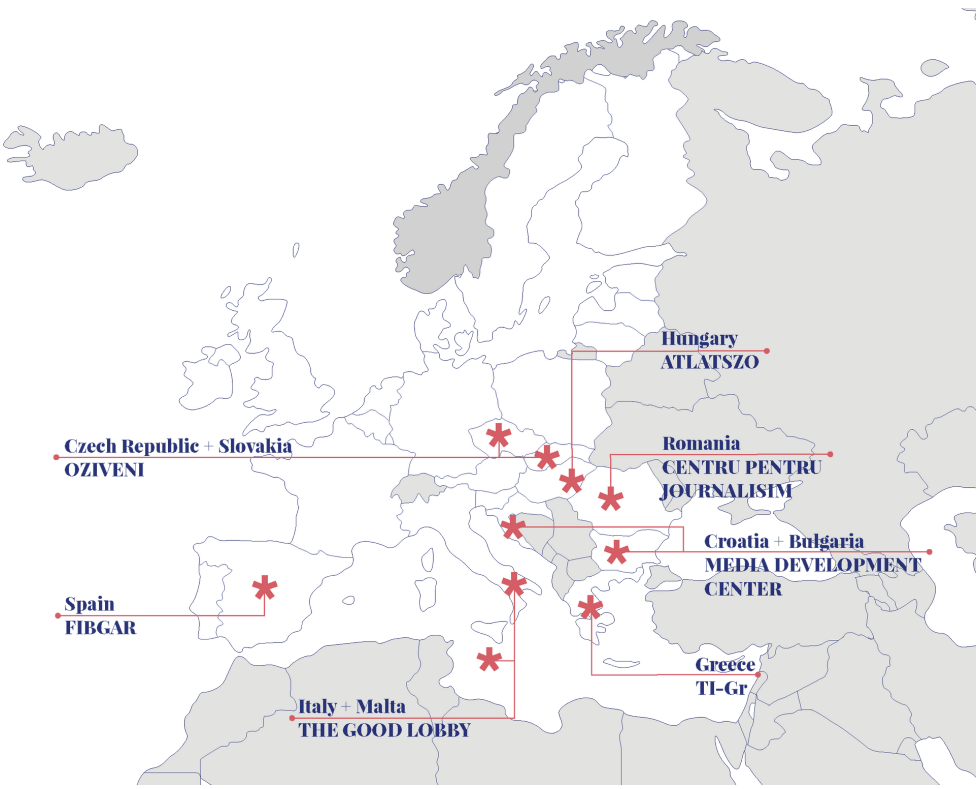
1. Cuando este informe se refiere a un envío a través del buzón "usando Tor", se hace referencia a esta configuración más segura en la que el usuario está obligado a acceder al buzón a través de la red Tor.
2. El buzón de WikiLeaks, generalmente considerado como el primero del mundo, fue lanzado en 2007.

2. Introducción

y quién los gestiona resulta complejo, ya que en última instancia no hay ninguna restricción sobre quién puede usar e instalar software de código abierto y las aplicaciones de código cerrado pueden no hacer públicas sus listas de clientes (Di Salvo 2020: 99). Para ver una lista de las entidades existentes con Globaleaks y SecureDrop, basada en la información actual de *Hermes* y la *Freedom of the Press Foundation*, véase el Apéndice A.

Expanding Anonymous Tipping (EAT)

El proyecto EAT se creó para facilitar la adopción y el uso de las tecnologías del buzón digital seguro en los 11 Estados miembros de la UE con las puntuaciones más bajas en el Índice de Percepción de la Corrupción de Transparencia Internacional. Muchos de estos países también carecen de marcos coherentes de protección de los alertadores y los introducirán por primera vez con la transposición de la Directiva de la UE sobre denunciantes a la legislación nacional. Los países del Proyecto EAT son Bulgaria, Croacia, Chipre, República Checa, Grecia, Hungría, Italia, Malta, Rumanía, Eslovaquia y España.



Un objetivo clave de EAT ha sido la difusión activa de las tecnologías de buzón seguro por parte de las organizaciones asociadas sobre el terreno, que cuentan con los conocimientos locales en sus respectivos países. Junto con *Hermes*, los socios de EAT son *Atlatszo*, con sede en Hungría; *Centru Pentru Journalism*, de Rumanía; *FIBGAR*, de España; *The Good Lobby*, con sede en Italia y también responsable del proyecto en Malta; *Media Development Center*, de Bulgaria, que también se ha acercado a los beneficiarios de Croacia; *Oživení*, responsable de la República Checa y Eslovaquia, y *Transparency International* Grecia. Además de estos territorios clave de EAT, el socio de investigación *Blueprint for Free Speech* también ha trabajado en la implantación del buzón digital en Chipre.

2. Introducción

Durante el proyecto, las organizaciones locales asociadas se pusieron en contacto con instituciones públicas y privadas (en adelante, "beneficiarios") para fomentar la adopción de la tecnología del buzón digital seguro basada en GlobaLeaks, suministrada y financiada por la organización asociada *Hermes*. Los socios de EAT también podían dirigirse a los medios de comunicación y a las organizaciones periodísticas de los países en los que trabajaban. Los buzones de EAT se alojan en una plataforma específica de disclosers.eu, con una disposición que permite ampliar el apoyo más allá del alcance de la financiación del proyecto.

Aunque la llegada del Covid-19 y el consiguiente bloqueo interrumpieron el proceso de incorporación de varias organizaciones asociadas, el proyecto EAT ha dado lugar a la instalación de nuevas peticiones de buzones digitales por parte de instituciones públicas y empresas privadas en Bulgaria, Chipre, la República Checa, Grecia, Italia, Rumanía y España. Es probable que le sigan otros una vez que los requisitos de la Directiva de la UE se hayan transpuesto a las respectivas legislaciones nacionales. En el Apéndice C figura una lista completa de los buzones instalados en el marco del Proyecto EAT, que están activos a partir del 26 de enero de 2021.

Buzones digitales seguros y el entorno normativo

Dada la aprobación de la Directiva de la UE sobre la protección de los alertadores en abril de 2019, a mitad del plazo del proyecto, el cumplimiento de los próximos requisitos legales formaba parte de la oferta. De acuerdo con los términos de la Directiva, todas las entidades que emplean a 50 personas o más están obligadas a establecer canales para comunicar irregularidades, al igual que las organizaciones facultadas para recibir informes externos ("organizaciones responsables").

Los sistemas de buzones digitales ofrecen una forma de implantar estos canales y tienen también otras potenciales ventajas, que pueden ayudar a cumplir otros requisitos de la Directiva. Al hacer un seguimiento de cuándo se presentan y se acusa recibo de las comunicaciones, así como de la forma en que se abren y concluyen las investigaciones, los sistemas de buzones pueden ayudar a las organizaciones a cumplir los artículos de la Directiva sobre mantenimiento de registros y gestión de casos.

La Directiva también establece requisitos estrictos de confidencialidad: las propiedades de anonimato de los sistemas de buzón pueden ser útiles en este caso, en combinación con políticas organizativas sólidas sobre el tratamiento de la información. La confidencialidad es clave incluso cuando las comunicaciones pueden hacerse de forma anónima. Esto es particularmente crítico en términos de canales internos. En organizaciones pequeñas o medianas, puede ser posible saber de quién procede una revelación con bastante certeza aunque no esté firmada. En estos casos, la credibilidad de los procesos de alerta dependerá de que el operador del buzón respete cierto grado de confidencialidad.

De ello se deduce que los sistemas de buzón digital seguro no son una solución total en sí mismos. La eficacia de los canales basados en los buzones también depende de la eficiencia e integridad de los sistemas en la parte receptora y, en particular, de los canales de denuncia externos, con configuración institucional más amplia.

2. Introducción

La experiencia de las organizaciones asociadas al EAT puso de manifiesto la necesidad de claridad en los requisitos legales. En muchos casos, las organizaciones se mostraron reticentes a la hora de adoptar la tecnología antes de la transposición nacional de la Directiva, sobre todo en los países en los que la transposición supondrá la primera introducción de normas de protección de los alertadores.

Las organizaciones también estaban preocupadas, no tanto por la instalación del buzón como por la gobernanza interna y las normas que serían necesarias para apoyarlo. Se expresó preocupación por la interacción de los mecanismos de denuncia de irregularidades con otros ámbitos normativos, en particular la protección de datos. Algunas organizaciones expresaron su deseo de que la transposición nacional traiga consigo orientaciones oficiales que aclaren exactamente lo que deben hacer para cumplir con la normativa. Las próximas recomendaciones de la norma ISO 37002 sobre sistemas de denuncia de irregularidades pueden servir para un propósito similar. (Pop 2021)

La incertidumbre normativa dificulta la implementación

El país “E” forma parte del Proyecto EAT en el que actualmente no existe una legislación independiente de protección de los alertadores. Varias autoridades municipales, comprometidas con los planteamientos de su organización local asociada al EAT, eran conscientes de los requisitos legales para instalar en el futuro canales de comunicaciones.

A pesar de este interés, los ayuntamientos se mostraron reacios a avanzar antes de que los requisitos de la Directiva se hubieran transpuesto a la legislación nacional. Se expresó la preocupación de instalar un canal con carácter "informal". Consideraban la transposición nacional completa como una especie de autorización para hacer algo de lo que no estaban seguros.

Una de las preocupaciones clave ha sido la gobernanza interna. Un municipio estableció una analogía con los procedimientos de acceso a la información publica, donde se sabía exactamente lo que había que poner en marcha y cómo relacionarlo con el resto de la organización. En la actualidad, la situación de los canales de comunicación de alertas es menos clara y no se ha querido dedicar recursos a desarrollar un sistema que podría ser sustituido por la legislación nacional en un futuro próximo.

Esta inquietud por parte de las organizaciones potencialmente beneficiarias influyó en nuestro enfoque de otros aspectos del proyecto, que supuso algunos cambios respecto a nuestro plan original. Inicialmente, los socios del proyecto se habían acercado a la ampliación de los buzones seguros con la idea de que se podría invitar a las grandes organizaciones a proporcionar canales seguros adecuados, pero si se negaban a hacerlo, se podría crear una instancia de GlobaLeaks dirigida, por ejemplo, a la dirección de correo electrónico del departamento de cumplimiento normativo para plantear preocupaciones. Este tipo de presión podría funcionar bien para un grupo que emprendiera una acción contra la corrupción.

Sin embargo, cuando los socios empezaron a relacionarse con posibles organizaciones beneficiarias, la situación se hizo mucho más clara. La comunidad de empresas y organismos públicos tenía tan poco conocimiento de la denuncia de irregularidades, y mucho menos de los buzones seguros, que había que hacer una enorme labor educativa. Los socios descubrieron que estas comunidades a menudo ni siquiera podían ponerse de acuerdo en una sola palabra, traducida al idioma local, para describir el hecho de comunicar una irregularidad.

2. Introducción

Los socios de EAT dedicaron más tiempo a tratar de explicar lo que podía hacer un buzón y lo que era la denuncia de irregularidades como sistema de integridad que a tratar de negociar acuerdos para incorporar a los beneficiarios al proyecto sin coste alguno para ellos.

Algunos de los potenciales beneficiarios ni siquiera tenían idea de que la legislación llegaría a través de la transposición nacional, y otros se negaban a creer que se aprobaría realmente. Esta afirmación se repite en las reuniones con altos funcionarios e incluso con parlamentarios que tampoco sabían nada de la aprobación de la Directiva ni del calendario de aplicación. La respuesta varía según el país.

En la oscuridad

En algunos casos estaba claro que los responsables políticos nacionales estaban completamente desinformados sobre la protección de los alertadores y los requisitos legales que se avecinaban en el horizonte. Sencillamente, no estaban preparados para un debate sobre los canales de denuncia.

En uno de los países, un socio del EAT mantuvo varias reuniones telefónicas con el funcionario federal encargado de la formación del personal en materia de anticorrupción e integridad. Esta persona no conocía los cambios legislativos que se avecinaban, ni la Directiva, ni la denuncia de irregularidades ni los buzones digitales.

El socio del EAT se dio cuenta de que, para ganar a cualquier departamento u organismo como beneficiario, primero tendríamos que coorganizar amplias sesiones de formación con el personal, y esto requeriría una gran cantidad de aprobación y gastos administrativos. También es probable que hubiera necesitado cartas de apoyo de la Comisión para poder llevarlo a cabo.

Explorar la Denuncia Anónima

El marco temporal del Proyecto EAT abarcó un periodo en el que la tecnología tras los buzones sigue avanzando y en el que los requisitos legales están entrando en vigor. Sin embargo, hemos comprobado que la adopción no puede darse por sentada. Hay que tener en cuenta una serie de factores.

Este informe examina sucesivamente algunas de estas cuestiones.

2. Introducción

Un elemento clave del Proyecto EAT ha sido ampliar la base de conocimientos en torno a los buzones online seguros. En el capítulo 3 se analiza el estado de los conocimientos académicos antes del inicio del proyecto EAT y cómo esto influyó en nuestra agenda de investigación inicial. Muchas de estas ideas se han confirmado: los problemas prácticos en torno a la adopción previstos por la investigación anterior se han visto reflejados en la experiencia de los socios del EAT.

Hasta la fecha, la investigación sobre los buzones seguros en línea se ha basado en gran medida en datos cualitativos, basadas en entrevistas, más que en datos cuantitativos, utilizando metadatos derivados de las propias circunstancias de los buzones. No obstante, la adopción de la tecnología de los buzones seguros por parte de las agencias nacionales y regionales, y en particular algunos trabajos pioneros en España, ha elevado el listón de la información sobre los resultados de los buzones, que se ha hecho necesaria tanto para el seguimiento interno como para la rendición de cuentas externa. En consecuencia, el capítulo 3 plantea la necesidad de contar con unas normas de información coherentes que protejan la privacidad y que, al mismo tiempo, permitan realizar comparaciones significativas entre las circunstancias del buzón.

La expansión de la denuncia anónima requiere comprender la tecnología y cómo se ha utilizado hasta la fecha. También requiere entender qué argumentos son los más atractivos en la práctica para convencer a entidades públicas y privadas de que instalen los buzones. El capítulo 4 examina la experiencia de los socios de EAT a la hora de acercarse a las organizaciones potencialmente beneficiarias tanto en el sector público como en el privado, en particular su actitud hacia la divulgación anónima. Esto suele ser una propiedad técnica clave para los que promueven los buzones digitales seguros, pero no es necesariamente el argumento más convincente para aquellos a los que intentan dirigirse.

Para contextualizar nuestra investigación, entrevistamos a un grupo variado de operadores de buzones. Entre ellos se encontraban organizaciones de los ámbitos de la lucha contra el fraude, la regulación, los medios de comunicación y otros. Entrevistamos a operadores de GlobaLeaks y SecureDrop, un grupo más amplio que los directamente implicados en el propio proyecto EAT, con el fin de analizar el tema a través de diferentes tipos de tecnología utilizada para el mismo fin. En el Apéndice D se ofrece información sobre los entrevistados.

Por último, a lo largo del proyecto, hemos ido preparando el terreno para realizar mejores estudios cuantitativos sobre los buzones online seguros. Desde el principio, la intención era que las nuevas instancias de dropbox que surgieran del proyecto EAT fueran capaces de producir datos comparativos significativos para llenar el vacío de la investigación[3]. El capítulo 5 explica cómo nuestras hipótesis de investigación han dado lugar a que Hermes realice cambios para garantizar que los metadatos estén disponibles en el futuro dentro de la plataforma de GlobaLeaks, algo que ayudará a los operadores de buzones y facilitará en gran medida las investigaciones futuras.

Además de aumentar la disponibilidad de los metadatos, está claro que hay preocupaciones sobre la privacidad asociadas a los datos enviados a través de los buzones digitales seguros que deben abordarse. Aunque es probable que las métricas estándar sean útiles para aumentar la comprensión de la eficacia de los buzones en el futuro, hay que tener cuidado al informar sobre ellas. En el capítulo 5 proponemos un innovador conjunto de herramientas basado en la privacidad diferencial que permitirá realizar comparaciones significativas sin el riesgo de identificar los envíos individuales y exponer a los usuarios de los buzones.

3. Los metadatos son información sobre los envíos realizados a través de una plataforma concreta, en contraposición al contenido de los propios envíos.

3. Entendiendo tecnología de anonimización

Evolución de los buzones digitales y la agenda de investigación de EAT

La llegada del buzón digital seguro no sólo ha cambiado la forma en que se produce la comunicación o denuncia de irregularidades, sino que ha supuesto un cambio fundamental en la visibilidad y la percepción pública de los alertadores. En consecuencia, puede decirse que los buzones digitales seguros han contribuido a aumentar la presión pública en favor de la protección de los alertadores en la legislación. La aplicación de esta tecnología en sí misma apenas tiene 15 años. (Vandekerckhove 2016)

En este capítulo se describen los principales avances en la evolución de estos buzones, antes de examinar las cuestiones centrales de la investigación en las que se basó el proyecto EAT, que a su vez, se inspiró en trabajos anteriores en este ámbito.

Dentro de la relativamente corta vida de la tecnología de los buzones seguros, es posible identificar tres "olas" distintas de adopción. Aunque desde 2001 se ofrecían sistemas de integridad comercial, la primera generación de buzones que hemos identificado se inspiró directamente en el ejemplo de la organización *WikiLeaks*, que fue pionera en el buzón digital seguro en 2007 y llamó la atención del público en general en 2010 y 2011 como resultado de las propiedades de anonimato de ese sistema incorporado en el buzón. Otras organizaciones pronto intentaron copiar la pionera innovación. Al no existir sistemas de buzones desarrollados externamente para que las organizaciones los adoptaran, la primera generación de buzones digitales para medios de comunicación se montaba a veces de forma precipitada y sus propiedades de anonimato y seguridad no siempre sobrevivían al escrutinio de expertos en tecnología.

En 2013, los dos principales sistemas de buzones de código abierto que se utilizan hoy en día, GlobaLeaks y SecureDrop, estaban disponibles para que las organizaciones externas los adoptaran. Aunque los principales usuarios de los buzones en esta segunda oleada seguían siendo principalmente organizaciones de medios de comunicación y grupos de la sociedad civil afines a los medios de comunicación, hubo cierto grado de innovación en los modelos de colaboración y el flujo de trabajo adoptados por los operadores de los buzones. Las organizaciones descubrieron que el buzón era una tecnología flexible que podía adaptarse a sus necesidades particulares.

La tercera y última ola de implantación aquí considerada se refiere a la expansión de los buzones digitales seguros más allá de su uso en los medios de comunicación, llegando a empresas privadas e instituciones públicas, en particular las administraciones locales y las autoridades anticorrupción. Esta evolución ha sido impulsada en parte por los cambios legales que exigen la introducción de canales internos, como en Italia, pero también por la innovación del sector público apoyada por la sociedad civil, como se ha visto en las Autoridades Anticorrupción de Cataluña (*Oficina Antifrau de Catalunya* o OAC) y de Valencia (*Agencia Valenciana Antifraude* o AVAF), ambas en España.

La expansión de la tecnología de las denuncias más allá del periodismo y la sociedad civil presenta cuestiones nuevas y diferentes. La gobernanza interna, el cumplimiento de la normativa y la presentación de informes externos son áreas que se han puesto de manifiesto gracias a la experiencia de los socios de EAT en la promoción de los buzones sobre el terreno. Esto es especialmente cierto cuando los organismos del sector privado han contratado dichos canales a empresas externas. La naturaleza de estos canales de divulgación tiene ventajas,

3. Entendiendo tecnología de anonimización

como la percepción de independencia y, por tanto, de fiabilidad. Sin embargo, las protecciones técnicas y la gestión de la información entrante no están estandarizadas ni existe ningún "sello de aprobación" de la industria en el que puedan confiar los que realizan las divulgaciones y los que compran los servicios para garantizar la calidad.

La llegada de las métricas publicadas por las instituciones públicas significa que podemos empezar a responder a las preguntas sobre el uso de los buzones y su eficacia en términos cuantitativos y cualitativos. En la actualidad, nos encontramos en el inicio de este proceso. Este capítulo describe el estado de los conocimientos existentes sobre algunas de estas cuestiones clave, que a su vez han informado la agenda de investigación del Proyecto EAT. En el capítulo 5 se explica cómo el Proyecto EAT pretende facilitar la respuesta a estas preguntas en el futuro.

Apoyo público a la mejora de la protección de los alertadores

Estudios recientes muestran un importante apoyo público a la protección de los alertadores en los países del proyecto EAT.

Una encuesta nacional realizada por Blueprint For Free Speech en España en colaboración con *IPSOS* en octubre de 2020 muestra que el 71% de los españoles piensa que se debería apoyar a los alertadores en lugar de castigarlos, incluso si revelan información interna de las organizaciones. Este apoyo se confirma en todas los tramos de edad y grupos sociales.

Otra encuesta reciente realizada por el socio del proyecto EAT, *Oživení*, en la República Checa, mostró que el 56% de los encuestados tenía una reacción positiva hacia los alertadores, pero la mayoría (71%) no estaba familiarizada con el concepto antes de que se les explicara. La familiaridad con el término "whistleblower" (alertador) era mayor entre los licenciados y los más jóvenes.

Esto indica que la concienciación entre la ciudadanía sigue necesitando sensibilización para dar a conocer este tema. La aprobación de la Directiva de la UE está cambiando activamente la percepción pública de la denuncia de irregularidades.

Primera generación de buzones digitales

Los buzones digitales seguros comenzaron a desarrollarse con el fin de hacer públicas información sensibles, aprovechando los métodos criptográficos para proporcionar cierta garantía de que los envíos pudieran hacerse sin revelar la identidad del remitente. A raíz de la notoriedad que alcanzaron las publicaciones de *WikiLeaks* en 2010

3. Entendiendo tecnología de anonimización

y 2011, varios medios de comunicación y organizaciones de la sociedad civil aprovecharon de inmediato el potencial de esta tecnología, aunque esta primera oleada de dropboxes no siempre se aplicó de forma muy eficaz. (Chen 2011, Sifry 2011, Greenberg 2012)

Al Jazeera y *The Wall Street Journal* crearon sus propios dropboxes en 2011, que imitaban la idea de *WikiLeaks* sin replicar sus propiedades de seguridad. Ambos proyectos fueron rápidamente criticados por sus defectos en materia de seguridad. Al final, ambos tuvieron una vida bastante corta[4]. Sin embargo, esta primera oleada sirvió para que otros desarrollaran el tipo de solución tecnológica "off the shelf" que claramente se necesitaba.

Sobreviven muy pocos buzones digitales de esta época, como el sistema Briefkasten del periódico alemán *Die Zeit*, que se lanzó en julio de 2012. Este proyecto - "una aplicación web razonablemente segura para enviar contenidos de forma anónima"- sigue siendo utilizado por *Die Zeit* y parece que se mantiene activo. El código empleado es de código abierto y auditable.

Un poco más comunes son los proyectos periodísticos o de la sociedad civil iniciados en esta época que han dejado de lado los sistemas de dropbox caseros o sui generis para adoptar sistemas desarrollados por terceros. El buzón digital de la *Comisión de Ética y Anticorrupción de Kenia* data originalmente de 2013 y desde 2015 se basa en el sistema de envío de BKMS. *BalkanLeaks* es un ejemplo de plataforma de "primera ola" de 2010 que ha evolucionado para reflejar las mejores prácticas en el diseño de buzones digitales. *BalkanLeaks* adoptó SecureDrop en 2013, poco después de que el sistema se hiciera público. La plataforma sigue en línea hoy en día, operada por el colectivo periodístico búlgaro *Bivol*. (Arnold 2020, Di Salvo 2020: 104)

Los inicios de los buzones digitales seguros forman parte de un movimiento más amplio de investigación colaborativa, de trabajo periodístico y de derechos humanos innovador que la tecnología ha hecho posible, y que en gran parte ha permitido una mayor participación en estas áreas de la que había sido posible anteriormente. Los analistas señalan en este sentido el papel emergente de las redes online en el trabajo periodístico y el de los derechos humanos. En algunos casos, como el de ipaidabribe.com de la India o el proyecto Rospil de Alexei Navalny, los proyectos se han convertido en sinónimos de movimientos sociales y políticos más amplios. (Arnold 2020).

¿Por qué es seguro un buzón digital?

La seguridad técnica ha sido un área importante de debate durante la "primera generación" de adopción de dropboxes y lo sigue siendo en la actualidad. Desgraciadamente, las propiedades de seguridad de los buzones también es un tema que se trata de forma inconsistente en las investigaciones académicas.

Un estudio sobre los sistemas online para alertadores define un sistema de comunicación de irregularidades como aquel que "*permite a los usuarios presentar denuncias de alertadores de forma anónima a través de Internet*". En este sentido, el anonimato tiende a significar algo más que la simple capacidad de hacer una revelación sin un nombre unido a ella. Está inextricablemente ligado a otras tecnologías de comunicación seguras que ofrecen cierto grado de resistencia a la vigilancia. (Lowry, Moody y Galetta 2014: 155, Di Salvo 2020)

_____
4. En la actualidad, ambas publicaciones utilizan instancias de SecureDrop.

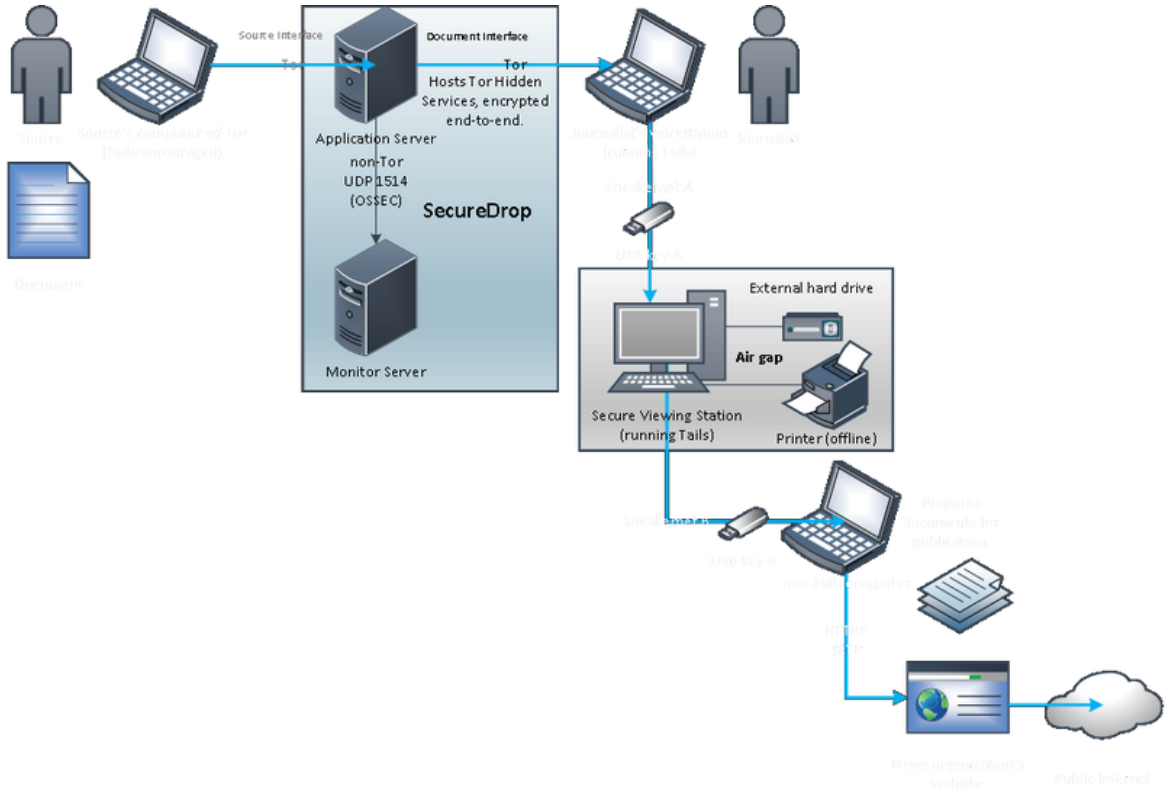
3. Entendiendo tecnología de anonimización

Casos de uso de GlobaLeaks

En algunos ámbitos, sigue habiendo una gran diversidad en los tipos de soluciones de denuncia digital que las organizaciones ponen a disposición. Esta fue la conclusión de una encuesta sobre plataformas de federaciones deportivas y agencias antidopaje realizada en 2017, un ámbito que había experimentado un período de rápido crecimiento como resultado de una serie de escándalos públicos. Los autores de esa encuesta descubrieron que el "nivel de sofisticación" en los canales de denuncia variaba de forma tan drástica (desde los buzones alojados externamente hasta las direcciones de correo electrónico suministradas) que era "difícil determinar cómo son las buenas prácticas en este contexto". (Universidad Leeds Beckett 2018)

De hecho, hay un mayor grado de consenso sobre lo que constituye un "buen" sistema de alerta online seguro de lo que esto sugiere. (Bausa 2016, Zafia et al 2017, Palumbo 2017) Hoy en día hay dos soluciones principales de buzón digital de código abierto -y por lo tanto auditables- con propiedades de seguridad ligeramente diferentes. Mientras que ambos sistemas, GlobaLeaks y SecureDrop, utilizan Tor, este último solo es accesible para los usuarios a través del paquete Tor Browser, en lugar de un navegador de Internet normal, mientras que GlobaLeaks permite a los operadores de buzones digitales establecer configuraciones alternativas. La variación en las opciones de diseño se debe en gran medida a los casos de uso previstos (el "modelo de riesgo") adoptados por los diferentes proyectos.

3. Entendiendo tecnología de anonimización



La seguridad de un SecureDrop

SecureDrop está diseñado para atender aplicaciones de alto riesgo (el ejemplo por excelencia es la revelación de un crimen transnacional a una importante redacción) mientras que GlobaLeaks está pensado para ser utilizado en un conjunto más amplio de situaciones. El hecho de que los potenciales denunciantes estén obligados a utilizar Tor para acceder al dropbox en lugar de un navegador de Internet normal, o que puedan hacerlo, es sólo una de las varias diferencias entre los dos sistemas.

Qué sistema adoptar es una decisión que, por tanto, requerirá un análisis de necesidades por parte de la organización en cuestión. Un informe de una evaluación de este tipo en un entorno académico indonesio describe por qué se eligió GlobaLeaks frente a SecureDrop. Básicamente se debió a acuerdos "más simples" y menos costosos para la configuración y el mantenimiento. (Zafia et al 2017)

La experiencia del equipo de Blueprint for Free Speech en la formación de los medios de comunicación en materia de ciberseguridad para proteger sus fuentes también ha funcionado así. Sirva como ejemplo el caso de un importante periódico con el que trabajamos, que optó por ofrecer dos vías para las revelaciones: una opción de alta seguridad de SecureDrop y otra de menor seguridad más fácil de usar. Esto tuvo éxito, ya que la mayoría de las divulgaciones se hicieron a través de la opción de menor seguridad, ya que era más fácil de usar. Sin embargo, la opción de alta seguridad seguía existiendo para las fuentes que estaban preocupadas por su seguridad personal, por ejemplo.

3. Entendiendo tecnología de anonimización

Evolución de los usos de los buzones: desde la sociedad civil y los medios de comunicación hasta las instituciones públicas y privadas

Más allá de estos relatos sobre la primera ola de interés en los sistemas de buzones digitales seguros a principios de la década, uno de los trabajos más detallados sobre la evolución del uso de los buzones es el reciente estudio del académico Philip Di Salvo, que examina un grupo de 21 buzones a lo largo de 2015. Entonces, tanto GlobaLeaks (cuyo primer prototipo se puso a disposición en 2011) como SecureDrop (lanzado públicamente en 2013) estaban a disposición de las organizaciones interesadas en adoptarlos.

Cuándo no es seguro utilizar la opción de alta seguridad

Los modelos de riesgo pueden ser complejos y el perfil de seguridad de SecureDrop significa (de forma un tanto poco intuitiva) que hay entornos en los que no es seguro utilizarlo.

En los países en los que se vigila el uso de Internet, el uso de la red Tor puede marcar a un individuo como sospechoso. En estas circunstancias, la fundación Freedom of the Press desaconseja el uso de SecureDrop y recomienda que los posibles operadores, en este caso predominantemente organizaciones de medios de comunicación, utilicen métodos alternativos.

El renovado interés por las tecnologías de mejora de la privacidad tras las revelaciones de Edward Snowden sobre la vigilancia online generalizada (Di Salvo 105) contribuyó a su implementación en ese momento. Como atestiguan numerosos estudios, esta importante noticia aumentó la conciencia del impacto de la vigilancia en el periodismo de investigación en general. Las redacciones se han visto obligadas a integrar las tecnologías de mejora de la privacidad en su práctica diaria y, a su vez, ha aumentado considerablemente el esfuerzo que se ha dedicado a desarrollar herramientas accesibles diseñadas para usuarios no expertos.

Signal, el protocolo y aplicación de mensajería instantánea encriptada, es uno de los ejemplos más exitosos de esto. (Blueprint for Free Speech 2018, Wiener 2020)

El estudio de Di Salvo, el primer intento de encuestar a una serie de operadores de Dropbox y encontrar puntos de comparación entre ellos, tiene como objetivo esencial comprender la heterogeneidad en un campo relativamente joven, en el que diferentes organizaciones estaban tratando de entender cómo hacer el mejor uso de la nueva tecnología. Di Salvo limita su estudio a las organizaciones "con un claro rasgo periodístico", que en ese momento representaban los principales usuarios de la tecnología. (Di Salvo 2020: 92)

Las organizaciones "con un claro perfil periodístico" es un grupo más amplio que las organizaciones con personal o dirigidas por periodistas e incluye a las ONG o grupos de activistas que suministran información a los periodistas o publican noticias basadas en la información que les llega. Incluye varias organizaciones asociadas al EAT. Sin embargo, los criterios de Di Salvo excluyen claramente a muchas de las organizaciones beneficiarias del EAT y a varias de las que hemos entrevistado.

Las plataformas estudiadas por Di Salvo incluyen 13 buzones de GlobaLeaks y 7 basados en la plataforma SecureDrop, con un sistema sui generis operado por el periódico alemán *Die Zeit*. No todas esas plataformas

3. Entendiendo tecnología de anonimización

siguen activas en la actualidad. De hecho, cuatro de los buzones estudiados por Di Salvo quedaron inactivos durante el estudio (enero-diciembre de 2015). La lista de buzones analizados en el estudio de Di Salvo se incluye en el Apéndice B.

La investigación se basó en entrevistas semiestructuradas de entre 30 y 45 minutos, complementadas con correo electrónico y conversaciones online y en persona. En general, las organizaciones de medios de comunicación tradicionales, limitadas por la necesidad de proteger sus fuentes, se mostraron más reacias a participar en la investigación, en comparación con las ONG y los grupos de activismo. Esto se ve reforzado por algunas decisiones políticas de los propios desarrolladores de Dropbox: la fundación *Freedom of the Press* suele desaconsejar a los usuarios de SecureDrop que hablen de los envíos, lo que incluye la identificación del papel de la plataforma en la generación de noticias.

El grupo de entrevistados de Di Salvo incluía organizaciones de medios de comunicación tradicionales, grupos de periodistas como cooperativas de trabajo o sindicatos, ONG y activistas. El investigador señaló que, en todas las organizaciones que encuestó, el acceso a los informes enviados a través del sistema de buzón online seguro estaba restringido a un número relativamente pequeño de personas. Su principal conclusión fue que los operadores de estos buzones eran innovadores en la forma en que situaban estos canales en su propio contexto organizativo y que eran posibles varios modelos diferentes de trabajo[5]. (Di Salvo 2020: 128)

De hecho, Di Salvo encontró cuatro grandes "enfoques y estrategias editoriales" entre las plataformas que estudió.

El primero lo denominó "plataformas editoriales". No se trata de organizaciones periodísticas tradicionales, sino que publican documentos fuente o sus propias historias a partir de los documentos que se les presentan. Un ejemplo sería el proyecto MagyarLeaks del socio de EAT, *Atlaszo*.

La segunda categoría identificada por Di Salvo son las plataformas colaborativas, que no publican filtraciones en sí, sino que forman un puente entre los alertadores y los periodistas.

Entre los ejemplos citados en esta categoría se encuentra el dropbox Wildleaks, enfocado a la preservación del Medio Ambiente.

Una tercera categoría son las plataformas integradas por múltiples partes con diferentes intereses. Éstas se basan en una funcionalidad específica disponible en la plataforma GlobaLeaks que permite a los que envían informes decidir a qué destinatarios, de entre una selección, debe llegar la revelación. Se trata principalmente de un servicio técnico y puede permitir que las comunicaciones se dirijan a periodistas o investigadores que trabajan para organizaciones totalmente diferentes. Este tipo de colaboración entre organizaciones de medios de comunicación es singular. Entre los ejemplos de plataformas multipartitas que siguen funcionando en la actualidad se encuentran Sourcesûre, Publeaks.nl y MexicoLeaks.

_____

5. En este sentido, Di Salvo se basa en el anterior estudio de Micah Sifry sobre WikiLeaks, que describe a la organización experimentando con diferentes formas de trabajo; desde operar como una especie de fuente para los periodistas, a un productor de contenidos a un facilitador de asociaciones periodísticas entre otras organizaciones de medios de comunicación. (Sifry 2011)

3. Entendiendo tecnología de anonimización

Por último, Di Salvo identificó una serie de plataformas de medios de comunicación, operadas por organizaciones de medios tradicionales para sus propios fines internos. Este es el modelo de trabajo más conocido para los buzones digitales seguros y la mayoría de las instalaciones de SecureDrop, que se ha adaptado a las principales redacciones, encajan en esta categoría.

Mirando más allá del ámbito temporal de su estudio, Di Salvo señala que después de 2015, los modelos de trabajo siguieron evolucionando y algunos periodistas también pusieron en marcha de forma individual sus propios buzones personales. Entre ellos, Jean-Marc Manach en Francia, Barton Gellman en Estados Unidos y Stefania Maurizi en Italia.

Aunque Di Salvo identificó una gran innovación en el mundo de los operadores de dropboxes, sobre todo en lo que respecta a la colaboración entre periodistas de diferentes organizaciones, existe una similitud básica entre las organizaciones que estudió. En algunos aspectos importantes, esto las diferencia de las instituciones privadas y públicas a las que se dirige el proyecto EAT como posibles beneficiarios.

Medios de comunicación dedicados a las noticias y otras entidades que podrían tratar con fuentes confidenciales de forma similar tienen un flujo de trabajo particular que a menudo está predefinido por las políticas existentes. Aunque la era digital plantea retos para los periodistas que trabajan con fuentes, los principios generales que rigen estas relaciones están bastante bien desarrollados. Una de las lecciones de la tercera ola de adopción de Dropbox -de la que forma parte el proyecto EAT- es que los entornos normativos y las políticas internas son fundamentales para la implantación generalizada de estos canales de denuncia.

Una tercera ola de adopción del buzones digitales: de la sociedad civil a las instituciones

Al mismo tiempo que Di Salvo estudiaba a los operadores de buzones seguros, la expansión de estos mecanismos en las instituciones públicas se estaba acelerando. El impulso para instituir un buzón de la ciudad de Barcelona data de 2015, cuando la activa agitación de la sociedad civil se encontró con un nuevo gobierno municipal receptivo. La puesta en marcha del buzón de Barcelona en colaboración con la organización de la sociedad civil Xnet en enero de 2017 allanó a su vez el camino para la Agencias Antifraude de Cataluña y Valencia siguieran su ejemplo en diciembre de 2017 y mayo de 2018 respectivamente. (Cambio de rumbo 2017, Xnet 2017, Beltrán 2018)

La difusión de los buzones seguros en las instituciones públicas coincidió con la introducción de obligaciones legales en el sector financiero. La Directiva 2015/849 de la UE sobre la prevención del blanqueo de capitales introdujo requisitos de un canal "específico, independiente y anónimo" para de información interna. Esto fue lo que impulsó a la Autoridad Federal de Supervisión Financiera (BaFin) de Alemania a establecer su propio buzón seguro en línea. La ley italiana n.º 179/2017 ha animado igualmente animado a muchas autoridades públicas a adoptar sistemas de dropbox.

También hubo algunos precedentes de autoridades españolas que solicitaron informes públicos, aunque no por medio de un buzón online seguro. Organismos nacionales como la *Comisión Nacional de los Mercados y la Competencia*, el *Ministerio de Trabajo y Seguridad Social* y la *Agencia Tributaria* habían solicitado previamente informes al público de alguna forma. (Benítez Palma 2018)

3. Entendiendo tecnología de anonimización

Pero lo ocurrido en Barcelona tenía muchas novedades. La *Directora de Analítica del Ayuntamiento de Barcelona* ha relatado el inicio de los buzones digitales seguros del Ayuntamiento y en su exposición destaca la relevancia de la construcción institucional que precedió a la puesta en marcha de este mecanismo. (Sánchez 2019)

El buzón de Barcelona se concibió como una vía para que los ciudadanos se pusieran en contacto con el ayuntamiento con información que correspondiera a un amplio mandato anticorrupción, solicitando información sobre cuestiones que pudieran afectar al buen gobierno. A finales de 2015 se creó una *Oficina de Transparencia y Buen Gobierno*. El buzón, basado en GlobaLeaks, se puso en marcha aproximadamente un año después, el 2 de enero de 2017.

Mientras tanto, se crearon varios comités. Se invitó a representantes de la sociedad civil a participar en un *Consejo Asesor de Transparencia*, que se creó en 2016. Hubo que formular una serie de reglamentos antes de la puesta en marcha del buzón para garantizar el cumplimiento de las normas de protección de datos y otras legislaciones. En 2018, se creó un Comité de Ética con funciones de supervisión para resolver las cuestiones derivadas del funcionamiento del buzón.

La experiencia de Barcelona ilustra cómo el establecimiento de canales de denuncia externos dentro de las organizaciones existentes puede ser más complejo que para los buzones seguros operados por periodistas o activistas. Cuando las investigaciones pueden requerir cambios en la organización que alberga el buzón, es fundamental definir las líneas de responsabilidad, las reclamaciones y otros procedimientos de gobernanza interna. Hacer este trabajo institucional desde cero, como ocurrió en Barcelona, requirió una importante inversión organizativa. Al final, la experiencia de Barcelona sirvió para que las dos agencias regionales de lucha contra la corrupción la adoptaran.

La llegada de la analítica

Otra consecuencia importante de la "tercera ola" de adopción de buzones digitales seguros es que se ha empezado a publicar una serie, aunque limitada, de medidas cuantitativas sobre el funcionamiento de esos buzones. Esto ofrece la posibilidad de obtener una visión diferente a la que se tenía hasta ahora, ya que las investigaciones anteriores sobre buzones se basaron en gran medida en los datos de las entrevistas.

Esta provisión de datos es incipiente y la información disponible no es exhaustiva, pero no por ello deja de ofrecer algunas perspectivas interesantes, que intentamos investigar más a fondo en el proyecto EAT. Hasta la fecha se han publicado cifras parciales del Ayuntamiento de Barcelona para los años 2016 y 2017 y de la *Agencia Valenciana Antifraude* para los años 2017-19. (Sánchez 2019, Agencia Valenciana Antifraude 2020)

Dada la naturaleza de los buzones digitales seguros, cualquier publicación de datos cuantitativos debería limitar la posibilidad de "reidentificar" las presentaciones que se han realizado de forma anónima. Esta es una preocupación especialmente grave en los casos en que el número total de presentaciones de denuncias es relativamente pequeño. En este sentido, las convenciones de información adoptadas en estas primeras publicaciones de datos pueden no ser óptimas. En el capítulo 5 se analiza detalladamente cómo solucionar este problema.

3. Entendiendo tecnología de anonimización

Página de inicio del buzón GlobaLeaks de la Agencia Antifraude de Valencia

Una cuestión absolutamente fundamental es si los alertadores utilizan realmente los buzones online seguros y si generan informes procesables. Una cuestión relacionada con ello es si, como forma de alerta anónima, los buzones digitales seguros generan informes más procesables -o útiles- que otros métodos de denuncia.

Las investigaciones anteriores sugieren cierta relación entre la propensión de los alertadores a presentar informes y su capacidad para hacerlo sin revelar su identidad. Un estudio australiano de 231 empresas que cotizan en bolsa, basado en las respuestas enviadas a la encuesta bianual de fraude de *KPMG* en 2004, 2006, 2008 y 2010, encontró que las empresas que operan con canales de divulgación anónimos informaron haber recibido más informes de fraude. (Johanssen & Carey 2015)

Una fuente de información relacionada son los informes anuales de la *Agencia Nacional Anticorrupción de Italia*. En virtud de la Ley Anticorrupción nº 190/2012, las instituciones públicas deben presentar anualmente información sobre sus procedimientos de denuncia.

Los académicos que han analizado estos datos han encontrado una fuerte correlación entre el número de denuncias recibidas y las organizaciones que han instalado un buzón seguro en línea ("un sistema de información dedicado con medidas criptográficas y sistemas de seguridad internos"), aunque estas organizaciones representaron una pequeña proporción del total. La asociación fue menos clara para los tipos más débiles de canal de denuncia. (Previtali & Cerchiello 2017: 11, Palumbo & Manna 2019: 14)

Sin embargo, cabe destacar que el número absoluto de informes de comunicaciones recibidas por estas organizaciones es bastante pequeño. Dado que se trata de canales de denuncia internos de instituciones individuales y no de canales externos operados por organismos nacionales o regionales, esto no es del todo

3. Entendiendo tecnología de anonimización

sorprendente. Sin embargo, refuerza la necesidad de tener cuidado al informar sobre los resultados del buzón para no volver a identificar las denuncias.

Un estudio en el que se examinaron los informes presentados por 69 universidades italianas de titularidad pública a la *Autoridad Nacional Anticorrupción* en los años 2015 y 2016 reveló que solo una cuarta parte de las instituciones (69 de un total de 365) había recibido al menos un informe durante esos dos años. En los casos en que las instituciones habían recibido al menos un informe, la media de informes recibidos en todo el periodo de dos años era de entre 2 y 3. Evidentemente, con cifras tan reducidas, la presentación de informes conlleva el riesgo de identificar informes individuales. (Previtali & Cerchiello 2017)

Las cifras de los buzones españoles son de una magnitud diferente, como cabría esperar. Las cifras de Barcelona sugieren un aumento significativo de las denuncias tras el lanzamiento del buzón seguro en línea el 2 de enero de 2017. El director de análisis de Barcelona afirma que en 2016 se recibieron 63 denuncias, que aumentaron a 499 en 2017. De esta cifra de 2017, 479 informes se dirigieron a través del buzón seguro en línea y 204 de ellos se presentaron de forma anónima. (Sánchez 2019)

Asimismo, la Memoria de la Agencia Valenciana Anticorrupción de 2019 ofrece cifras de denuncias recibidas a través de todos los canales de comunicación (incluidos el correo electrónico y el correo postal) para los periodos anteriores y posteriores a la puesta en marcha del buzón online seguro de la Agencia en mayo de 2018.

Agencia Antifraude de Valencia - Informe anual 2019

Comunicaciones recibidas en todos los canales de denuncia.

2017 - 35
2018 - 181
2019 - 168

En Valencia, la proporción de comunicaciones procedentes del buzón online seguro ha ido creciendo año tras año. Las comunicaciones realizadas a través del buzón representaron el 54% de todas las denuncias recibidas en 2018, a pesar de que el buzón comenzó a funcionar en mayo de ese año. Las comunicaciones del buzón representaron entonces el 76% de todas las denuncias realizadas en 2019. Curiosamente, las denuncias anónimas representaron el 50% de todas las recibidas en ambos años. (Agencia Valenciana Antifraude 2020)

Los datos de Valencia incluyen más detalles sobre las denuncias recibidas -no todas llegaron a través del buzón-, incluyendo su temática. Los temas más frecuentes de las comunicaciones fueron contratación pública y recursos humanos. A partir de los limitados datos disponibles, la agencia parece haber recibido un número cada vez mayor de comunicaciones (del 8% en 2018 al 16% en 2019) sobre cuestiones que no son de su competencia formal. Esto sugiere que existe una demanda para que los canales de divulgación estén disponibles en otras áreas.

La Agencia Valenciana también proporciona cierta información para las investigaciones abiertas y su estado. Gran parte de esta información se refiere a categorías internas - "en investigación", "en análisis", "pendientes", "interrumpidas"-, por lo que puede ser difícil de comparar con otras organizaciones, incluso si se dispusiera de datos comparables.

3. Entendiendo tecnología de anonimización

A partir de la limitada información disponible de Barcelona y Valencia, podemos decir que parece haber una fuerte correlación entre la presencia de un buzón digital seguro y un aumento de las comunicaciones. Cabe destacar que ambos buzones se pusieron en marcha con la atención de los medios de comunicación nacionales y, en el caso del municipio de Barcelona, internacionales.

El impacto de los marcos legales en las denuncias de los alertadores

Los datos italianos también ofrecen algunas indicaciones sobre la eficacia de los requisitos legales para conseguir que las instituciones instalen canales internos. Un sistema de denuncia de irregularidades era uno de los requisitos de la Ley anticorrupción nº 190/2012, pero la aprobación de la legislación por sí sola no ha sido suficiente para garantizar su adopción. La propia *Agencia Nacional Anticorrupción* identificó este problema en 2015.

Un estudio realizado tras la aprobación de la ley anticorrupción nº 190/2012 analizó un grupo de 365 administraciones públicas italianas, integrado por 86 hospitales, 137 organismos sanitarios, 39 universidades y 103 municipios importantes. Del grupo de 365, solo 240 organizaciones informaron de que habían adoptado canales de denuncia de irregularidades, a pesar de estar obligadas a hacerlo. Sólo 43 organizaciones implantaron un sistema de buzón seguro, en lugar de un número de teléfono o una dirección de correo electrónico. No obstante, las que lo hicieron recibieron más denuncias en general. (Previtali & Cerchiello 2017)

¿Son esenciales la promoción y las sugerencias?

Proporcionar canales de denuncia anónima puede ser una señal importante sobre la cultura ética de una organización. Algunos analistas han considerado que esta es su función más importante, y que la adopción de canales de denuncia está motivada por el deseo de mejorar la percepción externa de la organización, quizá en respuesta a un escándalo, siendo la eficacia de ese canal una preocupación muy secundaria. (Pitroff 2013: 409, Leeds Beckett University 2017, Verschuuren 2019)

Este no es necesariamente siempre el caso: al menos un estudio ha encontrado que las empresas que cotizan en bolsa con consejos independientes, que indican generalmente altos estándares de gobierno corporativo, eran más propensas a instituir canales de denuncia anónimos que otras. También puede ocurrir que los potenciales alertadores sean sensibles a ser etiquetados así. Varios estudios han revelado que una mayor confianza en el sistema establecido en una organización (incluyendo quién tiene la responsabilidad de tratar una denuncia y cuál podría ser el resultado) es un importante factor determinante para que las personas quieran denunciar. (Johanssen & Carey 2015, Pitroff 2013)

Es por ello que la presencia de un buzón digital seguro puede no ser suficiente para garantizar que se utilice la instalación, especialmente en un entorno en el que las personas se sienten amenazadas por las represalias. Varios estudios han analizado qué factores generan confianza en los sistemas de denuncia. La sanidad, donde la notificación de información es de vital importancia, ha sido un foco de atención particular para algunos de estos estudios.

3. Entendiendo tecnología de anonimización

Interpretando de la ausencia de comunicaciones

Un socio del EAT señaló que un buzón online seguro operado por un municipio no había recibido ninguna denuncia. Se hizo hincapié en que la ausencia de denuncias no debía interpretarse como una señal de que todo iba bien en la organización.

El buzón se había instalado tras una serie de escándalos y lo gestionaba una sola persona, un alto cargo en el municipio. La organización asociada indicó que esto no sólo podría suponer un filtro para cualquier denuncia que se presentara, sino que había razones para dudar de que la revisión de las denuncias fuera realmente independiente.

El ayuntamiento no había llevado a cabo ninguna campaña de concienciación para apoyar su buzón y no estaba claro hasta qué punto iba a aparecer en su nueva página web. La organización asociada concluyó que, en este caso, es poco probable que los potenciales denunciantes confíen en el nuevo buzón.

Si se observan los datos facilitados a la *Agencia Nacional Anticorrupción de Italia*, parece haber una relación entre la formación específica en materia de denuncia de irregularidades (en contraposición a la formación general en materia de ética) y la frecuencia de las denuncias recibidas en las instituciones sanitarias. (Previtali & Cerchiello 2017)

Además, un estudio piloto de un hospital británico que emplea a entre 700 y 800 médicos en formación descubrió que el respaldo del personal superior, la participación de los compañeros y la retroalimentación constante aumentaban la propensión de los médicos a utilizar un sistema de denuncias en línea.

Se puso a prueba un sistema de comunicación de quejas relativamente menores a través de la web para que los médicos en formación pudieran notificar preocupaciones como el nivel de personal que, aunque importantes, no podían ser canalizadas a través de los sistemas existentes para notificar incidentes importantes. El sistema instituido no cumplía los requisitos de un sistema de envío anónimo: en la práctica, cualquier envío individual podía vincularse trivialmente a un médico individual, independientemente de que incluyera o no su nombre junto con su informe. Sin embargo, se utilizaron otros medios para fomentar la confianza en el sistema.

3. Entendiendo tecnología de anonimización

Entre ellos, la publicidad interna (por ejemplo, con carteles en las áreas de personal), pero también las recomendaciones cara a cara en las reuniones de personal. La confianza en el sistema se vio favorecida por el hecho de que un médico en formación fuera uno de los tres miembros del personal encargados de responder a los informes. (Carr et al 2016)

Otros investigadores han observado que la retroalimentación, incluido el informe mensual de las denuncias recibidas, ha resultado valiosa para animar a las personas a presentar quejas. Con el paso del tiempo, un historial de respuesta puede convertirse en un componente clave de la confianza en el sistema. (Bausa 2016; Lowry, Moody, Galetta 2014)

4. Experiencias de los socios del EAT y de otros operadores de buzones

Expanding Anonymous Tipping requiere comprender qué argumentos son los más atractivos en la práctica para las organizaciones públicas y privadas a las que se podría convencer de que adopten buzones digitales seguros. Este capítulo examina la experiencia de los socios de EAT a la hora de acercarse a las organizaciones beneficiarias potenciales del sector público y privado, un proceso que ha producido resultados concretos y muchas ideas enriquecedoras.

Para contextualizar las cuestiones de investigación expuestas en el capítulo anterior, entrevistamos a un grupo variado de operadores de buzones y a quienes se dedican a promover el uso de los buzones entre los demás. Para este conjunto de entrevistas, nos dirigimos a un grupo más amplio que el de los directamente implicados en el Proyecto EAT, incluyendo importantes organizaciones de medios de comunicación, organizaciones que gestionan instancias de SecureDrop y dos organizaciones con sede fuera de la Unión Europea.

Lo que sigue se basa en un grupo de entrevistas cualitativas semiestructuradas realizadas entre agosto y diciembre de 2020. El grupo incluye tanto autoridades públicas como organizaciones no gubernamentales.

No todas las organizaciones entrevistadas gestionan ellas mismas buzones online seguros. Algunas (como la *Fundación Freedom of the Press*, con sede en Estados Unidos, que mantiene el sistema de código abierto SecureDrop) centran sus actividades en la difusión de sistemas de denuncia anónima en instituciones públicas y privadas.

Entre los entrevistados que sí gestionan sus propios buzones, existe una gran diversidad en la forma en que se aplican y utilizan esos canales de denuncia. Las organizaciones entrevistadas difieren en su misión y objetivos generales, en los recursos de que disponen y en su percepción de las necesidades de seguridad de quienes les denuncian. Las condiciones socioculturales y políticas regionales también influyen en el uso de los buzones digitales seguros.

Buzones seguros en línea y revelaciones anónimas

Para muchas de las organizaciones entrevistadas, dotar de buzones online seguros era sinónimo de facilitar medios para realizar denuncias o comunicaciones de forma anónima. En general, esto se consideraba una forma importante tanto de animar a los alertadores a realizar la denuncia como de protegerlos de posibles represalias, un punto de vista que, como hemos visto, tiene cierto apoyo en la literatura de investigación.

Sin embargo, en las conversaciones con las organizaciones beneficiarias potenciales, la disponibilidad de la denuncia anónima no fue necesariamente recibida de forma positiva. Para las organizaciones asociadas a EAT y otras implicadas en el fomento del uso de buzones digitales seguros como canales internos dentro de las organizaciones, un tema recurrente fue que el anonimato como tal puede seguir siendo una cuestión difícil de mantener.

Los entrevistados citaron varias razones por las que las instituciones públicas y privadas dudan en introducir canales de denuncia anónimos. Algunos informaron de que las organizaciones beneficiarias potenciales tienen una visión generalmente recelosa de la denuncia anónima y que el anonimato como tal es un concepto

4. Experiencias de los socios del EAT y de otros operadores de buzones

"aterrador". Las instituciones públicas, en particular, expresaron su preocupación por la posibilidad de que se produzca una afluencia incontrolable y no verificable de denuncias por motivos personales, que sería difícil de gestionar. No cabe duda de que los factores históricos y culturales desempeñan un papel en este sentido.

La ONG checa *Oživení*, dedicada a la lucha contra la corrupción y que confía en las denuncias de los alertadores para ello, observó que:

> "La gente en la República Checa, y creo que es lo mismo para todos los [países] del antiguo bloque del Este, desconfía en cierto modo del anonimato. Y en segundo lugar, no creo que la gente sea lo suficientemente consciente de su seguridad digital, o de que hay formas de mantenerse en el anonimato en línea, así que queríamos ofrecer un nuevo canal."

De forma similar la organización rumana de libertad de prensa el CIJ dijo:

> "El principal obstáculo para obtener acuerdos de colaboración con posibles beneficiarios en Rumanía sigue siendo la percepción general de los alertadores en nuestro país, que es la de soplones o informadores, no la de ciudadanos activos que hacen una revelación para proteger el interés público."

Un segundo problema que fue citado con frecuencia por las organizaciones asociadas al EAT es el hecho mismo de la corrupción imperante en los países en cuestión. Algunos funcionarios pueden tener razones de interés propio para resistirse a la introducción de sistemas de denuncia anónima en las instituciones públicas y pueden temer el establecimiento de vías que puedan llevarles a estar implicados en las revelaciones de los alertadores.

Un tercer tema recurrente entre las organizaciones asociadas al EAT fue que, a pesar de la Directiva de la UE, la falta de un marco jurídico nacional en torno a la protección de alertadores en varios países inhibía a las organizaciones de adoptar sistemas seguros de buzón en línea. Muchas se acogieron a la necesidad de esperar hasta que hubiera certeza. Además, las autoridades de los países de la UE encuestados para esta investigación citaron repetidamente la transposición en curso de la Directiva de la UE sobre la protección de alertadores como una de las razones para dudar en este ámbito.

Un factor que complica la situación es que la propia Directiva deja un gran margen de maniobra a los Estados miembros sobre el tema de los canales de denuncia anónimos y es posible que las normativas nacionales en este ámbito difieran. Si bien un alertador anónimo cuya identidad se revela en el curso de una investigación tiene derecho al mismo nivel de protección legal que otros alertadores en virtud de la Directiva, la legislación no llega a introducir la obligación de establecer el anonimato en los canales de denuncia.

Por lo tanto, corresponde a cada Estado miembro determinar el grado de apoyo que debe prestar al anonimato en los canales de denuncia, para determinar si deben fomentarse o incluso hacerse obligatorios. Quizás no sea

4. Experiencias de los socios del EAT y de otros operadores de buzones

sorprendente que las autoridades tengan en cuenta este aspecto.

Buzones digitales seguros en funcionamiento

Como ya se ha comentado en este informe, existen sistemas de buzón digital seguro de distintos proveedores. Los operadores de estos buzones entrevistados para este capítulo eran usuarios de tres sistemas bien establecidos: Globaleaks, SecureDrop y BKMS. Estos productos difieren en varios aspectos, pero lo que tienen en común es la posibilidad de comunicarse con una persona anónima a través de un canal cifrado.

Más allá de las diferencias en los sistemas adoptados, las organizaciones de la sociedad civil informaron que utilizaban sus sistemas de buzón digital seguro de diferentes maneras, recordando la diversidad observada por Philip Di Salvo y otros investigadores.

Algunas organizaciones, como *Xnet* en España y *Oživení* en la República Checa, han establecido canales de denuncia anónimos para recibir información privilegiada que les permita cumplir su misión organizativa. Anuncian una serie de puntos de contacto públicos además de su buzón.

Para las organizaciones de la sociedad civil que se encuentran en esta situación, el buzón digital seguro no suele ser su medio de contacto más utilizado. Las organizaciones de la sociedad civil entrevistadas que ofrecen un buzón online seguro junto con otras vías de contacto como el teléfono, el correo electrónico o los formularios en línea no cifrados, informan de que reciben de media aproximadamente el 10-15% de sus comunicaciones a través del canal cifrado. Las organizaciones que se encuentran en esta situación suelen señalar la preocupación por la pérdida de mensajes que, de otro modo, recibirían, como razón para seguir siendo accesibles a través del correo electrónico, las redes sociales y otras formas menos seguras de establecer el primer contacto.

El buzón digital seguro EAT ofrece resultados rápidos

Una autoridad puso en marcha un buzón seguro en línea como resultado del proyecto EAT e informó de que había recibido tres comunicaciones procesables en el primer mes de su buzón en línea.

Por el contrario, *Transparencia Internacional Italia* canaliza todas las consultas públicas a través de Globaleaks, haciendo explícita la posibilidad de comunicación anónima para cualquiera que quiera ponerse en contacto con ellos.

En el caso de las autoridades, que suelen ofrecer buzones digitales seguros para facilitar las denuncias anónimas sobre cuestiones específicas como la corrupción o el blanqueo de capitales, el uso de estos canales es relativamente alto. Instituciones como el regulador financiero alemán *BaFin* o la *Agencia Española Anticorrupción* AVAF informaron que aproximadamente el 85% de sus denuncias les llegan a través del canal cifrado.

Del mismo modo, la calidad de la información que llega a través de los buzones seguros parece ser diferente. Las organizaciones de la sociedad civil afirman tener dificultades para gestionar adecuadamente una considerable afluencia de informes que pueden ser infundadas o erróneas.

4. Experiencias de los socios del EAT y de otros operadores de buzones

En cambio, las autoridades con un ámbito de actuación definido informan de que la gran mayoría de los mensajes entrantes se consideran útiles y contribuyen a la misión de la organización de forma significativa. El regulador financiero alemán *BaFin*, que opera un buzón BKMS desde 2017, afirma que los beneficios de los sistemas de denuncia anónima superan con creces cualquier desventaja:

> "Creo que es importante que exista esta opción, porque permite a los denunciantes presentarnos su información sin exponerse a un peligro innecesario. Valoramos mucho la posibilidad de la denuncia anónima. Además, creo que no recibiríamos la mayoría de las comunicaciones que recibimos ahora si no tuviéramos la posibilidad de hacerlo de forma anónima. [...] Por supuesto, las motivaciones de los alertadores difieren. Sin embargo, yo consideraría el abuso como un problema menor. Hay que asegurarse de filtrar la información objetiva [...] y las cosas no siempre están claras. La conclusión es que estos inconvenientes pueden despreciarse en comparación con las ventajas de un sistema de denuncia anónima."

Hacer que el anonimato funcione

De nuestras entrevistas se desprenden tres temas principales: en primer lugar, el apoyo explícito a la denuncia anónima en los marcos jurídicos nacionales marca una diferencia considerable en la disposición a adoptar estos métodos. Como ya se ha mencionado anteriormente, varias de las organizaciones que abogan por la adopción de estos canales se han enfrentado a los retos derivados de la transposición en curso de la Directiva de la UE sobre la protección de alertadores. Algunas de ellas comprenden de primera mano el problema que supone el funcionamiento de los buzones anónimos dentro de un marco jurídico inexistente o incompleto, como se comentó con la rama italiana de *Transparencia Internacional* en relación con la protección de datos:

> "La ley sobre la denuncia de irregularidades en Italia, con fecha de diciembre de 2017, exigía a la Autoridad Anticorrupción que diera a conocer algunas directrices sobre cómo gestionar la información, y luego mostraba que estas directrices también debían afectar al almacenamiento de datos. Pero esta directriz aún no se ha publicado. Así que realmente no sabemos cómo comportarnos, es sólo una interpretación basada en los principios generales del RGPD. Pero no hay ninguna transposición de los principios del RGPD en la legislación sobre denuncia de irregularidades en Italia, o sobre cómo deben tratar la información que reciben terceras partes externas como las ONG."

4. Experiencias de los socios del EAT y de otros operadores de buzones

El deseo de una orientación explícita sobre cómo aplicar los procedimientos de comunicación de irregularidades es un tema recurrente en nuestras entrevistas. Nuestro entrevistado en el regulador financiero alemán *BaFin* sugirió que un marco jurídico bien definido constituye también una especie de seguro para los funcionarios que se encargan de las denuncias anónimas, ya que los posibles conflictos con otras normativas ya se han tenido debidamente en cuenta, definiendo claramente las responsabilidades y los deberes:

> "El establecimiento de una unidad independiente de denuncia de irregularidades se basa en un requisito legal que especifica la creación de canales dedicados que tienen que estar debidamente protegidos. Y, desde mi punto de vista, esta unidad de denuncia, la separación organizativa de algunos empleados, así como su independencia, es una medida realmente eficaz y valorada ".

Lo más importante es que las instituciones públicas que han implementado buzones online seguros suelen considerarlos muy valiosos. Curiosamente, cuando se les pidió que estimaran la proporción de informes recibidos a través de estos canales que eran procesables o útiles, informaron de que recibían más resultados viables de sus buzones digitales seguros en línea que algunas de las organizaciones de la sociedad civil.

Dejando a un lado la cuestión de los recursos, hay una serie de razones por las que los sistemas de denuncia anónima parecen, en muchos casos, dar resultados más eficaces cuando los gestionan las autoridades públicas que las organizaciones de la sociedad civil. Cuando se les pide que den una estimación del porcentaje de casos en los que la primera denuncia de los alertadores se dirige a la organización respectiva, hemos comprobado que las autoridades públicas que mantienen canales específicos reciben casi exclusivamente las denuncias iniciales, a diferencia de las organizaciones de la sociedad civil, a las que se dirigen con mucha más frecuencia los alertadores que ya han sufrido un perjuicio y cuyos problemas pueden ser, por tanto, más difíciles de resolver.

Además, cuando los canales anónimos son proporcionados por una institución oficial del Estado, esto puede contribuir a su mayor aceptación por parte del público en general. Como ya se ha dicho, en algunos países y sectores sigue siendo común la percepción negativa de las denuncias anónimas. La experiencia de las Agencias Anticorrupción en España muestra que es probable que la mayor implantación de buzones digitales seguros contribuya a una interpretación más favorable de la denuncia anónima e impulse a más denunciantes a presentarse en el futuro.

> "Lo que hemos observado es que el porcentaje de denuncias ha ido aumentando desde que se implantó el buzón, tanto en números totales como en porcentajes. [...] La intuición es que irá de menos a más. Preveo más publicidad, de poder dar a conocer más hechos irregulares he pensado en plataformas profesionales, es decir, sistemas donde un empleado público o privado pueda tener un acceso relativamente rápido con plataformas corporativas, que además de la posibilidad de un buzón de sugerencias pueda tener un buzón de denuncias anónimas y visualizo un aumento de las denuncias anónimas, una consolidación del buzón de denuncias anónimas."

4. Experiencias de los socios del EAT y de otros operadores de buzones

Esto no significa que la recepción de denuncias en otros contextos sea menos valiosa: el trabajo de organizaciones como la Fundación estadounidense *Freedom of the Press*, que ha asumido la misión de seguir desarrollando y difundiendo la tecnología de denuncia anónima SecureDrop, subraya la importancia de las denuncias para el trabajo de los periodistas. Además, los esfuerzos pioneros de las organizaciones de la sociedad civil han allanado el camino a las instituciones públicas que ahora se benefician de su experiencia:

> "Una de las cosas que nos ayudó mucho, para demostrar que realmente funciona, fue que les mostramos [al ayuntamiento] cómo es una comunicación, qué tipo de conversaciones manteníamos con el alertador; así vieron que realmente funciona, que trabajamos con eso y que es bastante fácil de usar. Así que creo que eso zanjó las dudas por su parte."

La adopción de sistemas de denuncia anónima en el marco formalizado de las autoridades está en sus inicios, pero ya está claro que no hay que subestimar su importancia. La experiencia expresada por las instituciones que utilizan buzones seguros en línea es ampliamente positiva.

Accesibilidad

Por último, se expresaron también preocupaciones sobre la facilidad de uso y la accesibilidad de los buzones digitales seguros. En particular, nuestras entrevistas apoyan la indicación de los datos cuantitativos de que, en la práctica, los denunciantes podrían priorizar la accesibilidad sobre la seguridad, incluso si quieren mantener su anonimato.

En muchos casos, el uso de canales seguros de denuncia anónima requiere un esfuerzo adicional por ambas partes: como se ha descrito anteriormente, SecureDrop requiere que los alertadores utilicen Tor y requiere una instalación adicional y exigencias de mantenimiento por parte del operador del buzón. GlobaLeaks recomienda que los alertadores hagan cualquier revelación a través de Tor, pero los operadores de Dropbox tienen la opción de no exigirlo.

No cabe duda de que estos obstáculos técnicos repercuten en el uso de los canales anónimos: la mayoría de las ONG encuestadas afirmaron que sólo reciben unas pocas denuncias a través de los respectivos canales anónimos. Organizaciones como *Atlatzso*, en Hungría, y *Pištaljka*, en Serbia, señalan que reciben la mayor parte de sus denuncias a través de un formulario online no codificado que figura en su sitio web, y consideran que Tor es un "obstáculo" para los denunciantes.

Que las configuraciones técnicas sigan siendo un obstáculo también depende de la percepción que tenga el alertador del riesgo al que se enfrenta si es descubierto. La ONG checa de lucha contra la corrupción *Oživení*, que apoya a los alertadores tanto dando apoyo legal como recibiendo denuncias, señala que es mucho más probable que las denuncias sobre casos reales de corrupción se presenten a través del canal anónimo que a través de otros medios de comunicación que la organización proporciona. Es decir, los alertadores que se perciben a sí mismos en riesgo actúan en consecuencia.

4. Experiencias de los socios del EAT y de otros operadores de buzones

Se pueden observar similitudes en el lado de las organizaciones que defienden y proporcionan canales seguros. La organización estadounidense *Freedom of the Press Foundation*, que mantiene el sistema SecureDrop centrado en el periodismo, no considera que sea la solución óptima para todos:

> "Cuando hablamos con los medios de comunicación, debatimos con ellos sus amenazas, analizamos qué tipo de historias esperan y quieren informar, si quieren ser la organización que puede recibir pistas y publicar la próxima revelación de Ed Snowden. Y si lo son, probablemente necesiten algo como SecureDrop. Si están más interesados en la delincuencia corporativa y quieren informar sobre infracciones menores de la ley en sus áreas, digamos que son un periódico local, algo como una línea de denuncias de Signal podría encajar mejor."

Al mismo tiempo, las organizaciones que han decidido introducir soluciones tecnológicas más complejas para proteger sus fuentes y su trabajo parecen beneficiarse de la inversión. Paul Lewis, jefe del equipo de investigación del periódico británico *The Guardian*, describe SecureDrop como "una parte integral" de la forma en que se trabajamos ahora, a diario, "a veces cada hora" y añade que, a pesar de que ese tipo de interfaz de usuario puede llevar un poco más de tiempo para familiarizarse con ella, "vale la pena ".

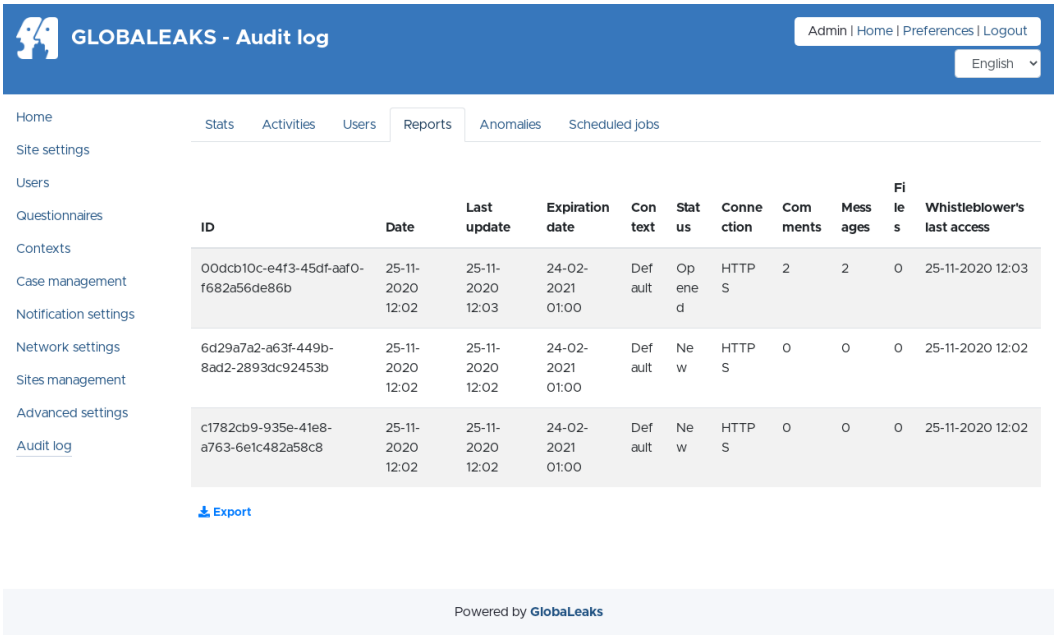
Nada de esto niega la necesidad de seguir desarrollando los canales de comunicación anónimos para hacerlos más fáciles de usar y eficaces. Ciertamente, la tendencia de los mensajeros anónimos ha sido buscar la adopción por parte de un público tan mayoritario como sea posible. (Wiener 2020)

No todas las soluciones de dropbox incluyen "recibos" de lectura u otras funciones que permitirían a quienes manejan las denuncias entrantes saber si un denunciante ha recibido su respuesta y tiene la intención de seguir comunicándose, funcionalidad que ayuda a las organizaciones a cumplir con los aspectos de gestión de casos de la Directiva de la UE y que han demostrado ser eficaces en su uso. Los cuestionarios, claramente estructurados y flexibles, ofrecen a los denunciantes una orientación a la hora de realizar las denuncias y facilitan el trabajo de quienes las reciben. Estas y otras mejoras en la configuración de los canales anónimos pueden hacer, y harán, que sean herramientas más eficaces.

5. Evaluación de la eficacia de los buzones con datos cuantitativos

Uno de los retos a la hora de evaluar la eficacia de los buzones digitales seguros es el acceso a los metadatos sobre su uso. Por su propia naturaleza, los datos asociados a un buzón están estrechamente protegidos, incluidos los metadatos (información sobre los envíos), así como su contenido. Aunque esto supone un reto especial para el análisis, el hecho de que estos datos estén protegidos y sean difíciles de obtener debe considerarse como algo tranquilizador y positivo desde el punto de vista del anonimato y de la privacidad en general.

El proyecto EAT ha permitido añadir una nueva funcionalidad a la plataforma de GlobaLeaks, con el fin de facilitar futuros trabajos de investigación. Esta nueva funcionalidad también mejorará la capacidad de las organizaciones para auditar sus propios buzones, al permitir a los operadores de los buzones descargar los metadatos seleccionados accediendo a la pestaña "Reports (informes)" dentro de menú auditoría. Aunque esta funcionalidad estaba originalmente pensada para permitir el análisis de los buzones creados como parte del Proyecto EAT, ahora está disponible para todos los que ejecuten la última versión de GlobaLeaks.



Apéndices E y F. Estos incluyen la información suministrada como parte del cuestionario, que se incluyó en los buzones del Proyecto EAT, así como algunos metadatos generales (visibles en la imagen de arriba y resaltados en azul en el Apéndice E), que ahora están disponibles para todos los usuarios de GlobaLeaks que se hayan actualizado con la última versión del software (versión 4 o posterior). Nuestros acuerdos con los beneficiarios incluían el acceso a estos datos con fines de investigación dentro de la duración del proyecto.

Los datos que hemos recibido de los buzones del Proyecto EAT, como consecuencia de esos acuerdos de beneficiarios, son limitados, en parte porque varios de estos buzones seguros en línea se pusieron en marcha relativamente tarde en la línea de tiempo del proyecto[6]. No obstante, el análisis de estos datos sugiere algunas ideas interesantes sobre la forma en que se utilizan los buzones, a las que nos referiremos en nuestro análisis del uso de Tor.

6. Los datos del buzón de EAT nos llegaron pre-limpiados. Algunos envíos realizados el día de la activación del buzón sin datos, lo que sugiere claramente que se trata de envíos de prueba - se excluyeron del conjunto.

5. Evaluación de la eficacia de los buzones con datos cuantitativos

Dada la dificultad que hemos tenido para obtener metadatos significativos dentro del período de ejecución del proyecto, nuestra experiencia en el acceso a los metadatos de los operadores de dropboxes con los que no ha habido un acuerdo previo ha sido igualmente desafiante, lo que ha impedido un estudio comparativo a gran escala. Sin embargo, enfrentando las relaciones existentes, hemos podido acceder a un número limitado de metadatos, lo que ha proporcionado información útil sobre el uso de los buzones seguros en línea. En reconocimiento de los retos asociados con el acceso y el intercambio de metadatos, también propondremos un marco y un esquema de especificación que podría desarrollarse para facilitar un intercambio más amplio de metadatos de una manera segura para la privacidad y el anonimato.

Evaluación de los datos de REF:DATA_PROV_1

Utilizando la nueva funcionalidad añadida a la plataforma GlobaLeaks, DATA_PROV_1 (una organización con sede en un país del Proyecto EAT aunque no es beneficiaria directa del mismo) nos proporcionó amablemente acceso a un conjunto de metadatos que cubría un periodo de 4 años de uso de su buzón seguro en línea.

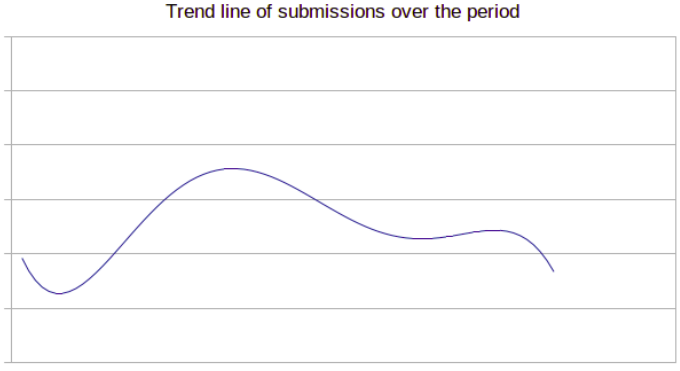
Esos datos mostraban un número limitado de campos para cada entrada, por ejemplo, si una entrada fue enviada a través de Tor o no, y cuántos archivos o mensajes habían sido enviados como parte de un envío. Aunque este conjunto de datos es de una sola organización en una sola jurisdicción, sigue proporcionando algunas ideas útiles, aunque no necesariamente a un nivel estadísticamente significativo. Más adelante detallaremos este análisis.

A lo largo de este análisis, la privacidad de los datos es primordial, por lo que sólo citaremos estadísticas agregadas de alto nivel, y sólo de una manera que consideremos que limita cualquier inferencia de datos adicionales. Por ejemplo, no proporcionaremos recuentos exactos, sólo tendencias o proporciones relativas y correlaciones.

Antes del análisis, excluimos los datos del primer año, que contenía un número reducido de presentaciones y, por lo tanto, no estaba lo suficientemente protegido como para ser publicado incluso como estadísticas agregadas a alto nivel. También excluimos un pequeño número de envíos que parecían incompletos o de prueba, que se produjeron con una hora de diferencia en el mismo día.

Tendencia de las comunicaciones

El número de comunicaciones registradas siguió una tendencia inicial al alza, que alcanzó su punto máximo en el segundo año de análisis. A partir de ese momento se ha producido un descenso constante. La figura 1 muestra una línea de tendencia polinómica de 5 grados. Se seleccionó porque se ajustaba mejor a los datos subyacentes sin revelar valores precisos. Hemos ajustado el eje del gráfico para desplazar los valores para una mayor protección, por lo que esta línea sólo debe utilizarse para interpretar una tendencia y no para extraer valores.



5. Evaluación de la eficacia de los buzones con datos cuantitativos

Aunque la tendencia ha sido a la baja desde el segundo año, no podemos estar seguros de que esto refleje el conjunto de las comunicaciones recibidas. A medida que se mejoran las protecciones de los denunciantes y más organizaciones comienzan a proporcionar buzones internos y/o externos, el número total de comunicaciones puede repartirse entre un mayor número de buzones. Este es un argumento más para ampliar la información de los metadatos, de modo que se pueda establecer una imagen amplia de la denuncia de irregularidades en un sector o jurisdicción concretos.

Interactuar con los alertadores

Una métrica adicional que hemos medido es el tiempo transcurrido entre el último inicio de sesión del denunciante y la fecha de creación original de su presentación. Aunque no podemos conocer los inicios de sesión intermedios, podemos utilizar este valor como indicador de compromiso, suponiendo que un denunciante que tiene un largo período entre la creación y el último inicio de sesión es probable que haya mantenido el compromiso con el buzón seguro en línea y la presentación que ha hecho. La observación de los valores absolutos para este análisis tiene una utilidad limitada, ya que los envíos del año 1 pueden tener valores mucho más altos que los envíos del año 4. Por ello, analizamos si había una correlación positiva entre el número de archivos enviados, el número de mensajes o el uso de Tor, y el número de días entre el primer y el último inicio de sesión. Estos resultados se muestran en la Tabla 1.

Table 1: Correlation between submission properties and days between first and most recent login

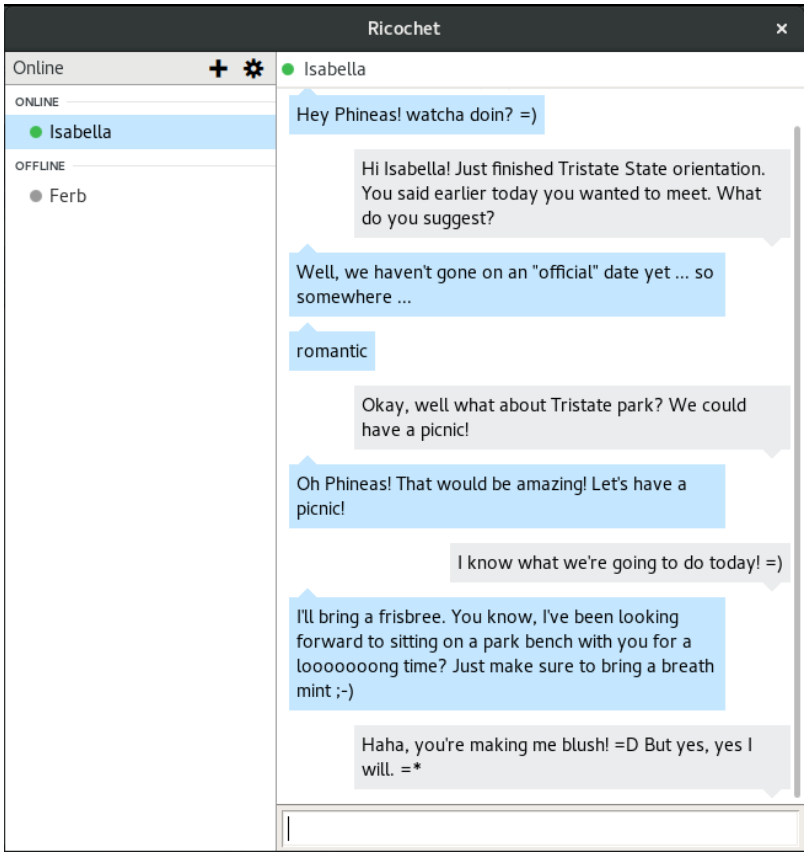
Test	Correlation (Pearson)
Number of files submitted and days between first and most recent login	0.35
Number of messages submitted and days between first and most recent login	0.81
Usage of Tor and days between first and most recent login	0.07

Como muestra la Tabla 1, no hay correlación entre el uso de Tor y nuestro indicador de compromiso. Esto es coherente con un uso generalmente bajo de Tor, que analizaremos más adelante. El número de archivos enviados muestra una baja correlación, indicando que un mayor número de archivos enviados no siempre resulta en un mayor compromiso, lo cual es razonable, ya que los archivos podrían ser entregados en una sola carga. Hay una correlación bastante fuerte entre el número de mensajes y el periodo de compromiso. Esto también es de esperar, ya que es probable que no se entreguen varios mensajes el mismo día y, por lo tanto, cabría esperar que cuanto mayor sea el número de mensajes, más largo será el periodo en el que se repartan.

Sin embargo, el resultado indica que la mensajería es un requisito fundamental de un buzón y, por tanto, podemos suponer que la provisión de una plataforma de mensajería fácil de usar, fiable y segura dentro del buzón es esencial para mantener el compromiso. Esta observación se ve respaldada por las observaciones publicadas por la *Directora de Analítica del Ayuntamiento de Barcelona*, que ha dicho que la capacidad de mantener una conversación continua entre un operador de dropbox y la persona que ha presentado una comunicación o denuncia es una de las características más importantes de un sistema de comunicación de alertas (Sánchez 2019)

5. Evaluación de la eficacia de los buzones con datos cuantitativos

También evaluamos si había una correlación entre el número de mensajes y el número de archivos enviados, para determinar si tendía a haber una mayor interacción con un envío mayor. Calculamos una correlación de 0,49, que es de baja a moderada y no indica una relación fuerte.



Blueprint for Free Speech apoya el desarrollo de Ricochet Refresh[7], una aplicación de software de mensajería de texto de escritorio gratuita y de código abierto. Este programa es el único software de chat de escritorio gratuito que utiliza Tor y que proporciona anonimato y privacidad reales (al menos no se conoce otro). En comparación, programas muy utilizados como Signal requieren un número de teléfono personal. Ricochet Refresh permite a los operadores de Dropbox mantener una conversación de chat en directo con alguien que realiza un envío, a la vez que salvaguarda la identidad y la privacidad de la comunicación de esa persona.

Las instalaciones de buzones digitales del proyecto EAT proporcionaron un acceso fácil a Ricochet Refresh, una mejora realizada al sistema estándar de GlobaLeaks como parte del proyecto. Como Ricochet se basa en la red Tor para proporcionar anonimato y confidencialidad, no pudimos recopilar fácilmente datos estadísticos sobre su uso sin comprometer las actividades de los alertadores.

El uso de Ricochet Refresh en este proyecto constituye un ejemplo útil de cómo una herramienta de software compartida, desarrollada para todos, puede facilitar y abaratar la transición de una organización a las nuevas normas a medida que se implanta la Directiva.

7. https://www.ricochetrefresh.net/

5. Evaluación de la eficacia de los buzones con datos cuantitativos

El uso de Tor

Un resultado sorprendente de nuestro análisis fue el uso relativamente poco común de Tor para los envíos. No hubo correlaciones significativas entre Tor y el número de mensajes (0,15), el número de archivos (-0,04) o el tiempo entre el primer y el último inicio de sesión (0,07). Además, como porcentaje de envíos, Tor fue siempre minoritario y se redujo a la mitad entre el año 1 y los siguientes.

Table 2: Percentage of submissions made over Tor

Year	Percentage of submissions using Tor
1	29%
2	13%
3	16%
4	15%

Este resultado plantea algunas preocupaciones. No sólo el porcentaje de comunicaciones que utilizan Tor ha tendido a la baja, sino que también ha disminuido significativamente en el año 2, que fue el año con más alertas. Esto indica que los alertadores no están utilizando el método más anónimo y seguro para los envíos, y que la gran mayoría de las comunicaciones vienen a través de canales que podrían ser susceptibles de una mayor vigilancia.

Esto supone un reto especial para los responsables de los buzones: cómo hacer que Tor sea más accesible y utilizable, de modo que se convierta en la opción por defecto para el denunciante. Es posible que los envíos provengan de ordenadores en los que el alertador no tiene permiso para instalar software. Sin embargo, esto en sí mismo es preocupante, ya que sugiere que los alertadores están haciendo envíos a través de una red de trabajo, que no se consideraría un lugar seguro para hacer este tipo de envíos.

Sin embargo, el resultado podría deberse a la falta de conocimiento de los usuarios o a su nerviosismo sobre el uso correcto de Tor. Investigadores anteriores han encontrado que a los usuarios menos familiarizados con la tecnología les resulta difícil evaluar los riesgos en línea en un contexto de denuncia (Lam y Harcourt 2019; Lowry, Moody y Galetta 2014). En muchos aspectos, este sería el resultado más deseable, ya que proporcionar una mejor formación es una tarea más manejable que superar una limitación técnica.

Querer el anonimato y usar Tor no siempre van de la mano

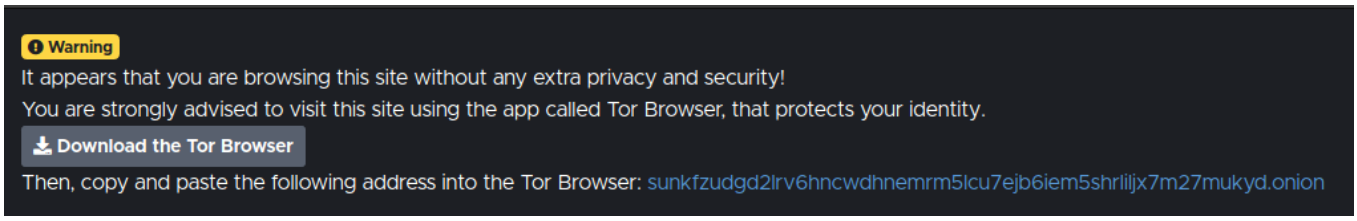
El análisis de los metadatos de los buzones del Proyecto EAT confirma estas conclusiones preliminares sobre el uso de Tor. El uso de Tor fue en gran medida consistente en un 20%. Sin embargo, es preocupante que más del 30% de las comunicaciones anónimas no se hayan realizado a través de Tor.

Esto sugiere que se necesita una mayor orientación o educación para asegurarse de que los alertadores que quieren permanecer en el anonimato eligen la opción técnica más adecuada a sus necesidades.

Aunque el número de comunicaciones por buzón es demasiado pequeño para sacar conclusiones, también parece haber variaciones en el rendimiento de los buzones de los distintos países con respecto al uso de Tor. Un análisis más profundo de los buzones que funcionan mejor, con una muestra más grande, ayudaría a poder determinar si este resultado es significativo, y si es así, cuáles son las mejores prácticas de las que pueden aprender otros operadores de buzones.

5. Evaluación de la eficacia de los buzones con datos cuantitativos

Sin acceso a un conjunto más amplio de buzones digitales no podemos decir si esta tendencia se da en todos o sólo en éste. Esto nos impide poder comparar diferentes enfoques educativos. Por ejemplo, GlobalLeaks muestra un banner que recomienda específicamente el uso de Tor y un enlace para descargar el navegador Tor, como se muestra en la Figura 2.



Con el acceso a los metadatos de diferentes buzones y proveedores sería posible determinar las mejores prácticas y evaluar qué enfoques educativos funcionan mejor para guiar a los usuarios hacia el uso de Tor.

Futuro de las estadísticas de los buzones digitales

Está claro que todavía hay lecciones que aprender sobre el despliegue y la gestión de los buzones. Sin estadísticas generalizadas sobre el uso y la eficacia, será difícil establecer, probar y compartir las mejores prácticas. Nos hemos enfrentado a importantes retos a la hora de adquirir cualquier metadato sobre el uso de los buzones. Como ya se ha comentado, por una parte, es reconfortante saber que los administradores adoptan un enfoque de seguridad ante todo. Por otro lado, indica que debemos buscar formas mejores y más seguras de compartir las estadísticas para garantizar a los administradores de dropbox que pueden compartir dichas estadísticas de forma segura.

¿Son seguras las estadísticas agregadas?

La respuesta sencilla es "no", debido a lo que se ha denominado la "Ley Fundamental de la Recuperación de la Información", que establece que "las respuestas demasiado precisas a demasiadas preguntas destruirán la privacidad de forma espectacular" (Dwork y Roth 2014). Ese tipo de ataques se denominan más comúnmente "Ataques de Reconstrucción", que abarcan cualquier método para reconstruir datos privados a partir de datos agregados disponibles públicamente.

Puede haber un pequeño conjunto de ocasiones en las que compartir dichos datos es seguro, por ejemplo, cuando los mismos datos están disponibles en otro lugar o se consideran de conocimiento común o una cuestión de registro público. Por ejemplo, el número de nacimientos o muertes en un año determinado en un país determinado. Sin embargo, hay muchas ocasiones, sobre todo cuando esos datos se publican de forma longitudinal, es decir, una vez al mes, al trimestre o al año. En tales circunstancias, los cambios en la población subyacente de registros pueden recuperarse potencialmente a partir de los cambios en la estadística agregada. Un ejemplo hipotético sencillo sería que una empresa declarara el número de miembros de su consejo de administración que padecen enfermedades cardíacas cada trimestre, algo que los inversores pueden querer saber para juzgar la resistencia o el estrés en el consejo. En primer lugar, los valores extremos revelan mucho, por ejemplo, si todos los miembros del consejo tienen una enfermedad cardíaca, un adversario se entera de la

5. Evaluación de la eficacia de los buzones con datos cuantitativos

situación de cada individuo. A la inversa, si nadie tiene una enfermedad cardíaca, se aprende el mismo atributo para todo el grupo.

Un ejemplo más matizado es cuando las estadísticas cambian durante un periodo de tiempo. Por ejemplo, si el número declarado en el primer trimestre fue de 4 y el número declarado en el segundo trimestre fue de 3, y un miembro de la junta directiva ha abandonado su puesto, el atributo de ese individuo puede deducirse diferenciando los resultados del primer y segundo trimestre.

El anterior es un ejemplo muy sencillo, se pueden realizar ataques de reconstrucción mucho más complicados.

Privacidad diferencial

Si las estadísticas agregadas no son seguras, ¿qué podemos hacer? La respuesta es que, en lugar de publicar las estadísticas agregadas en bruto, podemos publicar estadísticas protegidas mediante una técnica conocida como privacidad diferencial. La privacidad diferencial proporciona un método matemáticamente riguroso para limitar el coste de privacidad de una publicación. Aunque las matemáticas subyacentes pueden parecer complicadas, son relativamente sencillas desde el punto de vista conceptual. Cynthia Dwork, una de las co-creadoras de la Privacidad Diferencial, describe la definición en inglés de la Privacidad Diferencial de la siguiente manera:

> "El resultado de cualquier análisis es esencialmente igual de probable independientemente de si cualquier individuo se une, o se abstiene de unirse, al conjunto de datos."

En esencia, la afirmación anterior significa que si se tuvieran dos conjuntos de datos diferentes, uno que contuviera los datos del individuo y otro que no, la probabilidad de que se produzca cualquier estadística publicable es casi la misma en ambos conjuntos de datos. De este modo, al ver una de esas estadísticas no será posible, dentro de un límite probabilístico, determinar si los datos de un individuo concreto se incluyeron en el cálculo de la misma, incluso si el adversario conoce todos los datos de ambos conjuntos de datos. El "casi igual" está delimitado por un valor llamado épsilon, o más comúnmente denominado presupuesto de privacidad. Este valor se mantiene pequeño, normalmente 1.

Lo anterior puede parecer puramente teórico y demasiado complicado para su uso en el mundo real. Sin embargo, la Oficina del Censo de Estados Unidos se ha comprometido a publicar sus productos del censo de 2020 utilizando la privacidad diferencial, que describe como el "...mejor estándar en la protección de la privacidad de los datos". (US Census Bureau) Esto es importante por varias razones. En primer lugar, aumentará el conocimiento y la aceptación de la privacidad diferencial. En segundo lugar, hará que cualquier persona que desee utilizar las estadísticas del censo de Estados Unidos entienda cómo funciona la privacidad diferencial, lo que creará una mejora generalizada en el sector del análisis de datos.

Además, también existen herramientas automatizadas para calcular las publicaciones de privacidad diferencial de conjuntos de datos sencillos, por ejemplo, el paquete R DiffPriv, que proporciona un conjunto de herramientas para realizar la privacidad diferencial con un mínimo de conocimientos previos.

5. Evaluación de la eficacia de los buzones con datos cuantitativos

Buzones y privacidad diferencial

El tipo de metadatos necesarios para evaluar la eficacia de los buzones es ideal para la protección mediante la Privacidad Diferencial. Los datos son básicamente consultas de recuento, es decir, contar el número de comunicaciones hechas usando Tor, o el número medio de archivos enviados a través de Tor, o el número medio de archivos no enviados a través de Tor. Las estadísticas protegidas que se generarían incluirían ruido aleatorio, pero eso está bien para el análisis requerido, ya que no estamos interesados en valores exactos, sino en las tendencias y en determinar si los cambios realizados tienen un impacto positivo o negativo.

Por ello, proponemos que se acuerde la creación de un conjunto estándar de estadísticas que se compartirá con los investigadores y los organismos de supervisión. Dichas estadísticas deberían protegerse mediante la privacidad diferencial en el punto de extracción, es decir, dentro de la plataforma segura del buzón, utilizando un conjunto acordado de parámetros de privacidad diferencial. La tabla 3 muestra una propuesta inicial de estadísticas. Esto pretende ser un punto de partida para construir una lista colaborativa y acordar las estadísticas estándar de privacidad diferencial. Las estadísticas de publicación están emparejadas, una para los envíos hechos a través de Tor y otra para los envíos hechos sin Tor para permitir comparaciones y tendencias que se evalúen a través de los diferentes canales de envío. Los pares pueden sumarse para obtener los números globales independientemente del canal, si se desea.

Estas estadísticas están redactadas como una consulta, en lugar de un solo campo, para hacerlas compatibles con la Privacidad Diferencial. Como tales, representan los resultados de la ejecución de una consulta, por ejemplo, el recuento del número de envíos en un período determinado, o el cálculo de una media. El período de información queda a cargo de los administradores y puede variar entre los buzones en función del uso general. Recomendamos utilizar periodos divisibles, para que los diferentes proveedores puedan publicar en diferentes horarios pero que sigan siendo comparables. Un periodo base de 1 semana o 1 mes proporcionaría una buena flexibilidad. Si un buzón publica mensualmente y otro publica trimestralmente, las estadísticas mensuales pueden sumarse para cubrir el período equivalente.

5. Evaluación de la eficacia de los buzones con datos cuantitativos

Table 3: Proposed Statistics

Proposed Statistic Name	Purpose
Number_of_submissions_via_Tor	Capture the total number of submissions via Tor in a given period. Combined with Number_of_submissions_not_via_Tor gives the total number of submissions
Number_of_submissions_not_via_Tor	Capture the total number of submissions not via Tor in a given period. The combination of these two allow evaluation of Tor usage, as well as determining the efficacy of changes to support or encourage Tor usage over time
Average_files_per_submission_via_Tor	Calculates the average number of files that are attached to a submission that is made via Tor.
Average_files_per_submission_not_via_Tor	Calculates the average number of files that are attached to a submission that is not made via Tor. Combined with Average_files_per_submission_via_Tor will provide insights on the nature of submissions via different channels, as well overall performance by summing together and seeing trends in submissions overall
Average_messages_per_submission_via_Tor	Calculates the average number of messages that are attached to a submission that is made via Tor.
Average_messages_per_submission_not_via_Tor	Calculates the average number of files that are attached to a submission that is not made via Tor. This will act as one of the proxies for engagement, and also help to evaluate whether different channels provide different engagement results. It may also be possible to deploy different messaging services on the different channels, for example, Ricochet when submitting via Tor, and determine what impact that has on engagement.
Average_engagement_period_via_Tor	Calculates the average number of days since first and most recent login for all submissions that had a login in this period, and were sent via Tor.
Average_engagement_period_not_via_Tor	Calculates the average number of days since first and most recent login for all submissions that had a login in this period, and were not sent via Tor. Combined with Average_engagement_period_via_Tor provides an alternative proxy for engagement to allow analysis of overall whistle-blower engagement and efficacy of drives for greater engagement.

6. Conclusión

El proyecto EAT configura un momento en el que los buzones digitales seguros en línea se encuentran a punto de ser implantados de forma generalizada. En este sentido, se ha adelantado a su tiempo, pero no demasiado.

Nuestra experiencia en la promoción de la tecnología de denuncia anónima en instituciones públicas y empresas privadas de toda la Unión Europea demuestra que es necesario que exista una regulación nacional antes de que las empresas, pero también muchas instituciones del sector estatal, se sientan capaces de subirse al carro.

A pesar de ello, hemos comprobado que los primeros en adoptar la tecnología de buzón online seguro están sin duda alguna muy satisfechos con los resultados, y esto es especialmente cierto en el caso de las organizaciones del sector público.

El inicio de la disponibilidad de datos cuantitativos significa que estamos en el umbral de una comprensión mucho mejor de cómo funcionan los buzones en la práctica y qué factores fomentan su adopción por parte de las organizaciones y su uso por parte de los denunciantes. Sin embargo, todavía existen importantes obstáculos para la obtención de los datos.

A través de este proyecto, hemos empezado a facilitar el aspecto puramente técnico de esto. Hoy en día, cualquier persona que ejecute la versión actual de GlobaLeaks (versión 4 y posteriores) puede descargar un conjunto de metadatos desde el menú interno de la pestaña Auditoría. Esto será útil tanto para fines de auditoría interna como para investigadores externos. Esta función se ha inspirado en EAT.

No obstante, es probable que muchos operadores de buzones digitales se muestren cautelosos a la hora de compartir estos datos, lo cual es totalmente comprensible dada la importancia de proteger a quienes han enviado información de forma anónima. A los operadores de los dropbox también les puede preocupar la posición de la protección de datos, al no tener autoridad explícita para compartir los metadatos con otros. Sería útil contar con una aclaración en la ley o en la normativa sobre esta cuestión.

Los responsables políticos pueden ayudar en este sentido en dos aspectos. Sería valioso establecer los requisitos para compartir este tipo de datos, de modo que se puedan hacer comparaciones. Sin embargo, esto debe ir acompañado del establecimiento de convenciones para informar de estos datos de una manera segura que limite la posibilidad de que los denunciantes puedan ser reidentificados a partir de las estadísticas publicadas. Las técnicas de privacidad diferencial tienen un papel importante que desempeñar aquí y hemos sugerido cómo podría funcionar en la práctica.

7. Referencias

Agencia Valenciana Antifrau. (2020) Memoria 2019, https://www.antifraucv.es/wp-content/uploads/2020/03/MEMORIA_2019_VAL.pdf. Consulta realizada el 26 de enero de 2021.

Arnold, J.R. (2020) Whistleblowers, Leakers and Their Networks. Rowman & Littlefield.

Bausa, C., 2016. Tres controles efectivos a implantar para detectar y disuadir el fraude: el canal de denuncias, el análisis de datos y la autoevaluación del control interno. Revista de Contabilidad y Dirección, 23, pp.113-133.

Beltran, A. (2018) Las denuncias de la corrupción no solo son confidenciales, ya pueden ser anónimas. El Diario, https://www.eldiario.es/comunitat-valenciana/antifraude-buzon-denuncias-agencia-valenciana_1_2108701.html. Consulta realizada el 26 de enero de 2021.

Blueprint for Free Speech (2020) Whistleblower Protection Compliance Tool, https://tool.blueprintforfreespeech.net/. Consulta realizada el 26 de enero de 2021.

Blueprint for Free Speech (2018) The Perugia Principles for Journalism: Working with Whistleblowers in the Digital Age, https://www.blueprintforfreespeech.net/s/Blueprint_Perugia_Principles-3m6h.pdf. Consulta realizada el 26 de enero de 2021.

Carr, S., Mukherjee, T., Montgomery, A., Durbridge, M. and Tarrant, C., 2016. Developing the 'gripes' tool for junior doctors to report concerns: a pilot study. Pilot and feasibility studies, 2(1), pp.1-8.

A Change of Direction (2017). Xnet and Barcelona Municipality launch Whistleblower Platform, https://www.changeofdirection.eu/campaign-central/xnet-and-barcelona-municipality-launch-whistleblower-platform. Consulta realizada el 26 de enero de 2021.

Chen, N., 2011. Wikileaks and its Spinoffs: new models of journalism or the new media gatekeepers?. Journal of Digital Research & Publishing, 1, pp.157-167.

Di Salvo, P. (2020) Digital Whistleblowing Platforms in Journalism. Palgrave Macmillan.

Dwork, C. and Roth, A., 2014. The algorithmic foundations of differential privacy. Foundations and Trends in Theoretical Computer Science, 9(3-4), pp.211-407.

G20 (2019). High-level Principles for the Effective Protection of Whistleblowers, https://www.bmjv.de/SharedDocs/Downloads/EN/G20/G20_2019_High-Level-Principles_Whistleblowers.pdf. Consulta realizada el 26 de enero de 2021.

Gökçe, A.T., 2013. Teachers' value orientations as determinants of preference for external and anonymous whistleblowing. International Journal of Humanities and Social Science, 3(4), pp.163-173.

7. Referencias

Gonzalez, G. (2020) La Generalitat alienta la delación de la corrupción de forma anónima, El Mundo. https://www.elmundo.es/cataluna/2020/12/15/5fd8a4eb21efa0f47d8b4638.html- Consulta realizada el 26 de enero de 2021

Greenberg, A., 2012. This Machine Kills Secrets: How WikiLeakers, Hacktivists, and Cypherpunks Are Freeing the World's Information.

Johansson, E. and Carey, P. (2016) Detecting Fraud: The Role of the Anonymous Reporting Channel. Journal of Business Ethics. Journal of business ethics, 139(2), pp.391-409

Kenny, K. (2019) Whistleblowing: Toward a New Theory. Belknap Press.

Lam, H. and Harcourt, M., 2019. Whistle-blowing in the digital era: motives, issues and recommendations. New Technology, Work and Employment, 34(2), pp.174-190.

Leeds Beckett University. (2018) Global Whistleblowing Landscape for Reporting Doping in Sport, https://www.wada-ama.org/sites/default/files/resources/files/leeds_beckett_wada_report_on_whistleblowing_platforms_july_2018.pdf. Consulta realizada el 26 de enero de 2021.

Lowry, P.B., Moody, G.D., Galletta, D.F. and Vance, A., 2013. The drivers in the use of online whistle-blowing reporting systems. Journal of Management Information Systems, 30(1), pp.153-190.

Oživení. (2020) Whistleblowing - Quantitative research (interview survey CAVI), https://www.oziveni.cz/wp-content/uploads/2021/01/v4-Whistleblowing_EN.pdf. Consulta realizada el 26 de enero de 2021.

Palma, E.B., 2018. El control externo y el whistleblowing (canales de denuncia). Revista española de control externo, 20(59), p.32.

Palumbo, R. and Manna, R., 2019. Uncovering the relationship between whistleblowing and organizational identity. International Journal of Public Sector Management.

Pittroff, E. (2014). Whistle-blowing systems and legitimacy theory: A study of the motivation to implement whistle-blowing systems in German organizations. Journal of Business Ethics, 124(3), pp.399-412.

Pop, M. (2021) ISO standard 37002 on whistleblowing systems, https://cji.ro/en/iso-standard-37002-on-whistleblowing-systems/. Consulta realizada el 26 de enero de 2021.

Previtali, P. and Cerchiello, P., 2018. The determinants of whistleblowing in public administrations: an analysis conducted in Italian health organizations, universities, and municipalities. Public Management Review, 20(11), pp.1683-1701.

7. Referencias

Sánchez, R.M.S., 2019. El Buzón Ético y de Buen Gobierno del Ayuntamiento de Barcelona. Consultor de los ayuntamientos y de los juzgados: Revista técnica especializada en administración local y justicia municipal, (6), pp.59-72.

Sifry, M.L., 2011. WikiLeaks and the Age of Transparency. OR Books.

US Census Bureau (2020). Disclosure avoidance and the 2020 Census, https://www.census.gov/about/policies/privacy/statistical_safeguards/disclosure-avoidance-2020-census.html. Consulta realizada el 26 de enero de 2021.

Vandekerckhove, W., 2016. Freedom of expression as the "broken promise" of whistleblower protection. La Revue des droits de l'homme. Revue du Centre de recherches et d'études sur les droits fondamentaux, (10).

Verschuuren, P., 2020. Whistleblowing determinants and the effectiveness of reporting channels in the international sports sector. Sport Management Review, 23(1), pp.142-154.

Wiener, A. (2020) Taking Back our Privacy, The New Yorker. https://www.newyorker.com/magazine/2020/10/26/taking-back-our-privacy. Consulta realizada el 26 de enero de 2021.

Xnet (2017) Clonación del buzón anónimo de Xnet: nuevo buzón de denuncias anónimas de l'Oficina Antifrau de Catalunya, https://xnet-x.net/clonacion-buzon-xnet-antifrau-catalunya/. Consulta realizada el 26 de enero de 2021.

Apéndice A - Buzones digitales seguro en línea

La siguiente lista de buzones activos fue elaborada para el Proyecto EAT, basándose en parte en la información de Hermes y Blueprint for Free Speech. Los numerosos buzones italianos de GlobaLeaks creados como parte del proyecto WhistleblowingPA no se han incluido aquí (https://www.whistleblowing.it/adesioni/). La mayoría de los buzones proporcionados por entidades comerciales tampoco se incluyen en esta lista. Todos los enlaces estaban activos a 31 de enero de 2021.

Name	Sector	País	URL	Provider
2600	Medios de Comunicación	Estados Unidos	https://www.2600.com/securedrop/	SecureDrop
ABC	Medios de Comunicación	Australia	https://www.abc.net.au/news/securedrop/	SecureDrop
AfriLeaks	Sociedad Civil	Mundial	https://secure.afrileaks.org/#/	GlobaLeaks
Aftonbladet	Medios de Comunicación	Suecia	https://securedrop.org/directory/aftonbladet/	SecureDrop
The Age	Medios de Comunicación	Australia	https://www.theage.com.au/confidential-news-tips/securedrop	SecureDrop
Agencia Valenciana Antifraude	Sector Público	España	https://bustiadenuncies.antifraucv.es/#/	GlobaLeaks
Agenzia regionale per la tecnologia e l'innovazione (ARTI)	Sector Público	Italia	https://whistleblowing.arti.puglia.it/#/	GlobaLeaks
Al Jazeera	Medios de Comunicación	Catar	https://www.aljazeera.com/tips/	SecureDrop
Espen Andersen	Medios de Comunicación	Noruega	https://espenandersen.no/contact	SecureDrop
Angelini	Sector Privado	Italia	https://segnalazioni.angelini.it/	GlobaLeaks
Autorità Nazionale Anticorruzione (ANAC)	Sector Público	Italia	https://servizi.anticorruzione.it/segnalazioni/#!/#%2F	GlobaLeaks

Apéndice A - Buzones digitales seguro en línea

Nombre	Sector	País	URL	Proveedor
Atlatzso	Medios de Comunicación	Hungría	https://atlatszo.hu/magyarleaks/	GlobaLeaks
Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)	Sector Público	Alemania	https://www.bkms-system.net/bkwebanon/report/clientInfo?cin=2BaF6&c=-1&language=ger	BKMS
BalkanLeaks	Medios de Comunicación	Bulgaria	http://3qf4wewa5bojmcgr.onion	SecureDrop
Berliner Zeitung	Medios de Comunicación	Alemania	https://www.berliner-zeitung.de/missstandshinweis.226	SecureDrop
Bundesdruckerei	Sector Público	Alemania	https://report.whistleb.com/de/bundesdruckerei	WhistleB
Business Insider	Medios de Comunicación	Estados Unidos	https://www.businessinsider.com/how-to-tip-business-insider-securely-guide-signal-securedrop-2017-6	SecureDrop
Bústia Ètica Barcelona	Sector Público	España	https://bustiaetica.barcelona.cat/#/?lang=ca	GlobaLeaks
Buzzfeed	Medios de Comunicación	Estados Unidos	https://securedrop.org/directory/buzzfeed/	SecureDrop
CBC News	Medios de Comunicación	Canadá	https://www.cbc.ca/securedrop/	SecureDrop
Center for Investigative Reporting	Medios de Comunicación	Estados Unidos	http://leak.revealnews.org/	SecureDrop

Apéndice A - Buzones digitales seguro en línea

Nombre	Sector	País	URL	Proveedor
Center for Public Integrity	Medios de Comunicación	Estados Unidos	https://apps.publicintegrity.org/tips/	SecureDrop
ChileLeaks	Sociedad Civil	Chile	https://chileleaks.org/denuncia.html	GlobaLeaks
Dagens Naeringsliv	Medios de Comunicación	Noruega	https://www.dn.no/staticprojects/2016/12/securedrop/	SecureDrop
Daily Beast	Medios de Comunicación	Estados Unidos	https://www.thedailybeast.com/tips	SecureDrop
Dallas Morning News	Medios de Comunicación	Estados Unidos	https://interactives.dallasnews.com/secure-drop/	SecureDrop
Dr Oetker	Sector Privado	Alemania	https://coho.oetker-group.com/#/	GlobaLeaks
Edison	Sector Privado	Italia	https://segnalazioni.edison.it/#/	GlobaLeaks
Ethics and Anticorruption Commission	Sector Público	Kenia	https://www.bkms-system.net/bkwebanon/report/clientInfo?cin=111KACC33&language=eng	BKMS
Falck Renewables	Sector Privado	Italia	https://segnalazioni.falckrenewables.eu/	GlobaLeaks
Ferrocarrils de la Generalitat de Catalunya (FGC)	Sector Público	España	https://canalcompliment.fgc.cat	GlobaLeaks
FT	Medios de Comunicación	Reino Unido	https://ft.com/news-tips/	SecureDrop
Funding Fish	Sociedad Civil	Reino Unido	https://fishyleaks.eu/en/	GlobaLeaks

Apéndice A - Buzones digitales seguro en línea

Nombre	Sector	País	URL	Proveedor
Barton Gellman	Medios de Comunicación	Estados Unidos	https://tcfmailvault.info/	SecureDrop
Generalitat of Catalunya	Sector Público	España	http://governobert.gencat.cat/ca/bustia-etica/	GlobaLeaks
Global Reporting Centre	Sector Público	Canadá	https://globalreportingcentre.org/tips/	SecureDrop
Global Witness	Sociedad Civil	Reino Unido	https://www.globalwitness.org/en/securedrop/	SecureDrop
The Guardian	Medios de Comunicación	Reino Unido	https://www.theguardian.com/securedrop	SecureDrop
Claudio Guarnieri	Sociedad Civil	Mundial	https://nex.sx/contacts/	SecureDrop
Harvard IQSS	Sector Público	Estados Unidos	https://www.hmdc.harvard.edu/securedrop.html	SecureDrop
Heise Investigativ	Medios de Comunicación	Alemania	https://www.heise.de/investigativ/briefkasten/	SecureDrop
Houston Chronicle	Medios de Comunicación	Estados Unidos	https://projects.houstonchronicle.com/newstips/	SecureDrop
ICIJ	Medios de Comunicación	Mundial	https://www.icij.org/leak/	SecureDrop
IndonesiaLeaks	Sociedad Civil	Indonesia	https://www.indonesialeaks.id/	GlobaLeaks
The Intercept	Medios de Comunicación	Estados Unidos	https://theintercept.com/source/#securedrop	SecureDrop

Apéndice A - Buzones digitales seguro en línea

Nombre	Sector	País	URL	Proveedor
IrpiLeaks	Medios de Comunicación	Italia	https://irpimedia.irpi.eu/diventa-una-fonte/irpileaks/	GlobaLeaks
Le Journal de Montreal	Medios de Comunicación	Canadá	https://www.journaldemontreal.com/dossiers-secrets	SecureDrop
Jean-Marc Manach	Medios de Comunicación	Francia	https://jean-marc.manach.net/securedrop.html	SecureDrop
Kommunal Report	Medios de Comunicación	Noruega	https://securedrop.kommunal-rapport.no/	SecureDrop
Leaks.ng	Medios de Comunicación	Nigeria	https://www.leaks.ng/	GlobaLeaks
Lleida City Hall	Sector Público	España	https://www.paeria.cat/bustiaetica/ca/index.asp	GlobaLeaks
La Marzocco	Sector Privado	Italia	https://segnalazioni.lamarzocco.com	GlobaLeaks
Lucy Parsons Labs	Sociedad Civil	Estados Unidos	https://invisible.institute/contact	SecureDrop
Stefania Maurizi	Medios de Comunicación	Italia	https://stefaniamaurizi.it/en-contactme.html	SecureDrop
The Markup	Medios de Comunicación	Estados Unidos	https://themarkup.org/tips	SecureDrop
McClatchy DC	Medios de Comunicación	Estados Unidos	https://www.mcclatchydc.com/customer-service/contact-us/#navlink=mi_footer	SecureDrop

Apéndice A - Buzones digitales seguro en línea

Nombre	Sector	País	URL	Proveedor
Meduza	Medios de Comunicación	Rusia	https://meduza.io/cards/u-menya-est-vazhnaya-informatsiya-dlya-meduzy-no-ya-boyus-ee-peredavat-kak-sdelat-eto-po-nastoyaschemu-anonimno	SecureDrop
Government of Mexico	Sector Público	México	https://alertadores.funcionpublica.gob.mx/	GlobaLeaks
MexicoLeaks	Medios de Comunicación	México	https://mexicoleaks.mx/enviar.html	GlobaLeaks
NBC	Medios de Comunicación	Estados Unidos	https://www.nbcnews.com/securedrop	SecureDrop
New York Times	Medios de Comunicación	Estados Unidos	https://www.nytimes.com/tips#securedrop	SecureDrop
NOYB	Sociedad Civil	Austria	https://noyb.eu/en/securedrop	SecureDrop
NRK	Medios de Comunicación	Noruega	https://www.nrk.no/varsle/#part1	SecureDrop
OCCRP	Medios de Comunicación	Mundial	https://www.occrp.org/en/aboutus/securedrop/	SecureDrop
Oficina Antifrau de Catalunya	Sector Público	España	https://denunciesanonimes.antifrau.cat/#/?lang=esp	GlobaLeaks
Oživení	Sociedad Civil	República Checa	https://secure.oziveni.cz/#/	GlobaLeaks
PeruLeaks	Sociedad Civil	Perú	http://leaks.pe/#	GlobaLeaks

Apéndice A - Buzones digitales seguro en línea

Nombre	Sector	País	URL	Proveedor
Pištaljka	Sociedad Civil	Serbia	https://pistaljka.rs/	GlobaLeaks
Politico	Medios de Comunicación	Estados Unidos	https://www.politico.com/news-tips/	SecureDrop
Kevin Poulsen	Medios de Comunicación	Estados Unidos	https://freedom.press/people/kevin-poulsen/	SecureDrop
ProPublica	Medios de Comunicación	Estados Unidos	https://www.propublica.org/tips/	SecureDrop
Publeaks.nl	Medios de Comunicación	Países Bajos	https://secure.publeaks.nl/#/	GlobaLeaks
Public Intelligence	Sociedad Civil	Estados Unidos	https://publicintelligence.net/contribute/	SecureDrop
Radio Canada	Medios de Comunicación	Canadá	https://sourceanonyme.radio-canada.ca/	SecureDrop
Reflets.info	Medios de Comunicación	Francia	https://reflets.info/secure-contact	SecureDrop
Reuters	Medios de Comunicación	Estados Unidos	https://www.reuters.com/investigates/special-report/tips/	SecureDrop
RINA	Sector Privado	Italia	https://whistleblowing.rina.org/	GlobaLeaks
Rise.md	Medios de Comunicación	Moldavia	https://www.rise.md/leaks/	SecureDrop
Rue89	Sociedad Civil	Francia	http://alerte.rue89locaux.com	GlobaLeaks
RUV Kveikur	Medios de Comunicación	Islandia	https://www.ruv.is/kveikur/opnum-securedrop/	SecureDrop

Apéndice A - Buzones digitales seguro en línea

Nombre	Sector	País	URL	Proveedor
SAES Group	Sector Privado	Italia	https://segnalazioni.saesgetters.com	GlobaLeaks
Schwartz Media	Medios de Comunicación	Australia	https://www.themonthly.com.au/tips	SecureDrop
Siemens	Sector Privado	Alemania	https://www.bkms-system.net/bkwebanon/report/clientInfo?cin=19siem14&c=-1&language=ger	BKMS
Slate	Medios de Comunicación	Estados Unidos	https://slate.com/tips	SecureDrop
Gruppo Sole 24 Ore	Medios de Comunicación	Italia	https://segnalazioni.gruppo24ore.com/#/	GlobaLeaks
Sourcesûre	Medios de Comunicación	Francia	https://ensecurite.sourcesure.eu/#/	Globaleaks
Subterraneo	Sociedad Civil	Nicaragua	https://subterraneoni.org/	GlobaLeaks
Süddeutsche Zeitung	Medios de Comunicación	Alemania	https://www.sueddeutsche.de/projekte/kontakt/	SecureDrop
Stuff.co.nz	Medios de Comunicación	Nueva Zelanda	https://www.stuff.co.nz/securedrop/index.html	SecureDrop
Svenska Dagbladet	Medios de Comunicación	Suecia	https://www.svd.se/securedrop/	SecureDrop
Technopolice	Sociedad Civil	Francia	https://technopolice.fr/leak/	SecureDrop

Apéndice A - Buzones digitales seguro en línea

Nombre	Sector	País	URL	Proveedor
The Telegraph	Medios de Comunicación	Reino Unido	https://www.telegraph.co.uk/news/investigations/contact-us/	SecureDrop
Terrassa City Hall	Sector Público	España	https://bustiaetica.terrassa.cat/	GlobaLeaks
Toronto Crime Stoppers	Sociedad Civil	Canadá	https://www.222tips.com/SecureDrop	SecureDrop
Transparency International Ireland	Sociedad Civil	Irlanda	https://lostineurope.eu/	GlobaLeaks
Transparency International Italia	Sociedad Civil	Italia	https://alac.transparency.it	GlobaLeaks
Transparency International Kosovo	Sociedad Civil	Kósovo	https://raporto.kdi-kosova.org/#/	GlobaLeaks
Transparency International Portugal	Sociedad Civil	Portugal	https://provedoria.transparencia.pt/	GlobaLeaks
Transparency International Tunisia	Sociedad Civil	Túnez	https://billkamcha.tn/	GlobaLeaks
USA Today	Medios de Comunicación	Estados Unidos	https://newstips.usatoday.com/securedrop.html	SecureDrop
The Verge	Medios de Comunicación	Estados Unidos	https://www.theverge.com/a/tip-us-secure-contact-email	SecureDrop
VG	Medios de Comunicación	Noruega	https://www.vg.no/securedrop/	SecureDrop
Wall Street Journal	Medios de Comunicación	Estados Unidos	https://www.wsj.com/tips	SecureDrop

Apéndice A - Buzones digitales seguro en línea

Nombre	Sector	País	URL	Proveedor
Washington Post	Medios de Comunicación	Estados Unidos	https://www.washingtonpost.com/securedrop/	SecureDrop
WildLeaks	Sociedad Civil	Estados Unidos	https://wildleaks.org/how-wildleaks-works/	SecureDrop
Wired	Medios de Comunicación	Estados Unidos	https://www.wired.com/securedrop/	SecureDrop
Die Zeit	Medios de Comunicación	Alemania	https://meine.zeit.de/briefkasten	Briefkasten
Zvizgac	Medios de Comunicación	Eslovenia	https://zvizgac.si/	SecureDrop

Apéndice B - Buzones digitales instalados analizados por DiSalvo

Gestores de buzones online seguros analizados por Philip Di Salvo. No todos estos proyectos siguen activos online.

Fuente: Di Salvo 2020: 110

Plataformas	Colaborativo	De varios	Medios
BalkanLeaks	BayLeaks	AfriLeaks	Die Zeit Briefkasten
Ecuador Transparente	ExpoLeaks	MafiaLeaks	News Leaks
InfodioLeaks	IrpiLeaks	MexicoLeaks	NRKBeta
MagyarLeaks	Filtrala	PubLeaks	ProPublica
Pistaljka	WildLeaks	Source Sure	The Globe and Mail
POGO			The Sun

Apéndice C – Proyecto de buzones EAT

Esta lista refleja los buzones digitales que estaban activos durante el proyecto. Otros buzones está previsto que estén online al término del proyecto.

País	Organización	Descripción	Dropbox URL
Italia	Ferrovie Calabria	Empresa privada	https://ferroviecalabria.disclosers.eu/#/
Italia	Ciao people	Empresa privada	https://backstairfanpage.disclosers.eu/#/
Bulgaria	Anti Corruption Fund	ONG	http://acf.disclosers.eu/#/
Bulgaria	Ministerio de Defensa	Entidad pública	http://armymedia.disclosers.eu/#/
Bulgaria	Ayuntamiento de Tryavna	Entidad pública	http://tryavna.disclosers.eu/#/
Bulgaria	OffNews Media Group	Empresa privada	http://offnews.disclosers.eu/#/
Rumanía	Fair Mediasind	Sindicato de periodistas	http://fairmediasind.disclosers.eu/#/
Grecia	Autoridad única e independiente para la contratación pública (EAADHSY)	Entidad pública	http://whistle2eaadhsy.disclosers.eu/#/
Grecia	Sol Consulting	Empresa privada	http://whistle2solconsulting.disclosers.eu/#/
Grecia	Crowe Greece	Empresa privada	http://whistle2sol.disclosers.eu/#/
República Checa	Brno Stred	Entidad pública	https://brnostred.disclosers.eu/#/
España	Federación de Sindicatos de Periodistas (FeSP)	Sindicato de periodistas	http://aslertasfesp.disclosers.eu
España	FIBGAR	ONG	http://alertacovid19.disclosers.eu/#/
Chipre	Legal Legion Cyprus	ONG	https://3lcy.disclosers.eu/

Apéndice D - Lista de entrevistados

Las entrevistas incluyen representantes de las siguientes organizaciones:

Socios EAT

Atlatszo (Hungría)
CIJ (Rumania)
The Good Lobby (Italia)
MDC (Bulgaria)
Oživení (República Checa)

Medios de comunicación

OCCRP (varios países)

Organizaciones No Gubernamentales

Freedom of the Press Foundation (USA)
Pištaljka (Serbia)
Transparency International Italia

Instituciones públicas

BaFin (Alemania)
Catalunya Antifraude (España)

También contamos con la participación de *The Guardian* en el seminario:

https://www.youtube.com/watch?v=1mI3uQnXPdM

Algunos de los entrevistados pidieron no ser identificados y no están incluidos en la lista.

Apéndice E – Tabla de Metadatos

Project ID	Project Name	Creation Date	Timezone	Country	Language
1	Name 1			Italy	[it, en]
2	Name 2			France	[fr]
3	Name 3				

Project ID	Submission ID	Submission Date (UTC)	Anonymous	Sex	Age	Accept_Publication	Reported Internally
1	#1	date	1	F	24-34	1	1
1	#2	date	0	F	35-44	1	0
2	#3	date	1	M	35-44	0	1

Project ID	Reported to Regulator	Employee	Count Number Reports	Personally involved	Total Attachments Count	Attachments after submission
1	1	1	2	0	2	1
1	1	0	0	1	0	0
2	0	1	1	1	1	0

Project ID	Comments	Only obligatory fields	Anomalies	Ricochet	Returns count	Last return
1	#	1	0	0	0	date
1	#	1	0	0	1	date
2	#	0	1	1	2	date

Apéndice F – Cuestionario de la investigación

EAT – Cómo hemos recabado datos para la investigación

Instalar 250 buzones anónimos en 10 países de la UE es una empresa de gran envergadura. Una parte fundamental del proyecto EAT es utilizar esta experiencia para comprender cómo funcionan estas plataformas en la práctica y cuáles son los factores que las hacen más eficaces.

La plataforma EAT permanecerá operativa para su organización al menos hasta el 31 de enero de 2021. El *Centro Hermes para los Derechos Humanos* (encargado del mantenimiento de la plataforma) compartirá durante el proyecto ciertos metadatos[1] específicos con *Blueprint for Free Speech*, que realizará un análisis estadístico sobre los metadatos agregados y redactará un informe final. El tipo de datos que se compartirán se indica a continuación.

El proyecto adopta deliberadamente un enfoque conservador a la hora de compartir los metadatos. Los metadatos compartidos con *Blueprint for Free Speech* son los mínimos necesarios para realizar un análisis útil.

No se comparte el contenido del informe con los socios de EAT, y todos los metadatos están en un formato anónimizado: el consorcio, en particular *Hermes* y *Blueprint for Free Speech* no pueden vincular una respuesta al cuestionario con ninguna revelación específica.

¿Qué preguntas intentamos responder?

Hemos desarrollado una serie de preguntas de investigación que abordan las siguientes cuestiones principales:

- ¿Podemos replicar los resultados de otras investigaciones sobre la denuncia de irregularidades?
- ¿Depende el éxito de los canales de denuncia anónimos de su visibilidad? ¿Qué tipo de promoción funciona mejor?
- ¿Cómo se utilizan los canales de denuncia en la práctica? ¿Se utilizan de forma segura?
- ¿Ha cumplido el proyecto EAT sus objetivos?

Para ver la lista completa de preguntas de investigación, consulte el Apéndice 1.

¿Qué datos recogemos?

Hay tres categorías principales de datos que estamos recogiendo:

- Si un informe está marcado como "abierto" o "cerrado" en la organización receptora.
- Algunas categorías limitadas de metadatos ("información sobre la información", que se enumeran a continuación).

1 Los metadatos describen otros datos. Proporcionan información adicional. Por ejemplo, una imagen puede incluir metadatos que describan el tamaño de la imagen, la profundidad del color, la resolución de la imagen, cuándo se creó la imagen y otros datos.

Apéndice F – Cuestionario de la investigación

Lista de metadatos recopilados:

Debido a la naturaleza del proyecto, limitamos la recogida a unas pocas categorías establecidas. Éstas incluirán lo siguiente:

- Para cada instancia (cada buzón individual), registraremos un ID, el nombre del proyecto, la zona horaria, el país y el idioma.
- Para cada envío, registramos:
    - Un ID único
    - Cuando la persona que informa se conectó al sitio
    - La hora a la que se realizó el envío
    - Cuántos documentos se han presentado, en su caso
    - Si el denunciante utilizó Tor
    - Si el denunciante hizo clic en un enlace al sitio de Ricochet Refresh
    - Cuántas veces regresó el denunciante al sitio web después de hacer un envío
    - La última fecha en la que el denunciante se conectó al sitio
    - Si se ha registrado un evento anómalo (un ataque al buzón).

Nota:
Para cualquier duda o pregunta sobre el cuestionario completo en el lugar, por favor consulte el Apéndice 2.

Apéndice G - Preguntas de investigación del EAT

¿Utilizarán los denunciantes los canales anónimos si se les facilitan?

¿La provisión de canales de denuncia anónimos da lugar a denuncias procesables?

¿Prefieren los denunciantes utilizar los canales externos? ¿Es necesaria la denuncia interna obligatoria?

¿Les parece bien a los denunciantes que sus informes se compartan con terceros?

¿Qué características comparten los denunciantes?

¿Qué importancia tienen los intermediarios (abogados, ONG, sindicatos, etc.)?

¿Qué importancia tienen los marcos jurídicos?

¿Cuál es el riesgo de abuso y de que las denuncias no sean serias?

¿Afecta la cobertura mediática al uso de los canales?

¿Influye la actitud de la entidad receptora?

¿Qué tipo de respuesta pueden esperar los denunciantes?

¿Desean los denunciantes el anonimato?

¿Son accesibles los canales digitales de denuncia? ¿Se utilizan de forma segura?

¿Cómo utilizan los denunciantes los canales electrónicos? ¿Es importante la comunicación bidireccional?

¿Se atacan los canales digitales de denuncia?

¿Influye el modelo de presentación adoptado?

Apéndice H - Cuestionario EAT

Borrador del Cuestionario EAT con notas del programa (V3)

* indica un campo obligatorio

SECCIÓN 1 - INFORMACIÓN PRELIMINAR

NOTA PROG.:
AÑADA EN LA PARTE SUPERIOR DE LA PANTALLA EL SIGUIENTE MENSAJE Y UN DESLIZADOR HORIZONTAL QUE MUESTRE EL PORCENTAJE DE PREGUNTAS CONTESTADAS

"Se realizarán 28 preguntas. Éstas ayudarán al destinatario de su divulgación a entender de qué se trata.

También pedimos algunos datos estadísticos, que no le identifican. Lo hacemos para ayudar al equipo que apoya este buzón a entender cómo mejorarlo en el futuro.

Sólo tiene que responder a las casillas con un * junto a la pregunta para avanzar. Las demás preguntas son opcionales. Se puede salir del proceso en cualquier momento".

NOTA PROG:
AÑADIR A CONTINUACIÓN, CON UN ENLACE AL SITIO DE DESCARGA DEL NAVEGADOR TOR

Si se quiere anonimato, hay que usar el programa Tor para hacer un envío a este sitio. Puede descargar el navegador Tor aquí <Añadir hipervínculo>. Funciona como Safari, Chrome u otros navegadores web, excepto que oculta desde donde se hace el envío. Si se descarga el navegador, y luego vuelve a este sitio usando ese Navegador Tor, su dirección de internet estará oculta para cualquiera en este sitio.

Términos y condiciones de este dropbox

Por favor, confirme marcando esta casilla* <Insert Box> que entiende que si no utiliza Tor, resulta en la incapacidad de proteger su anonimato.

Para mejorar aún más su seguridad, siga las siguientes instrucciones:

- En caso de que quiera permanecer en el anonimato, no envíe ningún dato personal (como su nombre o el tipo de relación que tiene con la persona sobre la que hace la revelación, o cualquier información que pueda ser utilizada para localizarle).

- No envíe ningún dato desde un PC proporcionado por su empresa. Una conexión en una red de la empresa podría poner en peligro su anonimato.

Al marcar esta segunda casilla, confirma que acepta estos términos y condiciones.* <Insertar casilla>

Apéndice H - Cuestionario EAT

SECCIÓN 2 - CUÉNTENOS SOBRE LA INFRACCIÓN

P1. ¿De qué tipo de organización trata su informe? *

NOTA:
- RESPUESTA ÚNICA

1. Una empresa privada
2. Una entidad pública
3. Otra
4. No lo sé / prefiero no decirlo

P2. ¿Ha intentado denunciar esto antes?*

NOTA:
- RESPUESTA ÚNICA
- AL AZAR 1-2

1. Sí
2. No - continuar con 5
3. No lo sé / prefiero no decirlo - continuar con 5

P3. ¿A quién has intentado informar de esto? Seleccione todos los que correspondan. También puede "prefiero no decir nada".

NOTA DEL PROG:
- SE PERMITEN RESPUESTAS MÚLTIPLES
- ALEATORIAMENTE DEL 1 AL 9

1. Superior
2. Compañero
3. Responsable de cumplimiento
4. A un área de asesoramiento o contratada por mi empresa
5. Un regulador del sector o un defensor del pueblo
6. Un sindicato, grupo profesional u organismo industrial
7. Policía u otros cuerpos de seguridad
8. Un periodista o un medio de comunicación
9. Un abogado
10. Otro - especifique, por favor (cuadro de texto para escribir)
11. Prefiero no decir nada

Apéndice H - Cuestionario EAT

P5. ¿Hay alguna razón por la que no haya denunciado esto antes?

NOTA PROG:
- ABRIR CAMPO DE TEXTO

P6. ¿Cuál es su relación con la organización sobre la que informa? *

NOTA PROG:
- RESPUESTA ÚNICA
- AL AZAR 1-6

1. Empleado
2. Ex empleado
3. Proveedor
4. Subcontratista o asesor
5. Voluntario
6. Cliente
7. Otro – por favor, especifique (cuadro de texto abierto)
8. No lo sé / Prefiero no decir nada

P7. ¿Cuál es su nivel de implicación en el tema de su informe? *

NOTA DEL PROG:
- RESPUESTA ÚNICA
- AL AZAR 1-4

1. Estoy involucrado personalmente
2. Tengo conocimiento de primera mano
3. He oído hablar de ello
4. Me he visto perjudicado
5. Otro/Prefiero no decirlo

SECCIÓN 2 - SU ALERTA

[2.1 CAMPOS BÁSICOS DE LA ALERTA]

P8. Por favor, haga un breve resumen de su alerta (en un máximo de 200 caracteres). *

NOTA PROG:
- CAMPO DE TEXTO ABIERTO
- 50-200 caracteres

Apéndice H - Cuestionario EAT

P9. Por favor, describa su alerta con mayor detalle*.

NOTA PROG:
- CAMPO DE TEXTO ABIERTO

P10. Adjunte documentos que respalden su informe.

NOTA PROG:
- AÑADIR BOTÓN DE ADJUNTAR ARCHIVOS

[2.2 INFORMACIÓN ADICIONAL]

P11. ¿Cuándo se produjo la infracción?

NOTA PROG:
- ABRIR CAMPO DE TEXTO

P12. ¿Se está cometiendo la infracción o es probable que se repita?

NOTA PROG:
- RESPUESTA ÚNICA

1. Sí
2. No

P13. ¿Quién se ha beneficiado de la infracción?

NOTA PROG:
- CAMPO DE TEXTO ABIERTO

P14. ¿La infracción puso a alguien en peligro o alguien resultó perjudicado?

NOTA PROG:
- RESPUESTA ÚNICA

1. Sí
2. No

Apéndice H - Cuestionario EAT

P15. ¿Siente que está en riesgo o que ha sido perjudicado?

NOTA DEL PROG:
- RESPUESTA ÚNICA

1. Sí
2. No

P16. ¿Cuál de las siguientes opciones describe mejor el tema de su informe? Puede seleccionar más de una opción. *

NOTA PROG:
- RESPUESTA MÚLTIPLE
- AL AZAR 1-9

1. Fraude o robo
2. Prácticas desleales de contratación - continuar con 18
3. Conflicto de intereses u otra toma de decisiones indebida - continuar con 18
4. Uso indebido de la información, incluido el acceso o la divulgación no autorizados G- continuar con 18
5. Soborno o corrupción
6. Despilfarro o mala gestión de los recursos
7. Falta de responsabilidad, o encubrimiento de las irregularidades - continuar con 18
8. Peligro para la salud pública, la seguridad o el medio ambiente - continuar con 18
9. Condiciones del lugar de trabajo, intimidación o acoso - continuar con 18
10. Otros – especifique, por favor (CUADRO DE TEXTO ABIERTO)
11. No lo sabe / Prefiere no decirlo

P17. ¿Cuál cree usted que ha sido el coste económico de la infracción?

NOTA DEL PROG:
- CAMPO DE TEXTO ABIERTO

P18. ¿Puede proporcionarnos alguna información útil para verificar la autenticidad de su informe? Si no tiene la información usted mismo, ¿puede decirnos dónde existen los datos y se puede acceder a ellos?

NOTA PROG:
- CAMPO DE TEXTO ABIERTO

Apéndice H - Cuestionario EAT

P19. ¿Quiénes son las personas implicadas en el incidente?

NOTA PROG:
- CAMPO DE TEXTO ABIERTO

P20. ¿Qué empresas o entidades están implicadas?

NOTA PROG:
- ABRIR CAMPO DE TEXTO

SECCIÓN 3 - SOBRE USTED

Esta sección es completamente opcional. Puede elegir responder a algunas, a todas o a ninguna de las siguientes preguntas.

P21. ¿Quiere revelarnos su identidad?

NOTA PROG:
- OPCIÓN ÚNICA

1. No - continuar con 24
2. Sí

Por favor, no responda a ninguna pregunta sobre la que no esté seguro o se sienta incómodo. No es necesario que responda a ninguna de estas preguntas para presentar su informe.

P22. ¿Cómo se llama?

NOTA PROG:
- CAMPO DE TEXTO ABIERTO

Apéndice H - Cuestionario EAT

P23. ¿Cuántos años tiene?

NOTA PROG:
- RESPUESTA ÚNICA

1. Menor de 16
2. 16-24
3. 24-34
4. 35-44
5. 45-54
6. 55-64
7. 65-75
8. 75+

P24. ¿Cuál es su género?

NOTA PROG:
- RESPUESTA ÚNICA
- AL AZAR 1-2

1. Masculino
2. Femenino
3. Otros
4. Prefiero no decirlo

P24. Ubicación

NOTA PROG:
- CAMPO DE TEXTO ABIERTO

P25. Puesto de trabajo

NOTA PROG:
- CAMPO DE TEXTO ABIERTO

Apéndice H - Cuestionario EAT

P26. ¿Desea proporcionar algún dato de contacto?

NOTA PROG:
-RESPUESTA ÚNICA

1. No - continuar con 28
2. Si

Por favor, no responda a ninguna pregunta sobre la que se sienta inseguro o incómodo. No es necesario que responda a estas preguntas para presentar su informe.

P27. Por favor, facilite aquí sus datos de contacto si lo desea.

NOTA PROG:
- CAMPO DE TEXTO ABIERTO

P28. ¿Hay algo más que quiera decirnos?

NOTA PROG:
- CAMPO DE TEXTO ABIERTO

Sección 3. ¿Desea tener un chat en línea con nosotros?
Si desea que podamos ponernos en contacto con usted para pedirle aclaraciones o comentarios, pero quiere tener una garantía tecnológica de anonimato, descargue un software gratuito llamado Ricochet IM aquí <enlace a Ricochet IM>. Instálelo, obtenga un ID de Ricochet y escribe el ID aquí <espacio para un ID de Ricochet aquí>.

El Ricochet ID del destinatario de este dropbox es <ID AQUÍ>.
El ID de Ricochet del equipo técnico que gestiona este buzón es <ID AQUÍ>.

La próxima vez que nos conectemos, intentaremos ponernos en contacto con usted online, pero debe tener Ricochet abierto para hacerlo. No lo use desde el trabajo.

Nueva sección : ¿Necesita ayuda urgente?

Apéndice I - Formas de identificar a un alertador si no usa un buzón anónimo seguro

El anonimato proporcionado por un buzón digital seguro desempeña un papel crucial en la protección del alertador. El reto es tanto técnico como de usuario, ya que aunque la tecnología esté disponible, depende de que el usuario la entienda y sea capaz de utilizarla. En esta sección describiremos brevemente algunos de los riesgos que conlleva el uso de un buzón sin la adecuada protección del anonimato.

Se puede pensar que las amenazas contra un alertador operan a diferentes niveles:

- Local - la máquina, el dispositivo o el entorno que el denunciante utiliza para hacer sus presentaciones
- Red - la infraestructura de comunicaciones, tanto interna como externa, que se utiliza para enviar la denuncia
- Remoto - el buzón de recepción y los metadatos asociados

Local

Las amenazas locales son difíciles de contrarrestar, ya que dependen de que el denunciante tome las medidas adecuadas para protegerse. Esto puede ser particularmente difícil si un alertador intenta hacer un envío desde una red corporativa o de la organización, y por lo tanto no tiene un control total sobre el equipo o el entorno.

- Supervisión de los dispositivos: los dispositivos de la empresa y de la organización suelen ser vigilados tanto en lo que respecta a la instalación de software como a los sitios web y, potencialmente, incluso al acceso a los recursos. Esto puede perjudicar a los buzones anónimos, ya que supervisa efectivamente la fuente. Para contrarrestarlo, hay que enseñar bien a los usuarios, sobre todo si no son propietarios o no controlan el dispositivo que utilizan, ya que corren el riesgo de ser vigilados.
- Vigilancia del entorno: aunque el alertador controle el dispositivo, puede ser objeto de una vigilancia del entorno, es decir, de las horas en las que se encuentra en el edificio y del lugar en el que está. De nuevo, para contrarrestar esto se requiere una buena educación del usuario.

Red

La supervisión de la red es algo habitual tanto dentro de las organizaciones como, en general, por parte de los proveedores de comunicaciones. Los enfoques de seguridad estándar adoptados para servicios como la banca y las compras online no son suficientes para proteger frente la vigilancia y la elaboración de perfiles de un alertador.

Interceptación de TLS: la gente se ha acostumbrado a confiar en TLS como forma de proteger sus actividades en línea de la observación. Sin embargo, en la práctica, a menudo se intercepta TLS en las redes corporativas y gubernamentales. La interceptación de TLS es un componente central de la supervisión de la ciberseguridad en las redes corporativas, y es un proceso en gran medida automatizado. Puede ser transparente para el usuario medio, por lo que es extremadamente difícil de detectar. El uso de técnicas como el Certificate Pinning y el enrutamiento anónimo como Tor puede ayudar a detectar o, en el caso de este último, a contrarrestar tales amenazas. De nuevo, si el usuario no controla el dispositivo podría estar en riesgo.

Apéndice I - Formas de identificar a un alertador si no usa un buzón anónimo seguro

- Monitorización del DNS - Incluso cuando el TLS no está siendo interceptado, las búsquedas del Servicio de Nombres de Dominio (DNS), que asignan una dirección web a una dirección IP, pueden ser monitorizadas o redirigidas. Esto revela qué sitios visita una persona. No revela los contenidos ni las páginas visitadas, pero sería suficiente para detectar quién ha accedido a un determinado servicio de dropbox. El uso de un DNS seguro es cada vez más popular, pero si el servidor DNS es interno o está alojado en un tercero no fiable, este tipo de monitorización puede tener lugar. Esto es especialmente preocupante en el caso de los proveedores de servicios de Internet, que a menudo utilizan sus propios servidores DNS y, por tanto, pueden determinar todos los sitios que visitan sus clientes y, por tanto, identificar potencialmente a alguien que accede a un dropbox.

- Análisis del tráfico: aunque el DNS esté protegido y el tráfico esté encriptado, sigue existiendo el riesgo de que se analice el tráfico, sobre todo en el caso de los ISP y las redes corporativas. Aunque no puedan ver el contenido, pueden determinar el tamaño de la solicitud que se envía al servidor. Si conocen el documento que se ha subido, es posible que puedan determinar desde dónde se originó la subida buscando una solicitud de envío de tamaño adecuado. Esto depende de la naturaleza del envío y de lo diferente que sea del tráfico normal. Las cargas de gran tamaño representan un peligro potencialmente mayor, ya que pueden ser relativamente inusuales en la red.

Remoto

Las vulnerabilidades remotas se producen en el servidor de destino o cerca de él. Es difícil que el usuario sea consciente de ellas, ya que no tiene a la vista ni información sobre la infraestructura remota.

- Balanceo de carga/Proxy TLS - si un dropbox está alojado en una infraestructura de nube de terceros, o utiliza balanceadores de carga, Firewalls de Aplicaciones Web, o Redes de Entrega de Contenido, existe la posibilidad de que la conexión TLS sea interceptada por el proveedor de ese servicio. Esto es necesario para proporcionar el equilibrio de carga, o el cortafuegos/protección del servidor de destino final. Sin embargo, dicha interceptación será invisible para el usuario, pero requerirá que el usuario confíe en el tercero para proteger su anonimato. El uso de tecnología de enrutamiento anónimo como Tor puede ayudar a contrarrestar tales amenazas.

- Recogida de metadatos: las solicitudes a un servidor web suelen crear una gran cantidad de metadatos, desde información sobre el dispositivo que realiza la solicitud hasta la dirección IP del dispositivo. Es importante que estos registros estén protegidos e idealmente se destruyan en un breve plazo para proteger estos datos del acceso no autorizado por parte de los administradores, del robo durante un hackeo del servidor o del acceso por parte de las fuerzas del orden. Los usuarios pueden utilizar Tor para protegerse mejor.

Apéndice J - Otros recursos

Socios del EAT

Fundación Internacional Baltasar Garzón (FIBGAR)

Coordinador del proyecto, radicado en España. FIBGAR se basa en los pilares de la solidaridad, el respeto, la promoción de los Derechos Humanos, la cooperación al desarrollo de los pueblos, la mediación y la lucha contra la impunidad.

Con estas bases FIBGAR impulsa programas de actuación desde los ámbitos de la educación, la justicia, la sociedad, la política y la cultura para la defensa y aplicación de los Derechos Humanos en defensa de las víctimas y sus derechos a la verdad, la justicia y la reparación y para la persecución de la corrupción y el crimen organizado en todas sus formas.

Las herramientas básicas para promover las actividades que constituyen la esencia de la Fundación, serán la investigación, la formación y la cooperación con otras fundaciones, organizaciones y entidades académicas, sociales, políticas y jurídicas junto con la acción directa en coordinación con los actores relevantes.

web: https://www.fibgar.org/

Hermes Center

Nuestra misión es promover y desarrollar en la sociedad la concienciación y la atención a la transparencia y la rendición de cuentas, estén o no relacionadas con la sociedad en general. Nuestro objetivo es aumentar la implicación de los ciudadanos en la gestión de los asuntos de interés público e impulsar la participación activa de los trabajadores y empleados en la correcta gestión de las corporaciones y empresas para las que trabajan.

web: https://www.hermescenter.org/

Blueprint for Free Speech

Blueprint for Free Speech es una organización benéfica sin ánimo de lucro que trabaja a nivel internacional para promover el derecho a la libertad de expresión sin interferencias ni intrusiones indebidas. Nuestra investigación y promoción se esfuerzan por defender el artículo 19 de la Declaración Universal de los Derechos Humanos, que afirma el derecho a la libertad de opinión y de expresión de todas las personas.

web: https://blueprintforfreespeech.net/en/1577-2/

Apéndice J - Otros recursos

Atlatszo.hu Kozhasznu Nonprofit Korlatolt Felelossegu Tarsasag – Hungría

Atlatszo.hu es una ONG de vigilancia y un periódico online de periodismo de investigación para promover la transparencia, la responsabilidad y la libertad de información en Hungría.

Fundada en 2011, *atlatszo.hu* - "atlatszo" significa transparente en húngaro- elabora informes de investigación, acepta información de denunciantes, presenta solicitudes de libertad de información e inicia demandas de libertad de información en los casos en que sus solicitudes son rechazadas.

web: https://english.atlatszo.hu/about-us-fundraising/

Fundația Centrul Pentru Jurnalism Independent (CPJI) – Rumanía

El "Centro de Periodismo Independiente" es una organización sin ánimo de lucro, con 25 años de experiencia, que actúa como vigilante del periodismo profesional y de calidad, protegiendo los estándares periodísticos y desarrollando un entorno mediático equilibrado, honesto y responsable.

CIJ es un activo promotor del periodismo responsable, ético y profesional en Rumanía y aboga por un público informado, como requisito previo para cualquier sociedad democrática.

web: www.cji.ro

Transparency International Greece (TI-GR) – Delegación en Grecia

TI Grecia fue fundada en 1996 por un grupo de profesionales de alto nivel, entre los que se encontraban ex políticos, así como empresarios, científicos, periodistas, abogados, funcionarios públicos y empleados privados, que decidieron adoptar una postura contra la corrupción.

TI Grecia reclama la aplicación de principios transparentes y éticos para la buena gobernanza y la lucha contra la corrupción que socava el sistema político y financiero de Grecia. La visión de TI-G es combatir la indiferencia y la ignorancia hacia los temas de transparencia.

Para cumplir con su visión, TI-G está actualmente involucrada en proyectos anticorrupción como el Pacto de Integridad, Integrity Watch y la Expansión del Despliegue de la Tecnología de Denuncia Anónima, Operación y Confiabilidad para Combatir la Corrupción en Europa del Este y del Sur, promoviendo la adopción de plataformas de denuncia en línea a ciertas entidades públicas y privadas.

web: http://www.transparency.gr/ti-kanoume/whistleblowing/e-a-t/

Apéndice J - Otros recursos

Fondatsiya Tsentar Za Razvitie Na Mediite (MDC) – Croacia y Bulgaria

El "Centro de Desarrollo de los Medios de Comunicación" (MDC) de Sofía es una organización sin ánimo de lucro y no partidista fundada en 1998. Se creó para promover los medios de comunicación independientes en Bulgaria y para fomentar la capacidad de los medios de comunicación alentando las buenas prácticas en el periodismo, estimulando la ética profesional, institucionalizando el diálogo entre la administración estatal, los medios de comunicación y el sector de las ONG e impulsando la creación de redes y la cooperación transfronteriza en la región del sureste de Europa.

web: http://www.mediacenterbg.org/about-us/

Oživení – República Checa

Nos esforzamos por aumentar la transparencia de los procesos de toma de decisiones y la gestión financiera en las instituciones públicas de la República Checa, así como la responsabilidad personal de los funcionarios públicos e impulsar la participación activa de los ciudadanos. Nuestras principales áreas de interés son el derecho a la información, la contratación pública y la gestión de la propiedad pública. Por último, pero no por ello menos importante, participamos en la difusión de conocimientos técnicos sobre la lucha contra la corrupción y en la formación y creación de redes de activistas cívicos y contra la corrupción.

web: https://www.oziveni.cz/

The Good Lobby Italia – Delegación en Italia

The Good Lobby Italia es el sección italiana de la organización con sede en Bruselas The Good Lobby, en activo en Europa desde 2015. Trabajamos para que la sociedad sea más democrática, más participativa y más justa. Cada ciudadano puede hacer algo por su comunidad. Nuestro objetivo es influir en las principales decisiones políticas, hacer que nuestros representantes políticos rindan cuentas y compartir con ellos las nuevas soluciones a las que se enfrenta la sociedad.

web: https://www.thegoodlobby.it/