

Bruselas, 7.12.2012
COM(2012) 735 final

**COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL
CONSEJO**

**Refuerzo de la cooperación en materia de aplicación de la ley en la UE:
el Modelo Europeo para el Intercambio de Información (EIXM)**

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO

Refuerzo de la cooperación en materia de aplicación de la ley en la UE: el Modelo Europeo para el Intercambio de Información (EIXM)

1. INTRODUCCIÓN

Para garantizar un nivel de seguridad elevado en la UE y en el espacio Schengen es necesario luchar contra las redes de delincuencia mediante una acción concertada a escala europea¹. Esa acción no solo es necesaria para combatir la delincuencia más grave y organizada, como la trata de seres humanos o el tráfico ilegal de drogas o armas de fuego, sino también los delitos menos graves cometidos a gran escala por grupos itinerantes de delincuentes organizados, así como los cometidos por delincuentes individuales que actúan en distintos Estados miembros.

En este contexto, el intercambio de información entre Estados miembros constituye un instrumento esencial a disposición de los servicios con funciones coercitivas. Por esa razón, los acuerdos internacionales y bilaterales han sido completados por medio de instrumentos y sistemas de la UE, como, por ejemplo, el Sistema de Información de Schengen y el Sistema de Información de Europol, que cuentan con salvaguardias para proteger la vida privada y los datos personales de los ciudadanos tal como exige la Carta de los Derechos Fundamentales de la Unión Europea. En la presente Comunicación se describe y analiza **cómo funciona en la actualidad el intercambio de información transfronterizo en la UE** y se formulan recomendaciones para mejorarlo.

La conclusión a la que se llega en la Comunicación es que, en general, el intercambio de información funciona correctamente. Para apoyar esta afirmación se proporcionan a continuación ejemplos de resultados positivos. **En consecuencia no hay necesidad de crear ni nuevas bases de datos de los servicios con funciones coercitivas ni nuevos instrumentos de intercambio de información a escala de la UE.** Sin embargo los instrumentos actuales de la UE pueden y deben aplicarse y los intercambios se deben organizar de manera más coherente.

En consecuencia, en la presente Comunicación se formulan una serie de recomendaciones a los Estados miembros sobre cómo **mejorar la aplicación de los instrumentos existentes y racionalizar los canales de comunicación utilizados**. En ella se hace hincapié en la necesidad de **garantizar un nivel elevado de calidad, de seguridad y de protección de los datos**. También se explica la manera en que la Comisión prestará ayuda, sobre todo **financiación y formación**, a los Estados miembros. Por tanto, la Comunicación ofrece un modelo por el que debería guiarse la actividad de la UE y de los Estados miembros.

La presente Comunicación responde a la invitación dirigida a la Comisión en el *Programa de Estocolmo* para que evaluara la necesidad de crear un Modelo Europeo para el Intercambio de Información, basado en la evaluación de los instrumentos actualmente existentes. La presente Comunicación se basa en otra Comunicación de la Comisión de 2010 titulada «Panorama general de la gestión de la información en el espacio de libertad, seguridad y justicia» (en lo

¹ La Estrategia de Seguridad Interior de la UE en acción, COM(2010) 673.

sucesivo, «la Comunicación de 2010»² y en la *Estrategia de la UE para la gestión de la información* para la seguridad interior acordada en 2009³, junto con las acciones emprendidas por los Estados miembros, la Comisión y Europol para aplicarla («Acciones IMS»). Se basa asimismo en un inventario sobre el intercambio de información en la UE en el que participaron expertos nacionales e internacionales [Supervisor Europeo de Protección de Datos (SEPD), agencias de la UE, Interpol], un estudio sobre el intercambio de información entre los servicios con funciones coercitivas⁴, y en el intercambio de opiniones con las partes interesadas, entre las que figuran las autoridades de protección de datos.

2. SITUACIÓN ACTUAL

Los servicios con funciones coercitivas intercambian información con diferentes fines: para llevar a cabo investigaciones penales, para detectar y prevenir la delincuencia (por ejemplo, a través de operaciones de inteligencia penal) o para garantizar la seguridad y el orden público. Por lo que se refiere a los intercambios transfronterizos, el estudio de 2010, anteriormente citado, daba cuenta de las respuestas de los organismos nacionales de los Estados miembros según las cuales en alrededor de una cuarta parte de sus investigaciones y operaciones de inteligencia criminal habían solicitado la intervención de otros Estados miembros de la UE o del espacio Schengen.

2.1. Instrumentos

La Comunicación de 2010 describía todas las medidas de la UE que regulan la recogida, el almacenamiento o el intercambio transfronterizo de información personal con fines represivos o de gestión de la migración. La presente Comunicación se centra en los **instrumentos utilizados para los intercambios transfronterizos entre Estados miembros**. Los Estados miembros han facilitado ejemplos de cómo utilizan esos instrumentos.

La **Iniciativa Sueca**⁵ establece las normas, incluidos los plazos, para el intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros para llevar a cabo investigaciones criminales u operaciones de inteligencia criminal. Dicha Iniciativa aplica el principio del «acceso equivalente»: esto es, de que se debe facilitar la información al Estado miembro requirente de acuerdo con unas condiciones que no pueden ser más estrictas que las aplicadas a nivel nacional. La información también debe comunicarse a Europol y Eurojust en la medida en que el intercambio haga referencia a delitos sobre los que tengan competencia.

En 2012 un conocido estafador italiano engañó a una empresa sueca para que ingresara 65 000 EUR en una cuenta italiana. A través del canal SIRENE (véase más adelante), Italia solicitó al punto de contacto único sueco (véase el apartado 3.2 más adelante) que se pusiera en contacto con el director de la empresa con el fin de comprobar si se había realizado el pago, en cuyo caso Italia congelaría el dinero. Suecia intervino y respondió de acuerdo con la Iniciativa en menos de 24 horas. Gracias a esta rápida reacción, la policía sueca tuvo conocimiento de que una empresa había sido víctima de un fraude y las autoridades italianas obtuvieron la información que necesitaban para adoptar las medidas pertinentes, por lo que probablemente el dinero se recuperará.

² COM(2010) 385.

³ Conclusiones del Consejo de 30 noviembre de 2009, 16637/09.

⁴ http://ec.europa.eu/dgs/home-affairs/e-library/documents/categories/studies/index_en.htm

⁵ Decisión Marco 2006/960/JAI del Consejo.

En 2012 en el servicio de urgencias de un hospital cercano a París, un hombre nacido en Bélgica intentaba explicar de manera confusa el origen de una grave herida de bala. La declaración de la persona que le acompañaba indujo a los investigadores a pensar que los hechos podían haberse producido en Bélgica. Las primeras investigaciones revelaron que se trataba de un individuo fichado por la policía belga por, entre otros delitos, homicidio. De acuerdo con la Iniciativa Sueca, las autoridades francesas decidieron informar inmediatamente a la policía belga, que rápidamente relacionó los hechos con el secuestro de un empleado de una joyería perpetrado por cuatro hombres armados en Bélgica dos días antes. La intervención policial había hecho que los hombres se dieran a la fuga; los secuestradores consiguieron escapar, pero uno de ellos resultó herido en un tiroteo con la policía. Esta información llevó a las autoridades francesas a poner bajo custodia al herido a la espera de que se emitiera una orden de detención europea (ODE), lo que se hizo ese mismo día en Bélgica. La orden se transmitió a Francia vía SIRENE.

La Decisión **Prüm**⁶ prevé la transferencia automatizada de perfiles de ADN, datos dactiloscópicos (DD) y de determinados datos de los registros nacionales de matriculación de vehículos (DMV) a efectos de la investigación de delitos (ADN, DD, DMV), de la prevención de delitos (DD, DMV) y del mantenimiento de la seguridad pública (DMV). La comparación de datos biométricos (ADN, DD) se realiza mediante un sistema de correspondencia/no concordancia («hit/no-hit»): una comparación automatizada produce una correspondencia anónima (un «hit») cuando los datos del ADN o los datos dactiloscópicos en poder del Estado miembro requirente coinciden con los datos en poder de otro Estado miembro. Los datos relativos a la persona o al asunto en cuestión solo se facilitan si se recibe una nueva petición al efecto.

En un piso de un edificio de viviendas de una ciudad alemana se encontró el cadáver de un hombre apuñalado. En el marco de una puerta se descubrió una huella dactilar. A través de una búsqueda automatizada Prüm se comprobó que esa huella coincidía con otra de la base de datos búlgara. Al día siguiente, en menos de tres horas, Bulgaria solicitó información sobre el asunto, petición que se registró en el Sistema de Información de Schengen (SIS – véase más adelante). Al día siguiente se detuvo en Austria al individuo al que correspondía la huella.

En 2007, es decir, al comienzo de los intercambios Prüm, se robó diverso material de un coche de la policía en Viena. Un rastro de ADN hallado en el vehículo policial se cotejó con un rastro de la base de datos austriaca encontrado en un caso parecido, pero fue una correspondencia Prüm con un rastro incluido en la base de datos alemana la que condujo a la identificación de un delincuente de nacionalidad polaca autor de numerosos robos con efracción. Se emitió una ODE en Austria y el sospechoso fue detenido en Polonia (al encontrarse una correspondencia exacta con una descripción SIS), siendo condenado posteriormente en Austria.

Europol presta apoyo a la labor de los Estados miembros y a la cooperación entre ellos en materia de prevención y lucha contra la delincuencia organizada, el terrorismo, y otras formas de delitos graves (enumerados en el anexo de la Decisión del Consejo sobre Europol⁷) que afecten a dos o más Estados miembros. Proporciona una plataforma para que los Estados miembros intercambien — a través de las unidades nacionales de Europol (UNE) — inteligencia criminal e información. El Sistema de Información de Europol (SIE) es una base

⁶ Decisión 2008/615/JAI del Consejo.

⁷ 2009/371/JAI.

de datos que contiene información (183 000 entradas) facilitada por los Estados miembros sobre delitos transfronterizos que entran dentro de la competencia de Europol, las personas involucradas (41 000) y otros datos relacionados. Europol la utiliza para sus análisis y los Estados miembros pueden emplearla para sus investigaciones. Desde 2011 los Estados miembros pueden designar las autoridades con funciones coercitivas distintas de las UNE a las que se puede autorizar el acceso a la base de datos para realizar en ella búsquedas sobre una base de concordancia / no concordancia. Los ficheros de trabajo de análisis permiten a Europol facilitar análisis operativos con el fin de apoyar las investigaciones transfronterizas.

En Eslovenia se utilizaron tarjetas de pago falsificadas para retirar cuantiosas sumas de dinero de cajeros automáticos. Dos ciudadanos búlgaros estaban siendo investigados en relación con estos hechos; la utilización del SIE permitió descubrir que uno de ellos había cometido actos similares en Francia e Italia. Las autoridades francesas facilitaron información pormenorizada al SIE. Gracias a una rápida respuesta de Francia a través de SIENA, la aplicación segura de la red de intercambio de información, (véase más adelante), a la que siguió un cotejo de huellas dactilares y el levantamiento de una restricción de uso, las autoridades eslovenas pudieron utilizar los datos como prueba en los tribunales. El fichero de trabajo de análisis de Europol reveló la existencia de vínculos entre casos en SI, BG, FR, IE, IT y NO.

El **Sistema de Información de Schengen (SIS)** contiene descripciones de personas y objetos. Para compensar la supresión de los controles en las fronteras interiores, se utiliza tanto dentro del espacio Schengen, como en sus fronteras exteriores, con el fin de mantener un nivel de seguridad elevado en él. Se trata de un sistema a gran escala (más de 43 millones de descripciones) al que pueden acceder los agentes que están en primera línea de la lucha contra la delincuencia sobre una base de correspondencia/no correspondencia. Tras hallarse una correspondencia (un «hit»), esto es, tras comprobarse que los datos relativos a una persona u objeto coinciden con una descripción («alert») contenida en el SIS, se puede obtener información adicional a través de la red de oficinas SIRENE (véase más adelante). El SIS será reemplazado por el **SIS II**, que introducirá mejoras como, por ejemplo, la posibilidad de asociar descripciones relacionadas entre sí (por ejemplo, la descripción de una persona y la de un vehículo), nuevas categorías de descripciones, y dispondrá de un espacio para almacenar datos dactilográficos, fotografías y copias de órdenes de detención europeas. La Decisión del Consejo relativa al Sistema de Información de Schengen de segunda generación (SIS II)⁸ define diversas categorías de descripciones para contribuir a la cooperación entre las autoridades policiales y judiciales en asuntos penales. A tal efecto, todos los Estados miembros de la UE participarán en el SIS II, y Europol y Eurojust seguirán teniendo acceso a él. La gestión de las partes centrales del SIS II se transferirá a la Agencia de Sistemas Informáticos⁹.

Otros instrumentos de la UE o sistemas informáticos permiten el intercambio de información policial y judicial entre autoridades aduaneras [Convenio de Nápoles II; el Sistema de Información Aduanero, que forma parte de las bases de datos del Sistema de Información Antifraude gestionado por la Oficina Europea de Lucha contra el Fraude (OLAF); las Unidades de Inteligencia Financiera; los Organismos de recuperación de Activos y las plataformas de alerta de delitos informáticos]¹⁰. El acceso de las autoridades con

⁸ 2007/533/JAI.

⁹ Agencia europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia.

¹⁰ La futura Estrategia Europea de Seguridad Cibernética permitirá evaluar las necesidades futuras de intercambio de información entre la red y los organismos encargados de la seguridad de la información

funciones coercitivas a otros sistemas a gran escala de la UE se puede realizar a través del Sistema de Información de Visados o de EURODAC¹¹ con el fin de prevenir, detectar e investigar el terrorismo y otros delitos graves. La cuestión de si se concede ese acceso y, de hacerlo, en qué condiciones, también forma parte de los temas tratados en los trabajos preparatorios, actualmente en curso, encaminados a establecer un sistema de entradas y salidas que debe presentarse próximamente.

Se está trabajando en la creación de un Sistema Europeo de Vigilancia de Fronteras (EUROSUR) para el intercambio de información y la cooperación operativa de los Centros Nacionales de Coordinación entre sí y con Frontex con el fin de mejorar el conocimiento de la situación y la capacidad de reacción para la detección y prevención de la migración irregular y la delincuencia transfronteriza en las fronteras exteriores de la UE. Asimismo se está desarrollando un entorno común de intercambio de información (CISEI) para la vigilancia del ámbito marítimo de la UE, que, entre otros objetivos, pretende mejorar el conocimiento de la situación marítima para posibilitar el intercambio transfronterizo de información entre los organismos públicos de siete sectores importantes (incluido el del cumplimiento de la ley en general) y permitir al mismo tiempo la interoperabilidad entre los sistemas de vigilancia presentes y futuros como EUROSUR.

Los Estados miembros también intercambian información sobre la base de sus ordenamientos nacionales y de acuerdos bilaterales. De la misma manera, todos ellos son miembros de Interpol, a través de la cual pueden intercambiar información con países de todo el mundo bilateralmente o por medio de las bases de datos y los avisos de Interpol (por ejemplo, sobre documentos de viaje perdidos o robados).

2.2. Canales e instrumentos de comunicación

Se utilizan **tres canales principales** para el intercambio de información transfronterizo. Todos ellos cuentan con unidades nacionales en los Estados miembros que disponen de su correspondiente instrumento de comunicación:

- (1) Las oficinas **SIRENE**¹² pueden, una vez detectada una correspondencia con una descripción incluida en el SIS, obtener información adicional del Estado miembro que la introdujo. Las oficinas SIRENE trabajan veinticuatro horas al día, los siete días de la semana, y siguen los procedimientos descritos en el Manual SIRENE. En la actualidad, intercambian información a través de un sistema denominado SISNET, que será substituido por la red de comunicación del SIS II antes de que finalice marzo de 2013.
- (2) Las Unidades Nacionales de **Europol** (UNE) intercambian información con la sede de Europol. También pueden hacerlo bilateralmente, sin pasar por la sede, en lo que atañe a los delitos que no entran en el mandato de Europol. Las UNE pueden intercambiar información directamente o a través de los funcionarios de enlace de Europol, que forman parte de las UNE, pero trabajan en la sede de La Haya. Europol

y los organismos con funciones coercitivas, por ejemplo, a través del Centro Europeo de Ciberdelincuencia.

¹¹ Base de datos de la UE para la comparación de las impresiones dactilares de los solicitantes de asilo y de los que cruzan las fronteras de forma irregular.

¹² Supplementary Information **RE**quest at the **N**ational **E**ntry (solicitud de información complementaria a la entrada nacional).

ha desarrollado una aplicación de comunicación segura, denominada **SIENA**¹³, para el intercambio de información con Europol y entre Estados miembros. En 2011, los Estados miembros utilizaron SIENA para intercambiar 222 000 mensajes; en un 53 % de los cuales la información contenida se compartió con Europol.

- (3) Las Oficinas Nacionales Centrales de **Interpol**, que funcionan veinticuatro horas al día, los siete días de la semana, intercambian información con la sede así como bilateralmente entre ellas, sin que intervenga la sede. Las Oficinas Nacionales Centrales utilizan la aplicación de comunicación I-24/7 desarrollada por Interpol.

También existen **otros canales** como los funcionarios de enlace bilaterales (destinados en otros Estados miembros que, por regla general, intervienen en los casos más complejos) y los Centros de Cooperación Policial y Aduanera (creados por los Estados miembros vecinos para coadyuvar al intercambio de información y a la cooperación operativa en las zonas fronterizas).

La **elección del canal** está en parte regulada por la legislación de la UE: las solicitudes de información adicional SIS cursadas tras detectarse una concordancia con una descripción del sistema deben realizarse a través de las oficinas SIRENE, y el intercambio de información con Europol a través de las UNE. En otros casos la elección recae en los Estados miembros.

2.3. Interacción de los diferentes instrumentos, canales y aplicaciones

Existe un amplio abanico de instrumentos, canales y aplicaciones, cada uno destinado a un fin específico. Una investigación penal puede requerir la utilización paralela o secuencial de más de un instrumento. En los casos transfronterizos de delincuencia grave u organizada, los datos sobre una persona o un objeto pueden ser cotejados tanto con los datos del Sistema de Información de Europol como con los del SIS, y en caso de hallarse una correspondencia, las peticiones subsiguientes pueden realizarse a través de Europol o de SIRENE, respectivamente. Un dato biométrico puede ser objeto de un intercambio Prüm y posteriormente de una petición formulada de acuerdo con la Iniciativa Sueca utilizando la aplicación SIENA.

Cualquiera que sea la combinación o secuencia, se deben respetar las normas aplicables a cada instrumento. En esas normas se incluyen las relativas a la protección de datos, a la seguridad y calidad de los mismos, y a la finalidad con la que se pueden utilizar los instrumentos. El tratamiento nacional de datos para su intercambio transfronterizo debe asimismo atenerse a la legislación de la UE sobre protección de datos de carácter personal¹⁴. Debe respetarse el principio de proporcionalidad, lo que quiere decir que las solicitudes formuladas de conformidad con la Iniciativa pueden rechazarse si la transmisión de información resulta claramente desproporcionada con el propósito de la solicitud. El respeto de estas normas exige que solicitudes y respuestas sean validadas por un equipo altamente cualificado que cuente con los instrumentos de información adecuados.

2.4. Interfaz con la cooperación judicial

En los procedimientos judiciales penales intervienen tanto las autoridades con funciones coercitivas como las judiciales, pero existen diferencias entre los Estados miembros sobre en

¹³ Secure Information Exchange Network Application (Aplicación Segura de la red de Intercambio de Información).

¹⁴ Decisión Marco del Consejo 2008/977.

qué medida son estas últimas (incluidos los fiscales) las que supervisan o dirigen las investigaciones penales. Cuando las autoridades judiciales están al frente de ellas, así como cuando la información se necesita como prueba, suele tener que recurrirse a los procedimientos de asistencia judicial mutua en materia penal.

Además, puede suceder que en un Estado miembro las autoridades con funciones coercitivas puedan acceder directamente a una determinada información y que en otro Estado miembro necesiten una autorización judicial para ello. La Iniciativa Sueca exige que cuando sea necesaria una autorización judicial para acceder a la información solicitada, la autoridad requirente debe formular la correspondiente petición a la autoridad judicial, la cual deberá aplicar las mismas normas que aplicaría de tratarse de un caso estrictamente nacional.

Sin embargo, el inventario de los intercambios de información puso de manifiesto que según los expertos en materia de funciones coercitivas las divergencias normativas son una de las causas de la tardanza de las investigaciones transfronterizas. Aunque sea fuera del ámbito de aplicación de la presente Directiva, cabe señalar que Eurojust está disponible para facilitar la cooperación judicial. De cara al futuro, también podría ser importante el exhorto europeo de investigación, actualmente objeto de debate, que podría reemplazar las normas aplicables en la actualidad para la obtención transfronteriza de pruebas que aplican el principio de reconocimiento mutuo. Tendría que reconocerse y ejecutarse con la misma celeridad que en un asunto nacional similar y, en cualquier caso, dentro de los plazos previstos.

2.5. Principios

En su Comunicación de 2010, la Comisión sentó una serie de principios sustantivos y de principios orientados hacia el proceso con el fin de desarrollar nuevas iniciativas y evaluar los instrumentos actuales.

Los principios sustantivos son:

- (1) *Salvaguardar los derechos fundamentales de las personas, en particular su derecho a la intimidad y a la protección de los datos personales.* Se trata de derechos consagrados en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión y en el artículo 16 del Tratado de Funcionamiento de la Unión Europea.
- (2) *Necesidad.* Las restricciones del derecho a la intimidad solo pueden justificarse si son lícitas, persiguen una finalidad legítima y son necesarias en una sociedad democrática.
- (3) *Subsidiariedad.*
- (4) *Gestión precisa del riesgo.* Las pruebas de necesidad y la limitación de las finalidades son esenciales.

Los principios orientados al proceso son:

- (1) *Rentabilidad.* Es preciso tener en cuenta las soluciones ya existentes y evaluar si es posible cumplir los objetivos de la propuesta utilizando mejor los instrumentos existentes.

- (2) *Diseño de la política desde la base.* Un ejemplo es el inventario realizado durante la preparación de la presente Comunicación en el que participaron expertos en materia de medidas coercitivas.
- (3) *Asignación clara de responsabilidades.* En la Comunicación de 2010 se puso de manifiesto que los Estados miembros no disponían de un jefe de proyecto al que dirigirse para que les asesorara sobre la aplicación de la Decisión Prüm. El informe de la Comisión sobre la Decisión Prüm señala que en la actualidad esta carencia se subsana en parte gracias al apoyo de Europol. En cuanto a la idea formulada en la Comunicación de 2010 de que la Agencia de Sistemas Informáticos proporcione asesoramiento técnico, las prioridades actuales de la Agencia parecen ir por otros derroteros. La evaluación trienal que deberá estar finalizada antes de que acabe 2015 puede ser una buena ocasión para reconsiderar esta posición.
- (4) *Cláusulas de revisión y extinción.* La Comisión ha elaborado informes sobre la Iniciativa Sueca y la Decisión Prüm. La presente Comunicación los tiene en cuenta.

3. EVALUACIÓN Y RECOMENDACIONES

Esta sección se centra en la Iniciativa Sueca, la Decisión Prüm y el canal Europol. Aunque SIS y la aplicación SIRENE totalizan un volumen importante de los intercambios de información, no se formulan recomendaciones sobre ellos porque están en curso importantes modificaciones, en especial el próximo paso al SIS II.

3.1. Mejor uso de los instrumentos actualmente existentes

Con independencia de la futura reforma de Europol, la Comisión no tiene, a corto plazo, intención de proponer modificaciones de los instrumentos anteriormente citados. Tampoco parecen necesarios nuevos instrumentos en estos momentos. Ante todo hay que **aplicar los instrumentos existentes**.

Esta afirmación es especialmente válida en el caso de la Decisión Prüm. De acuerdo con el informe Prüm elaborado por la Comisión, que acompaña a la presente Comunicación, el intercambio de datos en el marco de la Decisión Prüm reviste gran valor para las investigaciones, pero su aplicación adolece de un considerable retraso. **Muchos Estados miembros todavía no intercambian datos con arreglo a la Decisión Prüm a pesar de que el plazo de transposición finalizó el 26 de agosto de 2011**¹⁵. Ese retraso se debe fundamentalmente a razones de índole técnica y a la falta de recursos humanos y financieros en los Estados miembros. Sin embargo, habida cuenta de las posibilidades de apoyo ofrecidas por la UE (financiación, equipo de expertos móvil, servicio de asistencia), parece que lo que realmente se necesita es voluntad política para aplicar la Decisión. Tal como se afirma en el informe, la Comisión continuará prestando su apoyo y ofrecerá financiación de la UE. Ahora bien, el contexto cambiará en diciembre de 2014, puesto que a partir de entonces la Comisión podrá incoar procedimientos de infracción. Las normas relativas al control de la aplicación

¹⁵ Los siguientes Estados miembros la han transpuesto:
ADN: BG/CZ/DE/EE/ES/FR/CY/LV/LT/LU/HU/NL/AT/PT/RO/SI/SK/FI;
DD: BG/CZ/DE/EE/ES/FR/CY/LT/LU/HU/NL/AT/SI/SK;
DMV: BE/DE/ES/FR/LT/LU/NL/AT/PL/RO/SI/FI/SE.
Para obtener más información, véase el Informe Prüm.

nacional no se aplicarán hasta entonces, ya que la Decisión Prüm, al igual que la Iniciativa Sueca, se adoptó de conformidad con el antiguo tercer pilar.

En lo que atañe a la **Iniciativa Sueca**, la Comisión comunicó en 2011 que este instrumento no había desarrollado todavía todo su potencial, pero que su importancia iba en aumento¹⁶. Esa valoración sigue siendo válida, puesto que aún quedan Estados miembros por transponerla a sus ordenamientos nacionales¹⁷. La mayoría de los Estados miembros han comunicado que ya lo habían hecho¹⁸, y algunos han señalado que no necesitaban hacerlo, ya que su legislación ya se atenía a ella¹⁹. No obstante, a pesar de sus ventajas, en particular el establecimiento del principio de acceso equivalente y la fijación de plazos, su uso todavía no está extendido. Dos de las razones esgrimidas para ello son que las alternativas se consideran aceptables y que el formulario es excesivamente complejo (incluso su versión simplificada de 2010²⁰).

Se pidió a la Comisión que examinará su utilidad para las peticiones Prüm realizadas a raíz de establecerse una concordancia²¹. En los casos en que la información subsiguiente es necesaria como prueba ante los tribunales, suele ser preciso formular una petición de cooperación judicial. Sin embargo, cuando, definitiva o temporalmente, no se necesita usar esa información como prueba, el recurso sistemático a la Iniciativa Sueca como base jurídica y a SIENA como aplicación de comunicación debe fomentarse con objeto de aprovechar al máximo las ventajas que ofrecen una y otra y de que los Estados miembros adopten una sola buena práctica.

En lo que respecta a **Europol**, una evaluación de 2012²² confirmó que los Estados miembros no comparten adecuadamente la información con Europol (y, por lo tanto, tampoco entre ellos). La Comisión abordará esta cuestión en una propuesta de modificación de la base jurídica de Europol. Por su parte, el Consejo ha pedido a los Estados miembros que utilicen en mayor medida el Sistema de Información de Europol²³.

En consonancia con el Programa de Estocolmo, la Comisión encargó la realización de un estudio sobre un hipotético **Sistema Europeo de Índice de Ficheros Policiales (EPRIS)**²⁴. Con su creación se daría respuesta a la necesidad detectada, habida cuenta de la cada vez más frecuente naturaleza transfronteriza de la delincuencia, de que los agentes de policía de un Estado miembro sepan si un sospechoso tiene antecedentes policiales en otro. De acuerdo con el principio de rentabilidad, la Comisión considera que **en estos momentos no está justificada** la creación de EPRIS, dado que los instrumentos y aplicaciones existentes, que podrían satisfacer parcial o totalmente esa necesidad si se utilizaran más y mejor, no se explotan convenientemente. Es el caso en particular del Sistema de Información de Europol (carga de informaciones pertinentes en él y ampliación del acceso al mismo a escala nacional), del SIS II (mayor uso de descripciones pertinentes de personas o vehículos a la hora de hacer comprobaciones con el fin de perseguir hechos delictivos y prevenir amenazas contra la seguridad), SIENA (ampliación de las posibilidades de acceso a escala nacional, interconexión con los sistemas nacionales y automatización de tareas en la medida de lo posible) y Prüm (plena utilización para mejorar la identificación de personas que delinquen en

¹⁶ SEC(2011) 593.

¹⁷ Los siguientes Estados miembros tienen que adoptar todavía la legislación de aplicación: BE/EL/IT/LU. BG/CZ/DK/DE/EE/ES/FR/CY/HU/LT/LV/NL/PL/PT/RO/SI/SK/FI/SE.

¹⁸ IE/MT/AT/UK.

¹⁹ 9512/1/10.

²⁰ Conclusiones del Consejo de 27 y 28 de octubre de 2011, 15277/11.

²¹ https://www.europol.europa.eu/sites/default/files/publications/rand_evaluation_report.pdf

²² Conclusiones del Consejo de 7 y 8 de junio de 2012.

²³ http://ec.europa.eu/dgs/home-affairs/e-library/documents/categories/studies/index_en.htm

diferentes Estados miembros).

Se pide a los Estados miembros que:

- apliquen plenamente la Iniciativa Sueca, en particular el principio de acceso equivalente,
- apliquen plenamente la Decisión Prüm, haciendo uso del apoyo facilitado por la UE,
- utilicen la Iniciativa Sueca y la aplicación SIENA para las peticiones Prüm subsiguientes al establecimiento de una concordancia.

La Comisión:

- seguirá facilitando financiación de la UE para coadyuvar a la aplicación de la Decisión Prüm,
- se preparará, de ahora a diciembre de 2014, para aplicar en este ámbito las normas que garantizan la aplicación de la legislación de la UE en los Estados miembros.

3.2. Racionalización y gestión de los canales

Elección del canal. El hecho de que los Estados miembros puedan elegir libremente el canal (si se exceptúan las disposiciones relativas a las oficinas SIRENE y a las UNE) se traduce en el uso de diferentes canales en distinta medida. El Manual de buenas prácticas relativas a las unidades de cooperación policial internacional a escala nacional (el «Manual de 2008»)²⁵ elaborado bajo los auspicios de los Jefes de Policía de la UE enuncia una serie de criterios²⁶, que al no ser vinculantes no han logrado la convergencia de las prácticas nacionales. Algunos Estados miembros han evolucionado hacia un uso más sistemático del canal Europol. Otros siguen utilizando mayoritariamente el canal Interpol, cuyo atractivo parece residir en parte en el papel tradicionalmente central que ha tenido en la cooperación policial internacional y en parte en su aparente facilidad de uso. Algunos Estados miembros utilizan SISNET cuando se trata de cuestiones no abordadas por el SIS, como, por ejemplo, las peticiones realizadas de acuerdo con la Iniciativa Sueca.

En opinión de la Comisión, ha llegado el momento de que la UE adopte un enfoque más coherente, un enfoque que confiera al canal Europol un papel central. De acuerdo con este planteamiento, cuando el canal no venga predeterminado por una exigencia jurídica, **el canal Europol, vía la aplicación SIENA, debe ser el canal por defecto** salvo que existan razones específicas para utilizar otro. Así, a guisa de ejemplo, las peticiones de cooperación policial, que actualmente se formulan a través de SISNET (que desaparecerá cuando entre en funcionamiento SIS II²⁷) deberán realizarse en el futuro por medio de SIENA.

Determinados Estados miembros se inclinan por un enfoque que deje una gran libertad en cuanto al uso de los diferentes canales, enfoque con el que la Comisión no está de acuerdo. La adopción por todos los Estados miembros de normas nacionales sobre la elección del canal y su convergencia hacia un único enfoque común sería preferible a la divergencia de enfoques

²⁵ 7968/08.

²⁶ Principios que se repiten en las Directrices sobre la aplicación de la Iniciativa Sueca, 9512/1/10.

²⁷ La red de comunicación SIS II está limitada por ley a los datos del SIS II y a la información suplementaria.

actual. La elección del canal Europol está justificada por sus ventajas. Se puede solicitar la intervención de los funcionarios de enlace de Europol siempre que resulta necesario. Utilizada para los intercambios bilaterales directos, SIENA facilita asimismo el intercambio de información con Europol de conformidad con las disposiciones de la Decisión Europol y de la Iniciativa Sueca. Los mensajes SIENA están estructurados, pueden contener un gran volumen de datos y se intercambian con gran seguridad. La protección de los datos aumenta cuando para intercambiarlos se utiliza un formato estructurado, por ejemplo a través de SIENA. El enfoque sugerido se atiene fielmente a la propuesta de reforma de Europol que la Comisión presentará próximamente y a las directrices estratégicas establecidas por el Consejo Europeo en el Programa de Estocolmo, según las cuales «Europol debería ser el eje para el intercambio de información entre las autoridades policiales de los Estados miembros, un prestador de servicios y una plataforma para los servicios policiales.»

Gestión de los canales. Un punto único de contacto (SPOC, por sus siglas en inglés) es una «ventanilla única» que centraliza la cooperación policial internacional, operativa las veinticuatro horas del día los siete días de la semana, en la que un Estado miembro reagrupa su oficina SIRENE, su UNE y su oficina nacional central de Interpol, así como los puntos de contacto de otros canales. La creación por cada Estado miembro de un SPOC (a pesar de que no siempre se empleara este término) figuraba, en 2007, entre las conclusiones de la tercera Ronda de Visitas de Evaluación Mutua²⁸ y la recomendaba el Manual de 2008. La mayoría de los Estados miembros cuentan con servicios de cooperación policial internacional, pero solo algunos de estos servicios responden a las características de un SPOC propiamente dicho. En 2012, el Consejo solicitó a los Estados miembros que analizaran las posibilidades de establecer un punto único de contacto²⁹. La Comisión pretende ir más lejos: con el fin de mejorar el intercambio de información en materia de medidas coercitivas en la UE, **todos los Estados miembros deben establecer un SPOC** que cumpla unas determinadas características mínimas.

Por lo que se refiere a las peticiones cursadas a otros Estados miembros, el hecho de reunir los diferentes canales en una única estructura organizativa que respete las normas nacionales sobre elección del canal, garantizará una elección correcta y coherente del canal, así como la calidad de las peticiones. La calidad está garantizada, puesto que los SPOC validan las peticiones y se cercioran de que son necesarias y apropiadas. Cuando la información no se intercambia a través de un SPOC [por ejemplo, a través de los Centros de Cooperación Policial y Aduanera (CCPA) o a través de los organismos nacionales que intercambian directamente información por medio de SIENA], un SPOC puede asumir la coordinación nacional. En cuanto a las peticiones recibidas, los SPOC deben tener, cuando sea legalmente posible, un acceso directo a las bases de datos nacionales para poder responder rápidamente, sobre todo dentro de los plazos previstos en la Iniciativa Sueca. Las reglas del Manual SIRENE (por ejemplo, sobre seguridad, sistemas de seguimiento informatizado de la gestión del trabajo, calidad de los datos y dotación de personal) podrían servir de base para organizar de manera coherente todos los canales. La puesta en común de recursos, como, por ejemplo, los recursos humanos o las infraestructuras, puede contribuir a reducir costes o, al menos, a utilizar mejor los recursos.

Los SPOC deberían agrupar a todos los organismos con funciones coercitivas, incluidos los servicios aduaneros. Es preciso establecer una cooperación entre los SPOC y los Centros Nacionales de Coordinación (CNC) en materia de vigilancia de fronteras. Siempre que sea

²⁸ 13321/3/07.

²⁹ Conclusiones del Consejo de 7 y 8 de junio de 2012, 10333/12.

compatible con los ordenamientos jurídicos nacionales, deben crearse vínculos con los órganos judiciales, en particular cuando estos supervisen las investigaciones penales.

Son cada vez más los CCPA³⁰ que intercambian fructíferamente información a escala local y regional. La celebración de conferencias anuales a nivel europeo permite compartir experiencias y debatir sobre enfoques comunes. Aunque un elevado número de los intercambios no se refieren a los delitos más graves o a la delincuencia organizada, uno de los retos que se plantean consiste en garantizar que la información sobre los casos importantes se transmita a escala nacional (SPOC) y, cuando sea pertinente, a Europol. En este contexto, la Comisión espera con interés los resultados de un proyecto piloto actualmente en curso (que se encuadra en una acción de gestión de la información) que utiliza SIENA en un CCPA.

La **Plataforma de Intercambio de Información** se encuadra asimismo en la estrategia de gestión de la información dirigida por Europol destinada a crear un portal común de acceso a los canales y sistemas existentes en la actualidad, que cumpla al pie de la letra sus normas sobre seguridad y protección de datos. Según la Comisión, facilitar el uso de los actuales canales y sistemas presenta ventajas siendo, no obstante, necesario proceder a una evaluación de la rentabilidad de la Plataforma de Intercambio de Información, determinar quién la financiaría y cómo se dirigiría el proyecto. En esta evaluación también participaría la Agencia de Sistemas Informáticos³¹.

Se pide a los Estados miembros que:

- cuando se trate de intercambios para los cuales el canal no venga predeterminado legalmente, utilicen por defecto el canal Europol y la aplicación SIENA, a menos que existan razones específicas para utilizar otro canal;
- elaboren instrucciones nacionales para la elección del canal;
- utilicen, especialmente tras la entrada en servicio de SIS II y la desaparición de SISNET, el canal Europol y la aplicación SIENA para los intercambios en materia de cooperación policial que se realizan actualmente a través de SISNET;
- creen, si todavía no lo han hecho, un punto de contacto único (SPOC) que abarque todos los canales principales, esté disponible veinticuatro horas al día los siete días de la semana, y agrupe a todos los organismos con funciones coercitivas y tenga acceso a las bases de datos nacionales;
- velen por que la información intercambiada a través de los Centros de Cooperación Policial y Aduanera se transmita, de ser pertinente, a nivel nacional y, en su caso, a Europol, y
- establezcan una cooperación entre los SPOC y los Centros Nacionales de Coordinación de EUROSUR.

³⁰ 38 al finalizar 2011.

³¹ Agencia europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia.

Se pide al Consejo que:

- modifique las directrices existentes en la UE para que reflejen las orientaciones sobre la elección del canal sugeridas anteriormente.

La Comisión:

- participará en la evaluación de la viabilidad de la Plataforma de Intercambio de Información.

3.3. Garantizar la calidad, la seguridad y la protección de los datos

Las garantías relativas a la protección de datos de los instrumentos actuales deben ser analizadas cuidadosamente. Con arreglo a la propuesta de Directiva de la Comisión, de 25 de enero de 2012, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales³², habrá que volver a examinar las normas relativas a la protección de datos de los instrumentos actuales con el fin de determinar si es preciso adecuarlas a las disposiciones de la Directiva.

Se precisa un **alto nivel de seguridad** para proteger la integridad de los datos de carácter personal intercambiados y lograr que los Estados miembros se sientan seguros al intercambiar información. Una cadena es tan fuerte como el más débil de sus eslabones: Los Estados miembros y las agencias de la UE deben garantizar que el intercambio de datos se realiza a través de redes sumamente seguras. La propuesta de Directiva anteriormente mencionada prevé normas en relación con la seguridad de los datos³³ y a nivel de la UE existen normas detalladas sobre seguridad para proteger la información clasificada de la UE³⁴.

Un **nivel de calidad elevado** es asimismo importante. El «proceso operativo», es decir, la manera en que el intercambio de información se lleva a cabo en la práctica, es importante en este contexto. Así, siempre que resulte posible y oportuno, habrá que **automatizar determinadas tareas**. Por ejemplo, la redacción de una petición de información dirigida a otro Estado miembro exige volver a introducir los datos registrados en un sistema nacional en la herramienta de comunicación utilizada; hacerlo manualmente puede dar lugar a errores y toma su tiempo. Automatizar esas tareas será posible gracias al formato universal de mensajes **UMF II**³⁵, otra acción enmarcada en la estrategia de gestión de la información. Este proyecto financiado por la UE y dirigido por Europol tiene por objetivo diseñar un formato estándar para los mensajes utilizado para solicitar información y responder a las solicitudes recibidas. Ello permitiría la automatización de la transferencia de datos entre diferentes sistemas, por ejemplo, entre los sistemas nacionales de gestión de casos y SIENA. Además de una posible reducción de costes o, al menos, de un mejor uso de los recursos, el abandono de la reintroducción manual de datos tiene una doble ventaja. Liberaría personal, que podría ser destinado a tareas de validación, y, además, al reducir los errores deslizados al copiar los datos y facilitar el intercambio estructurado de información, mejoraría la gestión y la protección de los datos.

³² COM(2012) 10.

³³ Artículos 27 a 29 de la Propuesta.

³⁴ Decisión 2011/292/UE del Consejo.

³⁵ Universal Message Format (Formato Universal de Mensajes).

La automatización de tareas no supone que todos y cada uno de los agentes de policía de la UE deba tener acceso a toda la información policial de la UE. Los intercambios deben circunscribirse a los que sean necesarios y procedentes, y tienen que ser gestionados de manera que se atengan a esos dos requisitos. **Las búsquedas automatizadas, como medio para solucionar problemas de capacidad, funcionan con los actuales instrumentos de la UE para el intercambio de información, sobre una base de correspondencia/no correspondencia** (por ejemplo la búsqueda de indicadores de ADN y datos dactilográficos realizada a través del SIS o de conformidad con la Decisión Prüm), o se limitan a tipos de datos extremadamente definidos (por ejemplo, los datos sobre matriculación de vehículos de la Decisión Prüm). Determinadas tareas ni pueden ni deben ser automatizadas, en particular la validación de las peticiones y de las repuestas. Este aspecto cobra especial importancia en el contexto de la Iniciativa Sueca, que exige que las solicitudes estén justificadas.

Por último, **la interoperabilidad** entre los diferentes sistemas nacionales y estructuras administrativas puede ser beneficiosa en términos de coherencia procedimental, mayor rapidez en las respuestas, mayor calidad de la información y simplificación del proceso de concepción y desarrollo. El Marco Europeo de Interoperabilidad³⁶ establece cuatro niveles de interoperabilidad: técnica, semántica, organizativa y jurídica. El proyecto UMF II desarrollará el nivel semántico³⁷. La convergencia hacia prácticas comunes (SPOC, elección del canal) incidirá en el nivel organizativo. No obstante, la información solo se puede intercambiar y utilizar si la ley lo autoriza.

Se pide a Europol y a los Estados miembros que:

- sigan trabajando en el desarrollo de la norma UMF II.

3.4. Mejora de la formación y aumento de la sensibilidad

Con objeto de proporcionar a los funcionarios que ejercen funciones coercitivas los conocimientos y competencias técnicas necesarias para cooperar de manera eficaz, la Comisión está preparando un Programa de Formación Europeo en materia de funciones coercitivas. Un inventario de los instrumentos de intercambio de información puso de manifiesto que los más importantes se estudian en la etapa de formación inicial que siguen los miembros de los órganos con funciones coercitivas, pero sin entrar a valorar la calidad de esa formación. Los funcionarios especializados en la materia, como los que trabajan en los SPOC, necesitan una formación más amplia y de mayor nivel. Los intercambios de este tipo de funcionarios también se consideran positivos y deben fomentarse³⁸.

Se solicita a los Estados miembros que:

- velen por que todos los funcionarios con funciones coercitivas reciban una formación adecuada sobre el intercambio de información transfronterizo;
- organicen intercambios de personas que trabajan en los SPOC.

La Comisión:

³⁶ COM(2010) 744.

³⁷ El proyecto UMF II tiene en cuenta otros trabajos sobre semántica, como los modelos de datos comunes elaborados en el marco del programa de la UE sobre soluciones de interoperabilidad para las administraciones públicas europeas.

³⁸ 10333/12.

- velará por que el Programa de Formación Europeo aborde el intercambio de información transfronterizo.

3.5. Financiación

La UE ha financiado con cargo al Fondo para la Prevención y la Lucha contra la Delincuencia (ISEC) proyectos relacionados con el intercambio de información, como, por ejemplo, el proyecto UMF II (830 000 EUR), así como la aplicación de la Decisión Prüm (11,9 millones EUR). Ese Fondo será substituido en el período 2014-2020 por un Fondo para la Seguridad Interior de la UE, del que podrán beneficiarse los proyectos europeos de intercambio de información.

Una parte del Fondo para la Seguridad Interior será administrada por los Estados miembros en el marco de una gestión denominada «compartida» de acuerdo con unos **programas plurianuales. Estos programas deberán tener en cuenta determinadas prioridades nacionales en materia de intercambio de información** en consonancia con las recomendaciones de la presente Comunicación. En paralelo, la Comisión estudiará la manera de financiar con cargo a las partes del Fondo para la Seguridad Interior que ella administra proyectos pilotos como, por ejemplo, el que pretende dar continuidad al desarrollo del proyecto UMF II.

En lo que respecta a los gastos propios de los Estados miembros, otras recomendaciones (por ejemplo, las relativas a los SPOC o el UMF II) podrían contribuir, como ya se ha indicado, a una reducción de costes o, al menos, a un mejor uso de los recursos.

Se pide a los Estados miembros que:

- tengan en cuenta determinadas prioridades nacionales en materia de intercambio de información en los programas plurianuales financiados con cargo al Fondo para la Seguridad Interior de la UE 2014-2020.

La Comisión:

- incluirá las políticas sobre intercambio de información en el diálogo con los Estados miembros sobre la programación del Fondo para la Seguridad Interior de la UE,
- pondrá en marcha una convocatoria de propuestas para la financiación directa (por la Comisión) de importantes proyectos pilotos.

3.6. Estadísticas

Las estadísticas actuales, a pesar de ser fiables en determinados ámbitos (por ejemplo, SIS o SIENA), no son exhaustivas. Unas estadísticas mejores permitirían conocer con más precisión el uso que se da a la Iniciativa Sueca (de la que solo se tienen cifras cuando se utiliza SIENA) y a la Decisión Prüm.

Ahora bien, la elaboración de estadísticas puede exigir considerables recursos, en especial si no constituye una actividad habitual. La realización de estadísticas *ad hoc* debe evitarse. Resulta preferible un enfoque progresivo, que se sustente en procesos ya iniciados, como el descrito en el Informe Prüm, que censa las concordancias Prüm que han sido útiles para las investigaciones. Un mayor uso de SIENA para cursar las solicitudes formuladas de

conformidad con la Iniciativa Sueca, tal como se ha recomendado anteriormente, se traduciría en un mayor peso de tales solicitudes en las estadísticas de SIENA.

Se pide a los Estados miembros que:

- mejoren las estadísticas Prüm.

4. CONCLUSIONES

La mejora de los intercambios de información transfronterizos no constituye un fin en sí misma. El verdadero objetivo es luchar más eficazmente contra la delincuencia y, de esta manera, minimizar el daño causado a las víctimas y a la economía de la UE.

El intercambio de información transfronterizo funciona, en general, correctamente y, como ilustran los ejemplos que se han dado anteriormente, constituye una valiosa contribución a la lucha contra la delincuencia grave y la delincuencia transfronteriza en la UE. Existe, no obstante, cierto margen de mejora. Los Estados miembros deben aplicar total y fielmente la legislación acordada. En particular, de cara al futuro, todos los Estados miembros deben utilizar de manera más sistemática el canal Europol y establecer puntos de contacto únicos nacionales que aglutinen a todos los organismos con funciones coercitivas (SPOC).

La Comisión, por su parte, seguirá analizando cómo se implantan y utilizan los instrumentos, proporcionando financiación y agrupando los diferentes aspectos en aras de una mayor coherencia. La Comisión no propone, a través de la presente Comunicación, ningún nuevo instrumento. Si lo hace en el futuro, este se atenderá a los principios sustantivos de la Comunicación de 2010: salvaguardar los derechos fundamentales y garantizar la necesidad, la subsidiariedad y una gestión rigurosa de los riesgos.

Habrá que trabajar aún denodadamente para garantizar que las informaciones importantes se comparten en Europol y para disponer de una visión de conjunto de la delincuencia transfronteriza en la UE. La propuesta de reforma de Europol, que la Comisión presentará en breve, responde a esa necesidad. No obstante, las recomendaciones formuladas en la presente Comunicación en pro de un uso más sistemático del canal Europol y de SIENA, su aplicación segura, contribuirán a facilitar la transmisión de información a Europol.

Con el fin de dar continuidad a la presente Comunicación, la Comisión seguirá trabajando con los Estados miembros en el marco de la Estrategia de la UE para la gestión de la información para la seguridad interior, y propone que el Consejo organice un debate anual en su Comité de Seguridad Interior. Asimismo la Comisión invita al Parlamento Europeo a analizar sus recomendaciones, en particular en su Comisión Especial sobre la Delincuencia Organizada, la Corrupción y el Blanqueo de Dinero.