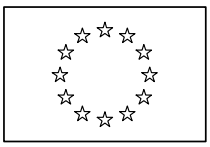

COMISIÓN DE LAS COMUNIDADES EUROPEAS

Bruselas, 16.6.2004
COM (2004) 429 final

COMUNICACIÓN DE LA COMISIÓN AL CONSEJO Y AL PARLAMENTO EUROPEO

sobre la mejora del acceso a la información por parte de las autoridades encargadas de garantizar el cumplimiento de la ley

ÍNDICE

COMUNICACIÓN DE LA COMISIÓN AL CONSEJO Y AL PARLAMENTO EUROPEO

SOBRE LA MEJORA DEL ACCESO A LA INFORMACIÓN POR PARTE DE LAS AUTORIDADES ENCARGADAS DE GARANTIZAR EL CUMPLIMIENTO DE LA LEY
(*POLÍTICA DE INFORMACIÓN DE LA UE*)

CAPÍTULO I –INTRODUCCIÓN, ANÁLISIS Y CONTEXTO POLÍTICO

Descripción

La declaración del Consejo Europeo sobre el terrorismo [1]da instrucciones al Consejo para que estudie medidas legislativas con el fin de simplificar el intercambio de información e Inteligencia entre las autoridades encargadas de garantizar el cumplimiento de la ley en los Estados miembros. Se invita asimismo a la Comisión a presentar propuestas al Consejo Europeo de junio en relación con el intercambio de información personal y el uso de información sobre pasajeros en la lucha contra el terrorismo. Las propuestas de la Comisión deben incluir también disposiciones que permitan a los órganos represivos nacionales acceder a los sistemas de información europeos.

La presente Comunicación es la primera contribución de la Comisión en respuesta a la petición del Consejo.
En esta Comunicación, la Comisión establece los elementos esenciales para lograr la libre circulación de información entre las autoridades encargadas de garantizar el cumplimiento de la ley en los Estados miembros de una forma más estructurada que la utilizada hasta hoy. Actualmente existen obstáculos a la libre circulación de información, lo que ha llevado, *entre otras cosas,* al Consejo a dedicar la tercera ronda de evaluaciones mutuas al examen del «intercambio de información e Inteligencia entre Europol y los Estados miembros y entre los Estados miembros entre sí». La compartimentación de la información, así como la falta de una política clara de canales de información obstaculizan ese libre intercambio. Los problemas legales, técnicos y prácticos que dificultan el intercambio entre los Estados miembros multiplican las dificultades para superar la división de la información entre los diversos ministerios nacionales. Para obtener una imagen más exacta de estos obstáculos, la Comisión propone emprender un inventario completo de las condiciones de acceso a la información, así como una consulta amplia y abierta con los interesados, en este caso, el Supervisor Europeo de Protección de Datos. La Comunicación también pretende facilitar los medios para evitar la materialización de amenazas importantes, como el terrorismo, introduciendo a escala comunitaria el concepto de sistema represivo basado en la Inteligencia. Asimismo prevé una un calendario con una propuesta para lograr este objetivo y anuncia la elaboración de legislación que elimine los problemas legales específicos. La Comunicación se centra en la mejora del acceso a la información necesaria y pertinente, así como en los conceptos generales para la introducción de un sistema represivo basado en la Inteligencia a escala de la UE, lo que tendrá también consecuencias en el papel internacional que la UE pueda asumir.

---

[1] Consejo Europeo de 25 marzo de 2004 *Declaración sobre la lucha contra el terrorismo*.

Estos dos elementos son los componentes esenciales de la Política de Información destinada a las autoridades encargadas de garantizar el cumplimiento de la ley. La acción común en estos campos apoyará la creación progresiva de un espacio de libertad, seguridad y justicia que garantice la libre circulación de personas frente a los nuevos retos en materia de seguridad que el terrorismo y otras formas de delincuencia organizada plantean a la Unión en su conjunto. La eficacia de la actuación de esas autoridades debe conjugarse con el respeto de los derechos humanos y libertades fundamentales protegidos por las tradiciones constitucionales, europeas e internacionales comunes a los Estados miembros. Además, en el proceso de construcción de esta política, la Comisión garantizará que se tengan debidamente en cuenta el Derecho y las políticas comunitarios. En concreto, la nueva política no debería crear incertidumbre legal o acarrear cargas económicas innecesarias para las empresas.

La Comisión invita a los Estados miembros y a las partes interesadas a participar con valentía en las siguientes acciones de cooperación.

En primer lugar, tomar las medidas imprescindibles para que las autoridades encargadas de garantizar el cumplimiento de la ley en la UE puedan acceder a los datos y la información necesarios y pertinentes para prevenir y combatir el terrorismo y otras formas de delincuencia grave u organizada, así como las amenazas que representan. A este respecto; debe tenerse en cuenta que a menudo existe una actividad delictiva que, si bien no parece entrar en la categoría de «delincuencia grave u organizada», puede conducir o estar relacionada con aquélla.

En segundo lugar, producir y utilizar servicios de Inteligencia criminal europea de alta calidad. Los conocimientos que se obtendrán en este proceso servirán a los responsables políticos para establecer prioridades de carácter represivo en la UE de manera concertada, y las autoridades competentes podrán enfrentarse con eficacia a los delitos y amenazas que comprometen la vida, la integridad física y la seguridad de nuestros ciudadanos.

En tercer lugar, aumentar la confianza entre los servicios represivos. La introducción de condiciones comunes, por ejemplo, para acceder a los sistemas de datos y el hecho de compartir conocimientos contribuirá a crear una plataforma común de política de información, eliminando obstáculos objetivos para el intercambio efectivo de información e Inteligencia.

Son varias las consideraciones que conducen a una política de información europea para las autoridades encargadas de garantizar el cumplimiento de la ley. Todas ellas están en relación con la toma de conciencia cada vez mayor de la vulnerabilidad de la Unión frente a la amenaza de la actividad terrorista, de la dependencia de la Unión de redes interconectadas; de la necesidad de establecer mayores flujos de información entre las autoridades competentes; de los beneficios de las nuevas capacidades basadas en la tecnología y la información que mejoran la actuación represiva y, al mismo tiempo, mejoran la protección de datos, la seguridad y los mecanismos relacionados de control y supervisión.

Esta Comunicación se propone perfeccionar el intercambio de información entre todas las autoridades encargadas de garantizar el cumplimiento de la ley, es decir, no sólo entre las autoridades policiales, sino también las autoridades aduaneras, las unidades de Inteligencia financiera, las autoridades judiciales y fiscales y demás organismos públicos que participan en el proceso que se extiende desde la detección precoz de amenazas a la seguridad y de los delitos hasta la condena y el castigo de los culpables. Es indiscutible el papel fundamental que desempeñan a estos efectos los servicios de seguridad e Inteligencia nacionales. En los siguientes párrafos se exponen los numerosos desafíos *interrelacionados* a los que la política de información europea se propone hacer frente.

Por último, debe tenerse en cuenta la dimensión exterior, debido al carácter internacional del terrorismo y la delincuencia organizada. Otros países han desarrollado o pueden desarrollar en el futuro sus propias políticas de información y ya hemos visto casos en los que dichas

medidas repercuten en la vida de los ciudadanos comunitarios y los operadores económicos. También pueden surgir cuestiones de reciprocidad. Habrá que buscar soluciones multilaterales en foros especializados. Deberá considerarse también debidamente el impacto de la política de la UE en los ciudadanos de terceros países, con el fin de evitar perjuicio alguno a la cooperación con esos países y garantizar el respeto de los derechos de los ciudadanos.

En primer lugar, esta política dará acceso a los datos y la información necesarios y pertinentes a las autoridades encargadas de garantizar el cumplimiento de la ley con el fin de prevenir y combatir el terrorismo y otras formas de delincuencia grave u organizada, así como las amenazas que representan[2]. En segundo lugar, fomentará la producción y el uso a escala europea de una Inteligencia criminal de alta calidad para facilitar la adopción de decisiones políticas y ayudar a las autoridades encargadas de garantizar el cumplimiento de la ley en la lucha eficaz contra estos delitos. En tercer lugar, facilitará asimismo la creación de un clima de confianza entre los servicios competentes. A la hora de elaborar esta política, se tendrán también en cuenta las políticas comunitarias y los instrumentos de Derecho comunitario; en particular, se respetarán plenamente los derechos fundamentales.

La política de información tendrá en cuenta los siguientes elementos:

- La **seguridad** exige una acción común y concertada a una escala sin precedentes; las partes implicadas son las autoridades encargadas de garantizar el cumplimiento de la ley, los Gobiernos nacionales, el ejecutivo y el legislativo europeos, y otros órganos de índole europea e internacional.
- **Los derechos humanos** obligan a buscar el equilibrio adecuado entre la protección de datos y el respeto debido de los derechos fundamentales, por una parte, y, por otra, un alto nivel de eficacia en la utilización de la información con el fin de salvaguardar intereses públicos esenciales como la seguridad nacional y la prevención, detección, y persecución del delito.
- Por lo que se refiere a **la tecnología**, se necesitan sistemas de información compatibles, protegidos contra el acceso ilegal, que cuenten con un nivel suficiente de protección de datos, incluidos el control y la supervisión del tratamiento de datos y de la investigación. La evaluación y análisis del riesgo delictivo debe poner de manifiesto las debilidades del sistema y las posibilidades de que se produzca actividad criminal y centrarse en el análisis de datos como la valoración de riesgos y perfiles.
- Para facilitar **la cooperación** efectiva, las normas comunes de obtención, almacenamiento, análisis e intercambio de información ayudarán a crear un clima de confianza entre los servicios competentes, tanto a escala nacional como de la UE.
- La **aplicación** de un enfoque en diversas fases requerirá una cooperación sostenida a largo plazo.

[2] A efectos de esta Comunicación la expresión «datos» o «información» significa «datos, información e Inteligencia» salvo indicación contraria. El término «Inteligencia» hace referencia a la Inteligencia criminal.

CAPÍTULO II – HACIA UN MEJOR ACCESO A LOS DATOS Y LA INTRODUCCIÓN DE UN SISTEMA REPRESIVO BASADO EN LA INTELIGENCIA A ESCALA DE LA UE

2. 1. Objetivos estratégicos

El objetivo de esta Comunicación es crear una política europea de información destinada a las autoridades encargadas de garantizar el cumplimiento de la ley, que contribuya a la realización de los objetivos del artículo 29 TUE al facilitar mejor información a través de canales seguros para la actual **cooperación entre las autoridades encargadas de garantizar el cumplimiento de la ley,** y sentar la base para **la creación de un sistema represivo basado en la Inteligencia** a escala local, nacional y europea, apoyado por el necesario clima de confianza. El plan propuesto engloba medidas de tipo judicial, técnico y organizativo que, juntas, proveerán a las autoridades competentes de un marco de cooperación que facilite el acceso y el tratamiento de los datos pertinentes para garantizar el cumplimiento de la ley, así como la producción de una Inteligencia criminal.

Si consideramos más de cerca la política de información, los resultados previstos son:

- optimizar el acceso a la información a otras actividades represivas, así como producir Inteligencia criminal ;
- garantizar que los datos pertinentes establecidos con fines distintos de los represivos estén disponibles mientras sea apropiado, necesario y proporcionado a los objetivos específicos y legítimos que se persiguen[3];
- crear o, en el caso de normas horizontales ya existentes, promover, la utilización de normas horizontales comunes sobre el acceso a datos, la habilitación, la confidencialidad de la información, la fiabilidad, la seguridad y la protección de datos, así como normas de compatibilidad de bases de datos nacionales e internacionales;
- establecer formatos acordados de información para ayudar a la toma de decisiones políticas y operativas y promover el desarrollo y uso de métodos equivalentes para el análisis, por ejemplo, de redes delictivas, amenazas de delito, riesgos y perfiles, que se completarán ulteriormente con valoraciones de los perjuicios económicos;
- proporcionar la base para dar prioridad a escala europea a la recogida y análisis de la información y, posteriormente, buscar la mejor vía de actuación para evitar y combatir el terrorismo y otras formas de delincuencia grave u organizada, así como las amenazas que representan;
- facilitar una acción represora cooperativa y coordinada con objeto de prevenir, investigar o interrumpir, eficazmente y cuando sea apropiado, actividades terroristas y actividades relacionadas con otras formas de delincuencia grave u organizada.

Un mejor acceso a los datos, la información y la Inteligencia facilitará la actividad represiva en cada Estado miembro y en la UE con el fin de prevenir y combatir el terrorismo y otras formas de delincuencia grave u organizada, así como las amenazas que representan. El valor añadido aparecerá cuando se analicen metódicamente los datos para producir una Inteligencia de primera clase. Con el fin de fundamentar el sistema represivo europeo basado en la Inteligencia, deberán adoptarse normas mínimas para los sistemas nacionales que permitan realizar evaluaciones de amenaza compatibles a escala europea.

[3] Cuatro Estados miembros presentaron una propuesta legislativa sobre la conservación de datos en el Consejo JAI de abril de 2004. La Comisión prevé celebrar una consulta abierta sobre la cuestión.

2. 2. Elementos básicos para un acceso, recogida, almacenamiento, análisis e intercambio de datos efectivos

2.2. 1. El principio de acceso equivalente a los datos de las autoridades encargadas de garantizar el cumplimiento de la ley

El primer objetivo fundamental de la política de información para garantizar el cumplimiento de la ley es la libre circulación de la información entre los servicios competentes, incluidos EUROPOL y EUROJUST. Actualmente, las autoridades competentes pueden utilizar bases de datos accesibles a nivel nacional. Sin embargo, las autoridades de otros Estados miembros no tienen acceso en la práctica debido a la cantidad de problemas que se les plantean.

La política de información pretende hacer accesible esta información a todas las autoridades de la UE, incluidos EUROPOL y EUROJUST, con el fin de asistirlas en el cumplimiento de sus funciones y de conformidad con el Estado de Derecho.

El principio que la política de información introduce para compensar los desafíos presentados en el capítulo anterior es el del **«derecho de acceso equivalente a datos».** Ello permitiría que las autoridades y funcionarios encargados de garantizar el cumplimiento de la ley pudieran acceder a datos y bases de otros Estados miembros en condiciones comparables a las de las autoridades y funcionarios nacionales competentes.

Los Estados miembros deben comprometerse a actuar con arreglo a un modelo europeo que incluirá, entre otras cosas, la sincronización, basada en una metodología común, de la evaluación de la amenaza y su apoyo sistemático con estudios sectoriales de vulnerabilidad.

El principio de acceso equivalente reconoce que:

– la seguridad de la Unión y sus ciudadanos es una responsabilidad conjunta;
– los Estados miembros dependen de la ayuda mutua para aplicar leyes de prevención y lucha contra el terrorismo y otras formas de delincuencia grave u organizada y contener las amenazas que representan;
– las autoridades represivas de cualquier Estado miembro cumplen tareas similares y tienen necesidades de información equivalentes;
– las autoridades represivas actúan legalmente cuando acceden a datos o bases de datos en el ejercicio de sus tareas y dentro de los límites establecidos por las normas comunes sobre protección y seguridad de datos.

Por principio, el derecho de acceso equivalente no debería disminuir la eficacia de los instrumentos de asistencia legal mutua ya existentes. Habrá que analizar cuidadosamente los posibles efectos legales.

Deberían fijarse, basadas en normas comunes, incluidas la protección y seguridad de datos, condiciones transparentes y sencillas para el acceso a la información necesaria y pertinente por parte de todas las autoridades encargadas de garantizar el cumplimiento de la ley en la UE. Los Estados miembros serán responsables de la aplicación de estas condiciones. Una vez establecidas las condiciones, se creará un sistema para supervisar su aplicación cuando se haga balance (véase el párrafo 2.2.2).

Los obstáculos fundamentales al intercambio de información entre las autoridades competentes sólo pueden superarse de manera eficaz con un compromiso firme por parte de los Estados miembros de adoptar medidas concretas encaminadas al establecimiento de un Modelo Europeo de Investigación Criminal (véase el párrafo 2.3).

La política europea de información tiene como objetivo introducir el principio del derecho de acceso equivalente a la información y los datos necesarios y pertinentes para las autoridades encargadas de garantizar el cumplimiento de la ley en la UE. La Comisión

examinará con los Estados miembros los obstáculos y, sobre esta base, valorará la conveniencia de presentar una propuesta legislativa al Consejo y al Parlamento Europeo.

2.2. 2. Delimitación de las condiciones de acceso

La Comisión propone realizar un balance completo sobre la base de la información disponible, así como de la que proporcionen a este fin los Estados miembros, para recoger los siguientes elementos:

- qué datos o bases de datos son accesibles a las autoridades encargadas de garantizar el cumplimiento de ley en los Estados miembros y cuáles son accesibles en el extranjero, incluidas las bases de datos de índices (*contenido*);
- cuál es el propósito de la base de datos *(definición del propósito)*;
- qué tipo de autoridad tiene acceso a estos datos (*usuarios*);
- en qué condiciones tienen estas autoridades acceso a estos datos y bases (*protocolo de acceso*);
- cuáles son los requisitos técnicos para el acceso a estos datos y bases (*protocolos técnicos*);
- con qué frecuencia se accede a los datos y las bases (*pertinencia*);
- qué datos o bases de datos son de interés para las autoridades encargadas de garantizar el cumplimiento de la ley, sin que puedan acceder a ellas; cuáles son las disposiciones aplicables de protección de datos (*determinación de las necesidades*).

La Comisión se propone:

- ***realizar un balance a finales de 2004 para determinar el alcance, las necesidades y los obstáculos del acceso a datos y bases de las autoridades encargadas de garantizar el cumplimiento de la ley;***

- ***iniciar un estudio sobre las disposiciones legales, las condiciones, incluidas las de tecnología e investigación, de acceso a datos ajenos a materias criminales, y los procedimientos relacionados con disposiciones sobre protección y seguridad de datos***

2.2. 3. Recogida de datos

Las autoridades encargadas de garantizar el cumplimiento de la ley en la UE utilizan distintos enfoques para recoger y categorizar los datos y la información. Hasta el momento no existe un solo foro para la clasificación de la confidencialidad de las diversas fuentes de información.

La fuente de información por excelencia son los datos recogidos por las autoridades competentes. El acceso a datos recogidos con fines no represivos es otra cuestión política. Requiere una consulta amplia y abierta con todos los interesados, teniendo en cuenta sus posibles implicaciones en operadores y usuarios y en legislación y medidas comunitarias.
Para una gestión eficaz del acceso serían necesarios un sistema que contemple los diversos derechos de acceso como las *normas europeas comunes para la autorización de acceso a la información clasificada*, un sistema común *de perfiles de acceso de los usuarios* para gestionar los numerosos derechos de acceso, y una manera autentificada de registrar a los usuarios autorizados (*cuentas de usuarios*). Los perfiles de usuario podrían también utilizarse sistemáticamente para supervisar y auditar el acceso y el tratamiento de datos que podrían guardarse en sistemas de *ficheros de registro y de pistas de auditoría*.

La Comisión se propone emprender estudios para apoyar la elaboración de iniciativas legislativas relacionadas con normas mínimas de recogida de datos, normas procesales comunes sobre la clasificación de la confidencialidad y la fiabilidad de los datos, normas comunes sobre la autorización del acceso a información clasificada y perfiles de acceso del usuario.
La Comisión organizará consultas y talleres multidisciplinares con motivo del Foro europeo sobre prevención de la delincuencia organizada para estudiar posibilidades de asociación pública y privada y, en particular, sobre el acceso a datos no recogidos con fines represivos.

2.2. 4. Intercambio y tratamiento de datos

Además del principio de acceso equivalente, otra forma de mejorar el acceso a datos y bases es incluyéndolos en una red o creando bases de datos centrales. En este contexto, el Consejo Europeo [4]invitó a la Comisión «a presentar propuestas para mejorar la compatibilidad entre bases de datos europeas (SISII, VIS y EURODAC) con el fin de aprovechar su valor añadido dentro de los respectivos marcos legales y técnicos de prevención y lucha contra el terrorismo»[5]. La compatibilidad mejorada deberá tener en cuenta las disposiciones legales aplicables sobre protección de datos.

La Comisión considera que la única opción viable en el futuro será la creación de sistemas europeos compatibles e interconectados. Una arquitectura informática conceptualmente amplia que integre interconexiones nacionales, europeas e internacionales ofrece a largo plazo un ahorro importante, sinergias y oportunidades de acción, tanto en el campo de la Inteligencia como en el contexto más amplio de una estrategia europea de seguridad en desarrollo.
Debería concebirse un enfoque en etapas basado en la creación de formatos armonizados de codificación de los datos y de normas de acceso a los diversos sistemas. En las primeras rondas de consultas de la Comisión Europea con las partes implicadas [6]se detectaron problemas que pueden dificultar el intercambio de información. Entre ellos se encuentran, en particular, la ausencia de:

- normas y condiciones comunes de tratamiento de datos;
- normas comunes de acceso a datos;
- definiciones y estadísticas compatibles sobre la actividad criminal;
- tecnologías informáticas compatibles en las administraciones represivas;
- cultura de cooperación en el ámbito de la represión más allá de los límites institucionales;
- cooperación entre actores de los sectores público y privado;
- conocimiento de normas comunes de protección de datos y ausencia de un marco común para la seguridad de los datos.

La Comisión prevé presentar una comunicación sobre métodos efectivos para eliminar los obstáculos que impiden el intercambio de datos y que, cuando proceda, apoyará con iniciativas legislativas.

---

4 Consejo Europeo de 25 de marzo de 2004, *Declaración sobre la lucha contra el terrorismo*.
5 Se preparará otra Comunicación de la Comisión sobre este tema.
6 Declaración de Dublín y Conclusiones de las reuniones del Foro europeo sobre prevención de la delincuencia organizada.

2.2. 5. Investigación

Los actuales programas europeos de investigación tratan la cuestión de la seguridad de los sistemas e infraestructuras de información y comunicación. La Comisión desea acelerar la preparación de un Programa europeo de investigación para mejorar la seguridad de los ciudadanos europeos poniendo en marcha una Acción Preparatoria en el ámbito de la investigación sobre seguridad[7]. Esta Acción, diseñada para los años 2004 a 2006 (con un presupuesto de 65 millones de euros) apoyaría y financiaría actividades preparatorias para el amplio Programa europeo de investigación sobre seguridad que se desarrollaría a partir de 2007.

El terrorismo y la delincuencia organizada son las dos mayores preocupaciones de los ciudadanos europeos (el 80% de los ciudadanos de la UE los señala como sus temores más importantes). En la actualidad, los programas de investigación no cubren suficientemente los sistemas de Inteligencia o las actividades represivas. Es necesario, por tanto, añadir a los programas actuales acciones de investigación concretas. Además el programa AGIS permite la cofinanciación de actividades de investigación.

- ***Promover la investigación sobre canales de comunicación seguros y confidenciales a través del programa AGIS;***
- ***Iniciar el desarrollo de normas sobre el intercambio seguro de información, en particular por parte de las autoridades represivas y entre ellas mismas.***
- ***Emprender acciones de investigación concretas sobre la utilización y aplicación de sistemas europeos de Inteligencia criminal, que incluyan estudios sobre normas comunes relacionadas para metadatos, seguridad en los intercambios de datos, mejora de los sistemas de protección de datos, análisis automatizado, valoración de amenazas y riesgos y métodos de elaboración de perfiles.***

2. 3. Elementos fundamentales de un sistema represivo eficaz basado en la Inteligencia a escala de la UE

El segundo objetivo fundamental de la política de información es proponer las medidas necesarias para desarrollar un sistema represivo basado en la Inteligencia a escala de la UE. La Inteligencia ayuda a las autoridades competentes en la ejecución de sus tareas estratégicas u operativas de prevención y lucha contra el terrorismo y la delincuencia grave u organizada, y las amenazas que representan[8]. La introducción de un Modelo Europeo de Inteligencia mejoraría la eficacia y facilitaría la cooperación. El método englobaría materias como la sincronización de la evaluación de la amenaza basada en una metodología común y daría una base sistemática a esta evaluación con los estudios sectoriales de vulnerabilidad y la asignación de recursos financieros y humanos.

La política de información de la UE pretende **poner la información precisa a disposición de una red de Inteligencia de primera magnitud a escala de la UE**, que realice periódicamente evaluaciones estratégicas y operativas de la UE. El Sistema de Información de Europol también desempeñará un papel importante en su desarrollo.
Las medidas resumidas a continuación deberían facilitar la disponibilidad inmediata de las evaluaciones estratégicas para que las autoridades competentes puedan revisar las prioridades

---

7 COM (2004) 72 final.

8 *la Inteligencia criminal* se divide en la estratégica y operativa (o táctica). La estratégica estudia *cuáles* son las amenazas y los delitos que hay que enfrentar y la operativa ofrece asesoramiento táctico sobre *cómo* abordarlos y priorizarlos mejor.

represivas con la frecuencia que sea necesaria. Además, las evaluaciones operativas estarían a disposición del Grupo de Trabajo de Jefes de Policía (Chiefs of Police Task Force - CPTF) que contaría así con los mejores conocimientos tácticos para prevenir o combatir las amenazas o los delitos, incluido el terrorismo, según las prioridades establecidas por el Consejo.
En la actualidad las autoridades represivas de la UE no cuentan con una Inteligencia que tenga como objetivo la UE en su conjunto. Hoy existe una necesidad urgente de proteger a los ciudadanos europeos contra nuevos riesgos y amenazas. Por tanto, es imperativo disponer rápidamente de las evaluaciones estratégicas y operativas de la UE. Asimismo el intercambio de información debería someterse al Estado de Derecho y respetar los derechos individuales fundamentales.
Por todo ello se propone el siguiente enfoque en dos etapas:

- A corto plazo, los servicios de Inteligencia de los Estados miembros deberían reunirse mensualmente, quizá bajo los auspicios de Europol, para discutir sus evaluaciones estratégicas y operativas nacionales. Europol debería contribuiría con todos sus medios. La información resultante se cotejaría para elaborar evaluaciones estratégicas de la UE, por ejemplo, bianuales, y evaluaciones operativas mensuales. Las evaluaciones estratégicas ayudarían al Consejo a establecer prioridades represivas. El Grupo de Trabajo de Jefes de Policía (CPTF) transmitiría las evaluaciones operativas a las autoridades nacionales.

Toda esta primera etapa estaría fundamentada en la información en materia criminal a la que Europol y las autoridades de los Estados miembros tengan legalmente acceso con arreglo a la legislación actual y deberían utilizarse los sistemas analíticos existentes.

- A más largo plazo, los servicios nacionales de Inteligencia podrán empezar a producir información recurriendo a los sistemas analíticos normalizados con los datos pertinentes en materia represiva de que se disponga en la Unión.

La importancia de Europol aumentaría, puesto que los datos y los procedimientos serán más europeos. Ello redundaría en una Inteligencia de calidad superior al estar más normalizada y comprenderse mejor. Las relaciones entre Europol, el Consejo y el CPTF deben adaptarse a la evolución de las circunstancias. En ese momento, la UE estará en condiciones de afirmarse en la escena internacional como socio en sistemas que garanticen el cumplimiento de la ley con su propio sello y calidad.

La Comisión prevé estudiar las medidas necesarias para crear un sistema de producción puntual de evaluaciones fiables de Inteligencia y para presentar un informe al Consejo a finales de 2005.
El Consejo establecerá prioridades sobre la base de las evaluaciones estratégicas del Grupo de Inteligencia Criminal. Esta evaluación operativa permitirá obtener resultados concretos, como realizar detenciones, decomisar o incautar bienes procedentes de actividades delictivas o trabajar para desmantelar un grupo criminal.
Los métodos de Inteligencia habituales deberían estructurarse de forma que se puedan utilizar no sólo a nivel de la UE, sino también para tratar problemas concretos a escala transnacional o regional (por ejemplo, el Grupo de trabajo del Mar Báltico sobre delincuencia organizada). La Comisión y Europol deberían realizar un estudio de los diversos métodos empleados por los servicios de Inteligencia de los Estados miembros y proponer, a finales de 2005, una metodología analítica europea. Paralelamente, se pediría a CEPOL que diseñara un plan de formación para enseñar a los analistas criminales a utilizar estos métodos y a los directivos a

hacer el mejor uso posible de las evaluaciones operativas. Los métodos analíticos habituales [9]deberían generar resultados utilizables en las evaluaciones estratégicas y operativas de la UE.

- ***El Consejo podría aprobar el contenido esta comunicación con el fin de adoptar las medidas adecuadas para su aplicación.***
- ***Bajo los auspicios de Europol, los representantes de los servicios de Inteligencia de los Estados miembros deberían reunir las evaluaciones estratégicas y operativas nacionales.***
- ***El Consejo podría invitar a los Estados miembros a poner la Inteligencia a disposición de Europol y encomendarle una evaluación del conjunto de la amenaza. Las autoridades de aduanas y las responsables del control de las fronteras podrían encargarse de coordinar con Europol la producción de su Inteligencia.***
- ***Deberían desarrollarse definiciones comunes de estadísticas criminales y normas para la preparación de informes***
- ***Deberían crearse, posiblemente bajo los auspicios de Europol, métodos comunes de análisis para la producción de Inteligencia a escala de la UE.***

2. 4. Clima de confianza

El tercer objetivo de base de la política de información es contribuir a la instauración de un clima de confianza entre las autoridades represivas, los funcionarios y demás partes interesadas europeas estableciendo una plataforma común de valores, normas y orientaciones políticas compartidos.

La introducción de normas comunes es crucial para crear un ambiente de confianza en la recogida, acceso e intercambio de información (véase el punto 2.2). Las normas comunes sobre acceso y tratamiento de datos, así como las metodologías compatibles relacionadas con la evaluación de amenazas, riesgos y perfiles serán una base imprescindible para el intercambio efectivo de información e Inteligencia a nivel estratégico y operativo. Estas medidas solamente serán efectivas si hay un apoyo político continuado a la puesta en práctica de un **espacio común de represión del crimen** en la UE, basado en los sistemas nacionales compatibles de Inteligencia, que formarán juntos un modelo europeo conceptualmente integrado.

Deberán desarrollarse, en consecuencia con todo lo anterior, las relaciones de trabajo formales e informales para que el sistema funcione. Formar al personal encargado de estas tareas para que aprenda a compartir una visión común de la Inteligencia contribuirá a mejorar estos aspectos. CEPOL debería desempeñar un papel importante en este contexto, en especial mediante:

- la creación de cursos de formación regulares para futuros responsables políticos y administradores de rango superior;
- el diseño de un modelo de plan de formación de mandos intermedios en asuntos de Inteligencia europea a escala nacional;

[9] Los métodos son el análisis de resultados, los modelos delictivos, los mercados ilegales, las redes de delincuencia, los riesgos (que se utilizan como herramienta de gestión en sí), los perfiles diana (llamados a menudo «definición de perfiles»), los perfiles de negocios delictivos, y las tendencias demográficas y sociales.

– la aplicación de medidas de formación relacionadas con todos los elementos de la política de información de la UE.

Otras medidas reforzarían el trabajo de red, incluidas las basadas en instrumentos ya existentes tales como evaluaciones mutuas, proyectos especializados dentro del marco del programa AGIS o actividades organizadas bajo los auspicios del Foro sobre la prevención de la delincuencia organizada.

Por último, debería tenerse debidamente en cuenta el papel de las autoridades nacionales supervisoras de datos, ya que contribuirán a establecer las garantías necesarias del Estado de Derecho y proporcionarán un control democrático efectivo.

Las medidas y técnicas encaminadas a crear un clima de confianza son de importancia fundamental (normas y metodologías comunes). La Comisión prevé presentar propuestas a finales de 2005.
Paralelamente, el Consejo podría invitar a CEPOL a iniciar un plan común de formación para los funcionarios de Inteligencia.

CAPÍTULO III – INICIATIVAS LEGISLATIVAS RELACIONADAS CON ESTA COMUNICACIÓN

La Comisión continuará desarrollando medidas, incluidas iniciativas legislativas de protección de datos personales, en el marco del tercer pilar, y sobre el uso de información de pasajeros a efectos represivos, de conformidad con los principios establecidos en la Comunicación de la Comisión de diciembre de 2003[10].

La propuesta de Decisión marco sobre protección de datos recogerá normas comunes de tratamiento de datos personales intercambiados con arreglo al Título VI del Tratado de la Unión Europea, con el fin de autorizar el acceso a todos los datos pertinentes a la policía y las autoridades judiciales, en el respeto de los derechos fundamentales. Esta Decisión debería facilitar un único marco general de protección de datos con fines de cooperación en la prevención, detección, investigación y enjuiciamiento de la delincuencia y las amenazas a la seguridad. Será un marco para las disposiciones más específicas contenidas en los diversos instrumentos jurídicos adoptados a nivel de la UE y seguirá reduciendo las diferencias prácticas en el intercambio de información entre Estados miembros, por una parte, y Estados miembros y terceros países, por otra. Asimismo preverá un mecanismo que garantice la protección de los derechos fundamentales.

***

[10] COM (2003) 826 final, de 16.12.03 Transferencia de datos de los registros de nombres de los pasajeros (PNR): Un enfoque global de la Unión Europea.