GESTIÓN DE PROYECTOS DE INNOVACIÓN TECNOLÓGICA PARA LA SEGURIDAD EN EL MINISTERIO DEL INTERIOR:

Nuevas tecnologías para la seguridad

Horizonte Europa 2021-2027

Autora: MACHIN PRIETO, ROSALÍA

Director: ÁLVAREZ SABUCEDO, LUIS

Contacto: lsabucedo@det.uvigo.es

Resumen: El acceso a Fondos de financiación europeos por parte del Ministerio del Interior para las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) y demás organismos dependientes de la Secretaría de Estado de Seguridad (SES), supone apostar y participar en el desarrollo de nuevas tecnologías y sus aplicaciones con la finalidad de mejorar la función pública y mantener la seguridad de la ciudadanía española.

Dichas iniciativas Europeas facilitan el acceso a importantes inversiones en investigación y nuevas tecnologías de información y comunicación claves, como son el 5G, el internet de las cosas (IoT), la Inteligencia Artificial (IA), la computación cuántica, el *blockchain* y la ciberseguridad, y en general toda la digitalización de datos, que a corto y medio plazo, crecerá de forma exponencial.

Si bien las tecnologías y las nuevas identidades digitales generan oportunidades y beneficios para todos, a la inversa, plantean nuevas amenazas y riesgos. La mayoría de los delitos tienen un elemento digital, y para garantizar investigaciones exitosas y una prevención efectiva del delito, las unidades de investigación competentes tienen que mantenerse actualizadas.

El presente trabajo expone como los proyectos de financiación europeos permiten desarrollar nuevas tecnologías para adquirir métodos y capacidades cada vez más innovadores en la lucha contra los diferentes tipos de delincuencia y cómo además, han surgido líneas de trabajo estratégicas en materia de seguridad tecnológica para España a través de los diferentes grupos de expertos, los consorcios de proyectos o las redes especializadas europeas.

Se pretende demostrar que la cooperación público-privada entre FCSE, industria y academia, es vital para garantizar el acceso al talento, al conocimiento, y a nuevos mercados nacionales e internacionales, y de este modo abordar eficazmente los desafíos tecnológicos en seguridad (ciberdelito, el crimen organizado y el terrorismo).

La Comisión Europea respalda la importancia de reforzar dicha cooperación tecnológica a través de diferentes Programas de Financiación I+D+i, entre los que destacan Horizonte2020 (H2020), Horizonte Europa (HE) y el nuevo Programa Europa Digital (DEP).

Palabras clave: Innovación Tecnológica, Sinergia, Clúster, Seguridad, Amenaza, Digital.

---

1. Introducción

La tecnología, la innovación y la digitalización son la base del nuevo orden global. No se puede negar que el cambio tecnológico ha llegado a todos los ámbitos de la sociedad, la economía y la política, generando una nueva dimensión en las relaciones internacionales y en el campo de la seguridad.

El conocimiento científico, el acceso a la tecnología, su desarrollo y regulación, se han convertido en elementos imprescindibles para los Estados y para sus sociedades. Las relaciones de poder ya no sólo se basan en la excelencia tecnológica, la defensa y la seguridad, sino también en la necesidad de alcanzar la hegemonía en el ciberespacio o en construir nuevos espacios de datos.

Las nuevas revoluciones tecnológicas vinculadas con los sistemas de información y de comunicación (TICs), han generado nuevas áreas de colaboración y competición. La digitalización y la creación de redes globales para el intercambio de información fueron lideradas en un primer momento por Estados Unidos. La segunda fase, y en la que actualmente nos encontramos, basada en las redes 5G, el Internet de las Cosas (IoT), la tecnología cuántica y la Inteligencia Artificial (IA), se está desarrollando entre una aguerrida competición entre China y Estados Unidos.

El poder acceder a las primeras generaciones de nuevas tecnologías, integrar algunas de las tradicionales o diseñar y mantener las nuevas infraestructuras de las redes de datos, son aspectos críticos en los que se basa la **seguridad nacional** de las nuevas sociedades.

Es por ello que la Unión Europea está realizando grandes inversiones a través de Programas de Financiación Europeos, entre los que se destacan en el presente trabajo **Horizonte Europa HE** (I+D+i) y **Programa Europa Digital DEP**. Se considera, que un mayor número de proyectos paneuropeos, en los que se ponen en común los recursos de todos los Estados Miembros, ayudará a alcanzar economías suficientes para ser más competitivos en los mercados globales, y competir con los grandes gigantes tecnológicos. Ésta es la apuesta que hace Europa para el 2030.

El análisis **de Big Data** y las técnicas de inferencia a través de procesos de **Inteligencia Artificial,** abren el campo para nuevos servicios, mucho más personalizados y también mucho más útiles en el ámbito de la Defensa y Seguridad. Se plantean importantes preocupaciones en cuanto a la privacidad del individuo y su autonomía individual. Muchos Estados buscan el equilibrio entre vigilancia y libertad, debido a la creciente tendencia de actividades delictivas relacionadas con el cibercrimen y el robo de identidades.

A tener en cuenta igualmente, que la **computación cuántica**, está destinada posiblemente, a convertirse en un importante elemento de cambio. Aquel estado que desarrolle una computadora cuántica alcanzará un estatus privilegiado, ya que conseguirá tener acceso a todas las redes, así como eludir sus sistemas de encriptación.

El equipamiento y los materiales adecuados a desarrollar por industrias estratégicas, son también elementos críticos en el ámbito de innovación tecnológica. La **fabricación aditiva** (impresión 3D), es posible que rediseñe las cadenas de suministro y a futuro, sustituya la fabricación

convencional en importantes áreas. Los investigadores ya están trabajando en **impresión 4D,** procesos de nueva generación para productos que se modifiquen a sí mismos, respondiendo a cambios ambientales como el calor y la humedad.

En paralelo, las sociedades se enfrentan a problemáticas generadas en el campo de la seguridad por las nuevas tecnologías en su uso diario. La posibilidad de interaccionar con otras personas de todo el mundo y acceder a todo tipo de información, no sólo ofrece ventajas para los ciudadanos. La sobreabundancia de información y las falsas propagandas con fines ilícitos (*fake news)* en el ciberespacio, pueden llegar a desacreditar personas o instituciones, incluso a desestabilizar a la población (**desinformación**).

El liderazgo tecnológico del sigo XXI ha sido asumido por el sector privado, ofreciendo nuevos servicios y bienes de consumo. La Industria de Defensa y Seguridad no ha sido financiada hasta el momento, en muchos casos, por los Estados en la medida que se debería, a través de programas militares o de seguridad interior. Pero sí, en el caso de Europa y concretamente de España, a través de los citados Programas de Financiación Europeo I+D+i.

Se van a presentar algunos de los proyectos de innovación tecnológica y digital de los últimos años, co-financiados por la UE (**STARLIGHT**, **CLOSEYE**, **BiObserver**, etc.), que ayudan a que los agentes españoles y europeos que velan por la seguridad de los ciudadanos (Fuerzas y Cuerpos de Seguridad, Guardias de Fronteras, Servicios de Control y Protección de Aduanas, etc.), se beneficien de nuevas herramientas para su trabajo operativo diario.

El principal objetivo del presente trabajo es ayudar al lector a entender cómo a través de Programas de Financiación Europeos y Nacionales de la Unión Europea (Horizonte Europa, Horizonte2020, Programa Europa Digital), y de la cooperación internacional, se facilita a las Fuerzas y Cuerpos de Seguridad del Estado (Ministerio del Interior) acceso a herramientas provenientes de la **investigación** y la **innovación que le ayuden a desempeñar su función esencial: El mantenimiento de la seguridad de los ciudadanos.**

2. Desarrollo

El presente trabajo pretende describir cómo la **investigación** y la **innovación tecnológica** en materia de seguridad contribuyen de forma estratégica a **definir políticas internacionales en materia TIC** de la UE y entre ellas la de España de la mano del Ministerio del Interior (Estrategia I+D+i Ministerio del Interior, Contribución al Espacios Seguro de datos Europeo, etc.).

Igualmente se ha puesto énfasis en la definición de los principios orientadores europeos en materia TIC para la seguridad de sus estados miembros, los que, junto con las tecnologías emergentes validadas en proyectos de corte europeo y tratadas en los diferentes grupos de expertos, han surgido líneas de trabajo en materia de tecnológica para España, como son:

- El apoyo por parte de España y el Ministerio del Interior para que Europa alcance su **autonomía estratégica** en el ámbito TIC.

- El impulso de la **cooperación internacional** a través de grupos de expertos, grupos de trabajo, alianzas tecnológicas, consorcios de proyectos europeos, etc., para definir la gobernanza de la tecnología en el campo de la seguridad.

- Entender cómo se facilita a través de Programas de Financiación Europeos y Nacionales (Horizonte Europa, Horizonte2020, Programa Europa Digital) **herramientas** provenientes de la **investigación** y la **innovación a los Cuerpos de Seguridad.**

Los últimos avances en materia de políticas de seguridad reflejan la situación cambiante de la UE, donde los Estados miembros se enfrentan a las grandes crisis que amenazan a las personas y a la sociedad. Las tecnologías innovadoras se utilizan cada vez más **para desempeñar actividades delictivas,** como la ciberdelincuencia, el extremismo violento y la radicalización que conducen a actividades de terrorismo, crimen organizado o abuso sexual infantil. Para participar en tales actividades, los delincuentes hacen uso de las últimas tecnologías aplicadas al uso de entornos como la *Dark Web* y al uso de nuevas herramientas de cifrado.

Los desarrollos para hacer frente a desafíos, como la crisis de refugiados de 2015 o la consolidación de **Espacio Schengen** (un espacio sin controles fronterizos en las fronteras interiores) (38), todavía están en pruebas y se validan a través de los correspondientes Programas I+D+i. En los últimos años, los Estados miembros de la UE, han restablecido temporalmente los controles en las fronteras interiores tras importantes ataques terroristas en ciudades europeas y tras la pandemia de COVID-19.

La investigación y la innovación apoyan los objetivos específicos establecidos en la Estrategia de Seguridad de UE. Estos incluyen la investigación en nuevas técnicas de análisis forense digital, detección de explosivos, técnicas para almacenar evidencias digitales en investigaciones de policía judicial, por ejemplo, para la detección de pornografía infantil online.

La Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad (SGSICS) representa ante la Comisión Europea al Ministerio del Interior en los proyectos de I+D+i en los que este participe, principalmente dentro de Programas como el 8º Programa Marco, **Horizonte 2020** y el actual 9º Programa Marco, **Horizonte Europa**, o aquellos proyectos de carácter innovador de fondos europeos ejecutivos como son una rama de los **FSI** (Fondos para la Seguridad Interior), o el nuevo Programa Europa Digital **DEP**.

A través de su área de I+D+i, la SGSICS y por tanto el Ministerio del Interior gestiona, coordina y fomenta la participación de proyectos de I+D+i en nuevas tecnologías a modo de **inversión eficiente**, haciendo de enlace con la **industria** y la **Academia** nacional y europea.

El Área I+D+i intenta aumentar la tasa de participación proporcionando apoyo a las unidades de las Fuerzas y Cuerpos de Seguridad del Estado (CNP y GC) y demás organismos dependientes, coordinando iniciativas a nivel Administración General del Estado (AGE) como la Comunidad de Usuarios Nacional (**CoU** España).

El área I+D+i SGSICS, fomenta además la **cooperación internacional** en materia tecnológica a través de los grupos de expertos, grupos de trabajo, foros y redes tecnológicas en los que participa como Punto Nacional de Contacto del Ministerio del Interior (**HLEGI-A** Comisión Europea, **WG-AI** Eu-lisa, Grupo de Expertos IA de EUROPOL, **CERIS-CoU** Europea, **ENLETS**, **IFAFRI**, etc.)

Por otro lado, y teniendo en cuenta que Europa seguirá mejorando los mecanismos para desarrollar los servicios TIC que ofrece a sus ciudadanos, es esencial poner en valor la **vigilancia tecnológica**. La revisión de las tecnologías que se consideran disruptivas en el entorno europeo e internacional de seguridad es uno de los principales ejes en el epígrafe IV del presente trabajo.

Igualmente se van a describir algunas de las medidas que el Ministerio del Interior español va a tomar para asegurar la **transferencia** de los resultados de los proyectos de investigación. En último término con la finalidad de diseñar mejor la estrategia de participación en dichos Programas, y subvencionar aquello que realmente es necesario en el ámbito operativo.

El uso de las redes **5G** y **6G**, la investigación en **computación avanzada**, la inclusión de nuevos procesos de IA en los sistemas, el diseño de los nuevos espacios seguros de datos y la aplicación de *blockchain* a las transacciones, supone un gran desafío.

El Ministerio del Interior está realizando fuertes inversiones para acelerar el despliegue del 5G, tanto en zonas urbanas como rurales para mejorar la conectividad y alcanzar un sistema móvil de banda ancha interoperable paneuropeo para radiocomunicaciones. Reflejo de ello es la participación coordinada por la SGSICS, de Policía Nacional y de Guardia Civil en el proyecto H2020 **BROADWAY[1].**

España también impulsará la investigación asociada al **6G**, como ya lo está haciendo con las principales empresas españolas que están participando de lleno en el proyecto comunitario **HEXA-X[2].**

La I+D+i Europea considera a la **Computación Avanzada (HPC)** también una tecnología disruptiva, prueba de ello es la inversión que ha realizado en los últimos Programas de Trabajo en éste ámbito. El Proyecto H2020 **Exscalate4Cov** (E4C[3]) es el consorcio público-privado que representa al centro de competencia más avanzado en Europa. Destinado a combatir el coronavirus, combinando recursos de supercomputación e inteligencia artificial, además de instalaciones experimentales donde se realizan la consiguientes validaciones técnicas.

Europa, desde 2018, dio un paso adelante en el desarrollo (I+D+i) de tecnologías cuánticas promoviendo la inversión en una infraestructura de comunicaciones ultra segura en toda Europa y una red de centros de operaciones de seguridad con inteligencia artificial. Dicha iniciativa, financiada con fondos EU, se conoce como ***Quantum Flagship.*** Quedan reflejados en el trabajo proyectos aprobados como el H2020 **2D-SIPC** y H2020 **Quantum Internet Alliance-QIA.**

La **inteligencia artificial IA**, puede ser una herramienta útil para afrontar las nuevas amenazas digitales. Su uso podrá ser extendido para acelerar la identificación y respuesta ante las vulnerabilidades y ataques dirigidos. El uso de ***la nube y el Big Data***, suponen nuevos desafíos relacionados, ya que la navegación de los datos libres en el ciberespacio, aumenta la posibilidad de su robo o de su uso indebido.

Haciendo uso de las correspondientes tecnologías, los cuerpos policiales, podrán aprovechar las fuentes de datos digitales a su máximo potencial ahorrando tiempo en la revisión de evidencias. Con Big Data y **algoritmos** cada vez más sofisticados será posible hacer predicciones cada vez más precisas. Se prevé tomar decisiones más consistentes. Prueba de ello son las validaciones técnicas que se están realizando por parte de las fuerzas y cuerpos de seguridad europeas, entre ellas Policía Nacional y Guardia Civil (SGSICS), en proyectos como H2020-AI-**STARLIGHT[4],** H2020-AI-**RED ALERT[5] H2020** o el proyecto nacional CIEN-**AIMARS**.

---

[1] **H2020-SEC-04-DRS** (Disaster and resilient societies)-2017 - Broadband communication systems Compra Pública Pre-comercial, el consorcio del proyecto BROADWAY estará formado 11 compradores de 11 países. Se están realizando pilotos, combinado modelos Tetra/Tetrapol con 5G para no sólo enviar radio, si no también compartir fotografías, videos y mensajes. En el caso de España, Ministerio del Interior, SGSICS (autoridad delegada responsable de operar las redes de comunicación de seguridad pública, para dar servicio a las FCSE).

[2] **H2020 (Flagship I+D+i)**, con una asignación de 12 millones de euros, pretende impulsar el liderazgo europeo en tecnología móvil de sexta generación ó 6G. Está desarrollando un primer concepto de sistema 6G complementado con 8 proyectos que investigan tecnologías específicas (macro-red).

[3] **Exscalate4Cov** Proyecto de supercomputación para identificar nuevas terapias para COVID-19. El consorcio E4C, coordinado por Dompé Farmaceutici, está compuesto por 18 instituciones de siete países europeos. En el núcleo de E4C se encuentra Exscalate (EXaSCale smArt pLatform Against paThogEns), en la actualidad la plataforma de supercomputación inteligente reconocida a nivel mundial.

[4] **STARLIGHT H2020-AI**-Sustainable Autonomy and Resilience for LEAs using AI against High priority Threats. validará procesos de Inteligencia Artificial, por parte de las Fuerzas y Cuerpos de Seguridad Europeas. El Ministerio del Interior de España[4] tendrá un papel relevante, liderando tareas de análisis y especificación de requisitos operativos, casos de uso y pilotos propuestos. Coordinado por Ministerio Interior Francia-Commissariat a l'Energie Atomique et aux energies alternatives (**CEA**). En total 53 socios de 18 países, 17 Fuerzas y Cuerpos de Seguridad europeos. 7 socios españoles, entre ellos el Ministerio del Interior España.

Otra parte importante de la seguridad será la protección de los datos cuando estos se intercambian. Vinculado a la IA, el ***Blockchain*** proporciona seguridad y descentraliza el entorno en el que se llevan a cabo muchas transacciones digitales. Esta nueva tecnología descentralizada ofrece a los usuarios (personas y empresas) la posibilidad de gestionar y controlar los flujos de datos y su utilización. Permitirá la portabilidad de los mismos en tiempo real, utilizando algoritmos para cifrar información, descentralizar los datos y aumentar de forma segura la privacidad entre los usuarios. Las aplicaciones del *Blockchain* son muy amplias, más allá de las criptomendas. Prueba de ello es el proyecto **H2020 LOCARD**, cuyo objetivo es desarrollar una plataforma de gestión integral que permita el almacenamiento de datos de evidencias digitales y pueda garantizar la cadena de custodia en investigaciones de policía judicial.

Es importante destacar que España apoya la reutilización de datos tanto privados como públicos, en particular los datos industriales en los que se basa las nuevas líneas estratégicas de I+D+i. Igualmente, el Ministerio del Interior también apoyará el desarrollo de un marco de la UE sobre el uso de inteligencia artificial. Este marco debe garantizar que la tecnología de inteligencia artificial pueda desarrollarse e implementarse en Europa y en España al tiempo que garantiza que la tecnología no se utilice de manera inapropiada. Es por ello que el Ministerio del Interior representado por la SGSICS trabaja con la Comisión Europea en grupos de expertos de IA, como en el **HLEG-AI**[6], y en **CAHAI**[7], entre otros.

Los **Espacios Seguros de Datos** van a cobrar especial importancia durante el período 2021-2027, y habrá que atender tanto a su infraestructura de carácter tecnológico como a la gobernanza de los mismos. El valor de los datos reside en su uso y reutilización.

En la actualidad, no hay suficientes datos disponibles para que sean reutilizados en I+D+i, por ejemplo, para el desarrollo de procesos de inteligencia artificial y entrenamiento de sus algoritmos. Las problemáticas empiezan por la titularidad de los datos, siguen por la identificación de los usuarios de los datos, y pueden llegar hasta la naturaleza que tienen los mismos.

La **interoperabilidad** y la **calidad** de los datos son aspectos clave para el despliegue de procesos basados en IA. Se han identificado problemas importantes de interoperabilidad que dificultan la combinación de datos que provienen de diferentes sectores. Estas problemáticas se agravan todavía más cuando se hace referencia a Estados o Naciones diferentes.

Para que los espacios seguros de datos sean operativos, se necesitan organismos públicos y privados que fomenten la innovación acorde a los marcos jurídicos existentes.

Aunque un espacio europeo seguro de datos para la Innovación no estaría únicamente dirigido al desarrollo de la IA en el ámbito científico, sí que supondría una mejora en los resultados de investigación de la UE, estableciendo vínculos entre los dos programas de financiación I+D+i más relevantes: HE y DEP.

El éxito de éstas iniciativas llegaría a suponer una mejora no sólo en la soberanía tecnológica de los Estados miembros, sino también en la lucha contra el crimen organizado y el terrorismo en el ámbito digital, y por ende, una mayor protección de la Seguridad Nacional. Los Estados miembros podrán validar sus propias herramientas digitales, y ofrecer **servicios centralizados**, basándose en esquemas comunes. Al **reducir la dependencia de proveedores** de terceros países, se podrían ver disminuidas amenazas de tipo malicioso, además de establecer estándares de calidad en el entorno UE.

---

[5] **RED ALERT** Real-time Early Detection and Alert System for Online Terrorist Content based on Natural Language Processing, Social Network Analysis, Artificial Intelligence and Complex Event Processing. SEC-12-FCT-2016-2017 - Technologies for prevention, investigation, and mitigation in the context of fight against crime and terrorism.

[6] High Level Expert Group-Artificial Intelligence, European Comission.

[7] **CAHAI** Ad hoc Committee on Artificial Intelligence, Council of Europe.

Las agencias europeas, **Eu-Lisa y EUROPOL**, con el *feedback* de los estados miembros, están evaluando en la actualidad las distintas arquitecturas posibles para implementar este espacio común de datos seguros, valorando cuatro posibilidades: individual, centralizada, federada e híbrida, explicadas en el trabajo.

El conocimiento del mapa de las diferentes convocatorias y ayudas públicas orientadas a la seguridad, los mecanismos de participación, la experiencia en preparación de ofertas y la experiencia en la gestión integral (técnica, administrativa y financiera) de proyectos europeos y nacionales I+D+i del Ministerio del Interior, a través de la SGSICS se ponen en valor en el presente trabajo. Para obtener financiación I+D+i europea y nacional que resulte impulsora de necesidades específicas de las Fuerzas y Cuerpos de Seguridad del Estado, el Ministerio del Interior, SGSICS va a utilizar los siguientes mecanismos:

El Área I+D+i SGSICS, qué articula su función en varios ejes prioritarios: gestión integral de proyectos I+D+i (H2020, HE, DEP, etc.), realización de prospectiva tecnológica (grupos de trabajo, networking), gestión tecnológica, que abarca la trasferencia tecnológica y explotación (PCPs[8], CPI[9], AI[10], etc.), Función Tractora (creación e impulso de consorcios nacionales y europeos, con industria y con universidad) y Difusión del Conocimiento (jornadas informativas, workshops, etc.).

La Comunidad de Usuarios finales española (CoU – CERIS), coordinada por la SGSICS, supone un fuerte impulso para Cooperación Público-Privada nacional en seguridad. El alto número de proyectos de I+D+i, la desconexión entre la investigación y la obtención de resultados tangibles en muchos casos, la dificultad de comercialización de soluciones provenientes de I+D+i, y la falta de mecanismos de engranaje entre los diferentes Programas de financiación dificultan la comunicación y el intercambio de conocimientos entre los usuarios finales nacionales y todavía más con los europeos.

Es muy necesario asegurar la transferencia de los resultados de los proyectos de investigación para los usuarios finales del ámbito de la seguridad. Lo que requiere un intercambio adecuado de información sobre actualizaciones de políticas o resultados de proyectos (de investigación). La principal función de la COU-España es **identificar oportunidades de financiación y sinergias** entre los diferentes programas I+D+i y proponer medidas para facilitar la interacción. Otra función importante será la de intentar evitar duplicidades en la participación por parte de los usuarios finales (FCSE, Policías Forales, Protección Civil, Defensa, Puertos del Estado, Instituciones Penitenciarias, etc.) en los diferentes programas de financiación, por ejemplo entre Policía Nacional y Guardia Civil. Si la necesidad es conjunta, es preferible participar conjuntamente, que desviar el doble de recursos del Ministerio del Interior para la misma tarea.

El Centro Tecnológico para la Seguridad, CETSE realiza funciones de observatorio tecnológico del Ministerio del Interior. Continuando con su misión de proporcionar el conjunto de herramientas tecnológicas que permitan conseguir sus objetivos de la manera más eficaz y eficiente a las Fuerzas y Cuerpos de Seguridad del Estado (Policía Nacional y Guardia Civil) así como al propio Ministerio del Interior, la SGSICS sigue impulsado el desarrollo de nuevas iniciativas TIC para dar soporte a las unidades operativas.

Claro ejemplo son los proyectos internos impulsados por el CETSE, por ejemplo, de reconocimiento facial avanzado, que incluyen procesos de IA, y que desarrollan conjuntamente con CNP, GC y CNI: **BiObserver[11]** y BioRetriever[12]. También reseñar el proyecto H2020 I-LEAD, a

[8] Pre-comercial-Procurement.
[9] Compra Pública Innovadora CDTI.
[10] Acciones Innovadoras.
[11] Plataforma de análisis de comportamiento de video, frame for frame, que permite la identificación de emociones y micro expresiones faciales. SGSICS

través del cual se comparten tecnologías y metodologías que utilizan las FCSE europeas en la actualidad para trabajar en Investigaciones Digitales.

La mayoría de los Estados Miembros dependían y dependen completamente de Horizonte 2020 y actualmente de HE, para cubrir sus necesidades de soluciones de seguridad innovadoras. Dichos Programas representan el 50% de la financiación pública global para la investigación de seguridad en la UE. Las convocatorias de H2020 ***Sociedades Seguras: protección de la libertad y la seguridad de Europa y sus ciudadanos***, están en consonancia con la investigación e innovación responsables, involucrando a la sociedad en temas sensibles de seguridad.

El objetivo tratado en el epígrafe V del trabajo, es explicar el alcance de la I+D+i en Seguridad en UE a través de los programas **Horizonte Europa HE** (9ºPrograma Marco) y **Horizonte2020** (8ºPrograma Marco).

No sólo como se trabaja en el desarrollo de nuevos productos tecnológicos para satisfacer las necesidades de aquellos cuerpos que se encargan del mantenimiento de la Seguridad, sino que también comprender fenómenos muy tenidos en cuenta por la Comisión Europea, como la radicalización violenta, la seguridad de las entradas fronterizas, la protección de las infraestructuras críticas contra cualquier tipo de amenaza, incluso los ciberataques, o el desarrollo de intervenciones más efectivas para el mantenimiento de la seguridad ciudadana en general.

Además se ha intentado reflejar las medidas (tópics) que se están implementando a través de los diferentes Programas Marco de Investigación e Innovación de la UE, en concreto los de HE (2021-2027)**,** Clúster 3, Destino: ***Seguridad Civil para la Sociedad***, para desarrollar e implementar por parte de los Estados Miembros y de España, herramientas de última generación, de utilidad para la función policial. (Lucha contra el crimen organizado y el terrorismo **FCT**, la gestión de fronteras **BM**, la resiliencia de infraestructuras **INFRA**, la resiliencia de las sociedades **DRS** y la Ciberseguridad **CS**).

En el epígrafe VI se han dado unas pinceladas del **Programa Europa Digital DEP** (2021-2027). Se ha explicado la fórmula para financiar las capacidades digitales estratégicas de los estados miembros de la UE, con un presupuesto global previsto de 7500 millones de euros. DEP complementa a otros programas como HE, el Mecanismo Conectar Europa para la infraestructura digital y, finalmente, los Fondo de Seguridad Interior (ISF).

El programa Europa Digital reforzará las capacidades digitales críticas de la UE centrándose en las áreas clave de inteligencia artificial (IA), ciberseguridad, informática avanzada, infraestructura de datos, gobernanza y procesamiento, el despliegue de estas tecnologías y su mejor uso en todos los ámbitos de las sociedades Europeas.

3. Conclusiones

Ha quedado patente que, cumpliendo con el objetivo inicial de **visibilizar el enfoque proactivo en la búsqueda de Programas y soluciones tecnológicas por parte del Ministerio del Interior** español, se facilita el acceso a los productos y soluciones tecnológicas de seguridad que puedan ser posteriormente aplicables con éxito por las unidades operativas de las FCSE. Además, la participación en dichos Programas y proyectos, crea **canales de comunicación** con los estados miembros de la UE y las Agencias europeas correspondientes, para que de forma colaborativa, se pueda acceder a las ayudas financieras europeas.

Queda reflejado también a lo largo del trabajo, no sólo la importancia de la cooperación internacional en materia de seguridad e I+D+i, si no la necesidad, para tener éxito en los proyectos, de la

[12] Plataforma Integral de videovigilancia, para análisis y reconocimiento de patrones e identificación simultánea de sujetos en entornos multitudinarios. SGSICS

colaboración entre Administración Pública, Industria y Universidad nacional y europea. La **cooperación público-privada** concluye como un factor esencial en la gestión de proyectos europeos I+D+i, y en general, en el impulso de las nuevas tecnologías para la seguridad.

El apoyo del Ministerio del Interior y del resto de Estados miembros, junto con las inversiones en I+D+i, no sólo económicas, sino también de **capital humano**, van a contribuir al posicionamiento de la UE como un actor tecnológico, industrial y normativo líder en tecnologías digitales, *Big Data*, IA, computación cuántica, 5G, *blockchain* y espacios seguros de datos. Los usuarios finales validando junto con la industria nacional y europea, todas aquellas tecnologías que cubren sus necesidades en el ámbito de la seguridad, van fomentar que España se convierta en **una nación emprendedora**.

Con la participación en los proyectos europeos anteriormente explicados y en los diferentes mecanismos de colaboración europea (grupos de expertos, foros tecnológicos, grupo de trabajo, etc.) se da **mayor visibilidad** a la profesional labor que realizan las Fuerzas y Cuerpos de Seguridad en nuestro país, gracias en cierta medida, a los nuevos desarrollos tecnológicos con los que cuentan para realizar su trabajo. Fortaleciendo de esta manera, aún más, la imagen y la **"Marca" de España** en la gobernanza de la tecnología, aplicada también al ámbito de la seguridad.

Se cumple con el objetivo del presente trabajo, ya que queda evidente cómo a través de Programas de Financiación Europeos y Nacionales (HE, H2020, DEP) se facilita a las FCSE acceso a **herramientas provenientes de la I+D+i que le ayudan a desempeñar su funciones esenciales**: El mantenimiento de la **seguridad** de los ciudadanos, la lucha contra el crimen organizado y el terrorismo, y la protección de las fronteras y de las infraestructuras críticas. La finalidad última es **completar ciclos de innovación**, desde que se investiga un producto hasta que llega a mercado. Y España, con la ayuda de los mecanismos del Ministerio del Interior, aunque no en todos los casos, lo consigue.

Estrategia UE en Seguridad, ***Fuente: ec.europa.eu***

Agradecimientos

A mis padres, ***Santos Machín Vázquez*** *y* ***Carmen Prieto Fuertes****, por la educación y valores que me han dado y me siguen dando. Por inculcarme la ilusión por aprender y superarme.*

A mis padrinos, ***Manuel FormigoVilas*** *y* ***María José González Briones****, por el apoyo incondicional y el cariño ofrecido lejos de casa.*

A mi director de TFM Luis Álvarez Sabucedo, *por su buena predisposición, su buen hacer y su paciencia infinita.*