UNIVERSIDAD DE SALAMANCA

FACULTAD DE DERECHO

ÁREA DE DERECHO PROCESAL

DILIGENCIAS DE INVESTIGACIÓN TECNOLÓGICAS PARA LA LUCHA CONTRA LA CIBERDELINCUENCIA GRAVE

ESPECIAL REFERENCIA A LA UTILIZACIÓN DEL REGISTRO REMOTO PARA LA INVESTIGACIÓN DE CIBERATAQUES CONTRA INFRAESTRUCTURAS CRÍTICAS Y ESTRATÉGICAS

IRENE GONZÁLEZ PULIDO

TESIS DOCTORAL

Dirigida por:

Dr. D. LORENZO M. BUJOSA VADELL

Dra. Dña. MARTA DEL POZO PÉREZ

PROGRAMA DE DOCTORADO "ADMINISTRACIÓN, HACIENDA Y JUSTICIA EN EL ESTADO SOCIAL"

Salamanca | 2022

A mi padre, Jesús, a mi madre, Ana,
y a mi hermana, Lydia.
POR TODO.

- ¿Es ahora? ¿Es ahora?

- Sí, todo esto está pasando ahora

Minority Report.

AGRADECIMIENTOS

Como bien conocen todos los doctores y las doctoras que leerán estas líneas, el desarrollo de una tesis doctoral es un trabajo que requiere una gran dedicación y esfuerzo individual, pero es producto del apoyo de muchas personas y sin las cuales este resultado no podría haber sido posible.

Gracias al área de Derecho procesal de la Universidad de Salamanca de la que formo parte desde hace cinco años, porque desde el primer momento me acogieron y me hicieron sentir un miembro más de su grupo, de la familia procesal. Gracias a su apoyo y ayuda, la finalización de esta tesis doctoral y mi formación como docente e investigadora ha sido posible, por eso reflejo aquí mis más sinceros agradecimientos a mis compañeros, compañeras, amigos y amigas de facultad; Federico Bueno de Mata, Adán Carrizo González-Castell, Alicia González Monje, Isabel Huertas Martín, Fernando Martín Diz, Walter Reifarth Muñoz, María Inmaculada Sánchez Barrios e Irene Yáñez García-Bernalt.

Mención y agradecimiento especial merecen mi maestro Lorenzo Bujosa Vadell y mi maestra Marta del Pozo Pérez, que me han acompañado en todos los pequeños pasos que he ido dando en este mundo académico, habiendo sufrido conmigo las dificultades y circunstancias que desmoronaban el trabajo realizado una y otra vez, sin soltarme de la mano.

Agradecimientos a Sergi Corominas Bach, por su disponibilidad y su necesario apoyo para la consecución de la mención internacional.

Mis agradecimientos a otras áreas de la Facultad de Derecho de la Universidad de Salamanca que han contribuido a que todo esto sea posible, particularmente al área de derecho administrativo, constitucional y mercantil. De igual modo, agradecer a los jóvenes nóveles y expertos procesalistas de todas las universidades españolas que me han acompañado en este camino hacia el grado de doctor, enriqueciéndolo en todos y cada uno de los rincones de España.

> "Teamwork is the secret that make common people achieve uncommon result".
> *Ifeanyi Enoch Onuoha*

Agradecimientos a la Universidad de Gante, al profesor Piet Taelman, por su apoyo en el desarrollo de la investigación, a la profesora Eva Lievens que tutorizó mi estancia en la *Faculty of law and criminology*, y a los doctorandos y doctorandas que me acogieron durante tres meses en su Universidad y en su mágica ciudad.

> "Travel makes one modest. You see what a tiny place you occupy in the world". *Gustave Flaubert.*

Agradecimientos a la *Universitá degli Studi di Messina,* personalmente agradecimientos al profesor Stefano Ruggeri, por su hospitalidad, su personalidad, su profesionalidad y su apoyo, los cuales han contribuido a culminar la investigación doctoral. Agradecimientos a los doctorandos, profesores y amigos del *Dipartimento di Giurisprudenza:* Antonella, Claudio, Diego, Martina, Michele y Viviana. Agradecimientos a Sicilia, a su cultura, sus ciudades, sus paisajes, sus playas y, sobre todo, a su gente que transmiten la fuerza y a la vez la calma necesaria para afrontar los últimos avances de la tesis doctoral.

> "There is a kind of magicness about going far away and then coming back all changed". *Kate Douglas Wiggin.*

Cuando decides realizar el doctorado y emplear todo tu potencial en la consecución del título de Doctora, se invierten muchas horas, días, meses y años, por ello, estos agradecimientos también son para todas las personas que entendieron lo que estaba haciendo todo este tiempo, que era importante para mí, y me apoyaron sin cuestionarlo, estando ahí en todos y cada uno de los momentos que los necesité. Agradecimientos a toda mi familia, a los que están y los que estuvieron, y a todas mis amigas y amigos.

> "Le plus beau cadeau que tu puisses faire à quelqu'un c'est ton temps", el mejor regalo que le puedes dar a alguien es tu tiempo, *Paulo Cohelo.*

Son muchos a los que debo agradecer su apoyo incondicional para el desarrollo de esta tesis doctoral, gracias a todas y a cada una de las personas que estuvieron o están y que no he mencionado expresamente.

El Arenal, 7 de febrero de 2022

ÍNDICE

ÍNDICE DE ABREVIATURAS, ACRÓNIMOS Y SIGLAS

ALECrim	Anteproyecto de la Ley de Enjuiciamiento Criminal
APT	Advanced Persistent Threats
BIT	Brigada de Investigación Tecnológica
CaaS	Crime as a service / crimen como Servicio
CCN	Centro Criptológico Nacional
CEDH	Convenio Europeo de Derechos Humanos
CEO	Chief Executive Officer
CEPOL	Agencia de la Unión Europea para la formación policial
CERT	Equipos de respuesta ante emergencias informáticas
CNP	Fraude de pago con tarjeta no presente
CSIRT	Red de equipos de respuesta a incidentes informáticos
DAO	Dirección Adjunta Operativa
DM	Decisión Marco
DNI	Documento Nacional de Identidad
DNS	Domain Name System / Sistema de nombres de dominio
DOEI	Directiva 2014/41/UE relativa a la orden europea de investigación en materia penal
DOEIT	Propuesta de Directiva relativa a la orden europea de investigación tecnológica en materia penal
DoS	Denial of service / ataques de denegación de servicio
DDoS	Denegación de Servicio Distribuidos
EC3	Centro Europeo de Ciberdelincuencia
ECI	Equipo Conjunto de Investigación
EDITEs	Equipos de Investigación Tecnológica
ENISA	Agencia europea de seguridad de las redes y de la información
EPOC	Orden Europea de Entrega
EPOC-PR	Orden Europea de Conservación
Eurojust	Agencia de la Unión Europea para la Cooperación Judicial Penal
Europol	Agencia de la Unión Europea para la Cooperación Policial

GDT	Grupo de Delitos Telemáticos
IA	Inteligencia artificial
ICE	Infraestructuras Críticas Europeas
ICS	Sistemas de Control Industrial
IM-RAT	Imminent Monitor Remote Access
IOCTA	Internet Organised Crime Threat Assessment
IoT	Internet of Things / Internet de las Cosas
IIoT	Industrial Internet of Things
J-CAT	Joint Cybercrime Action Taskforce
INTERPOL	Organización Internacional de Policía Criminal
IP	Protocolo de Internet
LAJ	Letrado de la Administración de Justicia
LECrim	Ley de Enjuiciamiento Criminal
LO	Ley Orgánica
LOPJ	Ley Orgánica del Poder Judicial
MaaS	Malware as a service / Malware como servicio
NASA	National Aeronautics and Space Administration
NCP	Network Control Protocol
NU	Naciones Unidas
ODE	Orden Europea de Detención y Entrega
OEI	Orden Europea de Investigación
OEIT	Orden Europea de Investigación Tecnológica
OLAF	Oficina Europea de Lucha contra el Fraude
OSCE	Organización para la Seguridad y la Cooperación en Europa
OTAN	Organización del Tratado del Atlántico Norte
PICI	Infraestructuras críticas de la información
P2P	Peer-to-peer
PoS	Fraude en el punto de venta
RaaS	Ransomware as a service / Ransomware como servicio
RAT	Remote Access Trojans

RGDP	Reglamento General de Protección de Datos
SCADA	Supervisory Control and Data Acquisition
SCDTI	Sección Central de Delitos en Tecnologías de la Información
SIS	Sistema de Información Schengen
SIRENE	Supplementary Information Request at the National Entry
SITEL	Sistema Integrado de Interceptación Telefónica
SOCTA	Serious Organised Crime Threat Assessment
TEDH	Tribunal Europeo de Derechos Humanos
TFUE	Tratado de Funcionamiento de la Unión Europea
TIC	Tecnologías de la Información y Comunicación
TCP	Transmisión Control Protocol
TOR	The Onion Router
TUE	Tratado de la Unión Europea
UE	Unión Europea
UCDI	Unidad Central de Delitos Informáticos
UCIBER	Unidad de Ciberseguridad
UCO	Unidad Central Operativa
UIT	Unidad de Investigación Tecnológica
VPN	Redes privadas virtuales

INTRODUCCIÓN

1. EXPOSICIÓN DE LA PROBLEMÁTICA OBJETO DE ESTUDIO

La aparición de las tecnologías de la información y de la comunicación ha provocado la progresiva globalización y digitalización a todos los niveles. El origen de Internet ha sido identificado como un hito del siglo XX en el ámbito tecnológico, ya que ha contribuido a la consolidación de un espacio cibernético que ha revolucionado la concepción existente del espacio y del tiempo en el medio *offline*. Entorno que ha adquirido, además, características propias que han permitido que millones de usuarios hayan materializado la práctica de diversas actividades de su vida cotidiana; del ámbito laboral, social o económico.

La evolución tecnológica no ha cesado, sino que ha experimentado cambios significativos en las últimas décadas; nos encontramos ante el auge de la inteligencia artificial, la robótica, el *deep learning*, el *machine learning*, el *Big Data*, el *Cloud Computing*, la realidad virtual, el *blockchain*, el Internet de las Cosas, la nanotecnología, las ciudades inteligentes, entre otros avances, los cuales han sido identificados como tecnologías disruptivas. Estas emergentes técnicas y servicios han condicionado tanto el comportamiento individual de los ciudadanos como el funcionamiento general de la sociedad.

La inmersión tecnológica de la ciudadanía se ha incrementado progresivamente desde la aparición de Internet. Desde los diversos niveles territoriales, persiguiendo el acceso universal a internet, se ha aprobado normativa para minimizar la brecha digital, lo que ha aumentado la conectividad con el objetivo de conseguir una digitalización global. Asimismo, el desarrollo y la evolución de los dispositivos portátiles que permiten el

acceso al ciberespacio han contribuido al aumento de internautas conectados al ciberespacio que se benefician con carácter ininterrumpido de los avances técnicos.

Las ventajas que ofrece el ciberespacio no han sido desaprovechadas por los ciudadanos como personas físicas individuales, pero tampoco han pasado desapercibidas en el marco empresarial e institucional; se ha mejorado el funcionamiento de las diferentes entidades públicas y privadas, las cuales se encuentran conectadas en la actualidad y entre las que encontramos a las infraestructuras críticas y estratégicas.

La digitalización de las últimas décadas, además, ha experimentado una obligada aceleración debido a la pandemia de la COVID-19. Desde el año 2020 la actividad personal, social y laboral a nivel global se ha visto afectada por las diferentes medidas gubernamentales desarrolladas para la contención del contagio, lo que ha ocasionado un aumento significativo de la utilización de Internet, incrementando el número de usuarios y el tiempo de uso de las TIC. En este sentido, debemos reseñar dos situaciones que han puesto en jaque a diferentes instituciones: por un lado, han tenido que adaptar su infraestructura para poder continuar ofreciendo los servicios esenciales de un modo remoto y, por otro lado, se ha producido el colapso de algunas de las entidades básicas para el funcionamiento estatal y la seguridad nacional.

Como ha sido señalado la digitalización ha generado una serie de ventajas que han mejorado la vida a nivel global, pero, sin embargo, todos los beneficios que podemos obtener de las TIC han sido rápidamente aprovechados por los delincuentes. La tecnología se ha convertido en un elemento básico para la actuación delictiva, lo que ha ocasionado la aparición de la ciberdelincuencia; desde la aparición de Internet ya se detectaron los primeros ataques, los cuales no han cesado desde entonces. La acelerada digitalización que se ha experimentado en los últimos años ha provocado, además, que la actividad delictiva se desplace significativamente al ciberespacio, aumentando los diferentes tipos de ciberdelitos que pueden perpetrarse a través del mismo.

Los ciberdelincuentes se han aprovechado de las características inherentes al ciberespacio, las cuales se presentan como obstáculos para los operadores jurídicos competentes para la investigación y represión de estas tipologías delictivas; dificultades como el anonimato que ofrece la red, el desarrollo del crimen como servicio, la inmediatez delictiva, la programación de ataques persistentes, la ausencia de fronteras,

entre otras. En particular los citados hándicaps se incrementan cuando nos encontramos ante ciberdelincuencia grave y organizada.

Entre los ciberdelitos graves en la presente investigación se ha centrado la atención en los ciberataques que se perpetran contra infraestructuras críticas y estratégicas. Estos ataques son aquellos que se dirigen contra los servicios esenciales de los Estados y cuya paralización puede comprometer la seguridad nacional e internacional; pueden ser instituciones del sector energético, de salud, de transporte, etc. Todas las tipologías delictivas que pueden enmarcarse en estas conductas han sido consideradas graves y su investigación se ha identificado como compleja, por lo que su tratamiento penal y procesal se realiza de un modo homólogo a la actuación contra la delincuencia organizada o el terrorismo; sin perjuicio de que las organizaciones o las agrupaciones terroristas pueden perpetrar también estos ataques. En los últimos años, ante el aumento de este tipo de delitos, han sido varias entidades y gobiernos los que han identificado que la protección de estas infraestructuras es una prioridad.

A nivel internacional, europeo y nacional se han aunado esfuerzos para aprobar normativa para tipificar este tipo de conductas en los diferentes niveles territoriales, con la finalidad de evitar que los paraísos cibernéticos favorezcan la impunidad de estos delitos. No obstante, como será objeto de análisis en la presente investigación, la previsión legal de los ciberdelitos no va a ser la única medida que deberá adoptar la comunidad internacional para poder reprimir y minimizar este tipo de ataques. En este sentido, se identifican las herramientas del Derecho procesal como necesarias para implementar medidas que permitan investigar y enjuiciar este tipo de hechos; entre las que destacan las diligencias de investigación tecnológicas. Además, se ha identificado la respuesta procesal como fundamental para garantizar la seguridad nacional e internacional.

Las medidas tecnológicas de investigación se convierten en instrumentos necesarios para poder actuar contra la ciberdelincuencia, ya que el factor tecnológico puede limitar o impedir la utilización de diligencias de investigación *offline* de un modo eficaz. En la actualidad, este tipo de investigaciones tecnológicas está adquiriendo un protagonismo en el marco del proceso penal incoado por motivo de ciberdelitos o delincuencia grave, ya que la digitalización a todos los niveles condiciona el devenir de todas las formas de criminalidad.

Desde hace varias décadas se han implementado diferentes diligencias de investigación tecnológicas, sobre las que se han aprobado diversas normas y leyes en todos los niveles territoriales y, de igual modo, han condicionado que los altos tribunales se pronuncien sobre la legalidad e idoneidad de su adopción. Sin embargo, las tradicionales investigaciones tecnológicas, en las que podía mediar una interceptación de las comunicaciones o un registro de dispositivos directo, presentan algunas insuficiencias para poder hacer frente a las actuales formas de criminalidad, ya que los delincuentes están incorporando todos los avances técnicos y aprovechando todas las oportunidades existentes. Debido a ello, se analiza en el presente estudio la posibilidad de que los operadores jurídicos recurran a formas de investigación novedosas, que han sido previstas en la Ley española, pero cuya adopción práctica no se ha materializado.

Es relevante destacar que debido a la transnacionalidad delictiva que caracteriza a la ciberdelincuencia grave y organizada debemos complementar el análisis con el estudio de la viabilidad de incluir la utilización de este tipo de medidas novedosas en el marco de instrumentos de cooperación, ya que a nivel estatal no se podrá abarcar la totalidad de la investigación. Esta cuestión también pone de manifiesto la necesaria aproximación de ordenamientos jurídicos y el refuerzo de la confianza en la UE.

Asimismo, en el marco de estas nuevas diligencias de investigación se debe valorar la posible incorporación a corto plazo de las últimas tecnologías emergentes, ya que podrían favorecer la actuación práctica de las autoridades policiales y judiciales. Estos avances técnicos podrían contribuir a mejorar la adopción de medidas como el registro remoto, aunque no se deberán utilizar de un modo arbitrario porque nos encontramos ante una diligencia muy invasiva y se pueden comprometer diversos derechos fundamentales; con ello, la eficacia de la medida y del proceso.

Los diferentes operadores jurídicos se pueden encontrar con obstáculos ante los que los instrumentos y la legislación vigente no les permitan responder, ya que muchas de las herramientas no han considerado la evolución tecnológica y existe el riesgo de que queden obsoletas. En contraposición la adaptación de los ciberdelincuentes a todas las ventajas que les puedan ofrecer las TIC no cesa, ni tampoco lo hacen los ciberataques, que pueden atentar contra múltiples víctimas y contra bienes jurídicos como la vida o la integridad, como es el caso de los que se cometen contra los servicios esenciales estatal.

2. OBJETIVO GENERAL Y ESPECÍFICOS

Considerando las cuestiones expuestas, el objetivo general de la tesis doctoral es analizar la viabilidad de la utilización de las diligencias de investigación tecnológicas novedosas en la lucha contra las formas graves de ciberdelincuencia que se dirigen contra las infraestructuras críticas y estratégicas, focalizando la atención en el registro remoto como medida tecnológica de la que todavía no existe una consolidada trayectoria práctica.

No obstante, junto con este objetivo general, se presentan algunos objetivos específicos que serán enumerados a continuación:

— Estudiar el desarrollo y la evolución de Internet. Especial atención a la masiva utilización de la red y al aumento de la conectividad global como factores que influyen en la oportunidad delictiva en el ciberespacio.

— Evaluar la influencia del factor tecnológico en la delincuencia grave, en particular, en el desarrollo de la ciberdelincuencia. Especial atención a los ciberdelitos puros y a los ciberataques contra infraestructuras críticas.

— Analizar la previsión legal de los diferentes tipos penales en los que pueden enmarcarse los ciberdelitos. Especial atención a los ciberataques contra infraestructuras críticas.

— Identificar la realidad actual de los ataques cibernéticos. Analizar todas las modalidades delictivas que pueden ser utilizadas y el contexto actual de la ciberdelincuencia para favorecer la detección y persecución de los delitos objeto de estudio en la presente investigación.

— Recopilar las características del ciberespacio con el objetivo de identificar los obstáculos que se van a presentar para las autoridades policiales y judiciales competentes en la investigación.

— Examinar los instrumentos de cooperación policial y judicial disponibles para la investigación transnacional de la ciberdelincuencia.

— Estudiar la incorporación del factor tecnológico en las herramientas de cooperación europeas e internacionales. Especial atención a las medidas de investigación tecnológicas.

— Analizar los requisitos y características básicas de las diligencias de investigación tecnológicas. Especial atención a la diligencia de registro remoto prevista en la LECrim española.

— Examinar la licitud de la práctica de registros remotos para la investigación nacional de ciberdelincuencia grave; en particular, los ciberataques que se dirigen contra infraestructuras críticas y estratégicas.

— Identificar las exigencias legales que se deben incorporar a todos los ordenamientos jurídicos nacionales para favorecer la lucha contra la ciberdelincuencia grave.

— Analizar los derechos y garantías que deben preverse en la legislación de un modo paralelo a la diligencia de investigación tecnológica para asegurar la eficacia de la medida.

— Comparar la diligencia de registro remoto con otras medidas tecnológicas de investigación.

— Evaluar la viabilidad de la práctica de diligencias de investigación novedosas, como el registro remoto, en el marco de instrumentos de cooperación europeos e internacionales.

— Estudiar la adecuación de las propuestas del presente estudio a los principios exigidos a nivel nacional para la investigación tecnológica y a nivel supranacional para la cooperación policial y judicial.

— Examinar la posibilidad de incorporar las últimas tecnologías disruptivas, en particular la IA, a la investigación policial y judicial como medidas para fortalecer la lucha contra los ciberataques graves.

— Analizar la vinculación entre la adecuación de la investigación procesal y la seguridad nacional.

— Emitir propuestas de *lege ferenda* que favorezcan una investigación de los ciberdelitos graves respetuosa de las garantías constitucionales; incluyendo los ciberataques que se dirigen contra las infraestructuras críticas y estratégicas.

3. METODOLOGÍA: CIENCIAS JURÍDICAS

Para la consecución de los objetivos señalados se ha seguido una metodología propia de las ciencias jurídicas. Esta metodología se constituye por varias fases en las que se realiza búsqueda, recopilación, selección, análisis y comparación crítica de la información procedente de diferentes soportes físicos y digitales.

En primer lugar, se ha requerido el análisis y seguimiento de los informes que se han elaborado durante los últimos años por entidades públicas y privadas en materia de delincuencia grave, organizada y ciberdelincuencia. Esta metodología se ha complementado con la reflexión sobre noticias de actualidad, ya que el carácter innovador de la investigación requería un seguimiento continuo del contexto de la ciberdelincuencia.

En segundo lugar, ha sido necesaria la consulta de normativa aprobada en materia de ciberdelitos, de investigación procesal, cooperación judicial y policial internacional, así como otras leyes específicas relevantes para la temática objeto de estudio. Lo cual ha requerido analizar normativa vigente y derogada, con el objetivo de poder realizar un análisis crítico de la tendencia que existe en los diferentes niveles territoriales.

En tercer lugar, como principal objeto de estudio para el desarrollo de la presente tesis doctoral, se ha recurrido a bibliografía que recoge estudios de expertos y jóvenes investigadores, ya que es fundamental incluir diferentes estudios doctrinales. Se ha analizado bibliografía general en el ámbito del Derecho procesal y, con carácter específico, se han consultado artículos, capítulos de libro y monografías específicas en materia de ciberdelincuencia, delincuencia grave e investigación tecnológica.

En cuarto lugar, ha sido muy importante recurrir a jurisprudencia de los altos tribunales, principalmente del TEDH, el Tribunal Supremo y el Tribunal Constitucional, ya que la práctica de diligencias tecnológicas tradicionales es óptima para realizar una evaluación previa de la futura incorporación práctica del registro remoto objeto de estudio.

En quinto lugar, para desarrollar una investigación sobre un tema tan delicado, la investigación invasiva sobre los derechos fundamentales, ha sido fundamental la participación en eventos y congresos nacionales e internacionales que han favorecido la formación en el ámbito procesal y en las materias que han sido objeto de estudio en la tesis doctoral.

De igual modo, en sexto lugar, la participación en proyectos nacionales, regionales y de la de Universidad de Salamanca ha contribuido a fortalecer el análisis crítico respecto a la investigación tecnológica. Estas participaciones se deben a la pertenencia de la autora al Grupo de investigación reconocido IUDICIUM: Grupo de estudios procesales de la Universidad de Salamanca, ya que ha permitido el contacto y el trabajo con profesionales expertos en la materia, que no cesan su actividad de investigación en materia de TIC y Derecho procesal.

Por último, se ha complementado la metodología previamente expuesta con dos estancias de investigación predoctorales en universidades europeas; la Universidad de Gante, *Gent University*, y la Universidad de Messina, *Università degli Studi di Messina*.

4. ESTRUCTURA

Para realizar un estudio exhaustivo de la investigación de los ciberataques graves, en particular aquellos que se dirigen contra las infraestructuras críticas y estratégicas, se ha dividido la presente investigación en cinco capítulos:

En el primer capítulo se analiza la evolución de Internet, así como la consolidación del espacio cibernético que existe en la actualidad. En esta primera parte se estudia cómo el factor tecnológico ha sido determinante en la evolución delictiva; desencadenando la aparición de nuevas modalidades delictivas, entre las que se han destacado los ciberataques contra infraestructuras críticas y estratégicas. En este sentido, la tecnificación de la delincuencia grave debido a la implementación de las TIC en los *modus operandi* ha requerido la respuesta desde el Derecho penal y desde el Derecho procesal, la cual también se expone en este momento. Se delimita, en este capítulo, el contexto y la realidad actual para favorecer el desarrollo de un estudio objetivo sobre la utilización de las diligencias de investigación tecnológicas en la actualidad.

En el segundo capítulo, teniendo presente algunas de las principales características del ciberespacio y, por consiguiente, de la ciberdelincuencia, se analiza cómo la comunidad internacional y el legislador a nivel estatal han tenido que incorporar el factor tecnológico a los instrumentos de cooperación judicial internacional. En este caso, convirtiéndose en una herramienta esencial para las autoridades policiales y judiciales que son competentes en la detección y represión de este tipo de criminalidad. Se examina

la doble tendencia que se ha seguido, por un lado, con la implementación de herramientas que favorezcan las investigaciones transfronterizas y, por otro lado, mediante la creación de instituciones, centros y redes ad hoc para la lucha contra la delincuencia grave; tipología delictiva en la que se incluyen los ciberataques objeto de estudio.

En el tercer capítulo se analiza cómo el legislador español ha incluido la investigación tecnológica al ordenamiento jurídico español. En este momento, se acota la investigación al estudio de los diferentes presupuestos y requisitos que se deben contemplar para la adopción de una diligencia de registro remoto con todas las garantías. Se centra la atención en la actual regulación de la LECrim, pero se incluyen las previsiones de las Circulares de la Fiscalía General del Estado, así como las propuestas que están en fase de evaluación. Asimismo, como nos encontramos ante una diligencia que todavía no se ha consolidado a nivel estatal, se atiende a las respuestas que se han ofrecido por el legislador en el caso de diligencias tecnológicas tradicionales que son próximas al registro remoto.

En el cuarto capítulo se continúan teniendo presentes todas las diligencias de investigación que, de algún modo, están próximas o pueden complementar a la medida del registro remoto. En este caso, se atiende a los derechos y garantías que deben protegerse para garantizar la efectividad de la diligencia y, por consiguiente, del proceso penal. Se manifiesta la importancia de regular de un modo exhaustivo y de practicar con cautela una medida de las características del registro remoto, ya que la injerencia desproporcionada sobre derechos fundamentales puede comprometer la represión de un ciberataque grave.

Por último, en el quinto capítulo, se ha estudiado de un modo más específico la viabilidad de la adopción de un registro remoto para la investigación de los ciberataques que se dirigen contra infraestructuras críticas y estratégicas. En este momento, de un modo crítico, se analizan las similitudes y diferencias existentes entre el registro remoto y otras diligencias tecnológicas de investigación, con el objetivo de valorar la posible utilización o exclusión de su adopción ante los delitos objeto de estudio. De igual modo, en relación con el estudio realizado en el segundo capítulo, se analiza la posible inclusión de diligencias de registro remoto o de similares características en instrumentos de cooperación policial y judicial internacional, con el objetivo de minimizar los obstáculos que se encuentran en las investigaciones transnacionales más complejas. En este capítulo se persigue dar respuesta a algunos de los principales interrogantes del presente estudio;

¿se están utilizando las medidas tecnológicas idóneas? ¿se han previsto diligencias de investigación novedosas que permitan responder a los avances técnicos de los delincuentes? ¿existen herramientas que favorezcan su adopción en el proceso penal con todas las garantías?, entre otros.

Para la realización de un estudio integral en los cinco capítulos citados se atiende a dos niveles supranacionales que son determinantes para el desarrollo normativo nacional. Por un lado, se encuentran los instrumentos aprobados en el marco de las Naciones Unidas y, por otro, los aprobados a nivel regional, centrando la atención en el Consejo de Europa y en la Unión Europea, destacando la copiosa actividad normativa de esta última.

En este mismo sentido, el estudio se enmarca principalmente a partir del año 2000, fecha relevante por ser coincidente con el comienzo de la principal actividad legislativa al respecto, iniciándose con la destacable Convención de Palermo en materia de delincuencia organizada y con el Convenio de Budapest en 2001, ambas desarrolladas en un contexto supranacional – en el marco de Naciones Unidas y del Consejo de Europa, respectivamente-. De igual modo, a nivel europeo y coincidente con este periodo temporal, encontramos como hitos en materia de cooperación el Consejo Europeo de Tampere y el Tratado de Lisboa, con la consiguiente repercusión de estos instrumentos a nivel nacional, con ratificaciones y trasposiciones en España. No obstante, a pesar de que los instrumentos se han desarrollado principalmente a partir del año 2000, debe analizarse brevemente la consolidación de los principios de cooperación, así como la homogeneización de las leyes procesales vigentes en los diferentes Estados con carácter previo, ya que de este modo se asegurará la respuesta de la comunidad internacional respecto a los ciberataques graves contra infraestructuras críticas.

5. RIESGOS DE LA INVESTIGACIÓN

Por otro lado, es oportuno identificar la problemática que podría presentarse en una investigación de estas características, atendiendo principalmente a la rápida evolución de la tecnología y al reciente desarrollo legislativo en algunas materias que son objeto de estudio. Asimismo, en particular, el alto grado de innovación de la temática seleccionada como objeto de estudio podría haber obstaculizado la realización del estudio, ya que también pueden aparecer algunas dificultades que se deriven de la falta

de experiencia práctica en la lucha contra estas modalidades delictivas, así como derivadas de la falta de consolidación de la diligencia de investigación del registro remoto.

En primer lugar, son muy pocos los ciberdelitos que se investigan en la actualidad, minimizándose la cifra de aquellos crímenes que finalmente se consiguen esclarecer. Además, el aumento de las amenazas que se dirigen contra las infraestructuras críticas y estratégicas se ha producido durante los últimos años y, por consiguiente, se ha profundizado la investigación en este ámbito recientemente. Estas cuestiones obligarán a realizar una cuidadosa investigación de los últimos informes y de las recientes manifestaciones sobre este fenómeno para poder realizar un análisis objetivo y actualizado de esta tipología delictiva.

En segundo lugar, el registro remoto, aunque ha sido legalmente previsto en la Ley de Enjuiciamiento Criminal a partir de la reforma operada en el año 2015, su implementación práctica no ha tenido lugar en España, no habiéndose consolidado la trayectoria de esta diligencia.

Asimismo, la acelerada digitalización que se está experimentando, desde que se ha iniciado la pandemia, provoca que nos encontremos ante una realidad cambiante que puede obstaculizar la dinámica de estudio. De igual modo, la aprobación de documentos, informes y de normativa diversa en la materia no cesa, lo cual también dificulta la exhaustiva recopilación de información para el desarrollo de la presente tesis doctoral. No obstante, el trabajo de investigación continuado, la citada pertenencia al grupo de investigación IUDIUCIUM y la participación y organización de eventos en esta temática favorece la obtención de un resultado con las principales novedades legislativas y la información más relevante en la materia.

CONCLUSIONES

Las ventajas que tiene la creación y utilización del ciberespacio y que son aprovechadas por los ciberdelincuentes, se presentan como grandes dificultades para los investigadores. Debido a ello, con el fin de practicar investigaciones eficaces en el marco de un proceso penal los operadores jurídicos deben contar con instrumentos tecnológicos que les permitan sortear los obstáculos que encuentren en el ejercicio de sus competencias. Asimismo, también es necesario desarrollar herramientas de cooperación y la previsión de diligencias que favorezcan las investigaciones transfronterizas, ya que la ausencia de fronteras y la transnacionalidad delictiva las van a convertir en una pieza clave para la lucha contra la ciberdelincuencia grave.

En este sentido, para finalizar la presente investigación formulamos las conclusiones que se extraen de los aportes obtenidos, como resultado del trabajo crítico y del análisis que se ha realizado en los cinco capítulos precedentes, atendiendo a los objetivos de trabajo planteados y, en consecuencia, proponiendo las vías de actuación que consideramos más adecuadas para enfrentar el fenómeno delictivo objeto de estudio:

PRIMERA. Con carácter general, se ha identificado la necesidad de tipificar los ciberdelitos, aproximar los ordenamientos jurídicos y armonizar la legislación en esta materia, con el objetivo de conseguir procesos penales eficaces; ya que se ha detectado en el marco internacional la problemática derivada de los paraísos cibernéticos y las dificultades ligadas a la investigación de este tipo de conductas. Por lo tanto, el reconocimiento y la tipificación de los ciberdelitos en todos los Estados va a determinar la investigación de estos hechos delictivos.

SEGUNDA. En las últimas décadas se ha apostado por la digitalización de las infraestructuras críticas y estratégicas para favorecer su funcionamiento, control y

accesibilidad, lo que ha ocasionado que sean consideradas como principales objetivos de los ciberataques; situación que se ha agravado en los últimos años por motivo de la COVID-19. Debido a ello, se ha previsto en los diferentes niveles territoriales el particular desvalor de las actividades delictivas que se dirigen contra este tipo de entidades. La trasposición de los mínimos recogidos en el ámbito del Derecho penal en la UE facilita la cooperación judicial internacional y favorece la respuesta procesal a nivel nacional, incluyendo la justificación de la adopción de las medidas de investigación. En este sentido debería evolucionar la legislación a nivel global, favoreciendo la represión internacional de estas modalidades delictivas graves.

TERCERA. En todos los niveles territoriales se debe garantizar una Internet segura, la seguridad nacional y los derechos de los ciudadanos que pueden ser víctimas de los ciberataques, pero la limitación de los derechos fundamentales de los investigados debe estar prevista en la ley de un modo exhaustivo para su protección y control, garantizando la seguridad jurídica y evitando la aplicación de preceptos obsoletos por analogía. En España, a partir de la reforma operada por la Ley Orgánica 13/2015, de 5 de octubre, aunque se ha logrado un avance muy importante para nuestro ordenamiento jurídico ya que prevé las diligencias de investigación tecnológicas y favorece la represión actual de múltiples formas de criminalidad grave, también se ha detectado que era necesaria una regulación más pormenorizada, lo cual debería ser considerado por el legislador para la elaboración de futuras propuestas o anteproyectos de la Ley de Enjuiciamiento Criminal. Por lo tanto, con carácter general, existe la necesidad de regular de un modo preciso y con una mejor calidad las diligencias de investigación tecnológicas que suponen la injerencia de derechos fundamentales.

CUARTA. La evolución de la tecnología ha condicionado la modificación e incluso la creación de diligencias de investigación tecnológicas. Esta adecuación a los avances técnicos también se ha acelerado por la imposibilidad de responder ante las nuevas formas de criminalidad. En este sentido, se creó el registro remoto previsto en la LECrim española, medida que va a depender directamente de la tecnología. Sin embargo, no se ha consolidado y estandarizado su utilización lo cual puede plantear dificultades en las investigaciones complejas del ciberespacio. Por lo tanto, los operadores jurídicos deben apostar no solo por la previsión de diligencias de monitorización remota sino también por su implementación práctica objetiva con todas las garantías. Para todo ello será necesario

contar con suficientes recursos técnicos, capacitación y legislación adaptada a la nueva realidad tecnológica.

QUINTA. En particular, en España, como legislación pionera que debe ser considerada por otros Estados para aproximar los diferentes ordenamientos jurídicos, se han identificado algunas carencias respecto al modo de actuación, a los delitos en los que se permite la práctica del registro remoto y en relación con la falta de previsión de su adopción urgente por otras autoridades no judiciales. En primer lugar, no se ha previsto -y, por ello, proponemos su incorporación- las diferentes técnicas de acceso que podían haber sido incluidas de un modo amplio en la LECrim; en segundo lugar, se debe considerar que las TIC están presentes en la mayoría de las actividades delictivas, aunque no se cometan a través de ellas, por lo que no se deberían dejar al margen del *numerus clausus* actual algunas formas graves de criminalidad; y, por último, en tercer lugar, se ha detectado que la volatilidad de las evidencias, el alcance de los ataques cibernéticos graves y las dificultades para determinar la autoría pueden requerir una actuación inicial urgente, cuestión que no ha sido prevista por el legislador español, aun cuando ha sido avalada a nivel nacional y europeo para la práctica de otras diligencias de investigación tecnológicas próximas al registro remoto, siempre que estuviera en riesgo la efectividad del proceso penal.

SEXTA. En relación con la atribución de la competencia, en la mayoría de los casos, los jueces de instrucción serán los que deberán dictar el auto para la adopción de un registro remoto en España. Sin embargo, encontramos bastantes problemas en este ámbito; como los ligados a la atribución de la jurisdicción. Esta cuestión parece resuelta desde hace décadas cuando el Tribunal Supremo estableció la determinación de la jurisdicción en base al principio de ubicuidad, no obstante, podría agravarse ante ciberdelitos complejos en los que estén involucrados múltiples Estados, autores y víctimas. En el caso de que encontremos ante casos complejos en simultánea investigación puede ser necesario recurrir a herramientas de investigación conjunta; por ejemplo, los equipos conjuntos de investigación son idóneos para actuar ante este tipo de conflictos. Debido a ello, los ordenamientos jurídicos estatales deben estar preparados para dar respuesta a esta problemática.

SÉPTIMA. El alcance del registro remoto es una de las principales características que individualiza a esta diligencia respecto a otras medidas tecnológicas; la posibilidad de monitorizar el equipo permite prever que, ante la evolución de las comunicaciones y de

las tecnologías de anonimización y cifrado, la opción de recurrir a esta medida se va a convertir en una frecuente necesidad. En casos complejos se ha identificado que se requerirá la realización de grandes intromisiones que solo se pueden llevar a cabo con un registro de estas características. Este alcance, asimismo, puede evitar que los conocimientos de los delincuentes, respecto a diligencias tradicionales, obstaculicen la investigación, ya que el equipo o los dispositivos deben emplearse necesariamente para cometer el ataque; por el contrario, pueden utilizar lenguaje en clave o evitar las vías de comunicación tradicionales que podrían ofrecer información practicando diligencias menos invasivas. Por lo tanto, podemos encontrarnos con que la única opción para esclarecer algunos ciberataques va a ser el acceso integral que no se puede alcanzar por medio de otras diligencias de investigación; como con la interceptación de las comunicaciones.

OCTAVA. La escueta previsión en la legislación de las garantías relativas a la autenticidad y a la integridad de la prueba electrónica, obtenida a través de un registro remoto, no sería en la actualidad un motivo de peso para excluir la adopción de esta diligencia en España. Aunque sería recomendable su regulación exhaustiva en la LECrim, la Circular 5/2019 ha expuesto los métodos a seguir para garantizar que el material probatorio obtenido no sea excluido y evitar que se comprometa de este modo la eficacia de la medida. No existiría en este caso, al menos por el momento, un sistema estandarizado y centralizado como SITEL, pero existen medios que permitirían mantener el carácter secreto de la medida hasta su finalización y garantizar la autenticidad, la integridad y la mismidad de prueba. Sin embargo, debe valorarse la detallada previsión de estas cuestiones en los diferentes ordenamientos jurídicos nacionales que vayan a incluir esta diligencia en su articulado.

NOVENA. Debido a la complejidad de algunas investigaciones las diligencias tecnológicas se pueden combinar con otras medidas. En particular, se podrán complementar con otras que fueron desarrolladas hace décadas para la práctica de investigaciones en el medio *offline,* como la entrada y registro en el domicilio. En este sentido, se ha detectado la necesidad de vincular el registro remoto al posible acceso físico que permita la instalación de un *software* o la obtención de claves en aras a practicar la adopción de un registro remoto, lo que puede facilitar o esquivar algunas dificultades técnicas ligadas a este tipo de diligencia. Se ha identificado que otras diligencias sí se han

vinculado a la entrada y registro, cuestión que sería oportuno que el legislador valorase en el caso de la medida de investigación objeto de estudio.

DÉCIMA. La diligencia del registro remoto que regula la LECrim española sería idónea para la investigación de ciberataques graves que se comentan contra las infraestructuras críticas. En todo caso, este tipo de ataques se van a poder enmarcar en los delitos en los que se permite practicar este registro y el *modus operandi* de los ciberdelitos puros estará siempre incluido, sin perjuicio de que además se cumplan otros presupuestos y de que el juez deba valorar que nos encontramos ante hechos graves en los que es necesario recurrir a su adopción. Asimismo, es claro que nos encontramos ante delitos graves, de gran trascendencia social, que se sirven de la tecnología y que su ejecución puede atentar contra múltiples bienes jurídicos o contra la seguridad estatal. Debido a ello, va a ser relativamente fácil motivar que la adopción de esta medida de investigación va a ser proporcionada, idónea y necesaria, ya que será difícil encontrar situaciones en las que el juez no pueda justificar objetivamente el cumplimiento de todas las exigencias legales previstas en la LECrim. No obstante, la autoridad judicial deberá valorar todas las circunstancias de cada caso concreto.

UNDÉCIMA. En definitiva, la previsión legal del registro remoto debe ser exhaustiva, incluyendo la necesidad del cumplimiento de todos los requisitos y exigencias legales que aseguren su práctica con todas las garantías, salvaguardando bajo control judicial todos los derechos del investigado, aunque la práctica de las diligencias tecnológicas suponga su limitación. En este sentido se han ido previendo las medidas tecnológicas en los ordenamientos jurídicos europeos, sin embargo se insta a la previsión detallada y exacta de diligencias que permitan un acceso integral remoto, ya que en la actualidad destaca la exhaustividad de la previsión de la interceptación de las comunicaciones en atención a su larga trayectoria; cuya normativa y jurisprudencia puede considerarse como base para el desarrollo de nuevas medidas de investigación.

DUODÉCIMA. En los diferentes niveles territoriales se han reconocido las dificultades inherentes a la investigación de la ciberdelincuencia y la necesidad de garantizar la eficacia de las diligencias de investigación tecnológicas, por ello el legislador y los tribunales han optado por retrasar o limitar el ejercicio de algunos derechos básicos del proceso penal. En particular, el carácter secreto que está ligado a la ejecución eficaz de estas medidas exigirá que se posponga el momento de información y de ejercicio de los derechos de las personas investigadas. Por esta razón, la regulación de este tipo de

diligencias de investigación tecnológicas invasivas debe, necesariamente, incluir todo un elenco de garantías que controlen la práctica de la medida y salvaguarden los derechos del investigado; los cuales no le serán reconocidos hasta que finalice la práctica de la diligencia pero que se protegerán desde su inicio con la exhaustiva previsión de requisitos y medios de control.

DECIMOTERCERA. Los mínimos que se han previsto en la normativa de la Unión Europea en materia de derechos y garantías que deben reconocerse a las personas investigadas han conseguido asegurar la eficacia de las investigaciones que se practican a nivel nacional, pero además han contribuido a la armonización de los ordenamientos jurídicos y, en este sentido, a reforzar la confianza y, por consiguiente, a mejorar la eficacia de la cooperación judicial a nivel de la UE. En este sentido deberían evolucionar todos los ordenamientos jurídicos a nivel global, para favorecer el funcionamiento de los procesos penales en general y, en particular, para mejorar la cooperación internacional cuando se recurre a ella para desarrollar investigaciones tecnológicas transfronterizas.

DECIMOCUARTA. El factor tecnológico se ha incorporado a los instrumentos de cooperación, en los que es destacable la previsión legal de medidas tecnológicas de investigación para hacer frente a los casos de delincuencia más complejos y de mayor gravedad; entre los que se identifican algunos ciberataques graves. Con carácter general, las TIC han revolucionado los parámetros de la cooperación y colaboración tradicional, la tendencia seguida en las últimas décadas parece condicionar el desarrollo de herramientas, centros y agencias que permitan mejorar los procesos penales. En definitiva, la tecnología se configura como un recurso necesario para la investigación transfronteriza en el ciberespacio, pero, sin embargo, se ha detectado que existe un déficit respecto a la previsión de novedosas diligencias de investigación que puedan contribuir a hacer frente a la tecnificación y evolución actual del crimen.

DECIMOQUINTA. Para poder adoptar registros remotos en el contexto de la cooperación europea, se contemplan dos posibilidades: por un lado, sería posible incluir el registro remoto en la Directiva que regula la Orden Europea de Investigación, con la consecuente ampliación de su catálogo de medidas. Y, por otro lado, considerando las particularidades de la investigación en el ciberespacio y las características de los ciberdelitos graves complejos, se valora la posibilidad de que el registro remoto se incorpore a una nueva Directiva que incluya la previsión legal de nuevas órdenes europeas de investigación tecnológica, la DOEIT propuesta. El registro remoto está muy próximo

a la interceptación de las comunicaciones por lo que aprovechar el instrumento preexistente sería una solución más rápida, sin embargo la aprobación de instrumentos específicos para mejorar la exhaustiva previsión legal de la investigación tecnológica sería una respuesta a largo plazo más acertada; si consideramos la globalización y la evolución de la tecnología, este tipo de diligencias, como el registro remoto, se van a convertir en un elemento esencial.

DECIMOSEXTA. El registro remoto también puede ser necesario en el marco de investigaciones internacionales, con terceros Estados que no sean miembros de la UE. En este sentido, se ha evaluado la posibilidad de incluir una medida de registro remoto, que permita la monitorización y el acceso integral, en el articulado del Convenio de Budapest. Su incorporación en este instrumento sería idónea debido a que el Convenio es referente en materia de investigación tecnológica de la ciberdelincuencia y, además, se podría materializar a medio plazo, ya que se está trabajando en un segundo protocolo que persigue mejorar las herramientas procesales recogidas en su articulado. Este Convenio podría ser de gran utilidad ya que se constituye como base jurídica para la práctica de investigaciones transnacionales cuando no existen otros tratados, acuerdos o normativa que incluyan con mayor exhaustividad o a un nivel territorial más reducido las previsiones necesarias para practicar las investigaciones en el ciberespacio.

DECIMOSÉPTIMA. La investigación conjunta que se realiza en los ECIs se podrá beneficiar del registro remoto, ya que la normativa permite el recurso a otras herramientas de cooperación siempre que no persigan el mismo objetivo. En este sentido, se podría recurrir a la emisión de una OEI para la práctica de un registro remoto en otro Estado miembro no parte del ECI, si se incluyera esta medida en el articulado de la DOEI o de otra nueva Directiva de similares características. De igual modo, se podría recurrir a herramientas internacionales de cooperación como al citado Convenio de Budapest para la práctica del registro remoto en un tercer Estado no miembro de la UE, si también se incluyera este tipo de medida en el articulado de Convenios internacionales. Asimismo, el registro remoto se podría practicar en los Estados miembros del ECI sin la necesidad de recurrir a otras herramientas. No obstante, de nuevo para que esta propuesta pueda aplicarse debe regularse este tipo de registro de un modo exhaustivo y con suficientes garantías en todos los ordenamientos jurídicos nacionales, incluso más allá de las fronteras europeas.

DECIMOCTAVA. La propuesta de Reglamento para la conservación y entrega de pruebas electrónicas en la UE se presenta para dar respuesta a algunos de los principales obstáculos que encontramos en el marco de la investigación de la ciberdelincuencia compleja: la colaboración de los prestadores de servicios y la obtención de prueba electrónica en el ciberespacio. En esta propuesta se han previsto todas las garantías que se han incorporado en los instrumentos preexistentes y que habilitan a la práctica de investigaciones tecnológicas transfronterizas, como en la DOEI, y, debido a ello, va a poder complementar las herramientas vigentes. Estas órdenes van a favorecer la investigación de ciberdelitos, pero también podrán contribuir a la eficacia de las diligencias como el registro remoto, previéndose tanto con carácter previo como complementario a este. Además, no supone la regulación de diligencias iguales ya que el alcance del registro a distancia continuará siendo mayor y necesario para realizar investigaciones complejas. En definitiva, se debe acelerar la aprobación de este instrumento con el objetivo de agilizar y mejorar la investigación transnacional, así como para fortalecer en algunas ocasiones la adopción del registro remoto, tanto a nivel nacional pudiendo ser necesario recurrir a información de proveedores de servicios que se encuentran fuera del territorio nacional, como a nivel internacional, en el marco de alguna de las herramientas de cooperación analizadas o propuestas.

DECIMONOVENA. La individualización del tratamiento de la prueba electrónica, en un Reglamento específico, nos permite apoyar la propuesta relativa a la creación de la DOEIT, ya que refleja que la comunidad internacional y los legisladores de los diferentes niveles territoriales están identificando las particularidades de la investigación tecnológica en el ciberespacio y, de un modo paralelo, apuestan por prever instrumentos específicos más eficaces.

VIGÉSIMA. Para garantizar el funcionamiento de las herramientas de cooperación que se han señalado y que podrían incluir la práctica del registro remoto, no solo va a ser necesario que se prevea con “calidad de ley” la diligencia a nivel nacional de un modo aislado, sino que se va a requerir la trasposición, por un lado, de la normativa supranacional que permite armonizar los ordenamientos jurídicos y, por otro lado, de aquella que favorece el recurso a este tipo de instrumentos de cooperación. Para evitar la denegación de las órdenes europeas o el rechazo de la práctica del registro remoto va a ser necesario prever todos los presupuestos, incluyendo los delitos específicos para los que esta diligencia compleja e invasiva se puede adoptar en el Estado en cuestión, y

también se va a requerir que exista una regulación exhaustiva sobre el procedimiento a seguir a nivel nacional para la emisión y ejecución de órdenes o bien para la utilización de otras herramientas de cooperación.

VIGESIMOPRIMERA. Las tecnologías disruptivas, en particular, los dispositivos que se sirven de la tecnología IoT van a almacenar y procesar grandes cantidades de datos. Dicha característica ya ha condicionado que se utilice en sede judicial en el marco de una investigación de un delito grave. Por lo tanto, hay que considerar que la digitalización a todos los niveles de la sociedad y el significativo aumento de la conectividad va a presentar también oportunidades a los investigadores, los cuales van a poder recurrir, como en estos casos, a nuevas fuentes de datos. Sin perjuicio de la necesaria salvaguarda de los derechos, principios y garantías inherentes a todo proceso penal.

VIGESIMOSEGUNDA. En la propuesta de Reglamento para establecer normas armonizadas sobre IA destaca que se han considerado como sistemas de IA de alto riesgo los sistemas que utilizan esta tecnología en los procesos penales. Asimismo, se ha previsto la delincuencia grave, en la que se incluyen los ataques contra infraestructuras críticas, como excepción para adoptar medidas de investigación que se sirven de la IA; como la identificación biométrica en tiempo real en espacio públicos que, con carácter general, debe estar prohibida. Por lo tanto, el legislador parece optar por permitir la utilización de la IA en el marco de la investigación de formas de delincuencia graves. Además, se señala que deberán cumplirse algunos requisitos para proceder a su adopción: el cumplimiento de los principios de proporcionalidad o necesidad, la autorización judicial y la determinación del alcance de la medida. En este sentido, considerando las garantías previstas para la adopción del registro remoto, todo indica que este tipo de tecnología podrá ser utilizada cuando concurran las circunstancias necesarias para autorizar dicho tipo de registro. Sin perjuicio de que esta propuesta ya podría haber sido aprovechada para valorar más formas de investigación que se pueden servir de la IA, más allá de la identificación mencionada.

VIGESIMOTERCERA. La incorporación de sistemas que utilicen IA al proceso penal está siendo objeto de estudio en los últimos años y ya se ha incorporado en algunos países como herramienta auxiliar en las administraciones de justicia. En España podemos plantear su utilización en diferentes momentos procesales, pero atendiendo al objeto de estudio destacamos tres opciones para el uso de esta tecnología en la investigación de un delito grave. En este sentido, debemos señalar que la IA se va a poder incorporar como

tecnología que auxilie a las autoridades policiales en el ejercicio de sus funciones previas a la adopción de una medida de investigación, para que mejore la práctica de las diligencias de investigación tecnológicas existentes o podrá permitir la creación de nuevas medidas que se desarrollarán en futuro por motivo de la evolución de la IA.

VIGESIMOCUARTA. A corto plazo, se podría utilizar la previsión legal del registro remoto y que la IA perfeccionara su aplicación. No obstante, a largo plazo, sería conveniente incorporar de un modo exhaustivo en la legislación nacional la utilización de esta tecnología, ya que sus múltiples funciones la convierten en un instrumento muy útil para los operadores jurídicos, pero muy peligrosa debido a su particular carácter invasivo. En este sentido, cuando se utilice esta tecnología para favorecer la práctica de una diligencia de investigación tecnológica a nivel nacional o internacional, no solo deberá la autoridad judicial acogerse a los requisitos y principios previstos en el marco jurídico que regula las medidas de investigación, sino que también se deberá atender a los que garantizan un control en la programación y en el funcionamiento de la IA: no discriminación algorítmica, transparencia, explicabilidad, etc.

VIGESIMOQUINTA. Asimismo, para incluir la regulación de los sistemas de IA no solo existe la posibilidad de que se lleve a cabo la previsión legal independiente en los diferentes Estados, sino que se prevé que los mínimos para incorporar la IA a los ordenamientos jurídicos nacionales emanen de un instrumento de cooperación europeo o internacional, garantizándose en este último caso una mayor armonización. En este sentido, debemos destacar que su incorporación no debe demorarse en el tiempo ya que se ha identificado la inminente introducción de esta tecnología a los *modus operandi* que emplean los delincuentes.

VIGESIMOSEXTA. La ciberdelincuencia grave y, en particular, los ciberataques que comprometen el funcionamiento de las infraestructuras críticas son hechos delictivos que se han identificado como amenazas que afectan a la seguridad nacional e internacional. En este sentido, se ha considerado la tecnología como un factor clave para hacer frente a las ciberamenazas y garantizar un uso seguro del ciberespacio. En definitiva, la actuación que realizan las autoridades competentes en el marco de un proceso penal incoado por la comisión de ciberdelitos graves forma parte de las líneas de respuesta estratégica. Las actuaciones realizadas, a nivel nacional e internacional, en aras de establecer y armonizar un marco jurídico estatal que prevea los recursos, la capacitación y las competencias necesarias para poder investigar y reprimir estas modalidades delictivas, son necesarias

para actuar contra los ciberdelitos y garantizar la ciberseguridad que determinará, en último término, la consecución de la seguridad internacional.

VIGESIMOSÉPTIMA. La necesidad de regular exhaustivamente modernas herramientas tecnológicas, que se sirven de los nuevos desarrollos técnicos, se ha convertido en una necesidad, siendo la tendencia que ha seguido la comunidad internacional y que no debería paralizarse en todos los niveles territoriales. Además, se ha detectado que la previsión de herramientas novedosas con las características del registro remoto en los ordenamientos jurídicos estatales será fundamental para su adopción tanto a nivel nacional como en el marco de herramientas de cooperación. En este sentido, la regulación deberá ser exhaustiva y garantista, para salvaguardar la eficacia de su adopción tanto en el interior de las fronteras estatales, así como el marco de los instrumentos europeos e internacionales de investigación transfronteriza. Solo de este modo los operadores jurídicos podrán perseguir los ciberataques que, cada vez de un modo más complejo, aumentan su incidencia y su alcance; comprometiendo en la actualidad múltiples bienes jurídicos y las infraestructuras críticas y estratégicas.