EGUZKILORE
Número 22.
San Sebastián
Diciembre 2008
169 - 187

EL CIBERTERRORISMO: UNA PERSPECTIVA LEGAL Y JUDICIAL

Ignacio José SUBIJANA ZUNZUNEGUI
Magistrado
Doctor en Derecho

Resumen: La globalización conlleva la implantación de un modelo social pergeñado en torno, entre otros, a los valores de ubicuidad, virtualidad y celeridad. En el orden penal ello conlleva la necesidad de afrontar fenómenos delictivos protagonizados por organizaciones criminales de carácter transnacional que hacen un uso perverso de las tecnologías de la información y la comunicación. Entre los mismos destaca, por la entidad de sus deletéreos efectos, el ciberterrorismo. La presente reflexión, tras definir el ciberterrorismo, hace un recorrido sobre las propuestas normativas que pretenden, a través de la aproximación de las legislaciones y la cooperación policial y judicial entre los Estados, garantizar una adecuada respuesta pública al mismo, superando la indiscutible insuficiencia de un tratamiento territorial de esta específica criminalidad.

Laburpena: Globalizazioak, besteak beste, nonahitasun, birtualtasun eta bizkortasun baloreen inguruan garatutako gizarte eredua dakarkigu. Ordena penalean, guzti honek nazioarte mailako erakunde kriminalen –informazio eta komunikazio teknologien erabilera maltzurra egiten dutelarik– delitu egintzei aurre-egiteko beharra dakar. Guzti hauen artean ziber-terrorismoa nabarmenduko genuke, bere ondorioak guztiz pozointsuak direlako. Ondorengo hausnarketak, ziber-terrorismoa zehaztu eta gero, legerien hurbiltzearen bidez eta estatuen arteko lankidetza poliziala eta judiziala babesten duten proposamen normatiboen bidez, erantzun publiko egokia bermatu nahi du, era honetan kriminalitate berezi honen tratamendu lurraldetarraren hutsune nabarmena gaindituz.

Résumé: La globalisation entraîne l'implantation d'un modèle social conçu autour des valeurs d'ubiquité, de virtualité et de célérité, entre autres. Dans l'ordre pénal cela entraîne la nécessité de faire face à des phénomènes criminels commis par des organisations criminelles transnationales qui font un usage pervers des technologies de l'information et de la communication. Entre ces usages le plus important, à cause de ses effets néfastes, est le cyberterrorisme. Après avoir défini le cyberterrorisme, la présente réflexion fait une analyse des différentes propositions normatives qui essaient de garantir une réponse publique adéquate à ce phénomène, au moyenne du rapprochement des législations et de la coopération policière et judiciaire entre les États, en surmontant l'indiscutable insuffisance d'un traitement territorial de cette sorte de criminalité.

Summary: Globalization entails a social model based on the values of ubiquity, virtuality and speed. In the penal order this gives us the need to face the criminal phenomenon created by trans-national criminal organizations, which do an evil use of communication and information technologies. We can emphasize, by its poisonous effects, the cyber-terrorism. This reflection, after defining cyber-terrorism, went all over normative proposals that want through the approximation to the legislation and the police and judicial cooperation between states, guarantee an adequate public response, exceeding the indisputable lack of resources of the territorial treatment of this specific criminality.

Palabras clave: ciberterrorismo, globalización, transnacionalidad, territorialidad, cooperación judicial y policial, aproximación de legislaciones penales y procesales.

Gako Hitzak: Ziberterrorismoa, globalizazioa, trasnazionalitatea, lurraldetasuna, lankidetza poliziala eta judiziala, zigor arloko eta auzibide legerien hurbiltzea.

Mots clef: cyberterrorisme, globalisation, transnationalité, territorialité, coopération judiciaire et policière, rapprochement des législations pénales et de la procédure.

Key words: Cyber-terrorism, globalization, trans-nationality, territoriality, police and judicial cooperation, criminal and procedural law approximation.

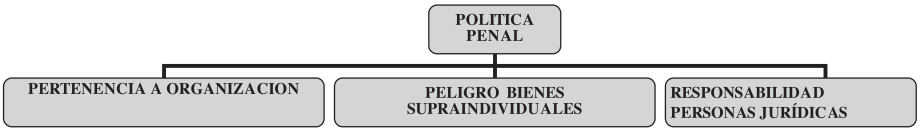
I. INTRODUCCIÓN

La globalización, entendida como interacción en tiempo real y a escala planetaria, es la semilla de la denominada Sociedad de la Información y el Conocimiento. Es una sociedad de funcionamiento en red (modelo comunitario reticular), en la que la velocidad, la ubicuidad, la virtualidad y la transversalidad sustituyen a la territorialidad, la rigidez y la jerarquización. Por ello, la comunidad social únicamente puede ser comprendida desde los valores de la complejidad, la diversidad y la versatilidad (DE LUCAS, 2008: 9).

El desarrollo de las tecnologías de la información y de la comunicación y la imparable consolidación de los contextos digitales en la sociedad plantean, además de indudables ventajas, riesgos específicos para intereses dignos de tutela penal. En concreto, el Derecho Penal tiene que prestar protección a nuevos valores concernidos por la implantación de los sistemas informáticos en los diversos sectores de la comunidad (personal, social, profesional, económico, financiero) y, también, ofrecer tutela a valores clásicamente amparados por el orden penal frente a nuevas modalidades de ataque derivadas del uso de los dispositivos telemáticos. Además, esta protección tiene que pergeñarse, en muchas ocasiones, frente a actuaciones protagonizadas por estructuras organizativas complejas (jerárquica, celular y fluida, preferentemente) de carácter transnacional (la denominada criminalidad organizada internacional) y que operan en el ciberespacio (redes interconectadas). Ello plantea indudables problemas de imputación subjetiva del hecho (atribución de responsabilidades criminales), de persecución (trabas inherentes a las limitaciones que el principio de territorialidad introduce en la persecución pública de los hechos) y de ponderación jurídico-penal (los distintos ordenamientos jurídicos potencialmente aplicables, dada la transterritorialidad del comportamiento, pueden ofrecer disímiles valoraciones sobre la ilicitud de las conductas).

En aras a lograr una política penal eficaz en esta materia se ha propugnado, incluso, un modelo diferenciado de represión del delito. En concreto, se ha defendido un Derecho penal de distintas velocidades, con plurales criterios de atribución y diferente tratamiento procesal en función de que tenga como centro de imputación al individuo delincuente o a estructuras criminales organizadas. En este último caso se defienden líneas de política criminal que acojan una panoplia de medidas sustantivas y procesales. En el plano sustantivo destacan las siguientes: creación de tipos que sancionen la pertenencia a determinadas organizaciones criminales, atendiendo al peligro que se deriva de la agrupación de personas en una asociación de determinadas características, a la vista de su abstracta capacidad de actuar; aparición de delitos de peligro presunto para bienes supraindividuales;

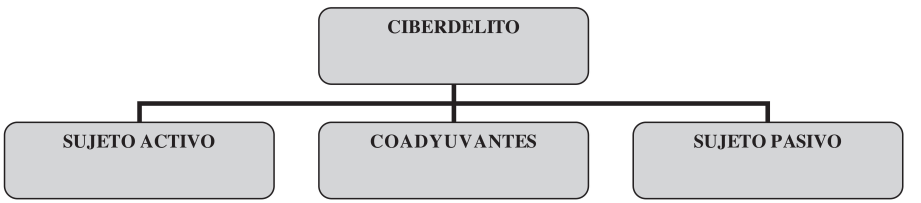
diseño de remedios eficaces para la confiscación del patrimonio criminal y reconocimiento de la responsabilidad penal de las personas jurídicas. En el plano procesal se fomenta (sobre todo cuando los Estados se integran en una estructura política supraestatal como la Unión Europea) la uniformidad progresiva de las legislaciones de los diversos Estados y la implantación de fórmulas ágiles de cooperación policial y judicial.



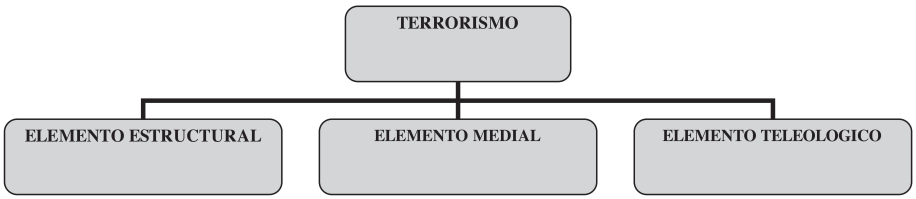
Con los términos cibercrimen, ciberdelito o ciberdelincuencia se hace referencia a los delitos cometidos en el espacio virtual. Los cibercrímenes tienen cuatro aspectos característicos:

- Se cometen fácilmente.
- Requieren escasos recursos en relación al perjuicio que causan.
- Pueden cometerse en una jurisdicción sin estar físicamente presente en el territorio sometido a la misma.
- Se benefician de las lagunas de punibilidad que pueden existir en determinados Estados, algunos de los cuales han sido denominados paraísos cibernéticos, debido a su nula voluntad política de tipificar y sancionar estas conductas.

La comisión de un ciberdelito suele producirse en el marco de una relación cuadrangular. El *sujeto activo* (A), de quien parte la acción de insertar en la red una información destructiva o un dispositivo pernicioso, persona que se sirve, para tal fin, de un ordenador. Los *coadyuvantes* no intencionados, que son el proveedor de servicios de Internet (B) que conectará al usuario, a través de la línea telefónica, a Internet y el servidor de web (C) en el que se aloja, en un disco duro, la información destructiva o el dispositivo pernicioso en que se materializa la acción antijurídica. Este servidor puede coincidir con el proveedor de servicios de Internet. El *sujeto pasivo del delito* (D), que es quien padece los daños derivados de la información destructiva o el dispositivo pernicioso y que, en muchas ocasiones, es indeterminado, desconocido e internacional.



Una de las manifestaciones más dañinas de la criminalidad global es el terrorismo. Básicamente el concepto jurídico-penal de terrorismo se vertebra en torno a un elemento estructural, otro medial y, uno final, teleológico. El elemento estructural es la vinculación del terrorista con una organización o banda armada. El autor realiza las conductas típicas en razón a su pertenencia a la banda criminal o, simplemente, con la finalidad de colaborar al logro de sus objetivos, aunque no pertenezca a ella. El elemento medial es la ejecución de actos de extremada violencia o grave intimidación. El elemento teleológico es la destrucción o claudicación del Estado de Derecho, garante institucional de los derechos fundamentales de las personas, arrumbando de esta manera una convivencia democrática vertebrada sobre la libertad y la diversidad. Para lograr este objetivo se busca el desistimiento cívico mediante la sumisión generada por el terror en amplios sectores de la sociedad.



Una de las modalidades específicas del terrorismo es el ciberterrorismo. A su análisis dedicamos las siguientes páginas.

II. CIBERTERRORISMO: ANÁLISIS SUSTANTIVO

II.1. Precisión conceptual: óptica medial y final

El ciberterrorismo puede ser analizado desde una perspectiva medial o final. La perspectiva medial tiene como referente el aprovechamiento por los grupos terroristas de las posibilidades que brindan las nuevas tecnologías de la información y de la comunicación para la consecución de sus fines deletéreos. Constituye una forma de terrorismo que utiliza las tecnologías de la información para intimidar, coaccionar o causar daños a grupos sociales con fines políticos o religiosos, básicamente. Desde esta perspectiva medial, el ciberterrorismo, por lo tanto, se estructura en torno a dos elementos: la presencia de un grupo terrorista y el empleo de medios provenientes de una infraestructura tecnológica para lograr la ampliación de su capacidad operativa. En este sentido, el Consejo de Europa define el ciberterrorismo como la forma de terrorismo que utiliza las tecnologías de la información para intimidar, coaccionar o causar daños a grupos sociales con fines políticos-religiosos.

Los medios tecnológicos permiten un ejercicio eficaz de las siguientes funciones o tareas:

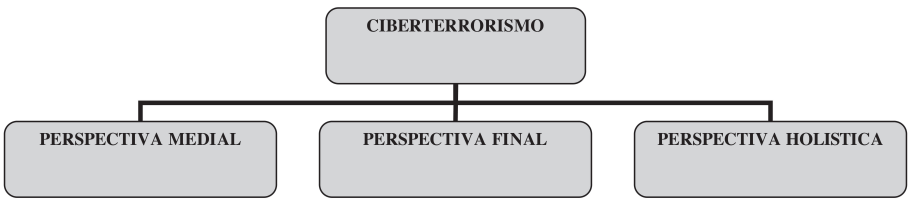
- Favorecer la ejecución transnacional del hecho.
- Dificultar la obtención de fuentes de prueba de la comisión y su autoría.
- Facilitar su acceso y manejo sin exigir una fuerte inversión económica.

- Permitir la potencialidad de producir efectos deletéreos sobre núcleos importantes de personas o significativos daños o detrimentos sobre infraestructuras públicas o servicios comunitarios básicos.
- Coadyuvar a sus comunicaciones para la transmisión de información de manera rápida y difícilmente detectable, máxime cuando se acude a técnicas como la encriptación o la asociación a fotografías u otros elementos neutrales.
- Transmitir su propaganda a través de sitios Web de escaso coste y fácil confección.
- Permitir la guerra psicológica, las incitaciones al odio y el crimen.
- Posibilitar el reclutamiento de sus miembros.
- Facilitar la instrucción de sus componentes y la planificación de sus acciones.
- Instar la búsqueda de nuevas fórmulas de financiación (por ejemplo, la extorsión infomática bajo la amenaza de ser ciber-atacados), la ejecución de complejas transacciones internacionales o la realización de pagos por la adquisición de materiales y equipos utilizados en la actividad criminal y blanqueo de cantidades de dinero que, procediendo de actividades ilegales, pretenden su aplicación a las actividades terroristas.

La perspectiva final toma como referente la destrucción de información sensible contenida en los sistemas telemáticos o informáticos. En concreto, el imparable desarrollo tecnológico ha conducido a una estructuración de la sociedad progresivamente vertebrada en torno a su tecnificación y automatización. Así, se ha producido una informatización de sectores básicos como los servicios públicos (sanidad, educación, justicia), las infraestructuras (regulación del tráfico viario, aéreo o marítimo), el sistema bancario y bursátil, la producción industrial, la distribución comercial y la defensa nacional, entre otros. Se trata, por lo tanto, de objetivos extremadamente codiciosos para el terrorismo, dada la enorme repercusión que en la vida cotidiana conlleva un ataque terrorista sobre ellos. Se ha llegado a afirmar que un ataque estratégico sobre cualquiera de estos sistemas abocaría a consecuencias apocalípticas para las naciones y la economía de las mismas.

Desde la óptica final se ha definido el ciberterrorismo en los siguientes términos: ataque ilegal contra ordenadores, sus redes y la información contenida en ellos cuando se lleva a cabo con la finalidad de coaccionar a un gobierno o a su población para conseguir objetivos políticos o sociales.

Integrando la perspectiva medial y final, se explicita el ciberterrorismo como cualquier acto realizado a través de tecnologías de información que pueda lograr directa o indirectamente causar terror o generar daños significativos a un grupo social o político a través de la destrucción del soporte tecnológico de cualquiera de sus infraestructuras fundamentales.



Una política de seguridad pública en el ciberespacio tiene que integrar una perspectiva preventiva y otra reactiva. La perspectiva preventiva pretende dotar de elementos de protección eficaces a los sistemas informáticos y de comunicaciones que rigen el funcionamiento de sectores institucionales y sociales básicos, así como la identificación rápida y efectiva de los peligros. La perspectiva reactiva trata de lograr la reparación de los daños en el menor tiempo posible así como el enjuiciamiento de sus responsables. En esta última tarea destaca la informática forense como disciplina que tiene por objeto la investigación en los sistemas telemáticos de hechos delictivos, entre los que destaca el ciberterrorismo.

II.2. La Unión Europea y el Consejo de Europa

La Unión Europea ha intensificado la lucha contra el terrorismo desde los atentados terroristas acaecidos en septiembre de 2001 (Estados Unidos), marzo de 2004 (España) y julio de 2005 (Reino Unido).

La falta de competencia penal directa de las instituciones comunitarias ha impedido la construcción de un Derecho Penal de la Unión Europea, de naturaleza supranacional y aplicación directa en los Estados miembros. La tutela penal de los intereses comunitarios se ha articulado a través de la aproximación de la legislación de los Estados miembros acudiendo como instrumento jurídico a la Decisión Marco (DE LA CUESTA, 2008: 141). En todo caso, las sentencias del Tribunal de Justicia de 13 de septiembre de 2005 y 23 de octubre de 2007 reconocen la existencia de una competencia penal complementaria de la Comunidad. Para ello es preciso que en un determinado sector comunitario resulte necesaria la aproximación de las disposiciones legales y reglamentarias de los Estados miembros para garantizar la plena eficacia de una política comunitaria o el buen funcionamiento de una libertad, particularmente si se trata de un área objeto de medidas de armonización con anterioridad.

Como primer paso, la *Decisión Marco 2002/475/JAI del Consejo, de 13 de junio de 2002, relativa a la lucha contra el terrorismo*, invita a los Estados miembros a unificar sus legislaciones, estableciendo normas mínimas sobre delitos terroristas. En concreto, fija unos criterios comunes sobre la definición y sanción de los delitos de terrorismo, de los delitos relativos a un grupo terrorista y de los delitos ligados a las actividades terroristas, las sanciones a imponer, la responsabilidad de las personas jurídicas y la aplicación de la ley penal en el espacio. Así: grupo terrorista es toda organización estructurada de más de dos personas, establecida durante cierto período de tiempo, que actúa de manera concertada con el fin de cometer delitos de terrorismo. Por organización estructurada se entiende una organización no formada fortuitamente para la comisión inmediata de un delito y en la que no necesariamente se ha asignado a sus miembros funciones formalmente definidas ni hay continuidad en la condición de miembro o una estructura desarrollada. Delitos de terrorismo son delitos graves (contra la vida, integridad física, libertad ambulatoria, básicamente) que pueden lesionar gravamente a un país o a una organización internacional y se cometen con alguno de estos fines: intimidar gravemente a una población; obligar indebidamente a los poderes públicos o a una organización internacional a realizar un acto o a abstenerse de hacerlo o, finalmente, desestabilizar gravemente o destruir las estructuras fundamentalmente políticas, constitucionales, económicas o sociales de un país o de una organización internacional.

Los Ministerios de Justicia e Interior de la Unión Europea acordaron, en la reunión celebrada en Luxemburgo el 18 de abril de 2008, tipificar como delitos en las legislaciones penales de los Estados miembros tres comportamientos específicos. A saber: incitar

al terrorismo, reclutar y entrenar personas, en estos dos últimos casos, cuando el destino sea la práctica del terrorismo. Se prevé de forma expresa la punición de estas conductas cuando se ejecutan por Internet, adaptandose a las circunstancias explicitadas en un reciente informe de Europol, en el que se pone de manifiesto la creciente utilización de la Red para la propagación de consignas, el aleccionamiento de terroristas o la difusión de técnicas de fabricación de explosivos. Se disciplina, también, que los jueces o las autoridades administrativas competentes, según el modelo de cada Estado, estarán facultadas para reclamar a los proveedores de acceso a Internet la retirada de los contenidos ilícitos de sus servidores.

De forma complementaria, *la Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, tiene por objeto los ataques de los que son objeto los sistemas de información*. En su seno se indican las infracciones penales perseguibles judicialmente: el acceso sin autorización a sistemas de información (art. 2); la intromisión no autorizada en sistemas de información, a fin de obstaculizar o interrumpir de manera significativa el funcionamiento de los mismos (art. 3); la intromisión no autorizada en datos informáticos contenidos en sistemas de información que produzcan el efecto de borrarlos, dañarlos, deteriorarlos, alterarlos, suprimirlos o hacerlos inaccesibles (art. 4). Las conductas deben ser cometidas intencionadamente, contemplándose la sanción autónoma de la inducción, la complicidad y la tentativa. También se describen las pautas básicas del régimen sancionador. En concreto, refiere que las sanciones serán penales y que las mismas serán efectivas, proporcionadas y disuasorias. Es más, tras disciplinar que la infracción de acceso no autorizado estará sujeto a la pena que fije cada Estado, menta que las conductas de intromisión serán sancionadas "entre uno a tres años de prisión como mínimo en su grado máximo". Se prevé una agravación (la sanción será de dos a cinco años de prisión "como mínimo en su grado máximo") cuando las acciones se cometan en el marco de una organización delictiva. Finalmente existe una previsión específica para los casos en los que el sujeto activo sea una persona jurídica. En este supuesto, con independencia de la sanción que corresponda a las personas físicas que la administren, podrá imponerse a la persona jurídica sanciones de naturaleza económica o la vigilancia de sus actividades. Estas sanciones podrán ser administrativas o penales.

Existe una Propuesta de Decisión Marco del Consejo por la que se modifica la Decisión Marco 2002/475/JAI del Consejo sobre la lucha contra el terrorismo. Esta Propuesta, presentada por la Comisión el 6 de noviembre de 2007, tiene por objeto adecuar la Decisión Marco al Convenio del Consejo de Europa para la represión del terrorismo.

Finalmente, el *Tratado de Lisboa, de 13 de diciembre de 2007, por el que se modifican el Tratado de la Unión Europea y el Tratado constitutivo de la Comunidad Europea*, conllevará, de entrar en vigor, la "comunitarización" del espacio de libertad, seguridad y justicia, con la consiguiente sumisión de la cooperación judicial penal y policial a los procesos de elaboración legislativa y control jurisdiccional previstos para el resto de materias comunitarias. En concreto, la regulación contenida en su Título V parte de una premisa fundamental: el reconocimiento mutuo de las resoluciones judiciales y la aproximación de legislaciones en materia penal y procesal penal. En concreto, el acercamiento de la normativa de los Estados miembros se contempla para materias procesales, sustantivas e institucionales. En el orden procesal abarca materias como la prevención de conflictos de jurisdicción, la admisibilidad mutua de pruebas entre los Estados miembros, los derechos de las personas durante el procedimiento

penal y los derechos de las víctimas de los delitos. En el orden sustantivo se estipula el establecimiento de mínimos comunes en lo que respecta a la tipificación y penalización de los hechos ilícitos, tarea de acercamiento normativo que vendrá impulsada por directivas del Parlamento Europeo y del Consejo, cuando se trate de ámbitos delictivos caracterizados por su especial gravedad y su dimensión transfronteriza (artículo 69 B).1), entre los que se hace expresa mención al terrorismo (artículo 68 B).1). En el orden institucional, se refuerza el papel de Eurojust, encomendándole tareas como el inicio de investigación e, incluso, la incoación de procesos penales en el ámbito de la protección de los intereses financieros de la Unión, así como la coordinación y resolución de conflictos de jurisdicción. No obstante la valoración positiva de estos avances, existe cierto recelo respecto al efecto debilitante que para la comunitarización del espacio de libertad, seguridad y justicia puede conllevar la previsión de que los Estados miembros puedan decidir descolgarse del proceso de plena comunitarización de esta materia (JIMENO; 2008, 4).

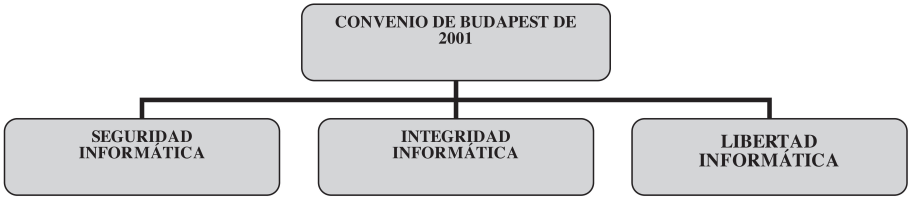
En el marco del Consejo de Europa, la necesidad de establecer una política penal común destinada a proteger a la sociedad de la criminalidad en el ciberespacio justificó la elaboración del *Convenio del Cibercrimen de Budapest,de 23 de noviembre de 2001* (el Protocolo adicional de 28 de enero de 2003 completa el Convenio en cuanto a la lucha contra el racismo y la xenofobia por Internet). El Convenio no define el cibercrimen, procediendo a enumerar nueve tipos de ofensas y exhortando a los Estados signatarios a adoptar las medidas legislativas o normativas que fueran necesarias para contemplarlas como infracciones penales.

En concreto, se pretende la protección de los siguientes intereses jurídicos: la seguridad informática, la integridad y disponibilidad de los datos y la libertad informática.

La seguridad informática se concibe como un bien jurídico colectivo que viene a dar protección anticipada a otros de naturaleza personal como la intimidad, el honor, el patrimonio, la libertad de información, el secreto y la inviolabilidad de las comunicaciones electrónicas. Su lesión se produciría cuando se atenta al uso y funcionamiento correcto de redes y sistemas informáticos. La posibilidad de prohibir tales comportamientos se fundamenta en que generan riesgos para los bienes jurídicos personales a cuya protección mediata sirve la seguridad informática.

La integridad y disponibilidad de los datos tutela la incolumidad de los datos, su libre disposición y su mantenimiento en los términos en que los ha configurado su titular.

La libertad informática protege el derecho a la autodeterminación informativa del individuo para determinar qué información personal se puede difundir sobre él y su familia así como el destino de la misma.



El Convenio prevé la incorporación a las legislaciones nacionales de un elenco de ilícitos penales, mayoritariamente destinados a proteger la seguridad informática, la integridad y la disponibilidad de los datos y la libertad informática. Son los siguientes:

- Hechos contrarios a la confidencialidad, la integridad y la disponiblidad de datos y sistemas informáticos. Aquí se incluyen: el acceso ilegal injustificado a todo o parte de un sistema informático (art. 2), la interceptación ilegal de comunicaciones entre sistemas informáticos o en el interior de un mismo sistema, mediante el empleo de sistemas técnicos (art. 3), los atentados a la integridad de los datos mediante un daño, borrado, deterioro, alteración o supresión intencional de datos informáticos (art. 4), o a través del entorpecimiento grave de un sistema informático mediante alguna de las conductas anteriormente reseñadas (art. 5), y el abuso de determinados dispositivos para la comisión de las infracciones anteriores (art. 6).
- Infracciones informáticas: falsificación informática (art. 7) y fraude informático (art. 8).
- Infracciones relativas a la pornografía infantil (art. 9).

Se contempla, en el ámbito del procedimiento, la cooperación internacional tanto a fines de investigación como de procedimientos o recogida de pruebas (art. 24).

II. 3. El Código Penal de 1995

El Código Penal de 1995 (en adelante CP) contiene diversos preceptos aplicables al ciberterrorismo.

Así califica como punibles las asociaciones ilícitas (artículo 515 CP) y atribuye tal consideración a las bandas armadas, organizaciones o grupos terroristas (artículo 515. 2º CP). En este caso, además de acordar, en todo caso, la disolución de las mentadas asociaciones (artículo 520 CP), impone severas penas a los promotores y directores de las mismas, a quienes dirijan cualquiera de sus grupos y a sus integrantes (artículo 516 CP).

El CP no contiene, sin embargo, un delito de mero instrusismo informático que tipifique el acceso ilegal injustificado a un sistema informático, conducta que, en ocasiones, se vincula al ciberterrorismo. En el referido texto legal, la relevancia jurídico penal de los accesos no autorizados se vincula a la existencia de específicas intenciones en el autor (descubrir la intimidad ajena, desvelar un secreto de empresa o causar un daño). En estos casos, por lo tanto, el acceso no autorizado a un sistema informático es el modo de ejecución de otras conductas delictivas que tienen a la privacidad, la libre competencia o el patrimonio como valores a proteger.

Reflexión disímil merece la figura del sabotaje informático. Como tal se entiende la destrucción de sistemas informáticos completos o la específica de equipos y datos, programas y documentos electrónicos. Puede existir una destrucción del *hardware* (mediante la aniquilación de los equipos informáticos) o del *software* (a través de la instalación de bombas lógicas, gusanos, programas maliciosos, troyanos o virus que conducen al borrado de la información almacenada o la alteración o corrupción de la programación). Cabe también la ejecución de comportamientos dirigidos a provocar significativas perturbaciones en los sistemas de información a través de ataques masivos de denegación de servicio que pretenden dejar un servidor inoperativo, provocando su colapso, de forma que los

legítimos usuarios no puedan acceder a los contenidos ofertados. Esta denegación de servicio puede conseguirse de dos maneras: el ataque de denegación de servicio distribuido, mediante el cual las peticiones son enviadas de forma coordinada entre varios equipos, o el uso de programas *malwere* que permitan la toma de control del equipo de forma remota. Todas estas conductas se incardinan en el delito de daños informáticos contemplado en el artículo 264.2 CP. La doctrina penalista mayoritaria estima que el delito de daños no se ciñe a los supuestos de destrucción material del objeto del delito sino que abarca, también, los casos de afectación de su valor de uso o funcional. Por lo tanto, es factible que el tipo de injusto descrito en el artículo 264.2 CP cobije las conductas de afectación de la sustancia de los datos, programas o documentos electrónicos (casos de destrucción material) y los comportamientos de alteraciones significativas en el funcionamiento del sistema informático sin necesidad de destrucción o alteración grave de sus componentes lógicos (casos de deterioro funcional).

La conducta de daño informático justificará una pena agravada si se realiza por quien pertenece, actúa o colabora con una banda armada o una organización o grupo terrorista con la finalidad de subvertir el orden constitucional o alterar gravemente la paz pública (artículo 574 CP) o por quien, con el mentado delito patrimonial, trate de allegar fondos a las referidas organizaciones o pretenda favorecer sus finalidades (artículo 575 CP).

Son variadas las modalidades de alteración del sistema informático. Las bombas lógicas son programas autoejecutables que se activan cuando el usuario realiza una determinada acción o se cumplen unos parámetros. Los gusanos son programas que consumen la memoria del ordenador y que se propagan por los sistemas de comunicación, como el correo electrónico. Los caballos de Troya son programas que se ocultan en otros y si se ejecutan producen daños. Las bacterias son programas que se replican hasta detener por completo las máquinas. Los virus son fragmentos de códigos que se unen a programas, activándose y replicándose al ejecutarse el programa.

III. CIBERTERRORISMO: ANÁLISIS PROCESAL

III.1. Insuficiencia del Estado-nación

El ciberterrorismo es una actividad criminal transnacional (es posible la ejecución del delito en cualquier área del mundo y por personas de cualquier nacionalidad, ya se trate de residentes estables o en tránsito) que, al tener lugar en un espacio virtual en el que no existen límites territoriales, no puede ser contrarrestada por políticas públicas sancionadoras que descansan en el poder punitivo del Estado-nación, cuya legitimidad radica en la soberanía plena y exclusiva en los confines de su territorio. La criminalidad transfronteriza precisa, como respuesta final, un sistema penal supranacional en el que converjan un Derecho Penal común y una estructura de enjuiciamiento internacional. Su ausencia conlleva serias limitaciones en su persecución, dada la existencia, en muchas ocasiones, de serias divergencias en la regulación normativa de los Estados y ostensibles dificultades en la colaboración estatal para la efectiva detección, enjuiciamiento y sanción de las conductas ilícitas. Mientras se construye un sistema penal global, la elaboración y ratificación de tratados sectoriales de uniformación de los delitos y penas, en lo sustantivo, y de cooperación policial y judicial, en lo procesal, pueden paliar las disfunciones derivadas de la asimetría entre una criminalidad transterritorial y un *ius puniendi* apegado a la territorialidad. La armonización sustantiva evita un tratamiento disímil del ciberterrorismo en

cada uno de los Estados en los que se planifica y ejecuta. La cooperación policial y judicial permite una obtención de fuentes de prueba que, en atención a su naturaleza electrónica y la existencia de dispositivos tecnológicos de ocultación de identidad (servicios anónimos y comunicaciones encriptadas, entre otros), son altamente volátiles y perecederas, lo que exije una actuación pública ágil y rápida.

III.2. La política de la Unión Europea

En el seno de la Unión Europea, la progresiva armonización de las legislaciones penales y procesales de los Estados Miembros se ha obtenido, hasta ahora, a través de los Convenios, las Directivas y las Decisiones Marco, aprobados como desarrollo de la política común en materia de justicia e interior (el denominado Tercer Pilar, cuya superación se pretende con el Tratado de Lisboa, a través de su "comunitarización").

En esta línea, el *Tratado de Amsterdam de 2 de octubre de 1997* (que entró en vigor el 1 de mayo de 1999) ofrece una base normativa para el desarrollo de una política criminal propia en el espacio de libertad, seguridad y justicia. En concreto se fomenta la aprobación de instrumentos dirigidos a favorecer la cooperación policial y judicial en materia penal, mediante la propuesta y recomendación de aprobación de Convenios por los Estados miembros, y la adopción de posiciones y acciones comunes. Esta política común se plasma en una triple vertiente:

- Una mayor cooperación entre las fuerzas policiales y otras autoridades competentes, directamente o a través de Europol. Los campos de convergencia son: el almacenamiento, análisis, tratamiento e intercambio de información; iniciativas conjuntas a través de funcionarios de enlace, comisiones de servicio, uso de equipos de investigación y evaluación común de técnicas de investigación.
- Una coordinación más fluida entre las autoridades judiciales y otras autoridades competentes de los Estados miembros.
- La aproximación de las normas de los Estados miembros en materia penal.

Uno de los campos de acción conjunta en la prevención y lucha contra la delincuencia es el terrorismo, estableciéndose, incluso, normas mínimas sobre delitos y penas.

Desarrollando estas previsiones, *el Consejo Europeo de Tampere (Finlandia), celebrado los días 15 y 16 de octubre de 1999, y el Tratado de Niza, de 26 de febrero de 2001*, implementa, en el campo judicial, las siguientes medidas:

- La creación de Eurojust.
- La potenciación de los magistrados de enlace, la institucionalización de la red judicial europea y de formación de magistrados.
- La difusión y codificación de buenas prácticas de asistencia judicial en materia penal y la prevención de conflictos de competencias.

Además, en el campo referido a la cooperación policial y judicial, destacan decisiones como:

- La creación de la policía europea (Europol).
- La aprobación de la orden de detención europea.

- El reconocimiento y ejecución de las resoluciones de los sistemas judiciales nacionales, fundado en la confianza recíproca de los Estados miembros en sus respectivos sistemas de justicia penal.
- La ejecución de las resoluciones de embargo preventivo y de aseguramiento de pruebas, para posibilitar la eficacia de las medidas cautelares reales y la disponibilidad de las fuentes de prueba.

El principio de reconocimiento de las resoluciones judiciales conlleva que cada Estado de la Unión Europea reconozca las decisiones que emanan de los órganos jurisdiccionales de otro Estado. Su plasmación garantiza básicamente tres efectos: permitir la ejecución de las resoluciones (el caso paradigmático es la orden de detención y entrega); impedir el doble enjuiciamiento de unos mismos hechos atribuidos a idéntico sujeto y, finalmente, posibilitar la toma en consideración de los antecedentes penales de una persona en otro Estado miembro de la Unión Europea. Es la forma de cooperación judicial más intensa, pues se asume como propia la decisión de un órgano jurisdiccional de otro Estado.

Para permitir la ponderación de la eficacia de las medidas estatales frente al terrorismo la Decisión del Consejo, de 28 de noviembre de 2002, establece un mecanismo de evaluación de los sistemas legales y su ejecución a escala nacional en la lucha contra el terrorismo.

En un intento de consolidar este proceso, *el Tratado por el que se instituía una Constitución para Europa,* aprobado por los Jefes de Estado o de Gobierno en su reunión de 18 de julio de 2004, implementaba (no llegó a entrar en vigor) las siguientes normas relevantes sobre la materia:

- Fomento de la aproximación de las disposiciones legislativas y reglamentarias de los Estados miembros sobre la cooperación judicial en materia penal.
- Potenciación de Eurojust, con reordenación de sus funciones.
- Creación de una Fiscalía Europea para combatir la delincuencia grave que tenga una dimensión transfronteriza así como las infracciones que lesionen los intereses de la Unión.
- Dinamización de la cooperación policial, con recogida de información pertinente, el apoyo a la formación de personal e intercambio del mismo y la puesta en funcionamiento de técnicas comunes de investigación.

La Ley 16/2006, de 26 de mayo, regula Eurojust, los Magistrados de Enlace y la Red Judicial Europea. Eurojust es un organismo cuya función consiste en apoyar y reforzar la coordinación y cooperación enre las autoridades nacionales de la Unión Europea encargadas de investigar y perseguir la delincuencia grave que afecte a varios Estados. El Magistrado de Enlace es un juez nombrado por un Estado que se desplaza al territorio de otro país con la finalidad de incrementar la rapidez y eficacia de la cooperación judicial, contribuir al intercambio de información sobre los ordenamientos jurídicos y sistemas judiciales de los Estados miembros. La Red Judicial Europea constituye una red de puntos de contacto en cada uno de los países de la Unión Europea que tiene por objeto intermediar activamente entre las autoridades judiciales locales de los distintos Estados.

De forma complementaria, el *Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea*, confeccionado en

Bruselas el 29 de mayo de 2000, introduce novedades tan significativas como las siguientes:

- Facilita la remisión de solicitudes de asistencia y de documentos procesales (así, salvo casos específicos en que intermedia una autoridad central, las solicitudes de asistencia mutua y las comunicaciones serán transmitidas y ejecutadas directamente por las autoridades judiciales).
- Contempla la posibilidad de ejecución del auxilio de conformidad con los trámites indicados por el Estado requirente.
- Regula determinadas formas específicas de asistencia: equipos conjuntos de investigación (de indiscutible trascendencia en la criminalidad transnacional), investigaciones encubiertas, entregas vigiladas, intervención de telecomunicaciones, audición por conferencia telefónica y por videoconferencia, restitución y traslado temporal de detenidos con fines de investigación.

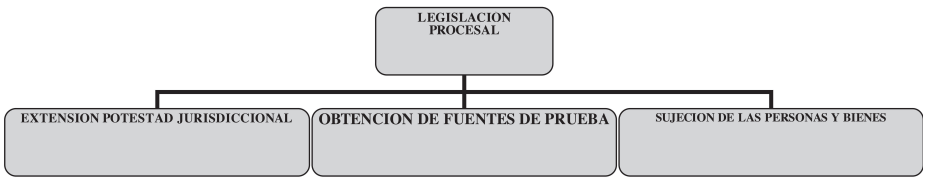
Este Convenio tiene un Protocolo, hecho en Luxemburgo el 16 de octubre de 2001, referido a determinados datos bancarios con fines de investigación penal, como la información de cuentas y la información y el control de transacciones.

Finalmente *la Decisión Marco 003/577JAI* regula la ejecución de las resoluciones de una autoridad judicial de un Estado miembro que acuerda en un proceso penal el impedimento de destrucción, transformación, desplazamiento, transferencia o enajenación de bienes que pudieran ser sometidos a decomiso o utilizados como medios de prueba, cuando dichos bienes se encuentran en el territorio de otro Estado miembro de la Unión Europea.

El recorrido efectuado sobre los distintos instrumentos normativos implementados para lograr la cooperación judicial en la Unión Europea denota la existencia de un complejo entramado normativo que no es fácil de aquilatar por los jueces para lograr una adecuada satisfacción del derecho a la tutela judicial efectiva de las personas. Y ello no es una cuestión baladí, dada la significación que la efectividad de la tutela conlleva para la legitimidad de un sistema judicial (GUTIÉRREZ, 2008: 51).

III.3. La legislación nacional

En nuestro ordenamiento jurídico existen varias leyes que contienen normas procesales de especial interés aplicativo para el ciberterrorismo. Las referidas reglas legales persiguen cuatro objetivos: definir la extensión de la potestad jurisdiccional, garantizar la obtención de fuentes de prueba, permitir la sujeción al proceso del acusado o sancionado penalmente y facilitar la preservación de los bienes o las fuentes de prueba.



Una primera norma significativa en materia de ciberterrorismo es la referida a la extensión de la potestad jurisdiccional de los órganos judiciales que conforman el Poder Judicial de España. La función jurisdiccional, en cuanto ejercicio de uno de los poderes del Estado (el de juzgar y hacer ejecutar lo juzgado), requiere normalmente, cuando se trata del ejercicio del *ius puniendi*, de la existencia de alguna conexión entre la infracción y el Estado. Este nexo puede ser el territorio (principio de territorialidad), la nacionalidad del infractor o la víctima (principio de personalidad) o la protección de los intereses esenciales del Estado (principio de protección de intereses). Una excepción a esta exigencia común de nexo entre el Estado y el delito constituye el principio de jurisdicción universal que permite al Estado perseguir y juzgar a las personas por los crímenes cometidos fuera de su territorio, cualquiera que sea la nacionalidad de los autores o víctimas. Pues bien, conforme a lo establecido en el artícuo 23.4 b LOPJ, el ciberterrorismo está sujeto al principio de justicia universal. Por lo tanto, la jurisdicción española puede proceder a su enjuiciamiento cualquiera que sea el lugar en el que se cometa el delito o la nacionalidad de sus autores o víctimas. La persecución internacional y transfronteriza que pretende imponer el principio de justicia universal se basa exclusivamente en las particulares características de los delitos sometidos a ella, cuya lesividad transciende de las concretas víctimas y alcanza a la comunidad internacional en su conjunto (SSTC 237/2005 y 227/2007). Se trata, por lo tanto, de crímenes que menoscaban intereses y valores esenciales compartidos por la comunidad internacional. La Audiencia Nacional es el órgano judicial competente para el conocimiento de los delitos cometidos fuera del territorio nacional, cuando conforme a las leyes o a los tratados corresponde su enjuiciamiento a los Tribunales españoles (artículo 65.1º e LOPJ).

Las SSTC 237/2000 y 227/2000 estiman contraria al derecho fundamental a la tutela judicial efectiva, en su modalidad de acceso a la jurisdicción, la interpretación de la Sala Segunda del Tribunal Supremo que estipulaba que la aplicación del principio de justicia universal de la jurisdicción española en el ámbito penal requería la existencia de vínculos o elementos de conexión de los hechos denunciados con el ámbito de la jurisdicción española, reseñándose entre los mismos que el presunto autor de los delitos se encuentre en España o que las víctimas tengan nacionalidad española.

La segunda regla de significativo interés en la investigación del ciberterrorismo es la obtención de determinadas fuentes de prueba. Se contiene en la Ley 25/2007, de 18 de octubre, sobre la conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

La mentada ley impone determinadas obligaciones a los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones (artículo 2). En concreto, dos son los deberes jurídicos:

- Conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación (artículo 1). Estos datos (referidos a la identificación del origen de una comunicación, identificación del destino de una comunicación, determinación de la fecha, hora y duración de una comunicación, identificación del tipo de comunicación, identificación del equipo de comunicación) deberán conservarse durante doce meses desde la fecha en que se haya producido la comunicación, si bien, reglamentariamente, puede ampliarse, hasta dos años, o reducirse, hasta seis meses, para determinados datos o categorías de datos (artículo 5.1).

- Ceder los datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales (artículo 1.1). Los agentes facultados son los miembros de las Fuerzas y Cuerpos de Seguridad, cuando desempeñen funciones de policía judicial, los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en el desarrollo de sus competencias como policía judicial, y el personal del Centro Nacional de Inteligencia en el curso de las investigaciones de seguridad sobre personas o entidades (artículo 6.2). Esta cesión se realizarán en los términos que fije la resolución judicial que se dicte conforme a lo previsto en la Ley de Enjuiciamiento Criminal y de acuerdo con los principios de necesidad y proporcionalidad (artículo 7.2).

La jurisprudencia del Tribunal Constitucional, desde la STC 114/1984, ha identificado las características delimitadoras del derecho al secreto de las comunicaciones protegido en el artículo 18.3 CE. Son las siguientes:

- La diferenciación y autonomía del ámbito de protección de los derechos fundamentales a la intimidad personal (art. 18.1 CE) y al secreto de las comunicaciones (art. 18.3 CE).
- La determinación de que el objeto protegido por el derecho reconocido en el artículo 18.3 CE es el secreto de la comunicación, secreto que se proyecta tanto sobre el proceso de comunicación como sobre el contenido de la misma, aunque este último no quede en la esfera de lo íntimo. Por lo tanto, el secreto de la comunicación abarca tanto el contenido de la comunicación como la identidad subjetiva de los interlocutores.
- El derecho comprendido en el artículo 18.3 CE alcanza frente a terceros ajenos a los propios comunicantes, nunca frente a éstos últimos.
- La protección alcanza frente a cualquier forma de interceptación en el proceso de comunicación mientras el proceso esté teniendo lugar, siempre que sea apta para desvelar bien la existencia misma de la comunicación, bien los elementos externos del proceso de comunicación, bien su propio contenido.

La injerencia en el derecho al secreto de las comunicaciones está justificada cuando la resolución judicial es acorde con los principios de idoneidad, necesidad y proporcionalidad. La medida es idónea cuando permite cumplir el objetivo público pretendido legalmente. Es necesaria cuando no puede obtenerse la satisfacción del referido objetivo público con un recurso que no conlleve una afectación del citado derecho fundamental. Finalmente es proporcionada cuando la obtención del objetivo público no supone un sacrificio desmesurado del derecho fundamental.

La tercera norma relevante tiene como finalidad la sujeción del acusado o sancionado penalmente al proceso penal. Es la *Ley 3/2003, de 14 de marzo, que regula la orden europea de detención y entrega*. Es una resolución judicial dictada en un Estado miembro de la Unión Europea con vistas a la detención y la entrega por otro Estado miembro de una persona a la que se reclama para el ejercicio de las acciones penales o para la ejecución de una pena o una medida de seguridad privativas de libertad (artículo 1.1). El Juez o Tribunal que conozca de la causa penal (que

recibe el nombre de autoridad judicial de emisión) podrá dictar una orden europea en dos casos (artículo 5.1):

- Para proceder al ejercicio de la acción penal por aquellos hechos para los que la ley penal española señale una pena o una medida de seguridad privativa de libertad cuya duración máxima sea, al menos, de doce meses.
- Con el fin de proceder al cumplimiento de una condena a una pena o una medida de seguridad no inferior a cuatro meses de privación de libertad.

La autoridad judicial podrá solicitar también la entrega de objetos que constituyan medios de prueba o efectos del delito (artículo 5.3).

Está prevista la entrega de la persona reclamada sin control de la doble tipificación de los hechos (principio de doble incriminación) cuando, conforme al derecho del Estado de emisión, se trate de un delito de pertenencia a organización delictiva o terrorismo y tenga asignada, como sanción, una pena o una medida de seguridad privativa de libertad cuya duración máxima sea, al menos, de tres años (artículo 9.1).

La orden europea de detención y entrega se funda en el principio de confianza en los sistemas jurídicos de los Estados miembros de la Unión Europea. Ello conlleva un novación significativa de la concepción de la extradición (unos sostienen que es la certificación de su desaparición, otros que es la plasmación de su simplificación) que se asienta, básicamente, en tres modificaciones (LÓPEZ ORTEGA, 2008, 296): se suprime la fase administrativa de la extradición, profundizando en una tendencia clara hacia la total judicialización del mecanismo de entrega; se sustituyen los instrumentos jurídicos convencionales por un nuevo marco jurídico en el que los obstáculos tradicionales a la extradición, como la exigencia de doble incriminación o la prohibición de entrega del propio nacional, se atenúan considerablemente y, finalmente, se instaura un procedimiento común de entrega extraordinariamente simplificado y específicamente orientado a proteger los derechos fundamentales del reclamado.

La última regla legal es la que tiene por objeto la sujeción de los bienes y el aseguamiento de las fuentes de prueba. Así la *Ley 18/2006, de 5 de junio, regula la eficacia en la Unión Europea de las resoluciones de embargo y aseguramiento de pruebas en procesos penales*. Es el mecanismo a través del cual se van a transmitir por parte de las autoridades judiciales españolas las medidas de embargo de bienes o aseguramiento de pruebas acordadas en procedimentos penales cuando los objetos, datos o documentos objeto de la medida se encuentren en otro Estado miembro de la Unión Europea (artículo 1.1). También regula de qué forma las autoridades judiciales españolas van a reconocer y cumplir tales resoluciones cuando provengan de una autoridad judicial de otro Estado miembro (artículo 1.2).

En nuestra legislación se atribuye a los Juzgados de Instrucción la competencia objetiva para la ejecución de las medidas de embargo y de aseguramiento de prueba transmitidas por un órgano judicial de un Estado miembro de la Unión Europea que las haya acordado en un proceso penal, cuando los bienes o los elementos de prueba se encuentren en territorio español (artículo 87.1 g LOPJ).

Las resoluciones de embargo podrán adoptarse en relación a cualquier tipo de bien, sea material o inmaterial, mueble o inmueble, así como a los documentos acreditativos de un título o derecho (artículo 2).

El aseguramiento de pruebas podrá adoptarse en relación a los objetos, documentos o datos que posteriormente puedan utilizarse como medio de prueba en un procedimiento penal (artículo 2).

En ambos casos el objeto de la medida es impedir provisionalmente la destrucción, transformación, desplazamiento, transferencia o enajenación de bienes que pudieran ser sometidos a decomiso o utilizarse como medios de prueba (artículo 2).

La medida acordada (embargo o aseguramiento de pruebas) se ejecutará con arreglo al ordenamiento jurídico del Estado en el que haya de tener lugar. En todo caso, cuando sea necesario para garantizar la validez de los medios de prueba, la autoridad judicial española solicitará a la autoridad judicial requerida que observe para la ejecución de la medida las formalidades y los procedimientos que expresamente se indiquen (artículo 7). De esta forma se evita incurrir en la prohibición de valoración de la prueba obtenida, directa o indirectamente, violentando derechos o libertades fundamentales (artículo 11.1 LOPJ).

Las mentadas reglas legales se complementan con los criterios jurisprudenciales y doctrinales que fijan las pautas a seguir cuando tratan de obtenerse fuentes de prueba en el curso de las diferentes formas de comunicación habilitadas en Internet. En este sentido, tienen especial relieve las labores de infiltración en el curso de la información entre dos o más usuarios de la red, en el seno de la búsqueda de información en la red o, finalmente, en el ámbito de la transferencia de datos entre usuarios. Destaca, a estos efectos, la doctrina sentada en la STS 236/2008, de 9 de mayo. El supuesto de hecho es la realización por el Grupo de Delitos Telemáticos de la Policía Judicial de la Guardia Civil de búsquedas en Internet rastreando las redes de intercambio de archivos (*Peeer to Peer*), utilizando para ello un programa P2P. El objeto era averiguar aquellos usuarios que descargasen o compartiesen archivos conteniendo fotografías o vídeos con contenido de pornografía infantil. Estos rastreos, que se realizaron sin autorización judicial, permitieron la obtención de las claves de acceso que los proveedores de servicios de Internet asignan a cada ordenador en el momento que se conecta a la Red (estas claves –IPS– permiten identificar de forma indubitada a través de los referidos proveedores el número telefónico desde el que se produce la conexión). De esta forma conocieron qué IPS habían accedido a los "Hash" que contenían pornografía infantil. Pues bien, el TS, tras realizar un recorrido sobre la legislación vigente y la jurisprudencia constitucional consolidada, plasma dos criterios jurídicos:

- Los rastreos policiales para desenmascarar la identidad críptica de los IPS no precisan de autorización judicial, dado que el acceso a dicha información puede efectuarla cualquier usuario (es público, por lo tanto) y es el propio usuario quien lo ha introducido en la red.
- El desvelamiento de la identidad de la terminal, teléfono o titular del contrato de un determinado IPS precisa de autorización judicial, al constituir una injerencia en el derecho a la intimidad personal (*habeas data*), todo ello de conformidad con lo regulado en el artículo 18.3 CE, Ley Orgánica de Protección de Datos de Carácter Personal y Ley General de Telecomunicaciones.

IV. A MODO DE CONCLUSIÓN

El ciberterrorismo es un fenómeno criminal que se nutre del desarrollo tecnológico de la sociedad digital. Por lo tanto, es una criminalidad del siglo XXI, caracterizada por un trazo ejecutivo transnacional que se pergeña en organizaciones complejas, carentes de una ubicación espacial definida y dotadas de estructuras de financiación y medios técnicos suficientes para ejecutar delitos muy graves y hacer desaparecer, en escaso tiempo, las fuentes de prueba de su comisión y autoría. Por ello, las respuestas públicas a este tipo de criminalidad no pueden confiarse a un sistema penal que responda a las claves políticas diseñadas en los siglos XVIII y XIX. Las políticas punitivas del Estado-nacional, elaboradas con arreglo a los criterios de soberanía que hacen del territorio delimitado por las fronteras un espacio físico infranqueable, constituyen una invitación implícita a la impunidad o a la insuficiencia sancionadora del cibercrimen. Ello hace plausible los esfuerzos, alentados por entidades supranacionales, como la Unión Europea, o internacionales, como el Consejo de Europa, tendentes a impulsar políticas de progresiva aproximación de la legislación penal y procesal de los Estados y a promover estructuras y dinámicas eficaces de cooperación judicial y policial. La actuación en el plano normativo permite, en el orden sustantivo, unificar los delitos y homologar las sanciones penales, cercenando, de esta manera, los espacios de impunidad o de un trato significativamente favorable. El esfuerzo en el orden procesal favorece la implantación de una línea de actuación procedimental respetuosa con los derechos de los acusados –estrategia garantista– y eficaz con la tutela de las víctimas –estrategia protectora–.

BIBLIOGRAFÍA

ÁLVAREZ, Maite; (2001), "Consideraciones político criminales sobre la delincuencia informática: el papel del Derecho Penal en la red", *Cuadernos de Derecho Judicial*, X, 255-279.

ARIAS, José Manuel; (2007), "La cooperación judicial penal y policial", *Estudios de Derecho Judicial*, 117, 17-144.

BAUMAN, Zygmunt; (2004), *La sociedad sitiada*, Fondo de Cultura y Económica de Argentina, Buenos Aires.

BLANCO, Isidoro; (2004), "Crisis del principio de jurisdicción universal en el Derecho Penal Internacional Contemporáneo", *La Ley*, nº 5980 y 5981.

CHOCLÁN, José Antonio; (2001), "Fraude informático y estafa por computación", *Cuadernos de Derecho Judicial*, X, 305-365.

DE LA CUESTA, José Luis; (2008), "Armonización penal en la Unión Europea", *La Reforma de la Justicia Penal*, 135-169.

DE LA MATA, Noberto J; (2007), "Los delitos vinculados a las tecnologías de la información y la comunicación en el Código Penal: panorámica general", *Cuadernos Penales José María Lidón*, 4, 41-84.

DE LUCAS, Javier; (2008), *La extensión de los agentes del pluralismo*, Colección Pensamientos-Pentsamendu, Taldea, 4, Servicio de Publicaciones, Gobierno Vasco.

DEL ROSAL BLASCO, Bernardo; (2001), "Criminalidad organizada y nuevas tecnologías: algunas consideraciones fenomenológicas y político-criminales", *Cuadernos de Derecho Judicial*, II, 145-167.

DELGADO, Joaquín; (2008), "Novedades del espacio judicial europeo penal", *Derecho y Jueces*, 43, 3-4.

GONZÁLEZ LÓPEZ, Juan José; (2007), "Infiltración policial en Internet: algunas consideraciones", *Revista del Poder Judicial*, 85, 81-117.

GONZÁLEZ RUS, Juan José; (2007), "Precisiones conceptuales y político-criminales sobre la intervención penal en Internet", *Cuadernos Penales José María Lidón*, 4, 13-40.

GUTIÉRREZ, Ángeles; (2008), "La orden de detención europea y el futuro de la cooperación judicial penal en la Unión Europea. Reconocimiento mutuo, confianza recíproca y otros conceptos clave", Consejo General del Poder Judicial, *Manuales de Formación Continuada*, 42, 17-51.

IRURZUN, Fernando; (2007), "Principio de confianza y reconocimiento mutuo", *Estudios de Derecho Judicial*, 117, 145-165.

JIMENO, Mar; (2008), "La conclusión del Tratado de Lisboa: avances y concesiones en materia de cooperación judicial penal", *La Ley*, 7023, 1-9.

LEZERTUA, Manuel; (2001), "El proyecto de Convenio sobre el Cybercrimen del Consejo de Europa", *Cuadernos de Derecho Judicial*, X, 15-61.

LÓPEZ BARJA DE QUIROGA, Jacobo; (2001), "Posición de la Unión Europea sobre el crimen organizado", *Cuadernos de Derecho Judicial*, II, 113-143.

LÓPEZ ORTEGA, Juan José; (2008), "La protección de los derechos fundamentales de la persona reclamada en el sistema de entrega instaurado por la orden europea de detención", *Manuales de Formación Continuada*, 42, 293-353.

MATA, Ricardo M; (2007); "Delitos cometidos mediante sistemas informáticos (estafas, difusión de materiales informáticos, pornográficos, ciberterrorismo)", *Cuadernos Penales José María Lidón*, 4, 129-171.

MIR PUIG, Santiago; (2007), "Constitución, Derecho Penal y Globalización", *Política Criminal y Reforma Penal*, B de f, Montevideo-Buenos Aires, 3-13.

MONTEIRO, Manuel; (2008), "La cooperación en materia procesal penal. Los engaños y las ilusiones formales de los instrumentos jurídicos europeos e internacionales", *La Ley*, Año XXIX, 6914, 1-5.

MORENO CATENA, Víctor; (2008), "La cooperación jurídica internacional", *Problemas actuales del Derecho Penal y de la Criminología*, Tirant lo Blanch, Valencia, 1165-1192.

MORÓN, Esther; (2007), "Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos", *Cuadernos Penales José María Lidón*, 4, 85-128.

RODRÍGUEZ, Antonio Pedro; (2006), "Los cibercrímenes en el espacio de libertad, seguridad y justicia".

SÁNCHEZ, Isabel; (2005), *La Criminalidad Organizada. Aspectos penales, procesales, administrativos y policiales*, Dykinson SL, Madrid.

SANZ, Ágata; (2003), "El futuro espacio europeo de justicia penal", *Revista Poder Judicial,* 71, 175-191.

SILVA, Jesús María; (2006), *La expansión del Derecho Penal*, B de f, Montevideo-Buenos Aires.