Criptología y Delito Informático

JESÚS MARÍA MINGUET MELIÁN
JOSE MARÍA MOLINA MATEOS
Asociación Española de Criptología
LUCRECIO REBOLLO
U.N.E.D.

1.- INTRODUCCIÓN.

Con la utilización de las nuevas tecnologías de la información y las comunicaciones está surgiendo un ámbito donde se reproducen las relaciones clásicas del individuo y de los grupos en que se integra, pero en un marco distinto, entre cuyas características está la facilidad de relaciones e intercambios, con eliminación de las barreras de la distancia y del tiempo.

El nuevo espacio relacional está creando formas diferentes de socialidad, a nivel global. Sobre las sociedades actuales se está superponiendo una nueva forma de sociedad con distinta delimitación y ámbito y con desiguales niveles de desarrollo de los elementos que la integran.

La Sociedad de la Información se encuentra en un momento donde tecnológicamente es posible la comunicación global, pero aún no dispone de los instrumentos de ordenación necesarios. Es una sociedad con un nivel incipiente de estructuración, en la que el desarrollo tecnológico no se corresponde con el desarrollo social.

En este particular el *estado de naturaleza* (cibernético) son frecuentes los ilícitos cometidos con la utilización de medios informáticos.

Estos ilícitos tienen unas características especiales en cuanto a la forma de su comisión y detección -llegando incluso a ser imposible su descubrimiento, en determinadas circunstancias- y en todo caso, tienen una gran dificultad probatoria, lo que les convierte en actos *sui generis*, cuya prevención y persecución requieren medios idóneos, adecuados al entorno tecnológico en el que operan.

Las características del medio en que se producen, la magnitud e intensidad de sus efectos, las dificultades probatorias y la irreversibilidad del daño causado orienta, en gran medida, la lucha contra este tipo de actos delictivos hacia la utilización de una prevención eficaz que incorpore activos tecnológicos y científicos de niveles similares a los utilizados para su comisión.

La prevención así entendida resulta de gran utilidad para la sociedad, pero también puede provocar graves peligros e incluso amenazar la democracia, si bajo el pretexto de evitar conductas antisociales o delictivas multiplica los obstáculos para el ejercicio de las libertades.

Las mayores aplicaciones de la teoría de la información se han realizado en la construcción de automáticos, esto es, en la cibernética.

La confluencia de teoría de la información y cibernética en la informática ha permitido que las cantidades y grados de certeza, se trate conjuntamente con los ingenios automáticos que permiten su tratamiento y las técnicas para su construcción. Lo que, desde el punto de vista filosófico, supone el vaciamiento de todo significado de las tradicionales antítesis metafísicas entre materialismo y espiritualismo y, positivamente, viene a descubrir y poner en práctica instrumentos que expresan la situación en la que se encuentra el hombre en el mundo, en el que lucha por un orden que nunca es definitivo.

Lo que caracteriza el desarrollo actual no es sólo la potencialidad de los intercambios de información, sino que ha transformado, tras un salto cualitativo, los propios contenidos de la información y los canales de comunicación tradicionales, debido, esencialmente, a la extensión e interconexión de los sistemas y redes de información; al desarrollo paralelo y convergente de la tecnología de las comunicaciones, y a la combinación de ambas tecnologías para conformar un contexto radicalmente nuevo de la información y la comunicación.[1]

■ [1] P. Sieghart, *'Privacy and Computer'*, Latimer, London, 1.976.

La tecnología, la sociedad, el derecho, podrían ser considerados, como unidades sistémicas, entendiendo por *sistema* una totalidad ordenada o sea, un conjunto de entes, entre los cuales existe un cierto orden.

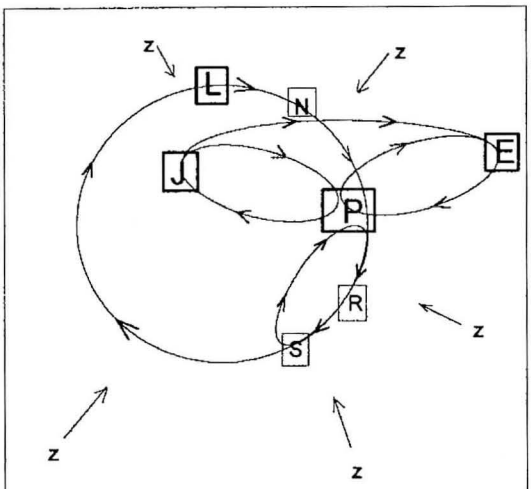
La tecnología se podría considerar un sistema que, como todos los sistemas, en ciertos aspectos interactúa con otros sistemas y en otros está aislado de los mismos.

La noción cibernética de sistema ha sido proyectada al análisis del sistema social y del sistema, o subsistema jurídico.

El sistema social es un elemento racionalizador dirigido a la reducción de la complejidad ambiental, mientras que el sistema jurídico aparece encaminado a la reducción de la complejidad autoproducida.

En todo caso y con independencia que la tecnología, la sociedad y el Derecho se consideren sistemas interdependientes o subsistemas integrados, existe una evidente interelación entre ellos.

Para la opinión pública y el pensamiento filosófico, jurídico y político de nuestro tiempo constituye un problema esencial el establecimiento de unas garantías que tutelen a los ciudadanos frente a eventuales agresiones tecnológicas de sus derechos.



L= Poder Legislativo.
E= Poder Ejecutivo.
J= Poder Judicial.
N= Normas.
R= Realidad social.
S= Sociedad.
P= Conductade los ciudadanos.
Z= Factores distorsionantes externos.

SISTEMA TECNOLÓGICO Y SISTEMA JURÍDICO
(Adaptación del cuadro de Andrzej Kisza)

Esta cuestión, que incide directamente en las estructuras jurídicas, tiene actualmente interés prioritario en una sociedad en la que el poder de la información ha adquirido una importancia capital y en la que la posibilidad de comunicación y de acceso a la información aparece como una forma irrenunciable de libertad.

En el conjunto que forman los medios telemáticos y sus relaciones al que nos atrevemos a denominar como *Cibersfera*, el Derecho debe dar respuesta a la ordenación del progreso técnico, y evitar un desarrollo irresponsable que desencadena poderes que pueden quedar fuera de control de no establecerse las oportunas garantías jurídicas.

La complejidad de la vida moderna, las inmensas posibilidades que se ofrecen para dejar en el anonimato o en la impunidad conductas antisociales o delictivas exigen la puesta en funcionamiento de medios de información y control.

La alternativa razonable no puede ser otra que la de una disciplina jurídica eficaz y democrática de los medios tecnológicos de información y control.[2] El principio de legalidad característico del derecho punitivo moderno, hace que el estudio del derecho penal tenga que versar siempre sobre un determinado derecho positivo, esto es, conjunto de normas condicionadas por circunstancias históricas de tiempo y espacio.

Cualquier indagación teorética ha de tener presente esa naturaleza concreta, individualizada, *existencial*, contingente y relativa del objeto de estudio, y abandonar cualquier pretensión de ver en todo ordenamiento jurídico-penal la versión de una justicia absoluta. Lo que sin duda le da un carácter dinámico.

El Derecho penal cubre con sus sanciones una parte fundamental de la constitución política del Estado y, además, generalmente las tendencias políticas tienen su traducción en la legislación punitiva.

La política criminal, en abstracto, como teoría de lo posible, es la adecuación de los medios que tiene el Estado para emplearlos en la lucha contra el delito. Se ocupa de los problemas utilitarios que presenta la realidad en la lucha contra el delito.

Y en concreto política criminal es aquella política relativa a cuales sean las soluciones legislativas más adecuadas a una determinada situación concreta lo que implica el conocimiento de las formas reales de comisión del delito y los medios idóneos de lucha contra el mismo, cuyo estudio es el objeto de la Criminología.

Por cuanto se refiere a la definición de delito informático tal vez sea de aplicación lo que dijo Javoleno Prisco *omnis definitio, in iure civile, periculosa est* , (Digesto, Libro 50, Texto 17, Par. 202). El brocardo advierte que las definiciones legales pueden ser peligrosas en cuanto que pueden provocar un aislamiento de la realidad y ser en este sentido cuestionables.

Por tanto los delitos cometidos con la utilización de nuevas tecnologías deben positivizar conceptos dogmáticos de Derecho penal que respondan a necesidades técnicas y político-criminales consolidadas.

La Criminología no se ocupa de las normas jurídicas, sino de los hechos que subyacen en esas normas. Es una ciencia empírica que opera con conceptos

■ [2] Antonio-Enrique Pérez Luño, llNuevas tecnologías, sociedad y derechomm, El impacto socio-jurídico de la N.T. de la información. FUNDESCO, 1.987.

criminológicos de delito previamente delimitados por el Derecho penal, lo contrario impediría distinguir el delito de la conducta antisocial, o la Criminología de la Sociología.

Con independencia del estudio de las formas reales de comisión del delito, etiología o prognósis, por lo que respecta a este trabajo destacaríamos el estudio de las formas de manifestarse la lucha contra el delito y , además de la criminalística y la penología, señalamos muy especialmente la llprofilaxis criminalmm a la que está encomendada la lucha puramente preventiva contra el delito.

La peligrosidad predelictual como elevada probabilidad de delinquir, en un grave problema social, y por la razones indicadas, en la Sociedad de la Información se pone especialmente de manifiesto cuando para llevara efecto ilícitos penales se utilizan las nuevas tecnologías, pero su estudio no es competencia del Derecho punitivo.

La adopción de medidas para combatir la peligrosidad antedelictual o lpeligrosidad sin delitomm, es materia del Derecho Civil y del Derecho Administrativo.

Mientras exista el principio de legalidad, es de todo punto necesario que estas medidas de carácter puramente preventivo o profiláctico guarden la debida distancia con las que corresponden al Derecho penal.

Estas medidas de seguridad, son medidas de defensa social o medidas de protección, dentro de las cuales estarían las restictivas de derechos, cuando la peligrosidad dimana de circunstancias ambientales.[3]

■ [3] Rodriguez Devesa,mmDerecho Penal Españolmm, Parte General,

2.- La Criptología como objeto de protección de derechos y libertades.

En el ámbito de los derechos y libertades, se establece por parte de la doctrina una tabla de generaciones de derechos: 1ª derechos individuales, 2ª derechos sociales, 3ª derechos económicos y 4ª derechos de solidaridad.

Con respecto a las nuevas tecnologías, no creemos conveniente establecer una quinta generación de derechos, pero por el contrario, sí se observa la necesidad de adecuar los planteamientos jurídico-normativos a las nuevas necesidades sociales.

A ningún observador de la realidad social se le escapa, que las violaciones de la legalidad están vigentes desde que el hombre lo es. Por el contrario, han evolucionado las formas de violación o lesión de los derechos y libertades, que constituyen el núcleo de protección jurídica de la persona. Siendo además unos derechos que gozan de una mayor protección, dada su capital importancia, no podemos obviar su ejercicio real y efectivo.

Los ordenamientos jurídicos europeo y español, han establecido ya los pilares normativos de esta regulación. Pese a todo, faltan regulaciones de rango inferior a la de ley, que configuren de forma conveniente la protección. También han de establecerse los mecanismos técnicos necesarios para que la ejecución y libre desarrollo del derecho sea efectiva, tenga plausibilidad.

La Criptología como elemento garante y sobre todo, como medio de prevención, viene a solventar de forma resuelta la problemática que deja abierta o que no resuelve, el ordenamiento jurídico.

A pesar de la insistencia de algunos autores en distinguir a la informática como una posibilidad nueva de agresión de derechos del hombre, nuestra postura se encamina en base a la idea de que los nuevos medios técnicos establecen nuevos mecanismos de lesión o violación, pero el fondo, lo substancial se resume prácticamente en los mismos fundamentos.

Con el nacimiento del Estado, la dialéctica política pretende discernir entre Estado intervencionista o abstencionista. La evolución del Estado Social y el Estado Social y Democrático de Derecho, y el surgimiento del Estado del Bienestar, no ha eliminado la dicotomía que sigue estando presente. Los problemas que plantea la informática y el posicionamiento del Estado, con respecto al respeto de los derechos, y en concreto al derecho a la intimidad, nos retrotraen a unas posibilidades de opción, que ya se planteaban en el siglo XVIII.

Por todo ello, no podemos analizar el papel de la criptología, salvadas las circunstancias técnicas, mas que desde el punto de vista que deslinde entre la protección de derechos y libertades y sus posibles lesiones. De esta forma, la criptología viene a ser un nuevo método, una técnica de aplicabilidad de algo reconocido históricamente y que ha evolucionado en su ejercicio, los derechos fundamentales. La pretensión de aquella se identifica de esta forma, aunque en mayor nivel, dada la socialización actual, y sobre todo por la eliminación de las barreras de tiempo y espacio, con una garantía asimilable al lhabeas corpusm, al derecho de inviolabilidad de la correspondencia que ya reconociera la Constitución Española de 1.812.

La criptología es un elemento de garantía, de eficacia y virtualidad de los derechos. Siendo los derechos fundamentales los configuradores esenciales de un orden social, viene a constituirse en un elemento esencial en una sociedad tecnológicamente avanzada.

Los derechos fundamentales, entre los que destaca en la actualidad deforma muy significativa, el de la intimidad, no son en ningún caso derechos absolutos y excluyentes, sino que por el contrario, pueden y deben ceder ante los límites que vienen establecidos en la constitución o los que deriven de otras normas (S.T.C. 11/1.981 y 2/1.982). Ahora bien, las limitaciones que se establezcan no pueden obstruir el derecho fundamental más allá de lo razonable (S.T.C. 532/1.986). De todo lo manifestado, se infiere, que todo acto o resolución que limite derechos fundamentales ha de asegurar que las medidas limitadoras sean necesarias para conseguir el fin perseguido, ha de atender a la proporcionalidad entre el sacrificio del derecho y la situación en que se halla aquél a quien se le impide y, en todo caso, ha de respetar su contenido esencial.

En resumen, todo lo manifestado se traduce en el término equilibrio. Equilibrio por parte del legislador, del aplicador (tribunales) y también de aquél que ejecuta el ordenamiento jurídico de forma más directa. La clave es sopesar derechos, buscar un punto equidistante. Y para ello, la criptología es un elemento de contrapeso muy significativo.

3.- La Criptología como medida de prevención.

La peligrosidad predelictual derivada de la de la Sociedad de la Información pone de relieve un problema que rebasa los límites de nuestras fronteras y requiere soluciones supranacionales, que demandan cooperación internacional como paso previo imprescindible para abordar la ordenación de un fenómeno que es planetario.

La seguridad como situación de la información y las comunicaciones exentas de peligro, daño o riesgo, resulta difícil cubrir en su plenitud conceptual y, en todo caso, viene determinada por los peligros, riesgos y amenazas a que puedan verse sometidas.

Resulta difícil hablar de seguridad, ya que la seguridad absoluta no existe. Para poder establecer que un sistema informático es seguro sería necesario identificar todas las amenazas a las que puede verse sometido y tomar todas las medidas preventivas y de seguridad correspondientes, por lo que tal vez sea más adecuado hablar de vulnerabilidad.

Para el profesor Sanz Caja, la vulnerabilidad de un sistema informático es la cualidad que le hace susceptible de ser afectado, alterado o destruido por algún hecho o circunstancia indeseados, de recibir algún daño o perjuicio en cualesquiera de las partes o componentes, que afecte al funcionamiento normal o previsto de dicho sistema informático.[4]

Análogamente define la seguridad de un sistema informático como el estado de protección del mismo, establecido con el fin de evitar la aparición de las distintas amenazas posibles que puedan alterar su normal funcionamiento, o de aminorar las consecuencias negativas de los distintos riesgos, una vez producidos.

Dada la naturaleza de la información y las comunicaciones, las medidas de seguridad pueden ser de diversos tipos, entre las que se destacan las medidas políticas, legales, organizativas, físicas y lógicas.

Dentro de las medidas físicas, además de las clásicas, se incluirían las destinadas a neutralizar las agresiones electromagnéticas y dentro de las lógicas se incluyen las medidas criptológicas, en cuya base se encuentra la Criptología que opera mediante procedimientos para la ocultación o cifrado de la información, lo que requiere una previa delimitación de ámbitos de confidencialidad en cuya defensa opera la Criptología.

■ [4] Sanz Caja, V., llVulnerabilidad y seguridad de los sistemas informáticosmm, Fundación CITEMA, Madrid 1.982.

A diferencia de las medidas legales que actúan lla posteriorimm, las medidas criptológicas operan lla priorimm en evitación que el hecho delictivo se produzca, lo que las configura como un medio esencial para la prevención de ilícitos cometidos con la utilización de las nuevas tecnologías.

La Criptología moderna como medio para la protección de la información y las comunicaciones, a través de la preservación de la confidencialidad, la integridad y el control de accesos en un sistema de información, da respuesta a las tres propiedades fundamentales de la seguridad de la información y brinda a las nuevas tecnologías la posibilidad de reparar, por sus medios, el desequilibrio que su aplicación introduce en la socialidad.

La Criptología se incorpora a la sociedad de la información como instrumento tecnológicamente eficaz para hacer efectivo el funcionamiento de los principios básicos reguladores de la ordenación social: Poder y el Derecho, cuya armónica combinación es el llarte de la políticamm.

La Sociedad de la Información demanda una ordenación política y jurídica, y en este contexto exige medidas de prevención eficaces contra la comisión de ilícitos y garantía de derechos y libertades, lo que puede lograr dando acomodo a las medidas criptológicas en las aplicaciones de las nuevas tecnologías de la información y las comunicaciones que han sido y son la razón de ser de este nuevo modelo de sociedad.

No obstante, la aplicación de medidas criptológicas comportan la eficacia en la sustracción de información al conocimiento público, por lo que puede suponer, eventualmente, una limitación del ejercicio de la democracia, y exige una regulación en consonancia con sus fines en una sociedad democrática.

El Convenio Europeo para la protección de Derechos Humanos y Libertades Fundamentales, de 4 de diciembre de 1.950, en su artículo 10 dice: 1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras... 2. El ejercicio de estas libertades, por cuanto implica deberes y responsabilidad, puede ser sometido a ciertas formalidades, condiciones, restricciones o sanciones previstas por la Ley, que constituyan medidas necesarias, en una sociedad democrática, para la seguridad nacional, integridad territorial o la seguridad pública, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, la protección de la fama o de los derechos de otro, para impedir la divulgación de informaciones confidenciales o para garantizar la autoridad y la imparcialidad judicial.

De igual modo, el artículo 29.2 de la Declaración Universal de los Derechos Humanos, de 10 de diciembre de 1.948, dice: *En el ejercicio de sus derechos y en el disfrute de sus libertades toda persona estará solamente sujeta a las limitaciones establecidas por la Ley, con el único fin de asegurar el reconocimiento y el respeto de los derechos y libertades de los demás, y de satisfacer las justas exigencias de la moral, del orden público y del bienestar general en una sociedad democrática.*

Para el artículo 19.2 del Pacto Internacional de Derechos Civiles y Políticos, de 16 de diciembre de 1.966, el ejercicio de la libertad de expresión entraña deberes y responsabilidades especiales, *por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la Ley y ser necesarias para: a) Asegurar el respeto a los derechos o a la reputación de los demás; b) La protección de la seguridad nacional, el orden público, la salud o la moral pública.*

O más recientemente la Resolución del Parlamento Europeo de 1.989, por la que se aprueba la Declaración de los Derechos y Libertades Fundamentales en la que se recoge la libertad de opinión y de información, la protección y respeto a la esfera privada, vida familiar, honor, domicilio y las comunicaciones, dentro de los límites razonables y necesarios en una sociedad democrática, sin que se permita el abuso de derechos.

De las normas reseñadas y de las contenidas en numerosas constituciones nacionales se deriva la existencia de dos bloques de comunicaciones claramente diferenciadas, las comunicaciones públicas regidas e inspiradas por la libertad de expresión donde la norma general es la transparencia y la excepción el secreto; y las comunicaciones privadas donde la norma general es el secreto y la excepción la transparencia. (En España la Constitución de 1.978 artículos 18.3 y 20).

Este carácter general o excepcional del secreto, así como la naturaleza de la información, pública o privada, va a determinar el uso de la Criptología y los niveles de protección.

Dejando al margen los niveles criptológicos dirigidos a la protección de comunicaciones que afecten a la seguridad y defensa del Estado que estaría dentro del ámbito de los servicios de inteligencia, la importancia dada a la protección criptológica de la información en general se pone en evidencia por las diversas iniciativas internacionales llevadas a cabo para su regulación.

El Secretario de Prensa de la Casa blanca anunció el 16 de abril de 1.993, la iniciativa de la Administración de los Estados Unidos conocida como *Clipper Chip*; la Recomendación del Consejo de Europa en relación con las Directrices para la Seguridad de los Sistemas de Información de 26 de noviembre de 1.992, la Directiva del Parlamento europeo y del Consejo de la Unión europea de 24 de

octubre de 1.995 sobre la protección de los individuos en relación con el procesamiento de datos personales y el libre movimiento de dichos datos, el Green Book on the Security of Information Systems, o las llevadas a cabo en el seno de la Organización para la Cooperación y el Desarrollo Económico (O.C.D.E.), de 26 de noviembre de 1.992, marzo de 1.996 y 27 de marzo de 1.997, ponen en evidencia la importancia de la cuestión.

La protección efectiva de la información y las comunicaciones tiene una serie de repercusiones en las que pueden colisionar derechos e intereses de distinta naturaleza, tales como las libertades de expresión e información, el secreto de las comunicaciones, la libertad informática, la privacidad, la averiguación y prevención del delito o la seguridad del Estado, que influyen en el normal funcionamiento de la sociedad y del Estado, lo que unido a su carácter supranacional de la información y las comunicaciones hace que sea un tema político esencial en el mundo contemporaneo.

Esta situación exige la armonización de todos los intereses en juego para obtener un resultado que posibilite el cumplimiento razonable de todos los derechos en presencia que son derechos que responden a principios distintos y las relaciones entre las normas que los sustentan pueden ser complejas.

La técnica de la ponderación de bienes, como método para determinar cómo, cuando y en qué medida debe ceder el derecho fundamental que entra en colisión con otro es consecuencia del carácter no absoluto de los derechos fundamentales y de las libertades públicas, otorga un gran margen de discrecionalidad al juzgador.

Dada la complejidad e importancia de unas comunicaciones globales se requiere reducir la discrecionalidad mediante la adecuada producción normativa, con independencia de que se esté en sistemas judiciales basados en la libre creación judicial como el Common Law, o sistemas judiciales continentales en los que el papel del juez es el ser *la voz de la ley.*

Como valoración de conjunto se podría afirmar que por cuanto se refiere a la protección efectiva de las comunicaciones aún estamos en un régimen de insuficiencia normativa, de donde se deriva la necesidad de caminar hacia un marco legal adecuado que dé respuesta a todas las necesidades de protección de la información y las comunicaciones en una moderna sociedad democrática, donde se contemple la protección criptológica como forma de asegurar al ciudadano el libre y tranquilo ejercicio de los derechos que le reconoce la ley y brinde a la Sociedad los elementos necesarios para garantizarlo.

4.- La Criptología como obstáculo en la persecución del delito.

La seguridad es el autentico talón de Aquiles de la Sociedad de la Información

El secreto de las comunicaciones privadas se configura como un derecho que garantiza a los particulares una esfera de libertad que debe ser respetada por los poderes públicos, y que puede convertirse en un derecho de no injerencia, salvo los supuestos de su limitación previstos por Ley y con las garantías debidas, y constituye una expresión concreta de la libertad de comunicaciones. Cualquier limitación de estas libertades sólo es válida en cuanto hecha por ley.

La seguridad de la información, en si misma, como bien jurídico digno de protección empieza a abrirse paso en la doctrina.

El Convenio de Roma de 4 de noviembre de 1.950, en su artículo 8º dice que *1.-Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.- 2.- No puede haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta interferencia esté prevista por la Ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral o la protección de los derechos y las libertades de los demás.*

El secreto de las comunicaciones tiene un carácter omnicomprensivo y es aplicable a cualquier medio o servicio que sirva para la transmisión de las mismas, la cobertura no se otorga sólo y exclusivamente a la correspondencia como dice el Convenio de Roma, -o a las comunicaciones postales, telegráficas y telefónicas, como dice la Constitución Española de 1.978 en su artículo 18.3-.

El empleo de la criptografía dificulta la investigación de actos delictivos y, de hecho, algunos casos judiciales se han visto obstaculizados en su investigación por esta causa, pero es previsible una mayor incidencia en el futuro, por eso es una preocupación general buscar leyes y medios técnicos que permitan esta investigación.

Fuera de los supuestos excepcionales, el Estado debe abstenerse de interferir las comunicaciones, y desde el punto de vista positivo tiene la obligación de procurar la efectividad del derecho de secreto de las mismas, lo que supone la obligación de garantizar de forma eficaz la seguridad de las comunicaciones y, consiguientemente su secreto -lo que se logrará mediante su adecuada protección criptológica- y también tiene la obligación de estar en condiciones técnicas de

poder -también de forma eficaz- llevar a término el cumplimiento del mandato legal o judicial, cuando a través de la oportuna resolución, se ordene la intervención de las comunicaciones, incluso en el caso de estar protegidas criptológicamente.

Ante esta situación el Estado tiene varias posibilidades:

1.- Prohibir el uso de sistemas criptográficos resistentes y permitir solo el uso de *criptología débil* que pueda ser solucionada mediante el criptoanálisis.

Esta opción tiene una serie de inconveniente:

a) Sería similar a no tener protección, pues estas comunicaciones podrían ser abordadas igualmente por terceros que dispusieran de estos medios de criptoanálisis.

b) La disponibilidad pública de algoritmos de cifrado de los más distintos niveles hacen imposible el control de uso solo de criptología débil.

c) La existencia de investigadores independientes produce que los niveles de protección de la criptología débil sean fácilmente desbordados.

d) Por todo ello este procedimiento no parece ser eficaz ante criminales, terroristas, narcotraficantes o la delincuencia en general. Y, por el contrario, impide el legítimo derecho de una protección eficaz del secreto de las comunicaciones.

2.- Imponer sistemas criptológicos robustos, pero diseñados de modo que no sea posible esconder el contenido de los mensajes durante una investigación judicial.

3.- Otras propuestas pretenden que la justicia tenga capacidad para exigir la entrega de la clave usada en una comunicación criptográfica, lo que puede suponer la vulneración del derecho de no autoinculpación reconocido en muchos países democráticos.[5]

[5] htt p://patas.eleinf.uv.es/ rosich/issii/legal.htu. Abril 1.997.

El alcance del concepto de intervención de las comunicaciones, cuando estas son cifradas, rebasa la mera interceptación e incorpora al proceso exigencias de naturaleza criptológica que hagan posible el conocimiento de su contenido, lo que añade una complejidad aún mayor tanto organizativa como tecnológica y obviamente jurídica.

El derecho al secreto de las comunicaciones no es absoluto y su protección jurídica se ha de construir sobre un delicado equilibrio entre el interés privado y el interés estatal en perseguir determinados objetivos que hagan necesaria la intromisión en la esfera privada y hacer que decaiga el secreto de las comunicaciones.

No cabe duda de la legitimación del Estado para interferir en este derecho, pero en determinadas condiciones y con las debidas garantías.

La complejidad tecnológica presente y previsible, exige para que el control judicial sea eficaz, un auxilio de elevado componente tecnológico, organizativo y criptológico. El Juez es vigilante constitucional tanto del derecho de secreto de las comunicaciones como de sus excepciones.

Las garantías internas que los Estados conceden a los derechos fundamentales a veces resultan insuficientes. Por lo que se refiere a la garantía real y efectiva del secreto de las comunicaciones, insuficiencias tecnológicas pueden impedir una protección adecuada o resultados positivos del criptoanálisis en los casos de intervención judicial, ambas, manifestaciones concretas de garantía de derechos, lo que tal encontraría respuesta en la instauración de un poder común por encima del estatal, con el que sea posible la resolución de problemas frente a los que el Estado está indefenso.[6]

La necesidad de colaboración internacional resulta obvia, sobre todo frente a los nuevos problemas surgidos por del desarrollo de las nuevas tecnologías, lo que viene a poner el acento en la imprescindible consideración del individuo como sujeto de Derecho internacional.

Pero el reconocimiento del carácter vinculante de una instancia supranacional, depende del poder estatal. Para que esa nueva instancia pueda desempeñar su papel, es necesario que el Estado reconozca su competencia[7].

■ [6] Peces-Barba, G., llDerecho positivo de los Derechos Humanosmm, edit. Debate, Madrid, 1.987.
■ [7] De Asis Roig, R., llLas paradojas de los derechos fundamentales como límites al podermm, Editorial Debate, Madrid, 1.992.

Tanto las normas internacionales, como las nacionales de rango constitucional, obligan a un desarrollo legislativo, ya que no basta con proclamar un derecho y su excepcional limitación, sino que hay que señalar los procedimientos, métodos y requisitos para que todo ello sea una realidad efectiva.

Ante la situación planteada por la vulnerabilidad de las comunicaciones se hace necesaria una efectiva actuación de los poderes públicos, que dado el carácter global de las comunicaciones, requiere acciones supranacionales, orientadas, en principio, hacia tareas de carácter normativo, y exige, además, para que la protección sea real y efectiva, la aplicación de medidas de seguridad -especialmente de naturaleza criptológica- que con carácter preventivo, impidan que la violación se produzca.

Con respecto a la criptología como obstáculo para la persecución y prevención del delito, surge el mismo problema apuntado con respecto de los derechos fundamentales. Esta circunstancia no es en absoluto nueva para el jurista. La problemática de la criptología en suma se reconduce a la protección de derechos. Idéntico es el problema de grabaciones (sonoras o de imagen), de violación de correspondencia (esté en el soporte que esté), de entrada en locales o viviendas particulares, o por poner un último ejemplo, del control de alcoholemia a los conductores de vehículos.

Desde la perspectiva jurídica, que es la que nos interesa, estas dicotomías, son clarificadas -en el caso de España- en parte por la Constitución, y de forma más significativa por la jurisprudencia del Tribunal Constitucional. Este alto tribunal, viene resolviendo estos conflictos entre derechos, y de forma más concreta entre derechos fundamentales, en base ala idea de primacía de unos derechos sobre otros o lo que es lo mismo, su mayor virtualidad. A título de ejemplo, conocemos por su jurisprudencia, que prima el derecho a la intimidad sobre el derecho a la información, salvo en determinadas personas que tienen una actividad de relevancia pública. De igual forma, conocemos que prima el interés social sobre el individual en cualquier tipo de manifestación social (sanidad, seguridad pública, etc.).

Así, la criptología, como reiteradamente hemos manifestado, no constituye una especialidad, sino un mecanismo más dentro del intrincado social. a primera vista, la criptología, no cabe duda de que se constituye en un elemento que obstaculiza la persecución del delito, pero a su vez, es un elemento de garantía de derechos.

De esta forma la criptología es un medio, que puede ser utilizado tanto por el ejemplar ciudadano, como por el más indeseable delincuente. Pero el mismo problema observamos por ejemplo en la presunción de inocencia de un terrorista.

Con todo, los análisis jurídicos, por muy sociales que sean, no pueden estar en el desconocimiento de la existencia de un ordenamiento jurídico. No podemos extraer los problemas de su contexto, o darles soluciones fuera del mismo. Así, el conflicto que plantea la criptología ha de solucionarse en primer lugar en base a las resoluciones ya establecidas por el Tribunal Constitucional, es decir, la primacía de unos derechos sobre otros, incluyendo en estos a los derechos fundamentales y a las libertades públicas. Un segundo paso viene establecido por una regulación, que sin vulnerar lo establecido en el ordenamiento jurídico intente delimitar el uso de medios, sistemas o tecnologías en base a un contexto ordenado mediante normas.

Somos conscientes, que esta construcción jurídica plantea dificultades de aplicación cuando hay que ponerse a establecer los límites precisos (pensemos por ejemplo en la delimitación entre intimidad y seguridad pública). Más aún, la Ley Orgánica para la Regulación y Tratamiento de los Datos de carácter personal, cuando se refiere a los ficheros pertenecientes a los cuerpos y fuerzas de Seguridad del Estado, emplea una serie de términos de difícil precisión conceptual. Pero a su vez, una interpretación amplia del derecho a la intimidad puede constituirse en cobertura o en pretexto legal de la comisión de delitos.

Por todo ello, no podemos apartarnos de la idea que la criptología es un mecanismo, y como tal hay que conceptuarlo y tratarlo desde la perspectiva jurídica. Otra visión no dejaría de ser errónea, ajurídica y en todo caso, negativa socialmente.

5.- La Criptología en instrucción del proceso penal. Su valor probatorio.

El concepto de policía entendido como buen orden exige una toma de posición ante la llegada de las nuevas tecnologías de la información y las comunicaciones por cuanto inciden en bienes y derechos de los ciudadanos y afectan al funcionamiento de la comunidad.

Las funciones de las policías en los países democráticos se orientan a proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana mediante la prevención de la comisión de actos delictivos y la

persecución de los delincuentes, con lo que comporta de aseguramiento de instrumentos, efectos, pruebas, etc. y su puesta a disposición del Juez.

La eficacia de la función preventiva es compartida por todas las policías de los países democráticos. Para ello, además de captar información de interés para el orden y la seguridad pública, han de estudiar, planificar y ejecutar los métodos y técnicas de prevención de la delincuencia.

La policía judicial también ejerce una labor destacada en la instrucción de las causas por delito lo que le exige un elevado componente científico y tecnológico que le permita dar cumplimiento efectivo a las resoluciones del órgano jurisdiccional.

En todo caso cubrir las lagunas existentes en los ordenamientos jurídicos, nacionales e internacionales, por lo que se refiere a la plenitud de una regulación de la protección de la información y las comunicaciones, tal vez provocaría que la investigación judicial y policial podrían ser más complejas pero sin duda se ganaría en respeto a la persona y a los derechos fundamentales y se fortalecerán las instituciones.

Todo ello, eventualmente obligaría a nuevos, más imaginativos y sofisticados métodos de investigación y mayores niveles profesionales y tecnológicos en la realización de estas tareas.

Por cuanto se refiere al valor probatorio de una comunicación cifrada, con independencia del soporte en el que aparezca, -y presupuesta la autorización judicial para llevar a cabo su criptoanálisis- nos encontraríamos ante una situación en la que son necesarios conocimientos científicos para aseverar cual es su contenido, esto es, para poder determinar cual es el texto claro con el que se corresponde el criptograma, por lo que, además de monstrar el texto descifrado, se requiere acreditar de forma indubitada que este surge por aplicación de determinados métodos, códigos, algoritmos, etc. propios de la Criptología y así obtener la evidencia criptológica, lo que se conseguirá a través de la correspondiente prueba pericial que en este caso, sería pericial criptológica. Evidencia criptológica que en algunos casos será muy difícil determinar. La complejidad de los algoritmos empleados puede dificultar hasta el extremo de impedir la obtención de esa evidencia criptológica pero se pondría de relieve la potencia del alglritmo utilizado.

Una vez situados procesalmente en el texto de un documento, con independencia del soporte en que esté -gráfico, magnético, sonoro...-, se nos plantearían los problemas probatorios ordinarios de la naturaleza de los mismo, lo que se ventilará en prueba documental, dentro de la que puede, eventualmente

aparecer de nuevo la necesidad de una pericial criptológica -o caligráfica en el caso de textos escritos y firmados en soporte papel- para determinar la autoría, y muy especialmente en los casos de utilización de firma digital.

En todo caso, es un medio de prueba complejo, que el juez debe valorar de acuerdo con lo establecido en el ordenamiento jurídico vigente.

6.- Criptoanálisis.

La Criptología produce esencialmente un efecto preventivo en defensa de la información y las comunicaciones y, consiguientemente, en la protección de derechos y libertades. Pero la Criptología también puede ser utilizada para ocultar el delito y, en este sentido se convierte en un instrumento eficaz para el éxito de narcotraficantes, terroristas o delincuentes comunes.

Antes estas situaciones el Estado debe reaccionar en defensa de la Sociedad y ha de procurarse medios tecnológicos suficientes que le permita, con todas las garantías legales del caso, estar en condiciones de poder neutralizar la ilícita protección de la que se han valido los delincuentes, como una forma más de preservar el Estado de Derecho.

Uno de los procedimientos para obtener con éxito esa neutralización de la protección criptológica ilícitamente utilizada es mediante el criptoanálisis constituido por el conjunto de pasos y operaciones orientadas a transformar un criptograma en el texto claro original pero sin conocer inicialmente el sistema de cifrado utilizado y/o la clave.[8]

Existen varios métodos de ataque a un criptosistema, aunque los principales serian tres: Ataques a partir solo del texto cifrado, ataques a partir de un mensaje conocido, y ataques por elección.

El ataque por elección del mensaje se produce cuando el criptoanalista tiene acceso al sistema de información para introducir mensajes y observar el resultado cifrado.

Si tomamos como ejemplo el sistema de cifrado más usado, el DES de clave privada, que generalmente utiliza una clave de 64 bits (56 bits de clave más 8 bits de paridad) su ataque supone valorar las 72.057.594.037.927.936 (256) claves distintas, lo que para un computador que pudiera probar un millón de claves por segundo supondría unos 2.285. Este tiempo se reduciría de forma considerable -a horas-, utilizando supercomputadores con procesadores en paralelo, pero su coste los hacen inaccesibles para muchas organizaciones.

En cuanto al sistema de cifrado de clave pública RSA (de Rivest, Shamir y Adleman) se le puede atacar mediante la factorización (algoritmo de Schroeppel) que es el más eficiente. De todas formas, los tiempos promedios de ataque para

■ [8] Glosario de términos de Criptología, Centro Superior de Información de la Defensa, revisión marzo de 1.993.

una clave de 100 dígitos y un computador que procese un millón de claves por segundo, llega a los 74 años. Si la clave se redujera a 50 dígitos, el tiempo de barrido es sólo de 3,9 horas.

De todas formas los avances en computación duplican cada 18 meses las potencias de cálculo facilitando el ataque y obligando al cifrado a aumentar el tamaño de la clave.

Los medios tecnológicos son fundamentales para un moderno criptoanálisis y una policía eficiente necesita disponer de ellos.

Los PC o los Workstations convencionales pueden usarse para explorar todas las posibles claves asociadas a un algoritmo, aunque por su relación rendimiento-coste son bastante ineficaces y requieren la utilización de dispositivos específicos como el FPGA (Field Programmable Gate Array); este chip montado en una tarjeta para su ensamblaje en un PC tiene un precio aproximado de unos 400$ USA y puede verificar hasta 30 millones de claves del conocido algoritmo DES, descifrando un criptograma cifrado con una clave de 40 bits en 5 horas, lo que significa (si su periodo de amortización es de 3 años, un coste por clave descifrada de 8 centavos de dólar.

Si el proceso de criptoanálisis se paraleliza, se podría con 25 equipos (equivalentes a una inversión de 10.000 $USA) descifrar una clave de 40 bits en unos 12 minutos).

Con mayores inversiones el tiempo se rebajaría a segundos.

También pueden construirse chips específicos para atacar cifrados concretos. Estos ASIC (Aplication Specific Integrated Circuit) son siete veces más eficaces que los FPGA a un coste de explotación veinte veces menor. Un chip ASIC puede comprobar 200 millones de claves del DES por segundo, por un coste aproximado de unos 10$.

La reducción del tiempo incrementa proporcionalmente la inversión; así por 300.000$, se podría romper un texto cifrado con DES en 19 días, y tan solo en 6 minutos con una inversión de 10.000.000 $.

Las nuevas tendencias tecnológicas se convierten en un aliado potencial de la Criptología, entre ellas destaca la computación configurable.

Los ordenadores capaces de modificar sus circuitos microelectrónicos mientras están funcionando, abre una nueva era en las técnicas de cifrado por su velocidad de filtrado.

En la Universidad de Caliafornia, en los Anteles (UCLA), se ha construido un prototipo de sistema criptográfico configurable para operar con el algoritmo DES. El microcircuito configurable sólo calcula una vez las subclaves y optimiza los circuitos de proceso de datos para estas subclaves. De esta forma una matriz programable de 13.000 puertas puede operar claves de 56 bits más eficientemente. Cuando se necesita cambiar la clave de cifrado, se puede especificar rápidamente una configuración nueva de los circuitos y trasladarlos a la matriz. El prototipo criptográfico es una pruba evidente de la versatilidad que se obtiene cuando los circuitos de un computador pueden modificarse a la medida de un conjunto diverso y variable de los datos siendo especialmente aplicable a las comunicaciones digitales.

Pero en la lucha constante entre criptografía y criptoanálisis, las nuevas tecnologías aplicadas a la protección criptológica también evolucionan en paralelo produciendo situaciones de gran dificultad para un criptoanálisis con resultado positivo o incluso impidiendo materialmente que tal resultado se produzca, como sería el caso de intercambio de mensajes que se hubiesen protegido algoritmos criptológicos que permitiesen el secreto absoluto.

El secreto perfecto, que matemáticamente es determinable, en la práctica ha encontrado dificultades para su realización en algoritmos concretos, pero es sin duda una tendencia permanentemente explorada. En esta línea está lo que se conoce como criptología cuántica, basada en principios de mecánica cuántica , se vale de fotones individuales y se basan en el principio de incertidumbre de Heissenberg, que postula que toda medida efectuada en un sistema cuántico provoca una perturbación en él por lo que la información que proporciona sobre su estado antes de la medición es incompleta. De esta forma, toda escucha de un canal de comunicación cuántico provoca perturbaciones que alerta al usuario. La criptografía cuántica utiliza este efecto para posibilitar una comunicación secreta entre dos personas que no compartan información secreta previa, ni siquiera claves. También puede capacitar a dos partes que no confían entre sí para alcanzar decisiones conjuntas sin poner en peligro su confidencialidad. El prototipo de esquema cripto-cuántico se desarrolló en el Centro de Investigación Thomas J. Watson de IBM.

7.- Conclusiones.

Primera.- Necesidad de delimitación y clasificación de ámbitos de confidencialidad.

Segunda.- Necesidad de elaborar una política criptológica mundial.

Tercera.- Necesidad de una ordenación jurídica democrática que preserve la información y las comunicaciones, con garantía de derechos y libertades

Cuarta.- Necesidad de utilizar la Criptología de forma sistemática, para control de accesos, integridad y confidencialidad.

Quinta.- Necesidad de unidades especializadas con alto nivel científico, tecnológico y criptológico dedicadas al delito cibernético.

Sexta.- Necesidad de divulgar entre las sociedades las características del entorno cibernético, sus posibilidades y riesgos y, especialmente, abordar la formación de jueces, fiscales, policía, abogados, auditores y, en general, autoridades encargadas de aplicación de la ley.

BIBLIOGRAFÍA

Bennett, Ch., Bressette, F.Salvail, L., Smolins, J., *Experimental Quantum Cryptography*, Journal of Cryuptografy, vol 5, nº 1, pag. 3-28, 1.992.
De Asis Roig, R., *Las paradojas de los derechos fundamentales como límites del poder*, Edit. Debate.1.992.
Ekert, A., *Quantum Cryptography Baredon Bell's Theorem.* RevieroLetters, vol 67 nº 6, pagb. 661-663, 1.991.
F.H. George, *Automation, Cybernetics and Society*, Londres, 1.959.
J.R. Perce, *La teoría del línformazione*, Milán, 1.963.
Peces-Barba, G., *Derecho positivo de los derechos humanos*, Edit. Debate, Madrid 1.987.
Quintero Olivares,G., *Comentarios al Nuevo Código Penal*, Aranzadi,1.996.
Ribagorda, A., *Tendencias en Técnicas Criptográficas*, Securmática 97, VIII Congreso de Seguridad en Tecnología de la Información y comunicaciones, 1.997.
Rodriguez Debesa, *Derecho Penal Español.*
Villasenor, J. and others, *Configuratole Computing Solutions for automatic Target Recognition*, IEEE Supsium for Custom Computin Machines (FCCM´96), 1.996.
W. Ross Ashby, *An Introductionto Cybernetics*, Londres, 1.956.