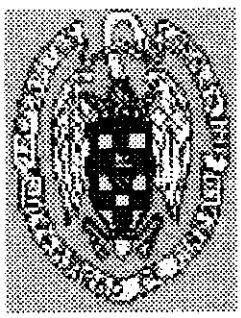
JOSÉ MARÍA MOLINA MATEOS



"ASPECTOS JURÍDICOS DE LA PROTECCIÓN CRIPTOLÓGICA DE LA INFORMACIÓN Y LAS COMUNICACIONES"

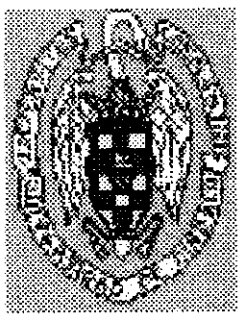
T E S I S D O C T O R A L

DIRECTOR: PROF. DR. D. MANUEL SÁNCHEZ DE DIEGO
FERNÁNDEZ DE LA RIVA
PROFESOR TITULAR DEL DEPARTAMENTO DE DERECHO CONSTITUCIONAL

UNIVERSIDAD COMPLUTENSE
FACULTAD DE DERECHO
MADRID, 1.998

A mis padres,
a María José,
y a mi hijo Rodrigo.
Todos ellos paciente soporte y estímulo
en este trabajo.

JOSÉ MARÍA MOLINA MATEOS



"ASPECTOS JURÍDICOS DE LA PROTECCIÓN CRIPTOLÓGICA DE LA INFORMACIÓN Y LAS COMUNICACIONES"

T E S I S D O C T O R A L

DIRECTOR: PROF. DR. D. MANUEL SÁNCHEZ DE DIEGO
FERNÁNDEZ DE LA RIVA
PROFESOR TITULAR DEL DEPARTAMENTO DE DERECHO CONSTITUCIONAL

UNIVERSIDAD COMPLUTENSE
FACULTAD DE DERECHO
MADRID, 1.998

PROLOGO

Las nuevas tecnologías de la información y las comunicaciones permiten el tratamiento y comunicación de abundantes cantidades de información con una amplificación exponencial de sus efectos. El nuevo ámbito social que surge se caracteriza por la facilidad de relaciones e intercambios, y por la eliminación de las barreras de la distancia y del tiempo.

Además, este nuevo espacio comunicativo está creando formas diferentes de relaciones sociales que vienen a superponerse a las ya existentes, redefiniendo sus perfiles, y contribuyen a la creación de un tipo de sociedad donde tecnológicamente es posible la comunicación global, pero aún no dispone de los instrumentos de ordenación necesarios.

La alternativa razonable no puede ser otra que una disciplina jurídica eficaz de los medios tecnológicos de información y comunicaciones.

La amplificación de los efectos de la información por el uso de las nuevas tecnologías comporta un incremento paralelo de las oportunidades para su violación, con escasa o nula posibilidad de hacer reversible el daño causado y grandes dificultades probatorias, que demanda un sistema de prevención real y efectivo.

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 a sus derechos. [1]

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.

Una prevención efectiva ante estas agresiones es un instrumento de gran utilidad para el individuo y para la sociedad, pero también puede provocar graves peligros e incluso amenazar la democracia, si bajo el pretexto de evitar conductas antisociales o incluso ilícitas, multiplica los obstáculos para el ejercicio de las libertades.

Esta tesis tiene como objeto efectuar un análisis de los aspectos jurídicos de la protección de la información y las comunicaciones, cuando se usan procedimientos para su ocultación, disimulo o cifrado, en suma, un estudio sobre la dimensión jurídica de la Criptología, [2] como medida de

prevención, en el entorno de una sociedad democrática. Se presenta para la obtención del título de Doctor en Derecho, y se centra en el tratamiento jurídico de la protección criptológica en el ordenamiento español, señala la colisión de derechos, y la necesidad de buscar respuestas que hagan compatible la necesidad de garantizar eficazmente la seguridad de la información y la libertad, partiendo de la hipótesis de una insuficiencia normativa.

Con este trabajo no se pretende aportar "la solución" al complejo problema consistente en la necesidad de armonizar seguridad y libertad en el ámbito de la información y las comunicaciones en una moderna sociedad democrática, -que por su propia naturaleza puede tener múltiples enfoques-, sino que únicamente se trata de hacer un análisis jurídico de lo que es, tan sólo una parte, de las grandes cuestiones derivadas de la implantación de la sociedad de la información y el uso de las tecnologías que la sustentan.

Los elementos del problema están constituidos por la colisión que se produce, en este ámbito, entre las libertades de expresión e información, la privacidad del individuo, la libertad informática, el secreto de las comunicaciones, la persecución y prevención del delito y la garantía de la seguridad y defensa del Estado, así como la necesidad de encontrar una solución que de respuesta a la protección real y efectiva de todos ellos, que permita a la vez, el normal funcionamiento de la Sociedad y del Estado y el pleno ejercicio de los derechos y libertades individuales.

Una profunda preocupación por las libertades y su efectiva implantación, producto del entorno académico y político, explican la curiosidad y el interés por abordar el estudio objeto de esta tesis.

Hablar de criptografía y libertades lleva, como referencia obligada, a la insigne figura de Thomas Jefferson, (1.743-1.826), Presidente de los Estados Unidos de América, autor de su Declaración de Independencia, e inventor de la máquina de cifrar conocida como "cilindro de Jefferson".[3]

Para Jefferson, padre de la democracia y de la criptografía americana, los principios éticos y morales que gobiernan la vida privada también deben gobernar los asuntos internacionales. El Estado no debe arrogarse una moral especial.

Sirva este trabajo como modesto homenaje en el 172º aniversario de su muerte.

El desarrollo de esta tesis no hubiera sido posible sin la ayuda del profesor Don Teodoro González Ballesteros, Catedrático de Derecho de la Información y Libertades Públicas de la Facultad de Ciencias de la Información de la Universidad Complutense que, junto a su espléndida labor docente en los cursos de doctorado, ha contribuido a un reciclaje teórico quince años después de mi licenciatura en la Facultad de Derecho y al Profesor Don Manuel Sánchez de Diego Fernández de la Riva, Profesor

Titular del Departamento de Derecho Constitucional de la Universidad Complutense y de Derecho de la Información y Libertades Públicas de la Facultad de Ciencias de la Información , Director de esta tesis.

Mi agradecimiento, a los profesores Rubio Llorente y al hoy fallecido, Sánchez Agesta, de quienes también fui alumno en los Cursos de Doctorado; a José Luis Ocasar y Vigil de Quiñones profesor de Criptología del que fui alumno, y al profesor de la U.N.E.D. Jesús María Minguet, por su contribución al estudio y difusión de la Criptología en los entornos universitarios.

Porto Colom, verano 1.997.

INDICE

JUSTIFICACIÓN Y MÉTODO

0.- JUSTIFICACIÓN Y MÉTODO.

La creciente importancia de la información en todos los aspectos de la vida de relación, amplificada por el uso y aplicación de las nuevas tecnologías, constituye un factor determinante de progreso económico y desarrollo político, con directa incidencia en la Sociedad, el Estado y en el Individuo.

Con el uso creciente de las nuevas tecnologías se incrementa la vulnerabilidad de la información y las comunicaciones, poniéndose de relieve una mayor necesidad de protección, como una forma de dar respuesta al cumplimiento de los derechos e intereses subyacentes y lograr así su efectiva implantación. Uno de los aspectos críticos dentro del proceso de la información, es el relativo a la garantía efectiva de su confidencialidad para lo que se suelen utilizar, procedimientos criptológicos que permiten la ocultación mediante el cifrado.

Pero la ocultación de información en el entorno de sociedades presididas por la transparencia tiene una incidencia, -de distinto signo-, en los derechos y libertades, y configura el perfil de uno de los temas de mayor calado político, económico y social derivado de la implantación de la "sociedad de la información". Los efectos de la ocultación de la información se hacen sentir en aspectos de naturaleza diversa entre los que destacamos a efectos de esta tesis la seguridad y defensa del Estado, libertades de

expresión e información, los intereses económicos, la persecución y averiguación del delito, el secreto de las comunicaciones y la intimidad del individuo.

Todos ellos bienes jurídicos que, aunque tienen elementos comunes en cuanto a la necesidad de utilización de protección criptológica, son de naturaleza distinta, se inspiran en principios diferentes, y operan bajo coordenadas o defienden intereses que en algunos casos pueden llegar a ser contrapuestos, lo que sitúa a la protección de la información y las comunicaciones en el punto de confluencia de diversas variables.

Para Luis Prieto, la fundamentalidad de los derechos es una escala que admite distintos grados, de modo que algunos derechos serán más resistentes en presencia de otras decisiones políticas. Lo que no serían en ningún caso es absolutos, pues ello equivaldría a reconocer derechos ilimitados.[4]

Por lo que para que el cumplimiento de los derechos sea real y efectivo, los medios criptológicos utilizados han de responder al grado e intensidad de los derechos a los que sirven, y estar en condiciones de garantizar la preponderancia de derechos prevalentes sin detrimento de los demás derechos, lo que supone alcanzar, además del necesario equilibrio jurídico entre los derechos en conflicto, encontrar la articulación criptológica y tecnológica que lo permita.

Al aproximarnos a los aspectos jurídicos de la protección criptológica de la información se suscitan diversas cuestiones, tales como la delimitación previa de los ámbitos de confidencialidad sobre los que va a operar, la naturaleza jurídica de la protección criptológica de la información, y su grado de regulación en el ordenamiento español, sin olvidar el entorno y carácter supranacional de algunos de los aspectos de la información y las nuevas tecnologías, así como la interdependencia de los estados y el creciente papel del individuo.

La operatividad y eficacia de la protección criptológica de la información y las comunicaciones exige un marco adecuado de regulación normativa, que requiere un previo análisis jurídico de los diversos aspectos que intervienen y sus relaciones, lo que constituye el objeto de esta tesis.

Nos inclinamos por concebir la protección criptológica de la información como un problema concreto, pero desde una óptica amplia y real, donde convergen factores jurídicos, tecnológicos, políticos, sociales, económicos o culturales y se aplica en ámbitos de naturaleza muy diferente.

El fenómeno a investigar es el fenómeno jurídico-social con un horizonte más allá de la dogmática legal. Para ello, además de las fuentes jurídicas, tenemos en cuenta el complejo sendero de las ciencias sociales y humanas en donde actúa el campo normativo estricto. Donde encontramos los factores y elementos que determinan el contenido de las normas, constituidos por las distintas situaciones que el legislador debe tener presente al

regularlas, e integrado por el conjunto de datos y actos que dan nacimiento a un orden normativo.

La ley como fuente jurídica, constituye una fuente hegemonica de nuestro sistema jurídico.

Las necesidades de tipo jurídico, bien sea porque las disposiciones legales carecen de la debida claridad, bien porque las instituciones van teniendo su natural evolución y difieren de las situaciones contempladas por el legislador en el momento de creación de la norma, o simplemente porque aparecen nuevas realidades no previstas, necesitan de la interpretación

Por cuanto se refiere a la doctrina, como estudios de carácter científico de los juristas, con influencia en jueces y legisladores, va contribuyendo a la acomodación del derecho a la vida social y así mismo a la preparación de nuevas leyes.

En cuanto se refieren al tema central de esta tesis, y tal vez por su novedad, la ley, la jurisprudencia, la doctrina científica, la costumbre y los principios generales del derecho, como fuentes de conocimiento del derecho, aparecen escasas y dispersas, y casi siempre parciales.

Pero las fuentes del conocimiento jurídico no se agotan en sus expresiones formales. Como ciencia social que regula conductas, la realidad es el universo material donde se dan las relaciones e interacciones entre individuos, grupos, administradores y administrados.

Los hechos sociales son los factores que generan las normas jurídicas. El dinamismo social impacta y afecta al orden jurídico evolucionando en forma dialéctica.

El Derecho como instrumento de ordenación, está destinado a configurar y corregir la vida social; si no lo logra, a la norma le faltará uno de sus elementos constitutivos: la eficacia.

Por consiguiente, en esta investigación, vemos la realidad del Derecho en el campo de interacción de los actores del medio jurídico y de los sometidos al Derecho, en una interdependencia de Derecho y Sociedad.

Este es el tipo de investigación que desarrollamos, cuya metodología y técnica, tiene como objeto el estudio de normas jurídicas y de los hechos políticos, tecnológicos, económicos, sociales y culturales que concurren en su nacimiento, vigencia y eficacia, considerando interdisciplinariamente a un sector de la realidad y el comportamiento de sus destinatarios y aplicadores.

Se pondrá el acento en la eficacia de la norma ante el hecho o problema regulados y se busca determinar si se cumple o no con las finalidades sociales que el legislador asignó a la norma jurídica en cuestión, su suficiencia, y la distancia que hay entre el discurso normativo y el hecho jurídico regulado, en su caso, o la falta de norma o su insuficiencia, en los supuestos que así sea.

La confidencialidad de la información, como manifestación concreta de uno de los factores de su seguridad, y el logro de su efectividad como forma de neutralizar uno de los aspectos más vulnerables de la sociedad de la información, constituye una seria preocupación en los países más avanzados, y, consiguientemente, en España, donde recientemente ha despertado un alto interés.

Sin embargo, no se ha producido el correspondiente avance en la regulación jurídica de esta nueva realidad, tal vez, de igual modo que ocurre en otros aspectos del proceso de la información. No existe en nuestro ordenamiento, ni en buena parte del derecho comparado, una ordenación sistemática y global de la protección criptológica de la información.

En su mayoría de los casos, las ordenaciones se limitan a referencias legales pobres y fragmentarias, desconexas, carentes del necesario sentido unitario, y concebidas para realidades pasadas. Falta una concepción clara del problema considerado en su conjunto, que aporte soluciones aceptadas por los diversos actores que intervienen.

En España, en estos momentos comienzan a surgir iniciativas legislativas que, al menos, contemplan de forma expresa el cifrado de la información.

Esta falta de respuesta jurídica supone no solo un obstáculo para el futuro desarrollo de la seguridad de la información, sino que es un obstáculo para una efectiva implantación de las nuevas tecnologías y para un

tratamiento global de la información, que constituyen un medio eficaz para superar los problemas del progreso y desarrollo en el siglo XXI.

Conforme al planteamiento general del trabajo en esta tesis se abordan aspectos diferentes distribuidos en, un Prologo, Justificación y Método, cinco Capítulos y un Epílogo.

El Capítulo I analiza la necesidad de proteger la información y el uso de medidas de seguridad , en el Capítulo II se aborda la Criptología, su historia y sistemas más conocidos, el Capítulo III se dedica a la aplicación de la Criptología en distintos ámbitos, diplomático, militar, comercial y cívico, así como profundiza en la relación de la Criptología con los Servicios de Inteligencia, el Capítulo IV se centra en la dimensión jurídica de la protección criptológica, analiza la relación entre Criptología y Derecho, los ámbitos de confidencialidad públicos y privados y la protección efectiva de los mismos, su regulación jurídica y los conflictos de derechos. En el Capítulo V se abordan las conclusiones generales del trabajo, con indicación de los principios que se considera han de inspirar una política criptológica y una propuesta de bases para la regulación sistemática del cifrado de la información y las comunicaciones.

Para llegar al objetivo central de esta investigación, consideramos imprescindible situar el objeto de estudio en su contexto, para ello, se abordan algunos aspectos de su evolución histórica, el entorno político y constitucional, las libertades de expresión e información, y la implantación

de las nuevas tecnologías y sus efectos, en cuyo entorno insertamos la percepción que tenemos de la protección criptológica de la información, consecuencia de una relación personal y directa con sus distintas manifestaciones y ámbitos.

La falta de respuesta jurídica indicada, no es sino la consecuencia de no acabar de asimilar y advertir las diferencias que definen a la información como una realidad de importancia y transcendencia inconmensurable, que requiere actualmente un tratamiento preferente, global y unitario, cuya adecuada protección, en los casos que lo precise, es un elemento imprescindible derivado de su propia naturaleza y del entorno en el que opera.

La falta de reconocimiento de esta realidad y su ordenación jurídica, afecta a la satisfacción de las necesidades vitales de bienestar, progreso, libertad y seguridad.

Los problemas derivados de la protección criptológica de la información tienen diversos aspectos de orden político, social, económico, tecnológico, jurídico, y también, filosófico y ético, y repercute en ámbitos tan diversos como el político, el económico, el diplomático o el militar, la sociedad y el individuo.

La hipótesis de trabajo es que la ordenación jurídica de la protección criptológica de la información resulta insuficiente, por lo que sería necesario primero, un estudio de la realidad actual con identificación y clasi-

ficación de los ámbitos de confidencialidad y, sobre ello, proponer una regulación de carácter global y sistemático.

La tesis pretende analizar los aspectos jurídicos de la protección criptológica de la información, poner de manifiesto la insuficiencia de la actual regulación, medir la distancia de ésta con la realidad social y, definir las necesidades a las que una nueva regulación debería dar respuesta.

Sería conveniente para atender de forma adecuada a las nuevas necesidades de garantía de confidencialidad, proceder a una ordenación global de la información, insertando su regulación en un sistema jurídico completo e integrado que contemple la protección criptológica como elemento imprescindible, unido al desarrollo de una "conciencia de seguridad".

Los trabajos de esta tesis vienen a dar satisfacción intelectual a las múltiples interrogantes surgidas a lo largo de más de veinticinco años de vida profesional relacionada con la Confidencialidad y el Derecho. Periodo en el que se ha tratado el tema objeto de estudio desde su dimensión más básica, como Especialista Criptólogo en el Ministerio de Asuntos Exteriores, pasando por el análisis y estudio en el ejercicio de la abogacía, consultor de OMNISEC, empresa internacional líder en criptología, y como analista y observador de la vida política nacional e internacional, todo lo cual suscitó el enfrentamiento, de modo directo, con uno de los problemas que sigue siendo una asignatura pendiente en las democracias occidentales.

Los contactos con el objeto de esta tesis rebasaron, desde el principio, los límites de las exigencias profesionales para trasladarse a las preocupaciones intelectuales y cívicas, en su vertiente jurídica, filosófica y política.

Todo ello lleva, en primer lugar, a una preocupación por un conocimiento histórico, e incluso científico, de la Criptología y de los ámbitos en que se proyectaba, desde una concepción unitaria, lo que comportaba un proceso de estudio y reflexión constante, tanto desde un punto de vista puramente técnico, como desde el de su campo de relaciones: la información, las tecnologías y los ámbitos de aplicación, en sus versiones clásicas: militar, diplomática y comercial, así como su fundamento jurídico y constitucional.

Junto a ello, una reflexión sobre sus implicaciones filosóficas, éticas y políticas en sus vertientes nacional e internacional, vinieron a completar el escenario donde se sitúa el análisis de un tema que es un factor de seguridad, pero que, en ultima instancia, es un mecanismo de eficacia para la sustracción de una determinada información al conocimiento público, con los riesgos jurídicos y políticos que conlleva.

Las razones personales y profesionales que han originado esta investigación, han sido expuestas, y se resumen en el intento de comprender como jurista y como ciudadano la dimensión de un fenómeno complejo,

abordado desde una perspectiva unitaria y pluridisciplinar, en una posición de proximidad al mismo.

El desarrollo de esta inquietud por el conocimiento de un problema concreto de mi entorno vital, ha sido, sin embargo, más bien fruto de la sugerencia propia de los datos e interrogantes del propio tema objeto de estudio, que de una hipótesis prefijada.

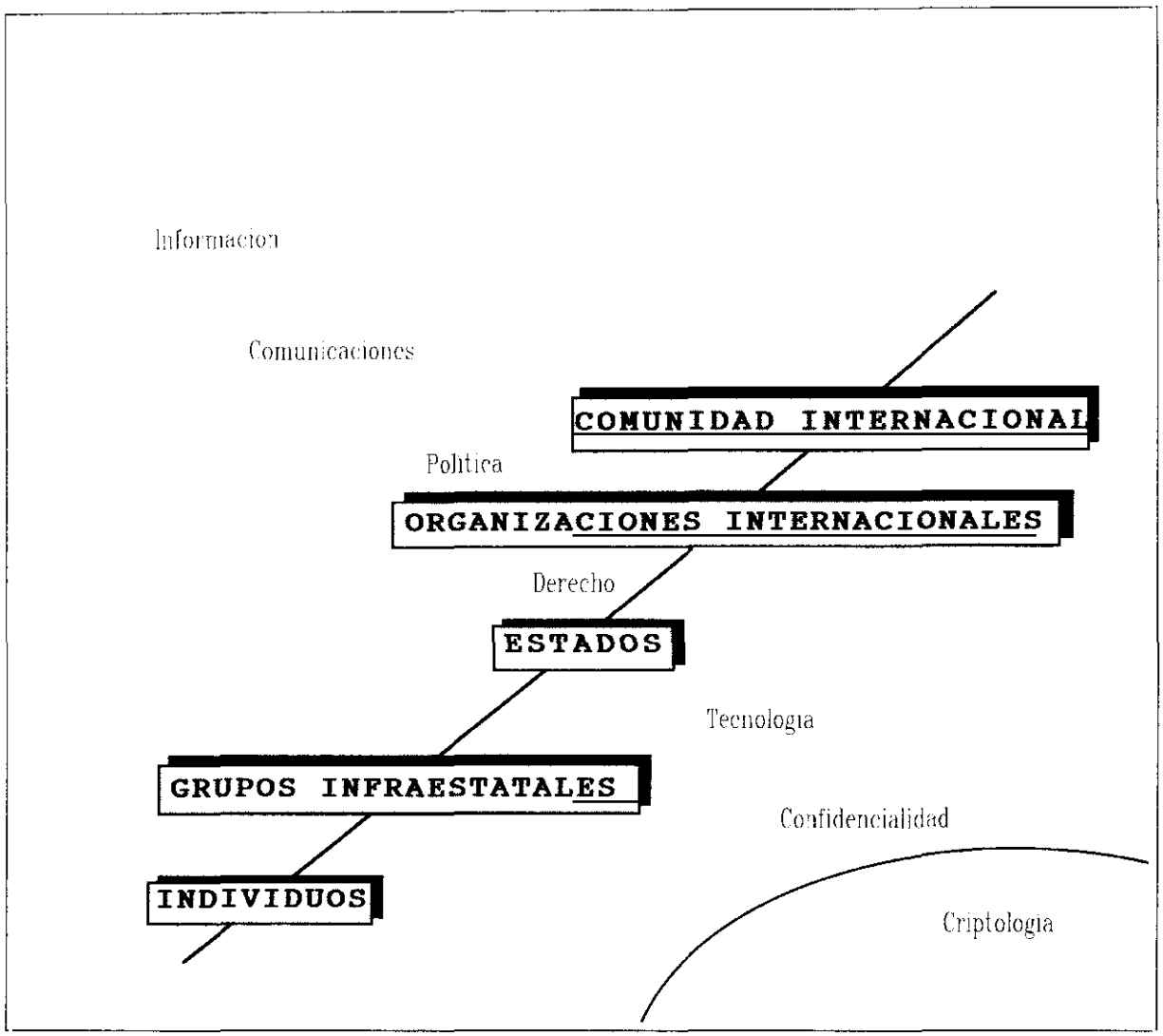
La reflexión se inicia, referida exclusivamente a la protección criptológica de la información clasificada para, posteriormente, ir madurando el enfoque del trabajo y extendiendose a todo el campo de aplicación, como entorno unitario, donde está presente la criptología y proyecta sus efectos, donde iban surgiendo nuevos aspectos, con aparentes contradicciones, que vienen a configurar un interesante problema de gran alcance político y social, con distintos perfiles que sugiere diversas interrogantes, que se plantean en las páginas siguientes.

El conocimiento empírico de los distintos aspectos de la criptología, no pasó de ser un conocimiento especialista, sus relaciones carecían de un sentido unitario y demandaban un grado de coherencia que permitiese contemplarlos en su conjunto como un todo integrado.

En un proceso inductivo se fue integrando la mente en el sentido unitario que informaba las relaciones de la protección criptológica de la información, objeto de estudio, que aparecían de forma dispersa. De esta manera se accede , desde conocimientos particulares a otro más general.

Ante los problemas surgidos en las sociedades occidentales a consecuencia de la colisión entre las necesidades de garantía de la confidencialidad de la información con los derechos y las libertades fundamentales, empiezan a tomar cuerpo los interrogantes, que se plantearon con anterioridad de forma dispersa, y dan paso a la elaboración de una hipótesis general de trabajo.[5]

C A M P O D E O B S E R V A C I O N



CAPITULO I

NECESIDAD DE PROTEGER LA INFORMACIÓN

1.1.- LA PROTECCIÓN DE LA INFORMACIÓN COMO "NECESIDAD".

Las indicaciones que nos da el sentido común sobre lo que pueden ser los contenidos de las necesidades son múltiples, toda vez que resulta difícil determinar la existencia objetiva de las mismas.

El vocablo *"necesidad"* se utiliza en el lenguaje cotidiano de formas muy diversas. Uno de los significados más comunes se refiere a la necesidad como impulso. Otro significado conceptúa las necesidades como unos objetivos que, se supone, todos comparten en alcanzar. Es precisamente esta universalidad lo que se presume que diferencia las necesidades de las preferencias o deseos.

El concepto de necesidad como fuerza motivadora, derivada de un estado de desequilibrio o tensión, a causa de una carencia específica,[6] fue el criterio que ha inspirado el análisis más conocido de las necesidades básicas.

Tras las necesidades más elementales del hombre de conseguir alimento y bebida, la siguiente necesidad en orden de importancia será la de "un mundo seguro, ordenado y sin imprevistos".[7] Una vez alcanzados estos fines, dominan otras necesidades superiores y así hasta llegar a una motivación abierta de realización espiritual e intelectual.

La necesidad como categoría específica de objetivos que se creen universalizables, marca claramente las diferencias con las aspiraciones, que

se describen también como objetivos, pero que se derivan de preferencias particulares del individuo y de su medio cultural.

Pero referirse a las necesidades como objetivos universalizables descansa en la creencia de que si no se satisfacen adecuadamente dará lugar a graves daños de algún tipo concreto y objetivo. Y, por consiguiente, no satisfacer las necesidades se considerará contrario a los intereses objetivos de los afectados y se reputará anormal y antinatural.

Para Maslow las cinco necesidades dispuestas en una jerarquía de "preponderancia" son: necesidades fisiológicas, necesidades de salud y seguridad, necesidades de pertenencia y de amor.[8]

El Diccionario de la Real Academia de la Lengua, al referirse al vocablo necesidad, en su acepción 5 dice "Especial riesgo o peligro que se padece, y en que se necesita de pronto auxilio".

En la vida cotidiana, al no quedar siempre explícito el último fin al que van dirigidas las necesidades, se cree que estas son objetivos *"per se"*, en lugar de serlo por lo que implican en realidad.

En el transfondo de una necesidad específica, que se considera como objetivo por derecho propio, debe haber siempre algún otro objetivo . De no ser así, resultaría imposible establecer la razón por la que el objetivo se identifica como necesidad y por la que pensamos que vale la pena perseguirlo.

Para entender lo que significa definir algo como necesidad, hemos de poseer un conocimiento previo de la razón por la cual es ese algo lo que hemos de procurar conseguir, si tenemos como objetivo evitar daños graves.

Las razones para tener necesidades son esencialmente de carácter general o colectivo, en tanto en cuanto se refieren a un conocimiento compartido de qué clases de estrategias son efectivas para evitar daños, o qué tipos de investigación empírica hay que realizar para facilitar dicho conocimiento.

Mientras que las aspiraciones son intencionales y referencialmente opacas, porque su veracidad depende de cómo lo entienda el sujeto.

La subjetividad de las aspiraciones contrasta con la objetividad de las manifestaciones sobre las necesidades.

Las necesidades son extensivas a su veracidad dependiendo de algo como "la forma en que es el mundo" y no de "las elucubraciones de mi mente".[9]

Hay objetivos vinculados, instrumental y universalmente, a la prevención de daños graves, lo que requiere establecer algún tipo de acuerdo sobre lo que se consideran daños graves, que a su vez requerirá, previamente, un acuerdo sobre lo que es un estado normal, próspero y libre de daños.

Lo que se contempla como necesidades, no viene determinado por normas universales de razón o certidumbre. Sino que será el entorno

cultural y político y, en definitiva el grado de desarrollo, el que defina los límites perceptibles de la experiencia.

En nuestro entorno cultural, social, económico y político, y con el grado de desarrollo de las nuevas tecnologías, será la naturaleza de la información -entendida como el cambio que se produce al pasar del desconocimiento o la incertidumbre de un hecho, al conocimiento o certidumbre respecto del mismo-[10] y el conocimiento y, concretamente, su valor, los que los sitúen en un nivel que demanda su posesión útil y controlada, que requiere su adquisición, procesamiento y distribución y, *"necesita"* protección para evitar pérdidas no deseadas, producidas por cualquier motivo, ya sean causas naturales, tecnológicas, derivadas de la acción humana, o producto de egoismos de terceros.

Si en el mundo hubiera existido y existiese confianza mutua, no sería necesaria la criptografía. [11]

La comunicación de información valiosa en un clima de desconfianza suscitó la necesidad de protegerla e, históricamente, dio lugar al nacimiento y uso de la criptología. Las reiteradas vulneraciones de los sistemas empleados provocan la necesidad de incrementar los niveles criptológicos de protección y aumento de la fortaleza de sus algoritmos.

La historia está llena de acontecimientos que confirman lo indicado, en medio de un proceso dinámico en constante evolución.

Ya en 1.593, IO.Baptista Porta, en su obra *"De occultis literarum notis"[12]*, dice:

"Quod his notis scribere pracipue solent, qui magna negotia tractant, quam earum cognitio utilis semper, necessaria extiterit.

Quod in rebus necessariis is notis maiores usi fuerint, clare inferius demostrabimus, cum modos referemus, quibus illi secreta tractatu riperscriberent, nam vel alieno & ignoto idiomate loquebantur, vel diuerfis characteribus, diuerfis; euroum transpositionibus, ut ab C. Caesare, ab Augusto, & à Cicerone postmodum factum referemus. Sed primo quantum harum notarum ars utilis semper, necessaria; extiterit, indicabiinus, ut ijs, si qui sunt, qui hanc memorabilem industria sensa occultandi, & ad literarii diuersos sonos, fue characterum notae accommodentur, quasi inutilem & vanam aspernantur, & propter ea in ea inuehutur, obuiemus. Quid enim utilius profecto, praestantius; esse potest, quam magnis in rebus, quarum si occulta consilia proderentur, maxima essent subeunda discrimina, antes ibi quem pia cauere, ut non modo missae literae non intelligantur, fed ne doli qidem ex se suspitionem relinquant quo fiet, ut ijs in detectis, & reru pofsit is pericula essugere, & fui facile voti compos euadere? Sed ne interim tormenta locu hageat, ut veritas exigatur quo astu possit praecaueti, ne literariae intercipiatur, post traditos nouos coponendi modos, indicabimus, at; alienas in separatas fraudes sic agnoscere, ...".

Valga como indicador de la situación actual algunas referencias a los hechos mas notorios dados a conocer por los medios de comunicación nacionales e internacionales, en los últimos años:

1.- Estados Unidos.

a) Pearl Harbor electrónico.

Winn Schwartau, asesor de comunicaciones de Inter-Pact, asegura que "Con más de cien millones de ordenadores inextricablemente ligados a través del más complejo despliegue de conjuntos de comunicaciones de base terrestre y de satélites de comunicaciones... los sistemas informáticos oficiales y comerciales se hallan hoy tan mal protegidos que en

esencia cabe considerarlos inermes. Nos aguarda un Pearl Harbor electrónico".[13]

b) *Instituciones financieras.*

En un informe de la General Accounting Office de Estados Unidos al Congreso se expresa una preocupación similar respecto a los fallos de seguridad de Fedwire, red electrónica de transferencia de fondos, que sólo en 1.988 manejó 253.000 billones de dólares, esta red padece fallos de seguridad y requiere al respecto la adopción de medidas rigurosas.[14]

En este mismo sentido, la firma consultora Booz Allen & Hamilton, ha efectuado un estudio sobre las comunicaciones en Nueva York y ha descubierto que las principales instituciones financieras operan sin respaldo alguno de telecomunicaciones. Las firmas similares de Francfort, París, Tokio y Londres se encuentran más o menos en la misma situación. ("El informe señalaba lo contrario").[15]

c) *Sistemas militares.*

Los sistemas militares, aunque más seguros, no resultan en modo alguno impenetrables. A finales de 1.992 y con relación a un mensaje secreto enviado por el Pentágono, Duane Andrews manifestó "La seguridad de nuestra información es atroz, nuestro (secreto) operativo es atroz, la seguridad de nuestras comunicaciones es atroz". Andrews fue Subsecretario de Defensa del C3I (Comando, Control, Comunicaciones e Información) y calificó la información de *"activo estratégico"*.

d) *Comunicaciones diplomáticas.*

El mundo de las comunicaciones diplomáticas no es ajeno a las deficiencias de seguridad, como quedó puesto de relieve por la intercepta-ción en junio de 1.993, de llamadas dirigidas a destacados políticos de todo el mundo por Warren Christopher, Secretario de Estado norteamericano, para advertirles del ataque de los misiles de Estados Unidos a la sede de los servicios iraquíes de información en Bagdad.[16]

e) *Pretty Good Privacy (PGP).*

Philip Zimmermann, criptólogo aficionado además de sentirse fascinado con los códigos, la escritura secreta y los mensajes en clave, es un acérrimo militante de los derechos cívicos y, entre ellos, del derecho a la intimidad y a la vida privada, un derecho recogido por la Constitución americana, cuya Cuarta Enmienda protege a los ciudadanos contra los "registros y los secuestros de correo".

Para Zimmermann, este derecho consiste en preservar, entre otras cosas, la inviolabilidad de su correo postal y, por lo tanto, proteger también de las indiscreciones su correspondencia electrónica.

En Estados Unidos los intercambios de "E-Mail" (Electronic Mail, mensajería electrónica) constituyen la forma de comunicación que está experimentando un mayor crecimiento.

Pero los inconvenientes de estas redes es que son "accesibles" a cualquiera, excepto las directamente explotadas por el ejército.

La única solución para proteger los datos que viajan a través de redes informáticas consisten en "ocultarlos", es decir, transformar los bloques de caracteres en salmodias.

El problema de Zimmermann no es poner de relieve la vulnerabilidad de la red de correo electrónico, es otro, y por ello ha tenido la notoriedad mundial que su caso ha alcanzado. Zimmermann desarrolló un código criptográfico para cifrar los mensajes electrónicos y ha distribuido decenas de miles de ejemplares por todas las redes informáticas mundiales, lo que es considerado en Estados Unidos como un delito federal. Durante años, Philip Zimmermann intentó adaptar el mayor y más complejo de los algoritmos a un ordenador clásico y, en 1.991 terminó la creación de un programa que bautizó con el nombre de PGP ("Pretty Good Privacy") y que consiste en una completa codificación adaptable a la correspondencia electrónica. La NSA (National Security Agency, el más importante servicio secreto de los Estados Unidos), que posee el mayor parque de ordenadores del mundo, se está especializando en la descriptación del programa de Zimmermann. Pero el programa es muy potente y nadie - que se sepa- ha conseguido violar el algoritmo de cifrado del PGP.

Zimmermann decidió poner su invento a disposición de los demás y le introdujo en la red Internet, que conecta a varias decenas de millones de ordenadores en todo el mundo y, sin pagar un céntimo, pueden almacenar en su ordenador personal toda una serie de informaciones sobre la

criptografía y, además, el PGP. El programa se extendió por todo el planeta y fue copiado por decenas de miles de ordenadores. La ley americana prohibe la exportación de tecnologías relacionadas con la codificación de datos, por motivos de seguridad nacional. Hasta el punto que todos los programas creados en los Estados Unidos y que disponen de un sistema de codificación tienen una versión para la "exportación". Al colocarlo en la red Internet, lo han exportado "de facto".[17]

La investigación judicial iniciada contra Zimmerman finalizó en 1.996 sin cargos de ningún tipo según anunció PGP News en Internet.[18]

f) *Violación de ordenadores.*

Durante 1.995 hubo 250.000 intentos de entrada en los sistemas de ordenadores del complejo defensivo de EE.UU., y en dos de cada tres casos el intento concluyó con éxito.

La General Accounting Office (GAO), instrumento de investigación del Congreso, llega a la conclusión que "En el mejor de los casos, estos ataques suponen un daño multimillonario para el sector de la defensa; en el peor, son una seria amenaza para la seguridad nacional".[19]

De los 160.000 piratas informáticos que entraron en los ordenadores, el Pentágono sólo detectó a tiempo al 4% de las intrusiones. El coladero está tan asumido que sólo se denuncia uno de cada 150 casos, según el Senador Nunn.

El Senador ofreció datos no menos preocupantes ante el Subcomité de Inteligencia del Senado: las intrusiones se duplican cada año, y el gobierno "no tiene una política coherente para proteger las redes informáticas, responder a los incidentes y valorar los riesgos de los daños que pueden ocasionar los ataques contra los ordenadores".

John Glenn, senador y antiguo astronauta, respecto a estos incidentes dijo que, "se corre el riesgo de que esta situación de debilidad de los ordenadores oficiales origine daños catastróficos".

El Pentágono asegura que los sistemas clasificados en los que se guarda la información más sensible están especialmente protegidos, pero eso sólo abarca al 10% de las redes. El 90% de los datos relacionados con la defensa no están tan protegidos, y la preocupación de los senadores tiene que ver con el provecho que individuos, empresas o terceros países pueden obtener a partir de las redes de información de transportes, telecomunicaciones, bancos, energía, negocios y contratos gubernamentales.

Un informe confidencial del Departamento de Justicia estadounidense ha dado la voz de alarma y destapa la vulnerabilidad de puntos claves para la seguridad como el Pentágono o el Departamento de Defensa. La nueva amenaza para la seguridad de EE.UU. se encuentra oculta en las redes informáticas y autopistas de comunicación, hasta el punto que se ha creado un cuerpo de elite dedicado a rastrear las infraestructuras vitales para el funcionamiento del país: redes militares, bancarias, de telecomunicaciones,

eléctricas y de suministro de agua, el Grupo para el Mantenimiento de la Seguridad en el Ciberespacio (CSAG).

Pero las dificultades para las iniciativas legislativas del Congreso y el Senado, que tratan de establecer leyes para incrementar el control sobre Internet chocan con los intereses de las empresas de "software" y científicos que defienden la libre circulación en el ciberespacio.[20]

g) *Visa Internacional.*

Kelley Knutson, Vicepresidente de Visa Internacional pone de manifiesto que la falta de seguridad es uno de los motivos que frena a las empresas a ofrecer sus productos a través de las redes. "Actualmente, la mayor parte de los consumidores que piden bienes y servicios en redes abiertas los pagan llamando por teléfono al establecimiento comercial y dando los datos. El cliente no quiere dejar sus datos de la tarjeta en un espacio donde cualquiera puede entrar".[21]

2.- Otros países.

Innumerables y notorios son los casos que ponen de relieve la falta de seguridad en todo tipo de comunicaciones -tanto públicas como privadas- efectuadas por teléfono, fax, telex, datos, -ya sean enviados por radio, satélites o microondas-, en numerosos países del mundo, y en las más variadas situaciones, además de lo que ocurre en los Estados Unidos.

a) *Gran Bretaña.*

En Gran Bretaña, un pirata informático obtuvo información confidencial de una red de datos secretos, en lo que se ha considerado una de las más serias violaciones de la seguridad nacional británica según reveló The Independent, en diciembre de 1.994.

La información incluía números telefónicos, direcciones de los servicios secretos MI5 y MI6 y la localización de instalaciones militares, sacados del archivo de la compañía "British Telecom" (BT),la cual negó que existiese una brecha en la seguridad de su centro de datos.

El desconocido copió del ordenador de la firma toda la información confidencial y después la colocó en "Internet", red mundial de informática a la que acceden unos 35 millones de usuarios.

El pirata pudo copiar, además, sin ser detectado por la BT, datos del centro de escuchas de Cheltenham, perteneciente al gobierno, direcciones del personal militar, e información sobre el "búnker" con el que cuenta la Administración del primer Ministro John Major en el centro de Inglaterra para el caso de ataque nuclear.[22]

b) *Tarjetas de crédito.*

Un francés de 22 años, residente en Mallorca, se confesó culpable ante un tribunal norteamericano de un fraude que supera los 140 millones de dólares (17.500 millones de pesetas), dirigiendo una red de piratas informáticos con ramificaciones en EE.UU., Gran Bretaña y España.

Llegó a apropiarse ilegalmente de 140.000 números de tarjetas de crédito, y organizó uno de los más amplios y complejos montajes tecnológicos registrados hasta ahora para estafar a compañías de teléfonos.

The Washington Post cita a David Adams, portavoz del Servicio Secreto del Departamento del Tesoro, para calificar al pirata como la figura principal de la organización en Europa. El Servicio Secreto que le detuvo, grabó una conversación con otros miembros del grupo en la que aseguraba estar ganando 18.000 dólares al mes con el montaje.

El joven pirata aceptó haber participado en la conspiración para robar cerca de 100.000 códigos sustraídos entre 1.992 y 1.994 de una instalación de MCI Telecommunications, la segunda compañía telefónica de larga distancia de EE.UU., detrás de AT & T.

La tarea consistía en introducirse en los programas y memorias de las compañías telefónicas para a partir de ahí apoderarse de los números de las tarjetas de crédito. Cada uno de estos números era después vendido y utilizado por una media de 20 personas que hacían llamadas internacionales desde Europa. El importe se cargaba en las tarjetas de crédito cuyo número había sido robado.[23]

c) *España, "Txiki" Benegas.*

En España, durante el mes de abril de 1.991 se produjo un escándalo con motivo de la divulgación de una conversación efectuada desde el

radioteléfono de su coche, del político del PSOE, "Txiki" Benegas, captada con un escáner de fácil obtención en el mercado.

La facilitad de acceso a las conversaciones efectuadas por este medio pone de relieve la vulnerabilidad de este tipo de comunicaciones.

El eco de la noticia y el tratamiento dado al hecho de captación de una conversación efectuada desde un radioteléfono tuvo su origen en la notoriedad del personaje afectado y la polémica se centró no tanto en la vulnerabilidad de este tipo de comunicaciones como en el dilema la intimidad frente al interés público a la hora de publicar este tipo de informaciones, cuando se refieren a una persona pública.[24]

El Gobierno español admitió la situación de falta de protección de las comunicaciones, al reconocer que no puede garantizar su secreto en las efectuadas por vía telefónica.

En diciembre de 1.993, durante una intervención parlamentaria, del entonces Ministro de Obras Públicas, Transportes y Telecomunicaciones, José Borrel dijo: "La garantía del secreto de las comunicaciones es más un objetivo permanente del Gobierno que una realidad que podemos dar por concluida" e indicó que es la compañía Telefónica la que "debe garantizar el secreto de las comunicaciones.[25]

Si bien es cierto que el artículo 2.2 de la Ley 31/1.987, de 18 de diciembre, de "Ordenación de las Telecomunicaciones", dice que: *"Los servicios de telecomunicaciones se organizarán de manera que pueda*

garantizarse eficazmente el secreto de las comunicaciones, de conformidad con lo previsto en el artículo 18.3 de la Constitución", no es menos cierto que el artículo 9.2 de la Constitución dice que *"Corresponde a los poderes públicos promover las condiciones para que la libertad y la igualdad del individuo y de los grupos en que se integra sean reales y efectivas; remover los obstáculos que impidan o dificulten su plenitud ..."*

El escándalo sobre escuchas ocurridas en España, -actualmente "sub iudice"- en el entorno de lo que se conoce como "escándalo CESID", sacado a la luz durante el primer semestre de 1.995, -con independencia de las consideraciones jurídicas y políticas que merezca-, viene a poner de relieve, una vez más, la vulnerabilidad de las comunicaciones.

d) *Grupo de los 7.* (G-7).

El G-7 y Rusia adoptaron en París el 30 de julio de 1.996 un programa de 25 medidas contra el terrorismo entre las que figuran el evitar en lo posible el uso de la red informática Internet por parte de los grupos terroristas y, en concreto, estudiar las posibilidades legales de intervenir en las redes de comunicación, con respecto a la intimidad, para detectar mensajes entre terroristas.[26]

e) *España, "hackers" en la Moncloa.*

De nuevo en España, el 29 de septiembre de 1.996, el diario ABC publica en primera página que un equipo de investigadores de ABC y "Blanco y Negro", con la ayuda de un grupo de "hackers", han podido entrar

en el ordenador de La Moncloa y ha podido comprobar que la seguridad de algunos de los principales ordenadores españoles deja mucho que desear.

Tras un amplio reportaje en el que indican que han sido descubiertos graves errores de seguridad en algunos de los más importantes ordenadores del país: Moncloa, Boletín Oficial del Estado, Universidad Nacional de Educación a Distancia o el Consejo Superior de Investigaciones Científicas, y en respuesta a la pregunta genérica de si son seguros los datos que contienen y transmiten cualquiera de los terminales de estas redes, finaliza afirmando que "hoy por hoy, la seguridad informática en España es poco más que una quimera". [27].

3.- *"Echelon".*

Que el sistema de telecomunicaciones que utilizamos diariamente no es seguro es algo intuido desde hace tiempo. Pero poco de sabe de la existencia desde finales de la Segunda Guerra Mundial de un complejo sistema de monitorización global, de capacidad y extensión extraordinarias, gestionado por Estados Unidos en colaboración con Canadá, Australia, Nueva Zelanda y Gran Bretaña.[28]

Echelon es el fruto tecnologícamente más avanzado de la Ukusa Security Agreement, pacto firmado en 1.948, a finales de la Segunda Guerra Mundial, por Estados Unidos y sus cuatro aliados. Su existencia nunca ha sido reconocida oficialmente por los países signatarios y, los demás gobiernos, han preferido ignorarlo. Tras el final de la guerra fría en lugar de su

desmantelamiento, ha sido remodelado y potenciado, utilizando bases espaciales. El sistema *Echelon* se ocupa esencialmente de instituciones e informaciones civiles y económicas, y en menor medida de objetivos militares.

Con el final de la guerra fría las prioridades de Estados Unidos han cambiado radicalmente. Hoy la mayor preocupación de Washington son los temas económicos y políticos.

El Parlamento Europeo ha tomado cartas en este asunto. La Comisión de Libertades Públicas debe determinar de qué forma *Echelon* puede atentar contra las libertades individuales y contra la democracia. Algunos eurodiputados consideran que la Comisión Económica debería pronunciarse sobre las consecuencias comerciales del caso.[29]

En febrero de 1.997, *Statewatch*, revista inglesa especializada, revelaba que la propia Unión Europea había decidido poner en marcha, "en el más absoluto secreto" una red internacional de escuchas telefónicas. No se tienen noticias de que se haya desmentido ni la existencia de *Echelon* ni las revelaciones hechas por la revista británica sobre el objetivo de la Unión Europea.[30]

A iniciativa del diputado británico Glynn Ford, el Parlamento Europeo puso en marcha un informe denominado "Evolución de las técnicas de control político", algunas de cuyas conclusiones fueron publicadas el mes de diciembre de 1.997.

En el informe se describe cómo los Estados Unidos y sus aliados anglosajones interceptan llamadas telefónicas, faxes y e-mail en todo el mundo. Este espionaje afecta de manera especial, al mundo económico y de la empresa.

Este sistema de vigilancia global cubre la totalidad del planeta y utiliza los satélites Intelsat, por los que pasan la mayoría de las comunicaciones telefónicas vía satélite, mensajes por Internet, correo electrónico, faxes y telex.

Los cinco países indicados se reparten los resultados de este trabajo, en el que Estados Unidos opera como socio principal.

A raiz de este informe el Parlamento Europeo va a poner en marcha una investigación sobre *Echelon* y su impacto en términos de libertades individuales y de guerra económica mundial.

A juicio de Alain Pompidou, presidente de la Comisión de evaluación de las opciones tecnológicas y científicas del Parlamento Europeo, "*Echelon* es, de hecho, un sistema de espionaje económico cuyo objetivo es distorsionar las leyes de la libre competencia, en la medida en que implica esencialmente al mundo anglosajón".[31]

Cada uno de los países que participan en Echelon controla una determinada zona del mundo. Dos de ellas están situadas en Gran Bretaña, una en la localidad de Morwenstow y otra en Menwith Hill.[32] Los cuatro

centros restantes están situados en Sugar Growe (Virginia), Yakima (Seattle), Waihopai (Nueva Zelanda) y Geraldton (Australia).

El satélite que controla Europa está controlado por la base inglesa de Menwith Hill, en el condado de Yorkshite y está considerada como la más potente del mundo.[33]

La característica principal del *Echelon* es su sistema de satélites unidos por las seis bases terrestres que, tras recibir las informaciones, las almacenan en un grupo de macroordenadores en red. Dicho sistema permite interceptar indiscriminadamente todas las comunicaciones que se transmiten por cualquier otro sistema. El *Echelon* intercepta los veinticinco satélites Intelsat utilizados por las compañías telefónicas de los cinco continentes, [34] y puede filtrar hasta dos millones de conversaciones industriales, políticas o privadas al minuto y en todos los continentes.

El método de selección que utiliza *Echelson* es aún más sofisticado que el de la propia interceptación de mensaje. Sus ordenadores comprenden el contexto general de la conversación y son capaces de proporcionar lo que suele llamarse información elaborada,[35] y clasificar en función de su importancias todas las conversaciones interceptadas sobre un tema específico preseleccionado. El procedimiento es el mismo si lo que interesa es fiscalizar trafico de drogas, actividades terroristas, nuevas tecnologías, industria de la construcción o un posible contrato entre dos empresas concretas.

Una vez analizados los mensajes, parten directamente al cuartel general de la NSA, en Maryland, donde se redistribuye el fruto de las escuchas a los paises socios de *Echelon.*

Todo ello hace previsible que *Echelon* sea una baza importantísima en la obtención de ciertos mercados por parte de determinadas empresas norteamericanas.

Echelon es, *de facto*, una red anglosajona, cuya creación se remonta al pacto de seguridad Ukusa firmado en 1.948 por los cinco países indicados con el fin de recoger el máximo de informaciones militares sobre la Unión Soviética y sus aliados. Tras la guerra fría se ha reorientado hacia la información civil y económica, lo que puede suponer, no solo una gran amenaza para las libertades públicas sino para el mundo económico libre.

Estrategia general de la información.

Cualquier organización, con independencia de su naturaleza, con respecto al conocimiento tiene que desempeñar al menos cuatro funciones esenciales: adquirir, procesar, distribuir y proteger la información mientras selectivamente la niega o la distribuye a sus adversarios y/o aliados.[36]

Cada una de estas cuatro funciones tienen una exacta analogía en el sector público y sector privado, ámbito civil y militar, y están interrelacionadas.

La *adquisición* de información se produce por los modos más diversos. Se obtiene de los medios de comunicación, de la investigación y el

desarrollo, de los servicios de espionaje e información correspondientes, de la cultura en general y de otras fuentes. Una estrategia de información sistemática relacionaría todas estas fuentes y determinará cual requiere su perfeccionamiento.

Relacionado con la adquisición están otras actividades como la "fuga de cerebros", lo que hace previsible que las estrategias del saber del futuro puedan concebir complejas políticas a largo plazo para absorber de determinados países, empresas u organizaciones, a sus cerebros más capacitados y trasladarlos al propio. Alternativamente, tales estrategias dispondrán cada vez más de planes para disuadir o prohibir los desplazamientos de científicos o ingenieros importantes a adversarios potenciales.[37]

Una vez adquirida la información, se tiene que almacenar y *procesar* grandes cantidades de datos, lo que requiere unas inversiones cada vez mayores en tecnología de la información. Sistemas informáticos de todos los tamaños y tipos. La naturaleza, distribución, capacidad, utilización y flexibilidad de estos sistemas y sus conexiones con otros y con las redes de satélites y comunicaciones distinguirán las organizaciones avanzadas de las demás.

Pero desde luego lo más importante en este proceso son los invisibles programas informáticos que procesan, analizan y distribuyen datos.

Durante la revolución industrial y todos los años que la siguieron los espías militares prestaban una atención especial a las máquinas herramientas de su adversario porque resultaban necesarias para hacer otras. Ahora la máquina-herramienta que más cuenta es la programación informática empleada en la elaboración de los programas que fabrican programas que a su vez, producen programas, porque de ello depende gran parte de la transformación de datos en información y conocimiento práctico.

"Las políticas que guían el desarrollo y el uso de la tecnología de la información en general y de la programación informática en particular constituyen un componente vital de la estrategia del saber". [38]

Aunque se haya adquirido y procesado convenientemente, el conocimiento resulta inútil si no es utilizado en el momento oportuno, de ahí la necesidad de alcanzar diversas maneras de *distribuirlo* cuando se precise.

Para ello resulta esencial la capacidad de enlace en las comunicaciones electrónicas. Capacidad de enlace es el término técnico que se suele emplear para referirse a las redes. La designación del tipo que éstas sean y de quienes tengan acceso a las mismas responde a consideraciones estratégicas de alto nivel en la organización de que se trate.

Pero la comunicación es tan sólo una parte del sistema de distribución del conocimiento. El aprendizaje, desaprendizaje y reaprendizaje se han convertido en un proceso permanente dentro de cada nivel profesional. En todas las ramas se desarrollan tecnologías avanzadas para acelerar el

aprendizaje. Entre ellas desempeñan un papel cada vez más importante las simulaciones de base informática.

Es conocido de la ventaja de las organizaciones que mejor adiestran, que aprenden más deprisa y que saben más tienen una clara ventaja, susceptible de compensar muchos fallos. "El conocimiento es el sustituto definitivo de otros recursos".[39]

Entre los elementos que las organizaciones distribuyen figuran información engañosa, desinformación, propaganda, verdad y un poderoso material gráfico para los medios de comunicación, en definitiva, conocimiento junto con anticonocimiento.

Por este motivo, la política de los medios de comunicación de masas, así como las de comunicación y educación constituirán conjuntamente los ingredientes principales de distribución de cualquier estrategia general del conocimiento.[40]

Ninguna estrategia del conocimiento se hallará completa sin un cuarto y último componente, la *defensa* del activo del propio conocimiento frente los competidores o adversarios.

Pero el conocimiento es un arma de doble filo y, como dice Sun Tzu, en "El arte de la guerra", "los que no son totalmente conscientes de las desventajas de servirse de las armas no pueden ser totalmente conscientes de las ventajas de utilizarlas".[41]

La superioridad en información y conocimiento es una ventaja extraordinariamente importante pero muy frágil, puede terminar por un cortocircuito, una mentira o por la incapacidad de proteger esa información de quienes pretender apropiarsela.

Privar a una organización de su activo de información y conocimiento puede comportar graves consecuencias, e incluso amenazar su supervivencia, por lo que en paralelo a estas amenazas y riesgos adquiere cada vez mayor importancia su protección.[42]

La fortaleza de un conjunto organizativo -sea civil, militar, empresarial o de otra naturaleza- depende cada vez más de la propia estrategia del conocimiento del conjunto. Lo que pone en evidencia la interrelación informativa de unos ámbitos con otros, dentro de una sociedad.

La promoción y defensa continuas de este activo son requisitos previos de la supervivencia de las sociedades en el siglo XXI.

Para llegar a una estrategia adecuada, cada país -o cada organización- habrá de enfrentarse con sus retos específicos, y tendrán necesidades de protección de distinta entidad.

Los hechos descritos son sólo una pequeña muestra de la realidad, pero tal vez sean representativos de una situación general en la que afloran riesgos de la más variada índole, con efecto distinto, según el ámbito a que se refiera, que afectan a la información y a las comunicaciones y de

los que conviene prevenirse e incorporar la función de protección de la información, y convierten a la seguridad en una necesidad.

Todos los elementos de un sistema de información y comunicaciones son susceptibles de ser atacados y sobre ellos se ciernen las más variadas amenazas.

Por lo que se refiere a las amenazas técnicas, más próximas al objeto de esta tesis, y a un ámbito concreto como podría ser un sistema informático, Morant Ramón las engloba en cuatro grandes tipos: Intercepción, Modificación, Interrupción y Generación.[43]

La *interceptación* se origina cuando una persona, programa, o proceso, logra el acceso a una parte del sistema a la que no está autorizado. Al no producirse, por lo general, una alteración en el sistema es por lo que se hace muy difícil su detección.

La *modificación* es una amenaza más peligrosa. Se intenta no sólo tener acceso a una parte del sistema donde no se tiene autorización sino, además, cambiar su funcionamiento.

La *interrupción*, es tal vez la de más fácil detección pero la que mayor dificultad presente para luchar contra ella. Puede ser temporal o permanente e incluye la posibilidad de destrucción de dispositivos informáticos.

La *generación* es una amenaza que se refiere a la posibilidad de incluir campos y registros en una base de datos, añadir líneas de código a un

programa o incluso programas completos en un sistema (virus), e introducir mensajes no autorizados.[44]

Aunque no se puede asegurar que cualquier información es igualmente útil, y menos aún, que toda información "es poder" -en determinados casos el exceso de información perturba el conocimiento-, en general, la información se considera como un bien preciado, puesto que es una fórmula susceptible de adoptar conocimiento.

Por ello, desde antiguo, todas las personas que poseían información de un cierto valor (reyes, militares, sacerdotes, etc.) utilizaron métodos y mecanismos para salvaguardarla e impedir que se extendiera fuera de los límites previstos.

Todo bien conlleva que su poseedor tenga una serie de riesgos y esté sometido a una serie de amenazas por parte de quienes quieren poseerlo.

En el caso que nos ocupa, y, al referirnos a la información, el riesgo ha de ser entendido como "Probabilidad de que una vulnerabilidad propia de un sistema de información sea explotada por las amenazas a dicho sistema, con el objetivo de penetrarlo" [45] y, la amenaza como "Condición del entorno del sistema de información que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad"

Desde el momento que la información puede proporcionar beneficios, siempre existirá alguien que ponga todos sus medios para

obtenerla. De la ratio de eficacia, como cociente entre el beneficio que obtenga de la posesión de un bien y el coste de los medios utilizados para conseguirlo, se deriva que existirá una proporcionalidad entre los medios utilizados para su obtención y el beneficio previsto.

La humanidad, permanentemente ha ido buscando medios para transmitir y utilizar la información, pero los grandes logros conseguidos en estos asuntos tienen como contrapartida el grave problema de aumentar la inseguridad de la misma.

En los últimos años se han realizado grandes avances en las tecnologías de la información y las comunicaciones cuyo impulso más significativo tal vez se produjese en la Segunda Guerra Mundial.

Se han creado sistemas capaces de almacenar, procesar y transmitir gran cantidad de datos e información a gran velocidad. Con una introducción masiva de los sistemas informáticos en el mundo de los negocios.

Pero a medida que los actuales sistemas de información se han ido haciendo cada vez más complejos, existen más elementos vulnerables y mayor facilidad para acceder a la información que por ellos fluye. Ha crecido el número de posibles "atacantes" al igual que, la posibilidad de obtención de grandes beneficios ha estimulado la imaginación. En paralelo, los medios necesarios para perpetrar la violación son tan sofisticados como el sistema mismo, ya que tienen el mismo origen tecnológico.

Por todo ello es difícil delimitar lo que hay que proteger y con qué niveles, sobre todo al tratarse de un intangible como es la información, donde determinados datos pueden carecer de un valor intrínseco aparente, pero que, unidos a otros, aportan un valioso conocimiento.

Las amenazas y riesgos a los que está sometido un moderno sistema de información, tanto en su aspecto físico, como lógico, datos u organización, hace que su vulnerabilidad sea muy elevada.

La tecnología hoy permite interferir todos los canales, y las comunicaciones electrónicas se usan para casi todas las actividades humanas. La posibilidad de violar la integridad, la confidencialidad, en definitiva, la seguridad, produce consecuencias inesperadas, imprevistas y quizás irreparables, para individuos, organizaciones y la sociedad en general. La criptografía moderna intenta dar respuesta a las necesidades de protección con algoritmos matemáticamente demostrables. [46]

Lo que no es otra cosa que la solución de un problema en un contexto determinado.

En el contexto de la matemática, junto al planteamiento de problemas, nace el concepto intuitivo de algoritmo como el conjunto finito de operaciones que, realizadas en un orden determinado, permiten resolver todos los problemas de un tipo dado.

Se considera resuelta una serie de problemas de un determinado tipo cuando se elabora un algoritmo para su resolución.

La "detección" de una violación encierra grandes dificultades y puede producir situaciones en las que la violación se prolonga indefinidamente en el tiempo.

El intento de violación puede ser: pasivo o activo. El pasivo tiene por objeto el simple conocimiento de la información almacenada o transmitida en cualquier sistema, mientras que la violación activa, más ambiciosa, pretende la modificación de la información almacenada o transmitida, en ambos casos, para favorecer los intereses del infractor.

Es obvio que una y otra, precisan de requerimientos previos diferentes, así como son diferentes sus consecuencias para la organización propietaria de la información.

El intento pasivo pretende conocer la situación o intenciones de un objetivo con tiempo suficiente para que el agresor tome las medidas oportunas que le favorezcan, mientras que el intento activo tiende a que el agredido base su actuación en la información errónea introducida en el sistema. Como es lógico, requiere un conocimiento perfecto del sistema de información.

Las medidas para evitarlas son conocidas: passwords, autentificación de origen, contenido y destino, cifrado de la información almacenada, etc.; dependiendo del sistema de información que se implante. En ambos casos, la detección del intento de violación no resulta fácil y todavía es más

ardua la determinación del autor, lo que tiene relación con las "dificultades de prueba" a que aludimos en este trabajo.

Por ello, es necesario, además, una "auditoria" permanente del sistema siguiendo una política previamente definida. Es decir, no basta con el establecimiento inicial de una política de seguridad, dándola por adecuada con carácter permanente.

Por todo ello, se hace necesario proteger la información y las comunicaciones en cada sistema, en función de los requerimientos del mismo y, previo un exhaustivo análisis de riesgos, establecer una política de seguridad que incluya un conjunto completo de mecanismos y servicios que permitan conseguir la seguridad necesaria.

Dentro del marco de una política de seguridad y por lo que se refiere específicamente al logro efectivo de la protección, se requiere la previa determinación de los riesgos de seguridad a que está sometido el sistema y una apreciación completa y conjunta de necesidades para, mediante su satisfacción, poder neutralizarlos.

Mediante el análisis de riesgos se puede conocer la vulnerabilidad y prever los efectos potenciales que podrían derivarse de la misma, identificando y justificando las medidas de seguridad a adoptar.

El análisis y gestión de riesgos es un presupuesto básico para la implantación de un programa efectivo de Seguridad en cualquier organización.

Pero la selección del método de análisis y gestión de riesgos más apropiado para aplicar a los requerimientos específicos de una determinada organización es un proceso difícil, toda vez que son múltiples las organizaciones y muy variados sus requerimientos como para que pueda existir un método completo y polivalente que dé respuesta tanto a las necesidades de las organizaciones públicas como privadas, las industriales, comerciales, militares, diplomáticas o policiales, etc.

En todo caso, sí que hay una serie de conceptos básicos que han de tenerse en cuenta en el análisis de riesgos de cualquier organización, sea del tipo que sea.

Tal vez el primer concepto que ha de tenerse muy claro es la necesidad de conocer las amenazas y estimar las pérdidas potenciales derivadas de la vulnerabilidad del sistema, así como los daños que se pueden producir en el caso de materializarse determinadas amenazas.

Una vez identificadas amenazas, pérdidas potenciales y daños, se podrían conocer los activos de información críticos que deben ser protegidos, pero sin olvidar los entornos en que captan, procesan, almacenan, transmiten y distribuyen dichos activos.

La identificación y valoración de activos es el paso previo para la evaluación de las posibles pérdidas en base a un análisis cuantitativo o cualitativo.

En el análisis de riesgos cuantitativo se calcula matemáticamente la frecuencia y probabilidad de una amenaza, mientras que el análisis de riesgos cualitativos, es de mayor subjetividad y suele realizarse sobre una serie de amenazas basadas en el conocimiento y juicio de las personas que realizan el análisis.

El análisis de riesgos es la piedra angular de un programa efectivo de Seguridad de Tecnologías de la Información dentro de una organización, [47] constituye la base para una eficaz gestión de riesgos mediante la que se tiene la certeza de que se han tomado las medidas razonables para prevenir situaciones que pueda interferir las misiones de la organización.

Pero el análisis de riesgos cuando tiene una mayor utilidad es cuando se realiza en la fase de diseño de un sistema de información al permitir, desde el principio, contemplar eventuales pérdidas y requerimientos de seguridad así como incorporar medidas, e incluso, rediseñar el sistema si fuese necesario.

Para los sistemas en funcionamiento, el análisis de riesgos permitirá detectar vulnerabilidades y abordar la gestión de riesgos, como forma de llevar a cabo la protección más efectiva contra los ataques al sistema de información.

La gestión de riesgos está constituida por el conjunto de actividades de todo tipo encaminadas a soluciones de seguridad basadas en una adecuada relación del coste y la eficacia.

Con los resultados de este análisis se ha de elaborar un Plan de Seguridad de la Información que contenga las amenazas a las que está sometido el sistema de información de la organización a que se refiera y las soluciones para neutralizarlas.

Es de fundamental importancia la determinación de quien establece las necesidades de protección de la información, sobre todo tratandose de un intangible inmerso en un medio de elevado componente político y tecnológico.

Pero con independencia de quien establezca la necesidad, se puede necesitar lo que se quiere, y querer o no lo que se necesita, pero *"lo que no puede suceder de forma consistente es no necesitar aquello que se requiere a fin de prevenir daños graves, con independencia de lo que se desee" [48]*

1.2.- LA SEGURIDAD DE LA INFORMACIÓN.

Seguridad que, según la formula contenida en el Diccionario de la Real Academia Española de la Lengua es la calidad de estar libre y exento de todo peligro, daño o riesgo. Situación que resulta difícil cubrir en su plenitud conceptual y que, en todo caso, viene determinada por los peligros,

riesgos y amenazas a que- en este caso la información- puede verse sometida.

Pero la variedad e intensidad de los riesgos y amenazas son tan diversas -y la propia naturaleza de la información lo complica- que, a priori, resulta extremadamente difícil establecer "la seguridad necesaria".

Si además se tiene en cuenta la diferencia entre la lógica del razonamiento del atacante -que en definitiva es el que puede elevar el nivel de exigencia de seguridad-, y la lógica de razonamiento del que elabora la defensa -seguridad, que para ser tal ha de ser superior a los niveles de agresiones potenciales-, resulta evidente la dificultad y complejidad del diseño de criterios de seguridad.

Quizás sea bajo el punto de vista de la teoría matemática de los juegos [49] bajo el que hay que estudiar el problema de la seguridad.[50]

Se trataría de estudiar el comportamiento de dos o de varios actores en sus relaciones mutuas en torno a un objetivo común.

El problema planteado no consiste sólo en describir el comportamiento de los actores, sino en calcular cuál puede ser, para cada uno de los jugadores en presencia, el mejor comportamiento posible frente a las reacciones previsibles de su adversario. Este comportamiento ideal consiste, por parte de los jugadores, en exagerar sus ventajas y disimular sus pérdidas, en función de la táctica adoptada por los otros jugadores.

El estudio de este género de confrontaciones ha demostrado que el tipo de situaciones en las cuales se encuentran los actores no es susceptible de variar indefinidamente. En la práctica, las combinaciones se reducen a varios "modelos" que difieren según la naturaleza del objetivo, la posibilidad de comunicación entre los adversarios y el número de jugadores.

En primer lugar, se distinguen los juegos de suma cero, en los que la ganancia de uno representa exactamente la pérdida del otro, y los juegos de suma variable, en los que pérdidas y ganancias se reparten, de una manera aleatoria, entre los dos jugadores.

A través de estos diferentes modelos, que evidentemente son susceptibles de numerosas combinaciones, se llega a determinar, matemáticamente, cuáles son los modos racionales de conducta en diversos tipos de circunstancias. Es, entonces, posible prever -e incluso prevenir- aplicando a la solución de uno u otro conflicto, unas fórmulas cuya eficacia se ha podido verificar anticipadamente.

La teoría de los juegos ha conocido y conoce todavía numerosas aplicaciones en el campo de las relaciones internacionales, en el ámbito militar para resolver ciertos problemas estratégicos y tácticos y en el estudio de situaciones políticas o político-estratégicas. De esta forma, se han podido construir matrices y esquemas utilizables en el caso de conflictos reales o eventuales. [51]

Para Morant Ramón el problema de la seguridad de la información quizás haya que estudiarlo bajo el punto de vista de la teoría matemática de los juegos.[52]

La situación ideal del diseñador de seguridad podría ser la de anticiparse al atacante, incorporar los códigos y lógica del atacante, "tener un atacante en la cabeza".

Gonzalo Abril, al hablar de transcodificación y transubjetividad en su trabajo "Puertas", dice: "...Invoca Piccini la "imagen del tejedor" de Serres, y el parangón que Barthes establece entre el texto y la telaraña, por un lado, y el sujeto que hace el texto y la araña misma, por otro...,este sujeto araña, que teje y acecha a la "puerta" de su tejido, es todavía demasiado preliminar. La metáfora resulta más comprensiva si se concibe la araña también en la liminaridad de su anticipar la mosca, hacerse mosca, como Deleuze y Guattari (en Mil mesetas) la presentan al aplicar la noción de "transcodificación": Hay un caso especialmente importante de transcodificación, cuando un código no se contenta con tomar o recibir componentes codificados de otra manera, sino que toma o recibe fragmentos de otro código como tal (...). Se ha observado, con frecuencia, que la tela de araña implicaba en el código de ese animal secuencias del propio código de la mosca; diríase que la araña tiene una mosca en la cabeza, un "motivo" de mosca, un "ritornelo" de mosca."[53]

El atacante, en este caso, sería el *criptoanálisis*, constituido por el conjunto de operaciones orientadas a transformar un texto cifrado en el texto claro original sin conocer inicialmente el sistema de cifrado utilizado y/o la clave.[54]

Resulta difícil definir en qué consiste la seguridad de la información, pero parece obvio que hay que establecer medidas para protegerla. De donde se podría derivar que la seguridad de la información es el conjunto de medidas encaminadas a la protección efectiva de la información frente a eventuales amenazas.

El Glosario de Términos de Criptología, del Centro Superior de Información de la Defensa, revisión marzo de 1.993, no recoge la expresión "Seguridad de la Información", sin embargo, recoge otras de cuyo contenido se puede derivar el alcance conceptual de "Seguridad de la Información".

Así, cuando habla de "Sistema de información" dice: "Cualquier sistema o producto destinado a almacenar, procesar, o transmitir información. Su seguridad se basa en el mantenimiento de la confidencialidad, disponibilidad e integridad de la información".

Cuando se refiere a "Seguridad de las comunicaciones" dice que es el :"Resultado de un conjunto de medidas, entre ellas las criptológicas, orientadas a impedir que entidades no autorizadas puedan tener acceso a la información transmitida o analizar el tráfico de una red", y, "Seguridad de los ordenadores" que es el: "Resultado de un conjunto de medidas aplicadas

a un sistema informático y orientadas a evitar accesos, manipulaciones, pérdidas, modificaciones o conocimiento de la información que contiene por personal no autorizado.[55]

La Propuesta de Decisión del Consejo de Europa en el ámbito de la seguridad de la información de 27 de julio de 1.990 , -convertida en Decisión del Consejo el 31 de marzo de 1.992 (92/242/CEE)- proponía un plan de acción cuyo objetivo es "desarrollar una estrategia global tendente a dotar a los usuarios de la información almacenada, tratada o transmitida por medios electrónicos, una protección de los sistemas de información frente a amenazas accidentales o deliberadas."

En ella se puede leer "... la protección de la información en todos sus aspectos, denominada aquí 'seguridad de la información', se ha convertido en un tema político esencial que preocupa en todo el mundo" y, en una llamada a pié de página se dice "La seguridad de la información (SI) se interesa por la protección de la información almacenada, tratada o transmitida electrónicamente frente a cualquier amenaza voluntaria o accidental. Los servicios de información electrónica exigen una infraestructura de telecomunicaciones segura, unas terminales seguras (incluidos procesadores y bases de datos) y una utilización segura".

De las diferentes definiciones manejadas por diversos autores, así como de las normas elaboradas y aprobadas por varios países [56], relativas a la seguridad de la información, se encuentran tres criterios o propiedades

fundamentales, que son tres dimensiones distintas de la seguridad de la información: la confidencialidad, la integridad y la accesibilidad.

Por virtud de la confidencialidad un sistema de información sólo permite el conocimiento de la misma a quienes estén autorizados. Es el corazón de la política de seguridad del sistema de información y requiere una previa delimitación del ámbito a proteger, una clasificación de la información.[57]

Para Miguel Ángel Dávara, la confidencialidad se refiere al mayor o menor secreto con que se van a guardar y tratar los datos.[58]

Confidencialidad es el "Servicio de seguridad que asegura que una información no puede estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados. Puede proteger toda la información que circula por un enlace, determinados campos de ella o contra análisis del flujo de tráfico."[59] Es la propiedad más directamente relacionada con los procedimientos criptográficos.

La integridad es la garantía contra la alteración de la información de forma indebida, errónea o no autorizada [60], permite asegurar que no se ha falseado la información [61]. Es, en definitiva, el "Servicio de seguridad que garantiza que la información recibida no ha sido mutilada o alterada de manera no autorizada durante su transmisión.

Como mecanismos de seguridad, incluye los procedimientos que garantizan la integridad de un campo de información, o de todos ellos,

contra desórdenes, repeticiones, inserciones, pérdidas o alteraciones, para lo que se utilizan secuencias numéricas, cadenas criptográficas o referencias horarias" [62].

La accesibilidad o disponibilidad, es la propiedad que asegura que cada elemento de información y cada funcionalidad del sistema puedan ser utilizados por los usuarios autorizados.

Estas tres dimensiones de la seguridad obligan a un equilibrio en la proporción en que cada una interviene en un sistema de información, en función del uso a que esté destinado.

Si bien es cierto que "para muchos, la seguridad, aplicada a la información, se asocia solo con aspectos parciales, generalmente relacionados con la disponibilidad y la seguridad física... olvidando otros enfoques importantes, más relacionados con la integridad y con la confidencialidad de la información, y con la seguridad lógica más que con la física"[63], no es menos cierto que esto se produce en entornos donde no ha existido una "cultura de seguridad" y que, por el contrario, en los ámbitos donde esta conciencia existe, la seguridad se concibe de forma integral con gran peso de la seguridad física, de la confidencialidad y su protección, esencialmente criptológica, de la organización, y del factor humano.

En seguridad informática se utiliza la expresión seguridad lógica como contrapuesta a seguridad física, y aunque en puridad ambas podrían ser consideradas como "lógicas"[64], generalmente se reserva la expresión

"seguridad lógica" para "las posibilidades de protección de los datos registrados en soportes magnéticos mediante el adecuado empleo de medios informáticos", mientras que el término "seguridad física" es referido a las posibilidades de protección de esos mismos datos empleando las medidas de seguridad oportunas de carácter físico.[65]

A lo largo de las últimas décadas se han producido importantes transformaciones, pero las que se avecinan pueden serlo aún más. Están desarrollándose los superordenadores de sobremesa, la radiodifusión directa vía satélite, las radiocomunicaciones móviles digitales, las comunicaciones integradas de banda ancha y otras aplicaciones de la tecnología que permitirán contar con unas comunicaciones móviles, económicas, de alto rendimiento y universales en una dimensión sin precedentes.

El advenimiento de unas comunicaciones globales eficaces viene a subrayar la necesidad de contar con una "protección" adecuada y unas medidas de seguridad eficaces, en cuanto a disponibilidad del servicio, integridad de los mensajes y confidencialidad, acorde con la previsible gravedad de la amenaza administrativa o técnica.

Los requisitos fundamentales de seguridad según el TCSEC, documento elaborado por el National Computer Security Center (NCSC) de EE.UU. en 1.985 y conocido como Libro Naranja, -en el que se contenían especificaciones de criterios de seguridad de hardware, firmware y software de base- son los siguientes: requisitos de funciones específicas de

seguridad y requisitos de adecuación. Estos requisitos permiten al personal evaluador examinar el sistema, comprobando si las funciones de seguridad necesarias están presentes y si trabajan correctamente.

Dentro de los requisitos de funciones específicas de seguridad está la política de seguridad, que debe ser explícita y bien definida, con identificación de todos los sujetos y objetos en el sistema, y con un conjunto de reglas que permitan determinar qué sujetos pueden acceder a qué objetos.

Los sistemas por los que fluya información sensible deben poner en práctica políticas de acceso no-discrecional u obligatorio en las que se establece un conjunto de compartimentos de objetos y sujetos de información y una clasificación de ambos en niveles de confidencialidad, de forma que un sujeto sólo puede acceder a un objeto si ambos pertenecen al mismo compartimento, y además, el nivel de confidencialidad de aquel es igual o mayor que el del objeto.

Entre los requisitos de adecuación, y por lo que se refiere a la seguridad, el sistema debe contener mecanismos que puedan ser evaluados independientemente.

Por lo que se refiere a la protección continua, los mecanismos que llevan a cabo estos requisitos básicos deben estar continuamente protegidos contra ataques o alteraciones no autorizadas. Ningún sistema se puede considerar seguro si sus mecanismos de seguridad son susceptibles de ser destruidos o modificados.[66]

La política de seguridad, es el conjunto de directrices generales que deben guiar la seguridad de la información, y constituye uno de los componentes más importantes de la arquitectura de seguridad de un sistema. Su materialización requiere la previa transformación en un modelo de seguridad, que puede ser expresado en lenguaje matemático.

Dentro de la política de información y del conocimiento, la política de seguridad se ha de centrar en resaltar el carácter de la información como activo de la organización y su necesidad de ser protegido.

Para ello es necesario implantar una cultura de seguridad que permita una toma de conciencia y mentalización de toda la organización, de la importancia de la información como activo de la misma y de la necesidad de tomar medidas al respecto.

De igual modo debe contemplar la organización, funciones, obligaciones y responsabilidades de una administración de seguridad de la información, así como los canales de comunicación a utilizar.

Esta política ha de definir las normas de protección de la información y establecer la estructura de recursos materiales, humanos y organizativos, con definición de funciones, para hacer frente a dicha protección, así como definir los procedimientos para la determinación de cualquier tipo de medidas de seguridad a tomar y la tecnología a utilizar.

Una organización puede tener, en sus diversos niveles, diferentes políticas de seguridad, que no serían contradictorias sino complementarias

entre sí. E incluso, en un mismo nivel se pueden establecer diferentes políticas.

Ademas de las políticas administrativas que se llevan a cabo a través de procedimientos de este tipo, los grupos fundamentales de políticas de seguridad de la información se centran en el control de accesos y el flujo de información.

Las políticas de control de accesos establecen en qué circunstancias un sujeto puede acceder a un objeto de información. Dentro de ellas y como polos opuestos está el conocido principio de *"Need-to-Know"* (necesidad de conocer), según el cual un usuario accede estrictamente a aquellos objetos de información que necesita conocer para la realización de su trabajo, frente al principio de máximo privilegio, escasamente aplicado, según el cual se tendría acceso a un amplio objeto de información.

Las políticas de control de flujo se ocupan de la utilización que se da a la información a la que se ha tenido acceso. Se ocupan de la difusión de la información obtenida, con indicación de los canales permitidos para la difusión de la misma.

Una política de control de flujos ha de establecer el orden de prioridad que ha de darse a cada una de las tres características de la seguridad: confidencialidad, integridad y disponibilidad. Indicando claramente si se debe potenciar el secreto, la evitación de modificaciones o destrucciones no autorizadas o la facilidad de acceso.

Los organismos vinculados a la seguridad y a la defensa se decantan por potenciar, sobre todo, la confidencialidad, seguida de la disponibilidad y la integridad. Mientras que los sectores gubernamentales no defensivos ni de seguridad se preocupan en primer lugar de la integridad seguida de la confidencialidad y la disponibilidad y, los sectores económicos, ponen el acento en primer lugar en la integridad, seguido de la disponibilidad y, solo en tercer lugar consideran la confidencialidad.[67]

Un modelo de seguridad, como formulación teórica de una política de seguridad, expresable matemáticamente, debe contener elementos suficientes para que los diseñadores del sistema conozcan lo necesario para determinar los controles de seguridad a construir, para que los usuarios puedan utilizar eficazmente el mismo, y para que los evaluadores dispongan de los elementos suficientes que les permitan determinar su consistencia y adecuación a las políticas que pretende poner en práctica, así como la correcta implementación de todo ello.

Dentro de los modelos de seguridad existen dos grandes grupos, los modelos de seguridad discrecional y los modelos de seguridad obligatoria.

En los modelos de seguridad discrecional los propietarios del objeto de información tienen la facultad discrecional de proporcionar a otros usuarios el acceso al mismo. Se ocupan de regular sólo el acceso de los sujetos al objeto.

En los modelos de seguridad obligatoria, además se ocupan de controlar la posible difusión de la información obtenida una vez se ha tenido acceso a la misma y en ellos se suelen especificar los canales por los que la información puede fluir. Se expresan mediante objetos de información, sujetos que pueden tener acceso a la misma y niveles de seguridad.

Dentro de los modelos de seguridad obligatoria, los modelos multinivel tienen una estructura en la que y los sujetos están agrupados en distintas áreas.

Además, los objetos están divididos por niveles de confidencialidad y, de forma análoga, los sujetos están divididos en niveles de autoridad según el principio de *"Need-to-Know"*.

De esta forma, la clasificación del objeto (la información) viene determinada por el nivel de confidencialidad y el área. Y la clasificación de los sujetos viene determinada por el nivel de autoridad y el área.

La determinación de la posibilidad de acceso de un sujeto a una información viene fijada por la relación entre ambos.

Igualmente, dentro del modelo de seguridad obligatoria, están los modelos de flujo de información que describen los caminos autorizados para el flujo de la misma dentro del sistema, especificando qué sujetos pueden acceder a qué información, según los niveles respectivos en que se encuentran clasificados, en función de la confidencialidad (los objetos) y la autori-

dad (los sujetos), estableciéndose una relación de orden entre confidencialidad y autoridad.

El modelo de seguridad se implanta en el sistema de información en forma de medidas y mecanismos de seguridad entre los que destacan las medidas criptológicas con específicos mecanismos constituidos por los equipos y sistemas de cifrado.

1.3.- LA SEGURIDAD DE LA INFORMACIÓN COMO GARANTÍA DE LA SOCIEDAD, DEL ESTADO Y DEL INDIVIDUO.

La creciente y recíproca dependencia de los Estados en la vida internacional conlleva la necesidad de abordar cualquier solución nacional teniendo en cuenta una perspectiva global o planetaria.

Existe toda una serie de realidades mundiales que determinan la prosperidad, los logros sociales o las libertades públicas de cada país. Las soluciones a estos problemas se podrán materializar en la medida que las grandes decisiones que configuran la vida nacional se adapten, con precisión, a una exacta percepción del ambiente internacional.

En este juego global internacional, cada nación persigue, de forma prioritaria, la consolidación de su seguridad como meta tradicional de su política exterior. Pero hoy, el concepto de seguridad nacional rebasa su componente militar y da entrada a una variedad de factores de tipo económico, político, ecológico, diplomático, tecnológico, sociales o culturales.[68]

El modo de vida de los ciudadanos, sus intereses, la consistencia de sus instituciones, la defensa de sus libertades, su seguridad, se sitúan en un punto de intersección entre los grandes ejes de la política nacional y las variables de una nueva configuración mundial.

Para Miguel Herrero y Rodríguez de Miñón, "el concepto de seguridad se ha transformado durante la década de los ochenta. Hoy, junto a sus dimensiones estrictamente militares, se le reconocen otras, políticas, sociales y económicas. La superación de las tensiones que el subdesarrollo (como situación, como comparación y como dinámica de equiparación) lleva consigo, sería, por lo tanto, un ingrediente de la estabilidad que la seguridad requiere".[69]

Hoy la seguridad de cada país y la paz mundial, están amenazadas por peligros económicos, tecnológicos, sociales, e institucionales en similar medida que por peligros militares. Tensiones étnicas y nacionalistas, hambre, pobreza y desempleo son noticias diarias.

La pérdida de la soberanía económica, o la dependencia tecnológica de un país, puede suponer el debilitamiento, e incluso la extinción de su autonomía política, con una subordinación de las libertades y el nivel de vida de sus ciudadanos a poderes exteriores, a los que no puede controlar.

Pero el fin de la "guerra fría" ha provocado una revolución en la forma de pensar las cuestiones de seguridad y defensa. En realidad es el principio mismo del uso internacional de la fuerza el que ha sufrido una

mutación radical. Los retos de seguridad atañen cada día más al planeta entero, nadie está libre de ellos y, en la mayoría de los casos, sólo un tratamiento colectivo parece ser eficaz. Aunque solo sea porque garantiza cierta legitimidad de la decisión de intervenir, con independencia de que se haga a través de sanciones militares o no, intervenciones humanitarias o con miras al mantenimiento de la paz, acciones de fuerza o preventivas.[70]

En el escenario internacional aparecen amenazas tales como la degradación del medio ambiente, las migraciones humanas, el terrorismo, la droga, el SIDA, el debilitamiento de las instituciones..., como fenómenos transnacionales, que no conocen fronteras, y que comprometen gravemente la supervivencia de toda nación económica y militarmente soberana, y cuyos efectos se ven potenciados, en muchos casos, por la aplicación de las nuevas tecnologías. De todo ello se derivan nexos de unión entre lo que es política exterior y política interior.

En la actualidad, el ciudadano ha de saber que sus derechos individuales, sus libertades, su seguridad en definitiva, se juega en una partida mundial cuyo resultado depende de todos.

Hace tiempo que persiste la idea de la exigencia ineludible de acceder a un sistema mundial que permita abordar un gran número de problemas estratégicos, que rebasan el modelo fundado en las soberanías nacionales, y en el que se daría un alto grado de reconocimiento y ejercicio de la libertad individual, en el que cada hombre en su peculiaridad, sería

sujeto de los derechos en el proceso de desenvolvimiento social, en tanto que las sucesivas instituciones históricas habrían sido expresiones correspondientes a fases históricas superadas, en la secuencia del proceso de incremento de la libertad individual. Situación que implica unos nuevos Derechos del Hombre que lo caracterizarán como titular y protagonista del desenvolvimiento social. [71]

En este contexto, el hombre deviene tal, desde su condición animal "porque toma parte activa en la formación de su propio ámbito", toma parte activa en la cosa pública, siendo, en este sentido, la condición de político inherente al hombre.

En la historia de los derechos fundamentales ha sido característica una tensión entre el individuo y el Estado, matizada por el creciente proceso de internacionalización, lo que viene a suponer que la historia de los derechos fundamentales no es solo un proceso de tensiones entre los individuos y el Estado, sino que en ella juegan también un papel relevante, además de los poderes supranacionales, los problemas de colisiones y conflictos entre los individuos.[72]

Por lo que no solo cabe hablar de relaciones entre individuos y estados, sino también de relaciones entre individuos y órganos supranacionales, entre estos órganos y los estados y de los estados entre sí.

La fórmula "derechos fundamentales como límites al poder", no parece que sea representativa de todas las proyecciones de los derechos, ya

que en ocasiones se presentan también como límites al poder de los ciudadanos. Solo tendría virtualidad esta formula entendiendo "poder" en sentido genérico, que abarcaría no solo al poder del Estado, sino también al poder de los grupos económicos, sociales, etc.

Existen ocasiones en las que los derechos fundamentales no son límites al poder político sino a la actuación de otros individuos.

Todo lo cual no hay que confundirlo con los "límites" de los derechos fundamentales, sino que se refiere a la posible transgresión de un derecho fundamental por un particular, con independencia de que este actúe a través de un derecho fundamental.

No siempre cabe entender a los derechos fundamentales como limitadores del poder estatal, sino también como limitadores de poderes privados, lo que viene a plantear el papel del Estado en relación con los derechos fundamentales.

En unos casos será negativa o de no interferencia y en otros, positivas, lo que implica promoción y actuaciones para la garantía efectiva, "un hacer" del Estado.

Y aunque esas obligaciones positivas no son trasladables al individuo, porque podría chocar con el valor de la libertad, la existencia de ciertos grupos en las sociedades modernas cuya incidencia social puede llegar incluso a trastocar el concepto clásico de poder público, una extensión

de la obligación positiva a su actuación favorecería el ejercicio y disfrute de los derechos y libertades.

En las relaciones entre el individuo y el Estado ha aparecido una nueva relación cuyos polos serían el Estado y la sociedad.

Como indica Bobbio, los derechos de libertad nacen contra el abuso del poder del Estado y para limitar este poder, mientras que los derechos sociales, para su protección efectiva, requieren un aumento de los poderes del Estado.

Hablar de derechos fundamentales como límite del poder, implica la abstención del Estado.

Pero ya no solo se habla de abstención, sino que se predica la actuación del Estado, entendiendo la abstención no como una restricción total de actuar, sino como señalización de los perfiles de una actuación obligatoria, esto es, no la prohibición de actuar, sino la obligación de hacerlo bajo determinados parámetros.

Para Pérez Luño, los derechos fundamentales han dejado de ser meros límites al ejercicio del poder político, para devenir en un conjunto de acciones positivas de los poderes públicos.[73]

Pero si el Estado tiene que actuar positivamente, no puede hacerlo de forma ilimitada, ha de respetar los límites constitucionales. Su necesaria actuación para el disfrute de ciertos derechos no puede atropellar

otros derechos que se consideran igualmente básicos, con lo que aparece el límite del límite. [74]

Para Peces Barba, la insuficiencia de una protección a nivel estatal de los derechos fundamentales, que siempre puede encontrar su límite en la razón de Estado, obliga a hablar de un proceso de internacionalización.

Las garantías internas que los Estados conceden a los derechos fundamentales resultan insuficientes e incluso en ocasiones inútiles, al ser los propios Estados los que producen la desvirtuación.

Se busca 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. [75]

La aparición de una instancia de poder superior que, en determinados ámbitos del Derecho permite la ampliación de su esfera de validez, limitada anteriormente a las fronteras nacionales, a la vez afecta y debilita el concepto clásico de soberanía.

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.

La necesidad de colaboración internacional es obvia, sobre todo frente a los nuevos problemas surgidos por el desarrollo de las nuevas tecnologías, lo que pone el acento en la imprescindible consideración del individuo como sujeto de Derecho internacional. [76]

Datos que afectan al honor, a la intimidad personal y familiar, a la propia imagen de los individuos, transitan a diario por las redes de telecomunicaciones, su seguridad resultan elementos constitutivos de su condición de individuos y de ciudadanos. La seguridad de estos y otros datos son también imperativo de eficacia para la Sociedad y para el Estado.

1.4.- MEDIDAS DE SEGURIDAD.

Dada la naturaleza de la información y el conocimiento y las características de las nuevas tecnologías, las medidas de seguridad a establecer son de lo más variado y de diversos tipos.

Se han hecho clasificaciones diversas. J.L. Morant considera que las medidas de seguridad a establecer en un sistema de tratamiento de la información pueden ser "medidas de seguridad lógicas, medidas de seguridad de carácter físico, medidas de carácter administrativo y medidas legales." [77]

Para Emilio del Peso y Miguel Ángel Ramos, refiriéndose a datos de carácter personal y sin ánimo de fijar una clasificación, agrupan a las medidas de seguridad en los siguientes apartados: De carácter físico, de carácter lógico, medidas relacionadas con el personal, medidas relacionadas con los desarrollos y medidas preventivas de pérdidas patrimoniales.[78]

Para Rafael Ortega García se refiere a las medidas tecnológicas, normas y procedimientos y, formación y entrenamientos, como tipos de

medidas de seguridad a implantar para asegurar las distintas características de la información (confidencialidad, integridad y disponibilidad) a través de sus distintos estados (proceso, almacenamiento y transmisión), llegando a definir la seguridad de la información en base a estos conceptos, "como todas aquellas medidas tecnológicas, de normas y procedimientos y de formación que aseguran la confidencialidad, integridad y disponibilidad de la información en sus estados de proceso, almacenamiento y transmisión". [79]

Miguel Ángel Dávara, habla de seguridad lógica, seguridad física y seguridad jurídica, señalando que las dos primeras son una protección a priori, mientras que la seguridad jurídica es una protección "a posteriori". [80]

A los efectos perseguidos por esta tesis consideramos conveniente agrupar las medidas de seguridad en los siguientes tipos o grupos: Medidas políticas, legales, organizativas, físicas, lógicas, electromagnéticas y criptológicas.

Son medidas políticas, las directrices generales de carácter estratégico, orientadas a preservar la información. Que tienen su anclaje en el propio orden constitucional.

Las medidas legales serían la concreción normativa de las medidas políticas y se orientarían a la delimitación de ámbitos de confidencialidad de la información y su protección jurídica.

Las medidas organizativas y administrativas, proporcionarían el elemento organizativo necesario para una protección eficaz de la información. Entre las que estaría el elemento humano, factor profesional y áreas de responsabilidad.

Las medidas físicas y lógicas están orientadas directamente a evitar el ataque contra la información protegida, mediante elementos materiales o procesos lógicos. En informática, las físicas, serían mediante elementos *"hard"* y las lógicas, mediante elementos *"soft"*.

Las electromagnéticas, aplicables a equipos informáticos y de telecomunicación que incorporen alta tecnología, serían las relativas al estudio y protección de las emisiones electromagnéticas no deseadas, lo que en ámbitos especializados se conoce como protección TEMPEST. (Término relativo al estudio y protección de las emisiones electromagnéticas no deseadas.[81]

Las medidas criptológicas son las producidas por equipos y sistemas que incorporan criptología, esto es, procedimientos para la ocultación o cifrado. Son las medidas sobre las que se centra el estudio de esta tesis.

[1] Pérez Luños, A.E., "Nuevas tecnologías, Sociedad y Derecho.El impacto socio-jurídico de las N.T. de la Información", FUNDESCO,Madrid, 1.987.
[2] Ribagorda Garnacho, A., "Glosario de Términos de Seguridad de las T.I.", Ediciones CODA, Madrid, 1.997.
[3] Sgarro, A., "Códigos Secretos", Edit. Pirámide, Madrid, 1.990, pag. 96.
[4] Prieto Sanchís, L., "El sistema de protección de los derechos fundamentales: el artículo 53 de la Constitución española", Anuario de Derechos Humanos, nº 2, Madrid, 1.983.
[5] Witker, J., "Cómo elaborar una tesis en Derecho", Edit. Cívitas, Madrid, 1.986.
[6] Doyale, L., y Gough, "Teoría de las necesidades humanas", Edit.Fuhem y Comunidad de Madrid, Madrid, 1.994.
[7] Doyale, L., y Gough, op. cit.
[8] Doyale, L., y Gough, op. cit.
[9] Doyale, L., y Gough, op. cit.
[10] Morant Ramón, J.L., y otros, "Seguridad y protección de la Información", Editorial Centro de Estudios Ramón Areces, Madrid, 1.994, pag. 15.
[11] Pastor Franco, J., "Criptografía moderna, informática y sociedad", Seminario dictado en la Universidad de Zaragoza, octubre de 1.989.
[12] Baptista Porta, Io., "De occultis liberarum notis", edición de 1.593, Capítulo cuarto, página 10. Facsímil de la ediciónde 1.593, editado por la Cátedra de Criptografía y la Biblioteca General de la Universidad de Zaragoza, 1.996.
[13] Tomado de Toffler, A. y H., "Las guerras del futuro", Plaza & Janes, Barcelona, 1.994, pág. 212.
[14] Toffler, A. y H., op. cit., pág. 213.
[15] Toffler, A. y H., op. cit., pág. 213.
[16] Toffler, A. y H., op. cit., pág. 213.
[17] El Mundo, Comunicación, viernes 10 de junio de 1.994.
[18] *cypherpunks@toad.com*
[19] El País, "Coladero del Pentágono", 24 de mayo de 1.996.
[20] El Mundo, 7 de junio de 1.996.
[21] El País, Negocios, domingo 19 de noviembre de 1.995.
[22] El Mundo, viernes 25 de diciembre de 1.994.
[23] El País, viernes, 28 de octubre de 1.994.
[24] El Mundo, Comunicación, sábado 27 de abril de 1.991.
[25] El Mundo, 16 de diciembre de 1.993.
[26] El País, 31 de julio de 1.996.
[27] ABC, domingo 29 de septiembre de 1.996, (Nacional).
[28] Ahmad Rafat, "Echelon": EE.UU. y Gran Bretaña espían a Europa. Revista Tiempo, abril de 1.998.
[29] Fabrice Rousselot, Liberation/El Mundo, "Stélites americanos para espiar a las empresas europeas", EL MUNDO, 29 de abril de 1.998.
[30] Fabrice Rousselot, op. cit.
[31] Tomado de Fabrice Rousselot, op. cit.
[32] Fabrice Rousselot, op. cit.
[33] Ahmad Rafat, op. cit.

[34] Ahmad Rafat, op. cit.
[35] Guisnel, Jean, "Guerras en el ciberespacio", citado por Fabrice Rousselot, op. cit.
[36] Toffler, A. y H, "Las guerras del futuro", Edit. Plaza & Janes, Barce-lona 1.994.
[37] Toffler, A. y H., op. cit.
[38] Toffler, A. y H., op. cit.
[39] Toffler, A. y H., op. cit.
[40] Toffler, A. y H., op. cit.
[41] Tse, S, "The Art of the War", The Clarenton Press, Oxford, 1.963.
[42] Toffler, A. y H., op. cit.
[43] Morant Ramón, J.L., y otros, op. cit., pag. 18
[44] Morant Ramón, Edit. Centro de Estudios Ramón Areces, S.A., Madrid, 1.994.
[45] Centro Superior de Información de la Defensa, "Glosario de términos de Criptología", revisión marzo, 1.993.
[46] Pastor Franco, J., op. cit.
[47] Ortega García, R., "Control Interno, auditoria y seguridad informática", Expansión, Madrid, 1.996.
[48] Doyal, L., e gough, y., op. cit., pág. 71.
[49] Neuman, von J., matemático de origen húngaro (1.903-1.957), creó junto con O. Morgenstern, la teoría de los juegos, que se aplica a "juegos" económicos, estratégicos y militares.
[50] Morant Ramón, op. cit., pág. 22.
[51] Merles, M., "Sociología de las relaciones internacionales", Alianza Universidad, 1.984, pág. 113.
[52] Morant Ramón, J.L. op. cit.
[53] Abril, G., "Puertas", Revista de Occidente nº 170-171, julio-agosto 1.995, pág. 87.
[54] Centro Superior de Información de la Defensa, op. cit.
[55] Centro Superior de Información de la Defensa, op. cit.
[56] Morant Ramónb, J.L., y otros, op. cit. pág. 23.
[57] Ortega García, R., op. cit.
[58] Dávara Rodríguez, M.A., "Derecho Informático", Edit. Aranzadi, 1.993, pág. 36.
[59] Centro Superior de Información de la Defensa, op. cit.
[60] Cuevas Calabia, J.L., "La LORTAD y la seguridad de los sistemas automatizados de datos". Actualidad informática Aranzadi, nº 13, pág. 7.
[61] Morant Ramón, J.L., y otros, op. cit. pág. 24.
[62] Centro Superior de Información de la Defensa, op. cit.
[63] Del Peso Navarro, E., y Ramos González, M.A., "Confidencialidad y seguridad de la información: la LORTAD y sus implicaciones socioeconómicas", Ediciones Díaz Santos, 1.994, pág. 17.
[64] Del Peso Navarro, E., op. cit.
[65] Dávara Rodríguez, M.A., "Derecho Informático", Edit. Aranzadi, nota 13, pag. 34.
[66] Morant Ramón, J.L. y otros, op. cit.

[67] Morant Ramón, J.L. y otros, op. cit.
[68] Olivares Salina, I., "Nuevos retos para la seguridad nacional", Revista Española de Defensa, nº 101-102, julio-agosto de 1.996, pag. 58
[69] Herrero y Rodríguez de Miñón, M., "Entre dos siglos: Reflexiones sobre la democracia española", Alianza Editorial, Madrid, 1.996, pág. 18.
[70] Valladao, A.G.A., "Las acciones de policía internacional tienden a sustituir la guerra clásica entre Estado", El Estado del Mundo, 1.998, Edit. AKAL, Madrid, 1.997.
[71] Elzaruro Marquez, F. y Martitegui Susunaga, J., "La crisis Mundial -de la incertidumbre a la esperanza-, Espasa Calpe, Madrid, 1.988, pág., 285-291.
[72] De Asis Roig, R., "Las paradojas de los derechos fundamentales como límites al poder", Edit. DEBATE, mADRID, 1.992, pág. 105.
[73] Pérez Luño, E., "Los derechos fundamentales", Edit. Tecnos, 1.986.
[74] De Asís Roig, R., op. cit., pág. 94.
[75] Peces-Barba, G., "Derecho positivo de los derechos humanos", Edit. Debate, Madrid, 1.987.
[76] De Asís Roig, R., op. cit. pág. 80.
[77] Morant Ramón, J.L., y otros, op. cit. pág. 22.
[78] Del Peso Navarro, E., y Ramos González, M.A., op. cit., pág. 41.
[79] Ortega García, R., op. cit., pág. 172,173 y 174.
[80] Dávara Rodríguez, M.A., op. cit.
[81] Centro Superior de Información de la Defensa, op. cit.

CAPITULO II
CRIPTOLOGÍA

2.1.- CONSIDERACIONES GENERALES.

La Criptología tiene un encanto ligeramente tenebroso; en su desarrollo histórico se combinan, el juego de la inteligencia, la reflexión científica, los problemas de la comunicación lingüística y la transmisión de mensajes. Pero es, ante todo, una disciplina científica de gran actualidad. [1]

La utilización técnica de códigos secretos ha tenido siempre una importancia vital para militares y diplomáticos. La Criptografía fue históricamente una actividad casi exclusiva de la diplomacia y la guerra, por lo que su importante contribución a desarrollos en Estadística y Cálculo se mantuvieron siempre bajo el más riguroso secreto. [2]

En la actualidad su campo de aplicación se ha ampliado considerablemente (expedientes clínicos de hospitales, sistemas de distribución automática de dinero, redes de ordenadores, las líneas telefónicas..., necesitan estar protegidas).

El debate sobre si la criptología es una ciencia o un arte, ha dividido a los criptólogos durante siglos y, hace ya algún tiempo dejó de tener interés, pero, en los diccionarios aún siguen apareciendo referencias considerándola como arte, lo que se puede interpretar como una reafirmación sucesiva en esta idea o, simplemente, una falta de actualización.

Las propias definiciones de *"arte"* y *"ciencia"* pueden darnos la respuesta.

Mientras que arte es la virtud o disposición para hacer algo, ciencia es el "conocimiento cierto de las cosas por sus principios y causas". [3]

Es comprensible que, en determinados momentos históricos no se tuviese un conocimiento cierto de la criptología y, consiguientemente se la pudiera calificar de arte,-y tal vez lo fuese en determinados estadios de desarrollo del conocimiento humano- pero, actualmente, el desarrollo de las distintas disciplinas que intervienen en los principios y causas de la criptología -fundamentalmente las matemáticas- son sobradamente conocidas como para que podamos considerar a la Criptología como ciencia.

Para José Pastor, la Criptografía como arte permaneció desde tiempo inmemorial hasta que en 1.949, Shannon publicó su Teoría de las comunicaciones Secretas.

La Criptografía como ciencia aplicada, hace uso de la matemática pura, Teoría de los Números, Teoría de comunicaciones y de los desarrollos en las ciencias del cálculo, ordenadores e informática.[4] Igualmente incorpora Teoría de la Información y Codificación y Estadística.

La Criptología es en la actualidad objeto de estudio, activo y muy serio, para matemáticos, informáticos, especialistas en estadísticas, ingenieros de telecomunicaciones[5], -y, esperemos que, también, para juristas, sociólogos y politólogos, por su incidencia en la sociedad actual-.

Es una ciencia que tiene sus principios, sus reglas y hasta sus teoremas.

El Glosario de Términos de Criptologia del Centro Superior de Información de la Defensa, dice: "Criptología.- Ciencia que estudia la ocultación, disimulación o cifrado de la información, así como el diseño de sistemas que realicen dichas funciones, e inversamente la obtención de la información protegida. Comprende la cifra y el criptoanálisis"[6].

El principio general más cierto y evidente en criptografía es que es mucho más fácil inventar una escritura o lenguaje secreto, que interpretar con facilidad los documentos escritos conforme al mismo.

Además de criptografía, este sistema de escribir ha recibido los nombres de Criptología, Poligrafía, Esteganografía,[7] Escritura cifrada, etc. Aunque realmente la Esteganografía, cifra encubierta o mensajes disimulados a través de tintas invisibles, micropuntos u otras múltiples e ingeniosas formas, más que criptografía son procedimientos encaminados a ocultar la existencia de un mensaje.

La palabra *"esteganografía"* no aparece en el Diccionario de la Real Academia Española de la Lengua, sin embargo aparece el vocablo *"estenografía"* y lo remite a *"taquigrafía"* que es el arte de escribir tan de prisa como se habla, por medio de ciertos signos y abreviaturas.

La Criptografía consiste principalmente en: 1° Sustituir las letras por cifras árabes, a las que se asigna un orden o valor convencionales; 2°

Sustituir las letras por otras letras, alterando su valor; 3° Sustituir las letras por signos musicales, algebraicos o taquigráficos (esto último es propio y exclusivo de lo que constituye la taquigrafía); 4° Sustituir las letras por otros signos arbitrarios; 5° Sustituir las letras de un idioma por caracteres propios de otro, y 6° Sustituir las letras sencillas por grupos de dos o más.

O bien en alterar el orden de los signos o letras que componen el texto, lo que se conoce como sistema de transposición.

Históricamente el uso de sistemas de transposición vino a proporcionar mejores resultados que el cifrado por simple sustitución, pues aunque el sistema continúa manteniendo la frecuencia de las letras del lenguaje, permitiendo su estudio por métodos estadísticos, destruye las estadísticas de otro orden, como diagramas o bigramas, trigramas, etc.[8]

Esta escritura ha recibido los nombres de escritura cifrada, diplomática[9], en clave[10], etc., por ser usada comúnmente por los gobiernos de las respectivas naciones y sus representantes diplomáticos, [11] con objeto de sustraer los secretos o negociaciones de Estado a la curiosidad de tercero y en tiempo de guerra, muy especialmente, es de uso muy corriente para transmitir órdenes y participar movimientos del enemigo, etc.[12]

El Diccionario de la Real Academia, recoge el término *"criptografía"* como "Arte de enviar mensajes en clave secreta o de un modo enigmático"[13]. El Diccionario Básico Espasa, en su acepción histórica,

añade "Este sistema ha recibido también los nombres de criptología, poligrafía, esteganografía, escritura cifrada y otros...".

Para Andrea Sgarro, criptografía es la disciplina que se ocupa del estudio de los códigos secretos, enseña a diseñar cifrarios que puedan soportar los ataques del criptoanálisis.[14]

Para José Pastor, "el arte de la Criptografía se convirtió en una ciencia, dedicada al estudio de las propiedades de las comunicaciones electrónicas y digitales en un ambiente vulnerable y de desconfianza mutua entre los comunicantes".[15]

No hay que confundir Criptología con codificación. La codificación que es convertir un texto claro en su equivalente pero utilizando un código público,[16] normalmente para obtener una mejora técnica en la calidad de comunicación.

Etimológicamente, la palabra criptografía procede del griego *"kriptos"*, oculto y *"graphos"* escritura, lo que nos permitiría poder definir a la criptografía como escritura oculta.

La palabra castellana "criptografía" se corresponde con las expresión francesa "*cryptographie*," las expresiones italianas, "*crittografía*", "*criptografía*", la expresión inglesa, "*cryptography*", y las expresiones alemanas *"chisffrierkunst"* y *"kryptographie".[17]*

Sin embargo, en ninguno de estos diccionarios aparece la palabra "criptología",que se podría definir como tratado de lo oculto y que, por el

contrario, sí está recogida en diccionarios o glosarios especializados.

Para Ribagorda, Criptología es la "ciencia que estudia los principios, métodos y medios de cifrado y descifrado de la información. Comprende dos ramas principales: Criptografía y Criptoanálisis"[18]

Para el Centro Superior de Información de la Defensa, Criptología es la "ciencia que estudia la ocultación, disimulación o cifrado de la información, así como el diseño de sistemas que realicen dichas funciones, e inversamente la obtención de la información protegida. Comprende la cifra y el criptoanálisis".[19]

En el Diccionario Técnico Militar, inglés-español, español-inglés, de Antonio Urquía, el término castellano "criptología" se corresponde con el inglés "*cryptology*".[20]

El término *"Criptología"*, tiene una mayor amplitud conceptual al referirse a todo lo relativo al tratamiento de lo oculto y, dentro de ello, como subconceptos, estarían la *"criptografía"[21]* referida al cifrado de la escritura , la *"criptofonía"[22]*, referida al cifrado del sonido y, en abierta contraposición a ambas, pero derivada del mismo tronco común, el "criptoanálisis"[23], como 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.

Para Ribagorda el criptoanálisis es el análisis de un sistema criptográfico, sus entradas y salidas, o ambas, para obtener variables o datos

sensibles, incluyendo el texto en claro (ISO 7498-2).[24]

El resultado positivo del criptoanálisis es denominado con el término *"descriptación"[25]*, "anglicismo de uso infrecuente, con el que se designa las transformaciones de descifrado de un texto sin el conocimiento de la correspondiente clave. Es por tanto la tarea propia del criptoanalista" [26], la descriptación se orienta a la violación de la protección criptológica de la información por procedimientos científicos, mediante el descubrimiento de la clave y, a través de ella, el texto original.

Los términos criptología y criptografía son utilizados generalmente como sinónimos, tal vez porque el desarrollo de esta ciencia se alcanzó coincidiendo con sus aplicaciones en el campo de la escritura, y el uso reiterado, ha asignado a la palabra criptografía un contenido conceptual que rebasa su alcance semántico.[27]

En la práctica habitual casi siempre se utiliza el término criptografía donde según Sgarro sería más correcto decir criptología: "este error es deplorable, pero es una costumbre demasiado arraigada para que tengamos esperanza de eliminarla".[28]

No obstante, la norma ISO 7492-2 define a la Criptografía como "Disciplina que estudia los principios, métodos y medios de transformar los datos, con objeto de ocultar la información contenida en los mismos, detectar su modificación no autorizada y/o prevenir su uso no permitido". Y Ribagorda Garnacho, además de aceptar la definición de ISO, considera a la

Criptografía como disciplina que estudia los principios, métodos y medios de transformar los datos para ocultar la información contenida en ellos, garantizar su integridad, establecer su autenticidad y prevenir su repudio. [29]

Aunque no queremos extendernos más en precisiones terminológicas, tal vez convenga señalar el inadecuado uso que, a nuestro juicio, se hace, de la palabra "criptógrafo"[30] para designar al especialista en criptografía o criptología, en lugar de "criptólogo".

No obstante, la utilización de la expresión "criptógrafo" como experto en criptografía ha venido siendo usada generalmente en épocas pasadas y coincidiendo con que la criptografía era la única expresión de la criptología.

Tal vez, en épocas de la criptografía manual, que ha sido durante toda la historia hasta el siglo XVIII, el proceso criptográfico descansaba en la persona y, en muchos casos, tal vez hubiera una coincidencia entre el criptólogo como científico y el criptógrafo como realizador del proceso de cifrado.

Estas dos funciones se separan nítidamente, cuando aparecen las máquinas de cifra, época en la que, obviamente persiste la función del criptólogo como científico pero que, los procesos criptográficos son realizados por máquinas y, la aportación humana es mínima.

Algo parecido puede haber ocurrido, más recientemente, con la palabra "cifrador", que es referida tanto a un equipo o parte concreta de un equipo que realiza las funciones de cifrado y a la personas que interviene en dicho proceso.

En la situación actual y, por la evolución de los conceptos, tal vez sea más adecuado utilizar la expresión *"criptógrafo"* para referirse al "equipo de cifra que se utiliza para el cifrado de texto", *"cifrador"*, como equipo o parte del equipo que realiza funciones de cifrado, *"criptólogo"* para referirse al especialista en criptología, y *"operador de cifra"* para denominar a la persona que utiliza los equipos de cifrar.

En España el título o diploma acreditativo de la condición de *"Especialista Criptólogo"*, hasta ahora, lo expide el Centro Superior de Información de la Defensa, tras la superación del Curso de Especialidades Criptológicas. No obstante existen diversas iniciativas académicas encaminadas a establecer estudios de Criptología en la Universidad.[31]

Ribagorda incorpora una definición nítida en su Glosario al referirse al criptógrafo como "equipo criptográfico usado para cifrar y descifrar texto".[32]

De igual modo es frecuente, la utilización del verbo *"encriptar"* tal vez por una inadecuada traducción del inglés *"to encrypt"*, cuando en castellano existe el vocablo *"cifrar"*, de larga tradición, que expresa adecuadamente el concepto que se pretende transmitir.

La acepción primera de la palabra *"cifrar"*, en el Diccionario de la Real Academia Española de la Lengua es "Escribir en cifra". Y la palabra "cifra" en su acepción segunda es recogida por el mismo Diccionario como "Escritura en que se usan signos, guarismos o letras convencionales, y que solo puede comprenderse conociendo la clave.[33]

El verbo *"cifrar"* para el Centro Superior de Información de la Defensa es el hecho de transformar una información (texto claro) en otra ininteligible (texto cifrado) según un procedimiento y usando una clave determinados, que pretende que sólo quien conozca dichos procedimiento y clave pueda acceder a la información original. Es un mecanismo de seguridad.[34]

Ribagorda, en su Glosario, introduce el término "Cifra o cifrado" considerandolo como el algoritmo que produce un texto cifrado mediante técnicas criptográficas (ISO 7498-2). Lo considera término sinónimo al de algoritmo de cifra.

Asimismo, considera estos términos como el resultado de aplicar un algoritmo de cifra un texto en claro. En este sentido es sinónimo de texto cifrado.[35]

F.L. Bauer, en su reciente obra "Decrypted Secrets", recoge que el término *"cryptología"* fué usado, como *"cryptographía"*, por Wilkins en 1.641, como sinónimo de secreto o sigilo en el discurso. En 1.645, el

término *"cryptology"* fué acuñado por James Howell, quien escribió *"cryto-logy, or epistolizing in a clandestine way, is very ancient".[36]*

El uso de las palabras *"cryptography"*, *"cryptographie"*, *"critto-grafía"*, *"Kryptographie"* han sido utilizadas hasta muy recientemente incluso cuando el concepto incluía al criptoanálisis.

Dentro de los títulos de libro *"Cryptologue"* fué usado por Yves Gyldén en 1.932 y *"Cryptologist"* fué usado por William F. Friedman en 1.961; *"cryptology"* aparece en el título de un artículo de David Kahn en 1.963; fué usado internamente por Friedman y Lambros D. Callimahos en los años cincuenta. Con "The Codebreakers" de Kahn, en 1.967, la palabra *"criptología"* quedó firmemente establecida para referirse al concepto general que incluye tanto criptografía como criptoanálisis y actualmente está muy aceptada.

La Criptología se podría definir como la ciencia que estudia los principios, medios, métodos, sistemas, procedimientos y algoritmos de cifrado y descifrado de la información y las comunicaciones, su clasifica-ción en función de los riesgos, análisis y evaluación.

2.2.- EVOLUCIÓN HISTÓRICA.

La Criptología es usada desde la más remota antigüedad. Los indios, chinos, persas, asirios, babilonios y egipcios[37], poseían ya signos convencionales equivalentes a las letras de sus alfabetos, con las que comunicaban órdenes secretas a sus emisarios, especialmente en tiempo de guerra.

Bajo el título "Los albores de la criptología", José Luis Ocasar y Vigil de Quiñones dice, que ya hace casi 4.000 años, en una ciudad llamada Menet Khufu a orillas del Nilo, un escriba trazó los jeroglíficos que contaban la historia de la vida de su señor y, al hacerlo, abrió la historia de la criptología.

En un principio fue más un juego que otra cosa, pretendía retrasar la comprensión durante el menor tiempo posible y no el mayor como es habitual. La adición de la reserva a las transformaciones produce la criptografía.

Señala J.L. Ocasar, recogiendo la opinión de David Kahn, corroborada por Eduardo Alfonso, que la criptografía no estaba destinada en sus orígenes a encubrir ningún secreto, sino que entrañaba un "juego del espíritu" que hace imposible el desciframiento de ciertas inscripciones de fondo completamente banal.

Se llegaron a usar medios muy curiosos para hacer llegar mensajes y noticias de un campamento a otro.

Herodoto, autor griego llamado "el padre de la Historia", en su obra "Historias", hace referencia a algunos procedimientos utilizados para enviar mensajes secretos. Se refiere a la introducción de la carta en el vientre de una liebre, que portaba un cazador entre varias piezas muertas; o grabar el texto en tabletas, que luego se recubrían con cera para ocultarlo.[38]

Eneas, el Táctico, autor griego del siglo IV a. de C. escribió una obra titulada "Comentarios sobre la defensa de las plazas". Uno de los capítulos se dedica a los sistemas de comunicaciones secretas, y llega a describir hasta veinticinco procedimientos diferentes: tintas simpáticas -zumo de limón, cebolla u otros vegetales, leche cruda, orín, saliva, agua de almidón, etc.- que se revelaban al ser expuestas a la acción del calor; colocación de piedras, troncos u otros objetos en posiciones convenidas; humos, escritura sobre la piel humana...

Temístocles, que en el año 471 a. de C. fue desterrado, para mantenerse informado utilizó los medios más imaginativos. Uno de ellos consistía en afeitar la cabeza de un esclavo que ejercía las funciones de mensajero. Se escribía el mensaje sobre el cuero cabelludo del mismo, con caracteres indelebles, y, una vez crecido de nuevo el pelo a dicho esclavo, era mandado al campamento a cumplir su misión. Si lograba llegar a él se le hacía afeitar por segunda vez al esclavo y así leía sin dificultad el mensaje

el caudillo a quien iba destinado, sistema en verdad poco recomendable por su falta de rapidez.[39]

El sistema se puso de moda entre los griegos pero con algunas variantes: a) En lugar de escribir con tinta se tatuaba el mensaje. b) Como, una vez leído, no podría destruirse el texto, se mataba al esclavo.

Quizás el primer criptograma de que se ha ocupado la Historia sea el que apareció milagrosamente escrito en la pared de la estancia donde Baltasar, último rey de Babilonia, celebraba su famosa cena.

La Biblia, en el Antiguo Testamento (Libro de Daniel, cap. 12, vers. 5) relata el hecho.

"Dió el rey Baltasar un gran banquete a mil de los grandes de su corte y cada uno bebió según su edad. Estando, pues, él ya lleno de vino, mandó traer los vasos de oro y plata que su padre, Nabucodonosor, se había llevado del templo que hubo en Jerusalén, para que bebiesen en ellos el rey y sus grandes, y sus mujeres y sus concubinas. Trajeron, pues, los vasos de oro y plata, transportados del templo que hubo en Jerusalén, y bebieron en ellos el rey y sus grandes, y sus mujeres y sus concubinas. Bebían el vino y celebraban a sus dioses de oro y plata, de bronce y de hierro, de madera y de piedra.

En la hora misma, aparecieron unos dedos, como de mano de hombre, que escribían enfrente del candelero, sobre la cal de la pared de aquel regio salón; y el rey estaba observando los dedos de la mano que escribía. Mudósele al instante al rey el color del rostro, llenábanle de turbación los pensamientos que le venían, y se le desencajaban las junturas de los riñones y batíanse una contra otra sus rodillas".

Los misteriosos dedos escribieron tres únicas palabras: *MANE, TECEL, FARES.* Baltasar aterrorizado, mandó llamar a los magos, caldeos y adivinos, para que le interpretasen el turbador enigma; ninguno supo hacerlo. Baltasar requirió los servicios de Daniel, ofreciéndole el título de tercer

gobernador del reino si acertaba a descifrar el criptograma. Daniel, tras declinar la oferta y censurar al monarca, explicó el significado de los misteriosos vocablos. *MANE*: Ha numerado Dios los días de tu reinado y le ha dado fin. *TECEL*: Has sido pesado en la balanza y has sido hallado falto. *FARES*: Dividido ha sido tu reino y se ha dado a los medos y a los persas.

Aquella misma noche murió asesinado Baltasar y al poco cae Babilonia, la conquista de la ciudad se llevó a cabo sin resistencia , por traición de los sacerdotes, que abrieron las puertas al general del ejercito medo-persa.

Según el Padre Petisco, S.J., el verbo caldeo *minah* significa numerar, el verbo *thecel* significa pesar y *phares* dividir.[40]

En 1.997 se ha publicado en Francia un libro bajo el título *"La Biblia: código secreto"*, editada por Laffont y cuyo autor es Michael Drosmin, periodista norteamericano que recoge los trabajos del científico judio Eliyahu Rips, -tras someterlos al análisis de los mejores especialistas de calculo de probabilidades y física cuántica- en los que llega a la conclusión de la existencia de un código secreto en los textos bíblicos, mediante el que debajo de la Biblia se puede encontrar otra Biblia.[41]

El código de la Biblia fue descubierto en el texto hebreo original del Antiguo Testamento, que es la primera versión escrita del libro sagrado.

Aunque la información de la Biblia va dirigida a todos, el código solo existe en hebreo, ya que este es el idioma original de la Biblia.

El rabino H.M.D. Wissmandel, hace más de cincuenta años, descubrió que si se saltaba cincuenta letras y luego otras cincuenta y otras cincuenta más podía leer la palabra *"Torá"* desde el principio del libro del Génesis. Y que lo mismo ocurría con el libro del Éxodo, en el de los Números y en el Deuteronomio.

"El análisis randomnizado señala la existencia de información oculta en el texto del Génesis, imbricada en forma de secuencias equidistantes de letras. Su nivel de significancia es del 99,998%".[42]

La expresión "randomnizado" tiene su origen en RAM, siglas que se corresponden con Random Acces Memory, o memoria de acceso aleatorio.[43]

Harold Gans, criptoanalista de la Agencia Nacional de Seguridad norteamericana, investigó el hecho el hecho y lo confirmó: en la Biblia había información acerca delpasado y el futuro codificada de manera tal que no existía posibilidad matemática alguna de que fuera casual; además, la información no aparecía en ningún otro texto.

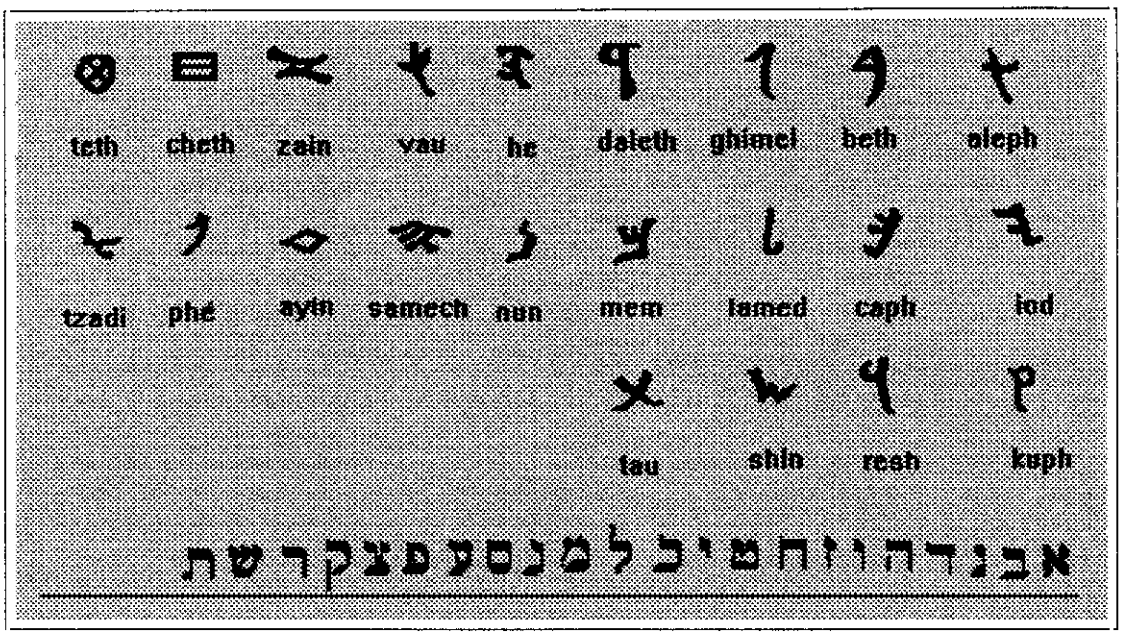
La Biblia tiene la forma de un gigantesco crucigrama. Está codificada de principio a fin con palabras que, al conectar entre sí, revelan una historia oculta.[44]

Isaac Newton, primer científico moderno, y hombre que formuló los principios mecánicos de nuestro sistema solar y descubrió la fuerza de la gravedad, estaba convencido de que la Biblia ocultaba un código capaz de

Alfabeto Hebráico Arcaico

con el que se escribió el Génesis

http://www.eon.com.br/alfabeto.htm



revelar el futuro. Aprendió hebreo y dedicó la mitad de su vida a buscarlo. [45]

Según John Maynard Keynes, Newton estaba convencido de que la Bibliba y el universo entero eran un "criptograma pergeñado por el Todopoderoso", y estaba deseoso de "leer el acertijo de la mente divina, el acertijo de los acontecimientos pasados y futuros que la divinidad había preestablecidos".[46]

Newton murió sin encontrar el código. Rips lo ha logrado. La diferencia estaría en que Newton no disponía de una herramienta esencial: el ordenador.

El código tendría una especie de protección temporal, un sello inviolable, salvo para los ordenadores.[47]

El experimento original probatorio de la existencia del código de la Biblia se publicó en *Satistical Science*, revista del Institute of Mathematical Statistics de Estados Unidos, volumen 9, número 3, agosto de 1.994, pp. 429-438.

Desde la publicación de este trabajo firmado por Rips-Witztum-Rosenberg, hace más de tres años, nadie ha enviado refutación alguna a la revista matemática.[48]

2.2.1.- Sistemas criptográficos.

A lo largo de la historia han sido muchos los sistemas criptográficos empleados. En este trabajo se pretende tan sólo dar una visión general que permita ver y dimensionar la evolución de la Criptología a lo largo de algo más de 2.000 años de historia, y conocer el alcance de los sistemas criptográficos presentes y futuros, lo que consideramos un presupuesto básico para abordar los aspectos jurídicos de su aplicación, que es el objeto de esta tesis.

a) El "Scytalo Lacedemonio".

El historiador Plutarco, contemporáneo de Suetonio, en "Vida de hombres ilustre:Lisandro", describe el primer sistema de transposición conocido, llamado "scytalo lacedemonio", que fue inventado y utilizado por los griegos de Esparta y se podría considerar como la primera máquina de cifrar. Se remonta al siglo V a. de C. y fue empleado por el general Lisandro en la guerra entre Atenas y Esparta.

Cuando un general partía para una expedición de tierra o de mar, los "éforos" (gobernantes), toman dos bastones cilindricos, perfectamente iguales en longitud y grosor, de manera que se correspondan exactamente el uno con el otro en todas las dimensiones. Guardan ellos uno de estos bastones y dan el otro al "estratega" (general): llaman a estos bastones *"scytalos"*.

Cuando quieren enviar al general algún secreto de importancia, cortan una banda de pergamino, larga y estrecha como una correa, y la

enrollan alrededor del *"scytalo"* que está en su poder, sin dejar el menor intervalo entre los bordes de la banda, de tal forma que el pergamino cubra enteramente la superficie del bastón. Sobre este pergamino así arrollado alrededor del *"scytalo"* escriben lo que desean; y cuando lo han escrito desenrrollan la banda y la envían al general sin el bastón. Las letras desordenadas y esparcidas, no presentan ninguna concordancia, y resulta imposible su lectura, pero con el *"scytalo"* que tiene en su poder, enrolla a su alrededor la banda de pergamino, devolviendo las letras al orden en que han sido escritas, y puede enterarse así del mensaje.

En la práctica no parece un sistema infalible, bastaba con tener un bastón igual.

La importancia de no soltar en ningún momento el bastón, producto de la necesidad y la prudencia, se instala como costumbre y, al parecer, así nació el actual bastón de mando militar, convirtiendo en un simple símbolo jerárquico lo que en su origen fue una útil máquina de cifrar.

b) Sistema de Julio César.

Según cuenta Suetonio (siglos I y II d. C.), en la "Vida de doce césares: César, Octavio", y Aulu Gelle, "Noches áticas", el célebre triunvirato usó a menudo en la correspondencia que sostenía con Oppio, Balbo, Cornelio y Cicerón un sistema de cifrado, basado en la sustitución del "alfabeto Julio César", del que recibe su nombre, por ser Cayo Julio César su inventor.[49]

El sistema consistía en sustituir la primera letra del alfabeto, A, por la cuarta, D, y así sucesivamente con todas las demás.

También Augusto, al parecer, utilizaba un sistema muy similar solo que ponía una B en lugar de una A, una C en lugar de una B, y así sucesivamente con todas las letras restantes.

El cifrado de Julio César se basa en la sustitución de letras, donde el alfabeto normal se sustituye por el alfabeto cifrante.

CIFRADO
DE UN TEXTO POR EL SISTEMA
DE
"JULIO CESAR"

1.- Alfabetos:

Claro	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cifrado	DEFGHIJKLMNOPQRSTUVWXYZABC

2.- Cifrado.- Cada letra del texto claro que compone el mensaje, tomadas en el alfabeto de textos claros, se sustituye por las letras que ocupan su lugar en el alfabeto para textos cifrados, que se haya desplazado con respecto al primero, de forma que la A del claro, se corresponde con la D del cifrado.

3.- Ejemplo:

Texto claro:	**A M A N E C E R**	
Texto cifrado:	**D P D Q H F H U**	*(criptograma)*

---

c) EL *"ATBASH"* HEBREO.

Otro sistema de cifrado, en este caso, basado en el alfabeto hebreo, es el *"atbash"* hebreo.

Se escribe una primera línea comenzando desde la izquierda, avanzando hacia la derecha y, en una segunda línea, debajo de la primera, se escriben las letras que faltaban, en este caso, de derecha a izquierda.

En el *"atbash"*, las letras del mensaje de origen se sustituyen una por una de forma que si la letra original se encuentra en la línea superior, se sustituye por la letra correspondiente en la línea inferior, y a la inversa.

El *"atbasch"* aparece utilizado en la Biblia y, concretamente, en el libro de Jeremías

Los sistemas de cifra a los que hemos hecho referencia, ilustran los dos principios esenciales en que se basa la criptografía: la sustitución y la transposición (el sistema de Julio Cesar y el *"atbasch"* son de sustitución y el *"scytalo"* es de transposición).

En los sistemas descritos y, sobre todo, en la época histórica en que se aplicaron, su uso gozó de lo que se denomina "secreto accidental", derivado del empleo de la lengua latina, la griega o el hebreo y, por supuesto, de las condiciones de alfabetización.

En condiciones de alfabetización reducida, cualquier escritura es, por si misma, secreta, e incluso mágica.

El secreto que perdura es el conseguido, de forma intencionada, por el empleo de un código secreto específicamente estudiado.[50]

D) FUGA DE VOCALES.

Durante la Edad Media el sistema criptográfico más en boga, consistía en lo que hoy se conoce con el nombre de fuga de vocales, las que se sustituían por uno o más puntos, hasta cinco, según su orden. A veces las vocales eran sustituidas también por consonantes arbitrarias. Rabano Mauro ha dado sobre este particular muy curiosas noticias paleográficas. Los copistas de códices, muchas veces escondían sus nombres usando estos procedimientos. Otros acudían a anagramas, o bien, a la inversión o alteración de las letras de sus nombres.

La República veneciana empleó la criptografía desde el siglo XIII. En un registro del Consejo de los Diez (1.290-91), se hallan mezclados con el texto latino varios caracteres griegos y hebraicos para expresar las palabras más importantes. Desde mediados del siglos XIV, los criptogramas (o frases de cifra o clave), aparecen en la correspondencia diplomática de la misma república y en las instrucciones que en 27 de septiembre de 1.350 se da a los embajadores enviados al rey de Hungría, se les hace presente que cuando escriban a su gobierno sustituyan la palabra Dux por una B, y el rey por una D. En 1.358 se ordena a otro embajador veneciano que pasa a Alemania, que llame al duque de Austria Meser Antonio, al emperador, Meser Nicoleto y al ducado de Prione, Módena.

En la República de Venecia existió un negociado en la Cancillería Secreta dedicado a la materia y puesto bajo el mandato e inspección directa del propio *"Consejo de los Diez"*. Sus especialistas, rigurosamente seleccionados y preparados, recibían el título de "Secretarios Diputados a las Cifras", y alguno de ellos fue extraordinario criptólogo, como Pietro Partenio, y otros como Agostino Armadi.

El Consejo ponía especial cuidado en renovar periódicamente la cifra, convocando concursos entre los "secretarios" para la construcción de nuevas claves, de las cuales era elegida y puesta en uso la que, en opinión de tres de los "Diez" -expresamente designados para ello, reunía mejores condiciones de empleo y seguridad.[51]

Los primeros tratados de criptografía datan de fines del siglo XV. Juan Tritemio, abad de San Jaime en Wurzburgo, escribió dos notables obras sobre escritura secreta, la una *"Libri Polygraphiae VI"* (Openheim, 1518) y la otra *"Steganographia, hoc est, ars per occultam scripturam animi sui voluntatem absentibus aperiendi certa"*.

En Nápoles, J.B. Porta, en la segunda mitad del siglo XVI, publicó otro tratado con el título "De furtivis litterarum notis vulgo de Ziferis".

María Remedios Moralejo Alvarez, Directora de la biblioteca universitaria de Zaragoza en la Presentación del facsímil de la edición de "De occultis literarum notis" de 1.593, editada por la Cátedra de

Criptografía y la biblioteca General de la Universidad de Zaragoza para Eurocrypt'96, dice:

"Graesse y Brunet mencionan una edición anterior en Nápoles, 1.563, por Jo. María Scotus, que es realmente la aparecida en 4° bajo el título *"De furtivis literarum notis vulgo de Ziferis libri* IIII" en esa misma ciudad y fecha, y a cargo de Scotus.

En 1.602 y también en Nápoles "apud Joannem Baptistam Subtilem", se publicaba otra edición *"De furtivis literarum notis vulgo de Ziferis Libri Quinque. Altero libro superaucti, et quam plurimis in locis locupletati"*, ahora en cinco libros e in folio; y al año siguiente aparecería en Estrasburgo, de nuevo a costa de Lazarus Zetner y con su marca tipográfica, la segunda edición de *"De occultis literarum notis seu artis animi occulte aliis significandi, aut ab aliis significata expiscandi enodandique. Libri* IV".

Duchesne, biógrafo de Porta, además de las ediciones citadas, menciona dos ediciones en 1.591, una en Londres en 4° y otra en Nápoles, así como otra en Estrasburgo en 1.606, reseñadas también por el P. Nicéron; pero , al igual que Graesse y Brunet, no hace distinción entre *"De furtivis literarun notis* y *De occultis literarum notis"*, considerándolas diferentes ediciones de la misma obra.

Tampoco parece haberla hecho el propio Porta, que titula el Capítulo I de nuestra edición de *De occultis literarum notis* "Quid sint furtivis literarum notae", y lo inicia diciendo: "Occultas seu furtivas notas..." Los

dos títulos van alternando en las sucesivas ediciones sin que uno u otro sea exclusivo de las primeras o de las últimas como afirmaba la Biographie Universelle.

En efecto, no solo la temática es igual bajo ambos, sino también la distribución de los libros y los títulos de los diversos capítulos; los índices coincidentes de todas ellas lo confirman, así como los grabados que, con ligeras diferencias, son los mismos.[52]

En Francia sobresalió Blas de Vigenère, muerto en 1.596, que tuvo a su cargo varias comisiones diplomáticas. El duque Augusto de Brunswick-Luneburgo, con el seudónimo de Selenus, compuso una extensa obra de criptografía, tomada en su mayor parte de la de Tritemio.

En España el primer estudio completo en esta materia es el de Don Cristóbal Rodríguez, Biblioteca universal de la poligrafía española, publicada en Madrid en 1.738, con un extenso y erudito prólogo de Don Blás Nasarre. En la obra del P. Andrés Marcos Burriel, Paleografía Española (Madrid, 1.758), también se hallan noticias muy cualificadas acerca de esta materia.

Rodríguez Prieto[53], en su obra, señala que se poseen testimonios como los de Muñoz y Rivero, que en su trabajo sobre Paleografía Visigoda habla de correspondencia cifrada y presenta como testimonio un documento atribuido a San Jerónimo.

En los archivos generales aparecen documentos desde la época de los Reyes Católicos, con información de Estado y de particulares. La actividad criptoanalítica y la interceptación de mensajes fue muy intensa. La Reina Isabel de Inglaterra consiguió estar informada de todo cuanto trataba el Conde de Olivares, embajador español en Roma.

Asimismo fueron descifradas correspondencias de numerosas personas, como la del gobernador de los Países Bajos, Luis de Requessens.

En el periodo de los siglos XV a XVIII, existen más de 400 claves distintas usadas . De ellas las más importantes fueron las utilizadas por Felipe II, Don Juan de Austria y el Duque de Alba.

Uno de los primeros actos del gobierno de Felipe II, fue variar las claves usadas desde Carlos V, por resultar inseguras.

Después del reinado de Felipe II, hubo una decadencia en el uso de las claves.

Como curiosidad, se puede señalar los códigos teresianos, usados por Santa Teresa en su correspondencia durante una de sus épocas difíciles. Los describe Carlos A. Moreyra en su obra "Los criptogramas de Santa Teresa"[54]. Estos códigos son una variante del sistema de cifrado utilizado en el periodo comprendido entre los siglos XV y XVIII, constituido por el empleo de palabras con un significado totalmente distinto al que realmente tienen en el mensaje en claro.

E) PROCEDIMIENTO DE ROTACIÓN.

Estos sistemas, parten de la base de la cifra empleada por Julio César, pero eliminan la limitación que los desplazamientos sean sólo en tres posiciones, pudiendo hacerlo en cualquier de las posiciones de las letras del alfabeto.

Los alfabetos se podían plasmar en dos discos concéntricos que giraban de forma independiente.

León Battista Alberti (1.402-1.472), Secretario de Claves de la Curia Vaticana y denominado "padre de la criptografía occidental", describe estos discos en su tratado *"Modus scribendi in ziferas"*.

En estos sistemas, las letras conservan el orden natural, y, la única diferencia está en la posición en que empiezan, pero cabe la posibilidad de alfabetos cifrantes totalmente desordenados, "caóticos", que vienen a proporcionar un sistema de cifrado de rotación con todas las permutaciones del alfabeto.

Las permutaciones de un alfabeto de 26 letras son 26! (26 factorial) = 26 x 25 x 24 x 23 x 22 x 21 x 20 x 19 x 18 x 17 x 16 x 15 x 14 x 13 x 12 x 11 x 10 x 9 x 8 x 7 x 6 x 5 x 4 x 3 x 2= ***40.329.146*** .[55]

F) SISTEMA DE CIFRADO HOMOFÓNICO.

El primer cifrado homofónico del que se tiene noticia se utilizó en 1.401, en la correspondencia cruzada entre la corte de Mantua y Simeone da Crema.

Si se utiliza un sistema de cifra homofónico, el alfabeto en el que se escriben los criptogramas tiene que ser más rico que el de las 26 letras en que están escritos los mensajes originales.

Se pueden aumentar el número de letras por varios procedimientos, duplicando las letras más frecuentes en el idioma utilizado, añadiendo signos, etc., con lo cual la frecuencia del idioma original se desvirtúa.

En este esquema, sería ideal que las frecuencias de las letras que componen el texto cifrado fueran todas, más o menos parecidas.

En criptografía todo lo previsible es peligroso, pero tampoco, por evitar el más mínimo peligro se puede llegar al extremo de elaborar sistemas demasiado complejos que, por los errores cometidos en su uso se comprometa la seguridad.

g) Nomenclator.

La historia de la criptografía se puede dividir, básicamente, en tres periodos: periodo de lápiz y papel, periodo del telégrafo y periodo de los ordenadores.

Desde el siglo XVI hasta la invención del telégrafo a mitad del siglo XIX, el sistema de cifra más utilizado en la correspondencia diplomática fue un sistema mixto denominado nomenclator.

Su núcleo está formado por un sistema en el que se utilizan letras de fantasía en lugar de las corrientes.

Otro elemento típico del nomenclator es la utilización de un código de símbolos especiales que se correspondían con términos o expresiones de uso frecuente.

H) Sistema Vigenère.

Para impedir que las letras del criptograma hereden la frecuencia de las letras correspondientes al mensaje original, entre otros medios, se utilizan los sistemas polialfabéticos y la alteración del empleo de las sustituciones-clave en el transcurso de la operación de cifrado, de forma que la misma letra de origen se transforme en distintas letras cifradas, en función de la posición que ocupan dentro del mensaje.

Un ejemplo de cifrado de sustitución tipo polialfabético es el sistema de Vigenère[56].

Blaise de Vigenère (1.523-1.596), diplomático francés, fue autor del famoso "Traicté des chiffres" (1.586), considerado como una "summa" de los conocimientos criptográficos de la época.

Una variante del sistema Vigenere, aunque muy débil, pero de gran importancia histórica fue el código secreto propuesto por Hohannes Trithemius, abad benedictino que nació en 1.462 en Tritterheim, pequeña ciudad alemana. Fue el primero en utilizar el cuadrado de Vigenère, en su tratado "Polygraphiae libri sex".

El almirante Francis Beaufort, conocido por la escala de vientos de su mismo nombre (escala Beaufort), desarrolla dos sistemas basados,

también, en el cuadro Vigenère, el primero denominado "auténtico" que ya fue descrito por Giovanni Sestri en 1.710 y, el segundo, denominado Beaufort variante.

En 1.553, Giovanni Battista Bellaso, publicó "El auténtico modo para escribir en cifra".

Los nombres de Bellaso y Vigenère están unidos al sistema de cifra de autoclave.

Partiendo de la base de un criptograma elaborado con un sistema Vigenère, se defiende mejor del criptoanálisis cuanto más larga es la palabra clave, Bellaso y Vigenère, concibieron la solución de construir una clave de la misma extensión que el mensaje.

En el siglo XVI, el italiano Girolamo Cardano, incorpora a la criptografía sistemas basados en rejillas, en cuya base estaba el sistema de transposición -que, a diferencia del de sustitución- consiste en cambiar el orden de las letras del mensaje.

El siglo XVIII no fue una época de grandes avances criptográficos. Incluso los códigos secretos de Napoleón se conformaban con un nomenclator anticuado para su época.

La aparición del telégrafo cambiará el curso de la historia de la criptografía.

El novelista francés, Julio Verne (1.828-1.905), que sentía gran pasión por la criptografía, la utilizó en tres de sus novelas: "Viaje al centro de la tierra", "Mathias Sandorf" y "La jangada".

En la primera parte de Mathias Sandorf, se centra en la criptografía y describe una acción situada a mediados del siglo XIX en Trieste, durante una conspiración en la que se utilización transposiciones de letras y se aplican unas rejillas que, al situarlas sobre el mensaje, solo permite leer el texto deseado.

Las rejillas se perfeccionan a lo que contribuye el coronel Fleissner.

Eduard von Fleissner von Wostrowitz (1.825-1.888), era un excelente criptólogo, que estudió a fondo los sistemas de rejilla, e inventó uno llamado Patronen-Gehemschrift -pero no fue el inventor de la rejilla-.

Durante la Primera Guerra Mundial, el italiano Luigi Sacco, introdujo unos sistemas muy sofisticados "con rejilla indefinida", a pesar de todo ello, el carácter de inatacable que le atribuyó Verne a estos sistemas, es exagerado.

El sistema de rejillas exige un secreto absoluto y un gran cuidado para evitar que la clave caiga en manos ajenas.

El cuadrado de Vigenère

A	B	C	D	E	F	G	H	I	J	K	L	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	**G**	H	I	J	K	L	M	N
P	Q	R	**S**	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Ejemplo: La clave consiste en una palabra secreta, por ejemplo PALOMA. El mensaje que hay que cifrar podría ser la frase DIARIO DE SESIONES. Debajo de este ponemos la palabra clave y la repetimos tantas veces como sea preciso. Cada letra del mensaje de origen posee su propia letra clave. A la D de DIARIO le corresponde una P, a la I le corresponde una A... a la S final de SESIONES, le corresponde una O. Para cifrar se busca la letra del mensaje en la primera línea del cuadro de Vigenere y la letra de la clave en la primera columna; estas definen respectivamente, una columna y una línea: la letra del mensaje de origen se sustituye por la letra que se encuentra en el punto en que coinciden la columna y la línea. De esta forma la D del mensaje de origen se sustituye por la S. En este caso, el mensaje claro, la clave y el criptograma es:

D I A R I O D E S E S I O N E S texto en claro

P A L O M A P A L O M A P A L O clave

S A L F U A S A D S E A D A P G *texto cifrado (criptograma)*

i) Criptografía estratégica.

El riesgo de que ciertos sistemas comprometan su seguridad por la pérdida o robo del mecanismo de cifrado, es el punto de partida del estudio y desarrollo de uno de los principios más importantes de la criptografía estratégica.

La finalidad de la criptografía estratégica consiste en garantizar el secreto de los mensajes cifrados sin límite en el tiempo, aún ante criptoanálisis efectuado con medios especializados, a diferencia de la criptografía táctica, que se conforma con garantizar el secreto durante un periodo de tiempo limitado, se supone que suficiente, para cubrir los hechos que está protegiendo.[57]

Auguste Kerckhoffs von Nieuwenhof (1.835-1.903), nacido en Holanda, formado en Alemania y naturalizado francés, es el autor de "La cryptographie Militaire", que fue publicada en 1.883.

Es también autor de un tratado de Volapuk, una lengua artificial del tipo del esperanto, que tuvo algún éxito en su momento.

La obra de Kerckhoffs es la piedra angular de la criptografía militar en la denominada "época del telégrafo".

Kerckhoffs establece claramente las diferencias entre los sistemas de tipo táctico y los de tipo estratégico, cuando afirma que hay que distinguir cuidadosamente entre un sistema de cifra pensando para la protección temporal del intercambio de cartas entre personas individuales y un

sistema criptográfico destinado, por el contrario, a proteger la correspondencia de jefes del ejército durante un tiempo ilimitado.

En la actualidad, al pasar del telégrafo a los ordenadores y el desarrollo e implantación de los PCs, la criptografía estratégica ha desbordado el ámbito estrictamente militar, penetrando en los centros de cálculo, donde se custodian muchos datos reservados y secretos.

En opinión de Kerckhoffs -compartida hoy por los criptólogos- un sistema de tipo estratégico debe poseer, como característica fundamental la siguiente: La seguridad de un sistema estratégico se basa totalmente, o de forma esencial, en el secreto de la clave, de forma que si el adversario descubre el tipo de cifrado utilizado, pero ignora la clave empleada para descifrarlo, el secreto del mensaje queda garantizado. Esto es lo que se conoce como principio de Kerckhoffs.

De este principio se deduce que para evaluar la eficacia de un cifrado estratégico hay que partir de la hipótesis pesimista de que ya se conoce el tipo de cifrado empleado. Hasta el punto, que en la criptografía de ordenador, el sistema de cifrado se explica a veces públicamente, con el fin de convencer a los posibles compradores de su eficacia.

Hasta 1.977, en que el algoritmo.[58] Data Encryption System (DES), fue ofrecido al público, incluso los que compartían el principio de Kerckhoffs, habían preferido no correr riesgos, manteniendo en secreto cuanto podían.

"La información sobre la información", que viene a añadir al valor de la información en sí misma, el valor de los soportes y medios tecnológicos que la sustenta, tuvo un extraordinario valor en lo referido a la criptología, y dio lugar a múltiples acciones de los servicios de inteligencia.

A partir de esta época -1.977-, se va perdiendo el concepto mítico de secreto atribuido a todo lo relacionado con la criptología, para dar paso a una situación en la que el secreto no es el instrumento, sino la información que se protege.

Kerchoffs, formuló varios principios:

1º.- El sistema de cifrado debe ser impenetrable, si no en teoría, al menos en la práctica.

2º.- El hecho de que el sistema se vea comprometido no debe dañar a los corresponsales.

3º.- La clave debe ser fácil de memorizar y fácil de sustituir.

4º.- Los criptogramas deben ser idóneos para su transmisión por telégrafo.

5º.- El aparato y los documentos de cifrado deben ser fáciles de transportar; es necesario que la operación de cifrado la pueda realizar una sola persona.

6º.- El sistema debe ser sencillo, no se debe basar en el conocimiento de largas listas de normas ni requerir esfuerzos mentales excesivos.

El principio de Kerckhoffs por antonomasia es el segundo, entendiendo por sistema comprometido aquella circunstancia en la que el adversario descubra el tipo de cifra empleado, pero desconozca la clave.

Kerckhoffs afirma, también, que solo los profesionales pueden evaluar la resistencia de un sistema de cifra. Ha sido frecuente a lo largo de la historia, que personas de gran autoridad, aunque totalmente inexpertas, impusieran, incluso en épocas de guerra, el empleo de códigos secretos cuya debilidad ya era conocida por los especialistas.[59]

J) CÓDIGOS.

Los sistemas de clave fija reciben el nombre de sistemas degenerativos, de códigos o, simplemente código, y resultan totalmente inutilizables en la criptografía estratégica.

Son de uso común, los códigos que no tienen otra función de convertir un texto claro en su equivalente sin pretensión alguna de añadir secreto. Son muy conocidos el código telegráfico o "alfabeto Morse", formulado por Samuel Morse en 1.838; el utilizado para comunicar con los ordenadores que emplea un alfabeto binario, formado por dos cifras (bit=binary digit= cifra binaria, 0 y 1), el ASCII (American Standard code of Information Interchange), u otros como el código Baudot.

Pero los códigos criptográficos, que incorporan sistemas de cifra degenerativa, no por ello han sido eliminados totalmente de la criptografía.

Estos códigos no son códigos criptográficos propiamente dichos, son sistemas de transcripción, conocidos por los especialistas, que sirven para pasar el alfabeto corriente a otros más en consonancia con las máquinas. Con ellos no se estaría cifrando información en el sentido que en el presente trabajo damos al concepto cifrar, sino que se estaría codificando, que no es otra cosa que convertir un texto claro en su equivalente utilizando un código público.[60]

En la criptografía táctica, se ha recurrido con frecuencia al empleo de estos sistemas, para garantizar el secreto por periodos muy cortos de tiempo y tuvo algunas aplicaciones en la criptofonía, para cifrar la voz.

Durante la Segunda Guerra Mundial, los americanos emplearon un sistema de criptofonía en el que, un modulador transformaba el mensaje original expresado en inglés, en un mensaje cifrado, que se transmitía por teléfono y se demodulaba en el otro extremo. La curiosidad viene porque modulador y demodulador eran indios navajos.

El navajo es una lengua de muy escasa difusión y de muy difícil o imposible pronunciación para cualquiera que no sea indígena.

Este hecho, conocido, tal vez ponga en evidencia el uso que las fuerzas norteamericanas dieron a lenguas étnicas, como sistema de cifrado de voz y, posiblemente, utilizasen alguna otra lengua, además de la de los indios navajos[61].

Fuentes orales comentan que la Flora del Pacífico utilizó el euskera para sus comunicaciones secretas, embarcando para ello pastores vascos en sus unidades.

En la época del telégrafo y hasta la Segunda Guerra Mundial, se solía utilizar un sistema que compilaba en un diccionario una serie de palabras y expresiones de uso más frecuentes y se traducían a un idioma inventado. Estos sistemas se suelen llamar de diccionario o repertorios.

Los diccionarios suelen ser voluminosos, fáciles de perder y difíciles de esconder.

Los códigos de lista sencilla, en los que tanto la palabra de origen como el número de código, van en orden, son poco seguros. Para solucionar esta debilidad, se recurrió a códigos de lista doble, donde los números tienen una secuencia totalmente desordenada.

Estos códigos se han utilizado en las dos guerras mundiales, y también han sido forzados en innumerables ocasiones, tanto por procedimientos de tipo estadístico, como por sistemas indirectos, basados en operaciones de inteligencia y el tráfico de material secreto.

Para reforzar este tipo de cifrado, en ocasiones se recurría a una operación de cifrado adicional, durante la cual, los criptogramas se cifraban por segunda vez (se sometían a una operación de recifrado).

K) CRIPTOGRAFÍA MECÁNICA.

Con la llegada de la revolución industrial a mitad del siglo XVIII, la pasión por las máquinas invade los campos más diversos.

En 1.820, el matemático inglés Charles Babbage, comienza a proyectar su máquina analítica, una especie de ordenador mecánico con tarjetas perforadas, que bien podría ser el antecedente de los actuales ordenadores electrónicos. Este proyecto, por su tremenda complejidad, no llegó a ser realidad.

Sin embargo, otras máquinas alcanzaron un éxito inmediato. El telégrafo electrónico que siguió al telégrafo óptico, tuvo una influencia decisiva en el desarrollo de la criptografía.

En 1.835, Samuel Morse expuso su modelo, ocho años más tarde, se inauguró la primera línea telegráfica entre Paddington y Slugh.

El desarrollo de las técnicas de comunicación tuvo también una influencia decisiva sobre las "técnicas de guerra": la situación de las operaciones militares ya se podría controlar a distancia. A todo ello se unió que los pequeños ejércitos de asalariados dieron paso a los ejércitos nacionales formados por multitud de hombres, los frentes de batalla se ampliaron y las comunicaciones fueron cada vez más importantes.

No menor importancia tuvo la influencia del desarrollo de las técnicas de comunicación sobre la diplomacia, como medio y modo de

comunicación informativa pacífica e institucionalizada entre los actores del sistema internacional.

A lo largo de la evolución histórica, la diplomacia ha ido incorporando los procesos técnicos, alterando simultáneamente sus métodos.

La diplomacia clásica, ejercida por representaciones permanentes y según hábitos y protocolos muy perfilados, gozando los embajadores de gran autonomía y procurando la consecución de objetivos generalmente limitados, a lo que se añade el carácter secreto de las deliberaciones, la profesionalidad de los negociadores, la concepción de Europa como centro de gravedad de la política internacional y el respeto a principios como el equilibrio o el sistema directorial.[62]

Este tipo de diplomacia a partir de la Primera Guerra Mundial, va incorporando serias modificaciones, fruto del nacionalismo y el progreso técnico.

Junto a la acción permanente de los diplomáticos acreditados en las distintas Cortes, tienen lugar importantes congresos Internacionales, que volverán a proliferar tras la Segunda Guerra Mundial. A estas reuniones de tipo político, hay que añadir, desde el siglo XIX, las especializadas y técnicas, que enlazan con la creación de las primeras Organizaciones Internacionales y el inicio de una diplomacia "monográfica" que adquirirá gran relevancia.

La quiebra de la diplomacia clásica coincide con la pérdida del eurocentrismo, la guerra total, la extensión de la democracia, el desarrollo industrial y tecnológico, el aumento de actores y la proliferación de diplomacias paralelas. Llegándose a la diplomacia contemporánea cuyas formas más representativas de diplomacia directa, multilateral y parlamentaria, además de la diplomacia "ad hoc", está caracterizada por una acción exterior de operatividad inmediata, universal, heterogénea, tecnificada y muy afectada por presiones políticas, económicas y de opinión pública.[63]

La historia de la criptografía corre ya paralela a la historia de los avances técnicos en el terreno de las telecomunicaciones.

La patente del teléfono se remonta a 1.871, la telegrafía sin hilo, también fue un invento importante, aunque por poco tiempo, fue patentada por Guillermo Marconi en 1.896.

El telégrafo, la radio y los ordenadores electrónicos que se construyeron durante la Segunda guerra Mundial, señalan momentos importantes en la historia de nuestra sociedad.

Hoy, las redes telemáticas entre ordenadores situados a gran distancia, posibilitan un sistema de "correo electrónico" de gran eficacia.

La revolución industrial intervino de forma directa en la criptografía, las operaciones de cifrado y descifrado se fueron mecanizando y automatizándose.

En la última década del siglo XVIII, Thomas Jefferson (1.743-1.826) autor de la Declaración de Independencia de los Estados Unidos de América en 1.776, primer Secretario de Estado y presidente electo en 1.801, fue Embajador en París, Vicepresidente y Presidente de los Estados Unidos.

Para Jefferson solo existe "un sistema único de ética para hombres y naciones: ser agradecidos, fieles a todos los compromisos en cualesquiera circunstancias, francos y generosos, y promover a largo plazo los intereses comunes de ambos". Rechaza la idea de que la moral de los Estados debía ser juzgada con normas distintas de la moral de los individuos.

Para Jefferson, *"el gran dilema de la ciencia del estadista radicaba en su aparente renuncia a los medios de que los Estados siempre habían dependido para garantizar su seguridad y satisfacer sus ambiciones, y en su simultánea repugnancia a renunciar a las ambiciones que normalmente conducían al uso de esos medios. En otras palabras, deseaba que los Estados Unidos pudiesen realizar ambas cosas: gozar de los frutos del poder sin ser víctimas de las consecuencias normales de su ejercicio".*

La misión especial de los Estados Unidos trasciende la diplomacia cotidiana, y los obliga a servir como faro de la libertad para el resto de la humanidad. La política exterior de las democracias es moralmente superior porque, el pueblo es, en esencia, amante de la paz. La política exterior debe

reflejar las mismas normas morales que la ética personal. El Estado no tiene derecho a arrogarse una moral especial.

Todos los liberales norteamericanos desde Jefferson insistieron en esta idea, que los mismos principios morales que gobiernan la vida privada también deben gobernar los asuntos internacionales.[64]

Jefferson fue defensor del aislacionismo de Europa, supo combinar su preocupación política por las libertades, con el derecho del ejecutivo a mantener en secreto determinada información.

Ante el dilema teórico de "prensa sin gobierno" o "gobierno sin prensa", Jefferson se decantó por lo primero y, en una carta dirigida a Edward Carrington en enero de 1.787 dice: *"If it were to me to decide whether we should have a government without newspapers or newspapers without a goverment, i should not hesitate to preffer the latter".[65]*

En la reunión del Gabinete de 2 de abril de 1.792, se llegó a la conclusión de que *"the executive ought to communicate such papers as the public good would permit, and ought to refuse those the disclosure of which would injure the public".*

En Marbury v. Madison (1.803), la existencia de los "secretos de gabinete" se admite, obiter dicta, como algo plenamente encajable en los esquemas de gobierno.

Los esfuerzos de Aaron Burr, en su juicio por traición, por obtener de la Administración Jefferson determinados documentos

exculpatorios, permitieron a Marshall argumentar sobre el derecho del ejecutivo a ocultar información cuando la misma "would endanger the public safety", reservando, la última palabra al Tribunal Supremo.[66]

La preocupación de Jefferson por el secreto le hizo pensar en su protección a través de la criptología, lo que le llevó no sólo al uso fluido de esta técnica de protección, sino a inventar una máquina de cifrar, consistente en un cilindro montado sobre un eje y cortado en 26 discos iguales que giran libremente, procedimiento en el que basaron los equipos electromecánicos de cifrado utilizados hasta mediados del presente siglo.

Todo ello le hizo acreedor a los calificativos de padre de la democracia y de la criptografía americana.

Jefferson, a nivel práctico, no hizo uso de su invento y sus necesidades criptográficas las cubría con sistemas más anticuados.

El invento cayó en el olvido, hasta que en 1.890, Etienne Bazeries, volvió a inventarla.

Estados Unidos adoptó el uso del "cilindro de Jefferson" en 1.922, para comunicaciones de bajo nivel; se utilizó en la Segunda Guerra Mundial y, en algunos casos, en periodos posteriores.

El elemento típico de las máquinas de cifrar que se fabricaron hasta la Segunda Guerra Mundial fue el rotor (disco rotativo, montado sobre un eje que pasa por su centro).

Una de las más famosas máquinas de cifrado utilizada por los alemanes, en la Segunda Guerra Mundial fue la "Enigma". Es representativa de una clase importante de sistemas de cifra de rotor, circularon varias versiones.

Hasta estas fechas, incluidas las máquinas Enigma y Magic, no fueron más que modificaciones y realizaciones con métodos mecánicos y eléctricos, cada vez más avanzados, de sistemas basados en sustituciones y transposiciones.[67]

La "Enigma" es una máquina electromecánica, que sirve para poner en práctica un sistema de cifra basado en sustituciones polialfabéticas con un periodo muy largo

Con cuatro rotores, la configuración inicial se recupera tras un periodo de 26 x 26 x 26 x 26 = 264= 456.976 saltos.

*Con cinco rotores, 265= 11.881.776 saltos, si fuesen seis los rotores, 266 = 308.915.776 saltos y, si fuesen siete los rotores, 267 = **8.031.810.176** saltos.[68]*

Las máquinas fabricadas por Boris Hagelin fueron auténticas joyas de la criptografía mecánicas comercializadas a partir de 1.927.

Frecuentemente se recurre al método de un cifrado adicional, -como ocurría con los códigos-, lo que conduce a los sistemas compuestos. Un texto cifrado se pasa por un nuevo sistema de cifra y se vuelve a cifrar por segunda vez (recifrar).

Esta operación, teóricamente, se puede repetir cuantas veces se considere conveniente, pero tal vez, en un punto crítico, la complejidad total sería excesiva.

En principio se puede considerar que la complejidad de un sistema de cifrado compuesto es la suma de la complejidad de los sistemas de cifrado que lo componen y los criptólogos aspiran a construir un sistema cuyo grado de complejidad sea el producto de los grados de seguridad de los sistemas que lo componen.

Aunque no siempre una mayor complejidad se traduce en un incremento de seguridad e, incluso, de la mayor complejidad se pueden derivar mayores probabilidades de errores que comprometan al sistema y requerir, si se quiere evitar esto, la asignación de recursos en cantidades que pueden ser desproporcionadas para la finalidad que se persigue.

El impulso decisivo de la criptografía y el criptoanálisis, tuvo lugar durante las dos guerras mundiales.[69]

Acontecimientos de singular importancia y máxima transcendencia para las partes contendientes propiciaron el uso de la cifra y el criptoanálisis.

En 1.930, la necesidad de utilizar elementos más complejos para neutralizar el avance del criptoanálisis, lleva a la aparición de las primeras máquinas de cifra. Y tras la Segunda guerra Mundial, se amplía el ámbito de

la criptografía con el desarrollo de métodos y sistemas más consistentes con aplicación de la electrónica.

2.2.2.- Presente y futuro de la Criptología.

En criptografía, como en otras ramas del saber, resulta difícil hacer un diagnóstico exacto de la situación presente, pero si además, se le une la lógica reserva con la que, en algunos casos se lleva lo relacionado con la criptología, puede resultar aún más complejo.

Se podría decir que en la actualidad conviven sistemas de diversas épocas, pero no son representativos de nuestros días .En plena sociedad de la información, al hablar de presente nos referiremos a la cifra electrónica y, al hablar de futuro a las posibilidades matemáticas y computacionales con la vista puesta en un "cifrado perfecto".

a) Criptografía electrónica.

Entre los sistemas de cifrado compuestos, algunos recurren a sistemas mixtos, entre ellos, uno de los más conocidos es el Data Encryption Standard (DES), de la International Business Machines (IBM), posteriormente adquirido por la NSA para la Administración norteamericana, y según señala Menezes en su reciente obra "Handbook if Applied Cryptography", en 1.977 fue adoptado como "U.S. Federal Information Processing Standar" para información no clasificada.

Su funcionamiento se describe en los informes técnicos que están al alcance de cualquiera y el secreto reside única y exclusivamente en el secreto de la clave.

El comunmente conocido por DES, es un sistema de cifrado de tipo binario, formado por secuencias de bit ,0 y 1, lo que implica que el mensaje, antes de ser ofrecido al DES, tiene que ser traducido utilizando el código ASCII. Tiene 2^{56} claves.[70]

En el presente siglo, la criptografía ha avanzado a grandes pasos y utiliza elementos matemáticos de enorme sofisticación.

A Claude Shannon se le considera el padre de la criptografía moderna. En 1.949 publicó "Communication Theory of Secrecy Systems" (Teoría de la comunicación de los sistemas secretos). Esta obra se escribió durante la Segunda Guerra Mundial pero no se publicó de inmediato. Shannon es también el padre de la teoría matemática de la transmisión de información o teoría de la información.

Junto al planteamiento de problemas, en el contexto de las matemáticas, nace el concepto de algoritmo como conjunto finito de operaciones que, realizadas en un orden determinado, permiten resolver todos los problemas de un tipo dado.

La resolución de un tipo de problemas venía determinado por la descripción de un algoritmo que lo resolvía.

Se considera resuelto una serie de problemas de un determinado tipo cuando se elaboraba un algoritmo para su resolución.

Alan Turing habló de las funciones computables algoritmicamente,-problemas decidibles-, para los que se puede obtener una máquina que los resuelva y, los problemas indecidibles, son algoritmicamente irresolubles y, para ellos, no se puede obtener una máquina que los compute.[71]

En el sistema de cifra que utiliza clave no reutilizable, el criptograma por sí mismo y a falta de clave, no ofrece información alguna sobre el contenido del mensaje de origen. Es en terminología de Shannon un "cifrado perfecto". Debajo de esta afirmación hay todo un teorema matemático.

A diferencia de los sistemas imperfectos en los que, los criptogramas, por muy caóticos que puedan ser en su apariencia, esconden algún rastro de regularidad, que, de ser descubierto por el criptoanálista, le ofrece el punto de partida para desentrañar el código secreto.

Shannon midió el secreto de un sistema criptográfico como la incertidumbre acerca del mensaje, conocido el cifrado recibido.

El criptosistema alcanza el secreto perfecto si el conocimiento del cifrado no proporciona información alguna acerca del mensaje salvo, posiblemente, su longitud.[72]

El secreto perfecto se alcanza si las probabilidades, una vez conocido el cifrado, son las mismas que "a priori", donde mensajes, claves y cifrados tienen las mismas probabilidades. Un sistema con secreto perfecto

necesita que el espacio de las claves sea, al menos, tan grande como el de mensajes.

La idea de encontrar cifrados perfectos mediante el uso de claves no repetitivas de tamaño igual al del mensaje, llevó a Gilbert Vernam de AT & T, (1.917), a diseñar un método inmune a la mayoría de los ataques del criptoanálisis.

El procedimiento consiste en combinar una larga secuencia aleatoria de números, no repetitiva, con el mensaje en claro.

Vernam utilizó una cinta perforada de teletipo que contenía números aleatorios y se usaba una sola vez, de forma que el texto cifrado no mostraba nunca la estructura de la clave.[73]

Shannon especificó los criterios para un cifrado perfecto en un entorno de comunicación mediante el uso de la criptografía, enunciados antes de la aparición comercial del ordenador, y antes de que el proceso de cifrado y descifrado se hiciese mediante un ordenador electrónico.

La disponibilidad de una gran potencia de cálculo, de almacenamiento y los diferentes modos de representación codificada de la información, obligaron a efectuar una revisión de los criterios de Shannon para actualizarlos, transformándose en las siguientes reglas:

"*Uno. La cantidad de seguridad deseada, determina la cantidad de trabajo y tiempo de cálculo necesario para vulnerar el mensaje cifrado.*

Dos. Las claves utilizadas deben ser de fácil construcción, lo más cortas posibles, fáciles de alimentar y modificar y consecuentemente que ocupen poca memoria.

Tres. Las operaciones de cifrado y descifrado, conocida la clave deben implicar la menor cantidad de cálculo posible.

Cuatro. Las claves y el sistema de cifrado deben ser tales que destruyan los parámetros estadísticos del lenguaje, o bien su estructura natural.

Cinco. Los errores de transmisión en los criptogramas, no deben originar ambigüedades o pérdida del sentido en la información original, haciéndola inútil.

Seis. La necesidad de almacenamiento para los criptogramas no debe ser mayor que la necesaria para los mensaje en claro equivalentes.

Siete. El análisis de un criptograma tratando de vulnerarlo debe necesitar una cantidad de cálculo tal, que sea considerado como un problema intratable, incluso con ordenador como apoyo".[74]

Con el logro del cifrado perfecto, podría parecer que la criptografía ha agotado sus posibilidades de investigación y desarrollo. Pero el problema del cifrado perfecto es que resulta difícil de utilizar, la clave es excesivamente larga y son muy costosos.

F.L. Bauer refleja en cinco "máximas de criptología" la experiencia recogida durante siglos:

1.- No se debe despreciar al adversario.

2.- Sólo un criptoanalista puede juzgar la seguridad de un criptosistema.

3.- Al valorar la seguridad criptográfica de un sistema hay que tener en cuenta que el adversarios conoce el sistema.

4.- Una complejidad superficial puede ser ilusoria, por que genera un falso sentido de seguridad.

5.- Al valorar la seguridad criptográfica de un sistema, han de tenerse en cuenta los errores criptográficos y las infracciones de seguridad. [75]

B) CRIPTOGRAFÍA AVANZADA.

La investigación de la criptología se orienta hacia los sistemas de cifrado pseudoperfectos y la criptografía de clave pública.

Para algunos investigaciones de las empresas más importantes del mundo, la falta total y absoluta de regularidad de un cifrado perfecto ofrece ya un dato para el criptoanálisis, que no lo ofrece el cifrado pseudoperfecto.

En la actualidad se dispone de toda una serie de métodos que permiten generar cifras binarias pseudocasuales y que podrían, en apariencia, satisfacer las necesidades de la criptología, entre ellas, el método formulado en 1.946 por John von Neumann, padre de la teoría de los juegos.

Se pueden, por tanto, construir sistemas cómodos que, aunque son periódicos, disfrutan de un periodo astronómico que puede llegar, por ejemplo a $10.^{80}$

Construir sistemas de cifrado psudoperfectos es un objetivo razonable, que parece más que suficiente para cubrir las necesidades de la

criptología. De hecho empresas que fabrican sistemas criptográficos estratégicos, tanto para uso militar como para uso diplomático, lo utilizan.

Pero en los métodos corrientes de generación de cifras pseudocasuales se obtienen cifrados frágiles. De ahí que uno de los campos de investigación de la criptología actual se centre en el estudio de métodos de generación de cifras pseudocasuales distintas a las habituales, con el objetivo puesto en aproximarse al cifrado perfecto que resulta inatacable.

Algunas de estas investigaciones están protegidas por el más riguroso secreto.

Una de las líneas de investigación se centra en el estudio de largas series de números primos.

En 1.978, Ronald Rivest, Adi Shamir y Leonard Adleman, sacan a la luz un algoritmo de cifra conocido como RSA (que corresponde a las iniciales de los nombres de sus autores, Rivest, Shamir, Adelman).[76]

Este algoritmo no requiere mantener en secreto la clave de cifrado y abre paso a la criptología de clave pública que se contrapone a la tradicional de clave secreta.

En el RSA existen dos claves, una para cifrar y la otra para descifrar. Esta segunda (clave inversa), está formada por dos números primos muy elevados, el secreto radica en estos factores primos, la clave secreta de descifrado no la conoce ni el remitente legítimo del mensaje.

No obstante , si alguien logra descubrir un algoritmo rápido para descomponer números compuestos el RSA caería.

Para José Pastor, la seguridad de los sistemas criptográficos clásicos era un concepto mal definido y discutible. La historia ha demostrado que todos los sistemas que se consideraron en su día inviolables, han sido violados. Los sistemas clásicos tenían una seguridad "probable", mientras que los sistemas modernos tienen una seguridad "matemáticamente demostrable". Son métodos incondicionalmente seguros hacia los que se dirigen todos los desarrollos teóricos y prácticos.[77]

La llegada de comunicaciones globales eficaces, viene a subrayar la necesidad de contar con una protección adecuada en cuanto a disponibilidad de servicio, integridad de los mensajes, respeto a la intimidad y garantías de la confidencialidad. En definitiva, contar con seguridad.[78].

Alvin Toffler[79] afirma que hay "planes en marcha para crear una sola red mundial e inconsútil de comunicaciones militares que trascienda la esfera de las fuerzas armadas de Estados Unidos, un sistema modular que pueda ser compartido simultáneamente por las fuerzas de muchas naciones... La nueva red concebida pretende precisamente superar este tipo de problemas (problemas de coordinación) y hacer más fluidas que en el pasado las operaciones combinadas con los aliados".

"La naturaleza de las redes de comunicación implica a menudo supuestos estratégicos tácitos. En este caso, la noción de una red global con

la que puedan conectar otras naciones refleja claramente el supuesto estratégico de Estados Unidos de que en el futuro luchará en combinación con otros aliados, en vez de actuar en solitario como "gendarme del mundo".

El sistema propuesto conjura imágenes de un futuro marcado por alianzas temporales de conexión/desconexión, de acuerdo con la fluidez de condiciones del mundo posterior a la guerra fría. Podría simplificar además las futuras operaciones de la ONU.

Más también suscita la sospecha de que, si Estados Unidos diseña básicamente el sistema, sea capaz de enterarse de todos los mensajes que fluyan a través de dicha red. No necesariamente, se afirma, porque cada una de las naciones puede especificar su *"cripto"*, como se conoce a la codificación."

En este supuesto, el "cripto" elegido por cada nación redobla su importancia y exije niveles organizativos, criptológicos y tecnológicos del máximo nivel.

Además, para hacerlo posible en el plano de la realidad, Mary Ruscavage, subdirectora del Mando Electrónico de Comunicaciones del Ejercito de Estados Unidos, afirma "tratamos de desarrollar una arquitectura genérica y de tomar en consideración todos los tipos de equipo que tenga un país".

Un sistema modular de equipos permitiría adaptarse, en condiciones optimas, no sólo a las nuevas exigencias de la red futura (RDSI), sino

también a las redes y medios de transmisión existentes. Ha de asegurarse, asímismo, la comunicación por otras vías, por ejemplo, los enlaces por canales de onda corta.

Los futuros sistemas de cifrado personal parecen indicar la dirección de la criptología. Cifrarán el contenido de la comunicación dejando en claro la dirección y las informaciones de control. De forma que un sistema de cifrado personal puede ser conectado en un lugar cualquiera de la red -e intercambiar con otros sistemas de cifrado personal en la red-, de forma cifrada, conversaciones, informes, y documentos, O también fotografías o croquis gráficos. Y puede ser utilizado, incluso, como un ordenador personal, parcialmente, con los mismos paquetes de software, tanto en una oficina como durante un desplazamiento. Todos los datos almacenados están en clave y sólo podrán ser leídos o tratados con la ayuda de un módulo de seguridad personal.[80]

En el cifrado de enlace se cifrarían flujos de datos enteros entre dos puntos de la red, lo que implicaría que los equipos terminales de las líneas de conexión, y los equipos del nudo de la red, habrían de encontrarse en zonas inaccesibles a terceros. Esto unido a una adecuada organización de claves, a través de módulos de seguridad personal, garantizaría la seguridad.

Los futuros servicios y redes se irán integrando progresivamente en la Red Digital de Servicios Integrados. Pero en la mayor parte de los

países, aún se tardará algún tiempo para que una red, completamente integrada, llegue a todos los interesados.

Las fases de introducción serán diferentes, en función del desarrollo individual de la infraestructura de cada país. Lo que implica que también los sistemas de cifrado plantearán exigencias diferentes.

Por cuanto se refiere a España, la Disposición Adicional Primera de la Ley 31/1.987, de 18 de diciembre, sobre Ordenación de las Telecomunicaciones, en su punto 2, indicaba que se establecerá un Plan que "...tendrá como horizonte la integración progresiva de las redes de telecomunicación, en primer término, hacia una red digital de servicios integrados de banda estrecha basada, esencialmente, en la evolución de la actual red telefónica conmutada y, en segundo término, hacia una integración compatible con la consecución a más largo plazo de una red digital de servicios integrados de banda ancha..."

El sistema de cifrado personal en la red redundante, es una opción de futuro, al conseguir que un conjunto de equipos terminales para la transmisión de la palabra, el texto, o la imagen, comuniquen con una red compuesta de los más diversos medios de transmisión. Cuando alguno de ellos falla, el siguiente medio toma el relevo de la transmisión.

En este tipo de redes, y en general, en la sociedad de la información, a la hora de plantearnos la protección criptológica de una información, hemos de tener en cuenta que el tratamiento automatizado de datos hace que

el carácter de "información sensible" no dependa sólo de su conexión directa e inmediata con los aspectos centrales de la información a proteger. Existen toda una serie de datos colaterales, aparentemente inócuos, que, adecuadamente procesados, pueden aportar un conocimiento substancial.

En definitiva, la preservación del núcleo esencial de una información requiere la protección de toda una serie de datos situados en la periferia del mismo. Por eso, en determinadas redes, ha de plantearse la posibilidad de ir a una *"cifra total"*.[81]

Pero, hoy por hoy, los sistemas de cifra estratégica, elaborados por las más prestigiosas firmas mundiales especializadas en criptología, para usos militares y diplomáticos, descartan el sistema de clave pública y se mantienen en el sistema de cifra de clave secreta, y algoritmos propios, que alcanzan niveles de sofisticación tales, que se sitúan próximos al "cifrado perfecto", y permiten que cada mensaje se cifre con claves distintas e irrepetibles, elegidas entre billones de combinaciones.

Las nuevas tendencias tecnológicas se convierten en un aliado potencial de la Criptología en todas sus dimensiones.

En esta línea ya no son expresiones infrecuentes las de *"criptología digital"*, *"criptología cuántica"* o *"criptología biológica"*.

Destaca por su importancia la *computación configurable*. Los ordenadores son capaces de modificar sus circuitos microelectrónicos

mientras están funcionando, abriendo así una nueva era en las técnicas de cifrado por su velocidad de filtrado.

De no menor importancia es lo que se conoce como *criptología cuantica*, basada en principios de mecánica cuántica, que se vale de fotones individuales y se basa en el principio de incertidumbre de Hedissenberg, de forma que 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.

El auge y desarrollo de la información y las comunicaciones, y su necesidad de protección, anuncia un crecimiento del uso de la criptología.

2.3.- CRIPTOSISTEMAS.

Todo criptosistema o sistema criptográfico como conjunto de claves y equipos de cifra que utilizados coordinadamente ofrecen un medio para cifrar y descifrar. Un criptosistema está formado por cinco elementos:

a) Espacio de mensaje, generalmente denominado M, es el conjunto de todos los posibles mensajes $\{m_1, m_2, m_3 ...\}$ en claro, es decir

inteligible, formados con caracteres de un cierto alfabeto A, siguiendo sus reglas sintácticas y semánticas.

b) Espacio de cifrado, denominado C, está formado por los mensajes cifrados $\{c_1,c_2,c_3, ...\}$ utilizando un alfabeto B que puede o no coincidir con A.

c) Espacio de claves, denominado K y formado por el conjunto $\{k_1,k_2,k_3 ...\}$ de las claves utilizadas para el cifrado.

d) Familia de transformaciones de cifrado. Una transformación E_k, aplicada a un mensaje del conjunto M obtiene un mensaje cifrad dentro del conjunto C, dependiendo de la clave k utilizada.

e) Familia de transformaciones de descifrado. Una transformación D_k utiliza el parámetro k del conjunto K para pasar del mensaje cifrado al mensaje en claro.[82]

Durante mucho tiempo las claves de cifrado y descifrado eran las mismas y las transformaciones para descifrar eran las inversas de las transformaciones de cifrado. Pero esto no tiene, necesariamente, que ser así, lo único que tiene que cumplirse es,

$$E_k(D_k (c) = c$$

Pueden existir infinitos sistemas de cifrado pero para que realmente sea útil en la práctica y resistente a los ataques del criptoanálisis debe cumplir los siguientes requisitos:

1°.- Las transformaciones de cifrado y descifrado deben ser, para todo el espacio de claves, computacionalmente eficaces y eficientes.

2°.- La seguridad del sistema debe depender en exclusiva del secreto de las claves y no del secreto de las transformaciones.

Por ello, aunque el algoritmo sea de dominio público, la fortaleza del criptosistema se basa en la imposibilidad de inferir la clave de cifrado de la de descifrado, o al revés.

Se distinguen dos tipos de criptosistemas: los de clave privada y los de clave pública.

1.- En los criptosistemas de clave privada, también denominados simétricos o de clave única, la fortaleza del sistema está en el secreto de la clave K. La pareja emisor-receptor del mensaje comparten el secreto de la clave. El sistema será útil siempre que sea computacionalmente imposible determinar la clave mediante un ataque sistemático aún conociendo las funciones de cifrado y descifrado. Es de advertir que los avances de las tecnologías de los computadores hace que el concepto de incomputabilidad varíe continuamente.

2.- El sistema de clave pública propuesto por Diffie y Hellman en 1.976 es un sistema de comunicación privada que emplea un directorio de claves públicas de forma que cada usuario fija un procedimiento E para que sea usado por otros usuarios cuando cifren mensajes que vayan dirigidos a

él, mientras que mantiene en secreto su propio procedimiento D de descifrado.

Para que el sistema sea viable se debe establecer un procedimiento simple mediante el cual, cada usuario pueda producir su propio E y D.

Siguiendo a Rodríguez Prieto,[83] un criptosistema de clave pública puede ser definido como un par de familias

$\{E_k\}, K \in \{K\}$ y $\{D_k\}, K \in \{K\}$

de algoritmos que representan transformaciones invertibles.

Ek: {M} → {M} (cifrado)

Dk: {M} → {M} (descifrado)

Siendo M un espacio finito de mensajes.

Las propiedades que deben cumplir estos procedimientos deben ser las siguientes, siendo M y C los conjuntos de mensajes y criptogramas, respectivamente:

1.- $C = E(M) \Rightarrow M = D(C)$ y

$D(E(M) = M \vee M$

2.- Tanto E como D deben ser rápidas de obtener y fáciles de aplicar.

3.- El conocimiento público de E no implica el conocimiento ni pérdida de seguridad de D, de modo que la obtención de D a partir de E es un problema intratable desde el punto de vista de teoría de la calculabilidad.

Los cifrados asimétricos pueden ser sistemas de cifrado de clave pública, en los que la clave para cifrar y para descifrar son distintas y prácticamente imposible de obtener esta a partir de aquella.

Son necesarias la funciones "un solo sentido" como herramientas fundamentales a utilizar en los cifrados de este tipo, de relativa facilidad para cifrar pero de gran dificultad para descifrar si no se conoce la segunda clave.

En los sistemas de clave pública, al estar separadas las capacidades de cifrar y descifrar se puede proteger la información sin guardar en secreto las claves de cifrado, ya que no es necesaria para descifrar.

Los sistemas de clave pública, al estar separadas las capacidades de cifrar y descifrar se puede proteger la información sin guardar en secreto la clave de cifrado, ya que no es necesaria para descifrar.

Los sistemas de clave pública disponen de dos claves para cada usuario U, la clave pública *ub* y la clave privada *uv*, siendo coputacionalmente imposible obtener una de otra. Las funciones de transformación E y D son conocidas.

Quien quiere mandar un mensaje a U lo hace cifrando con la transformación E_{ub}. U descifra el mensaje con la transformación D_{uv}.

En este tipo de criptosistemas se proporciona el secreto con la clave ub, pero no se puede garantizar la autenticidad, que necesitaría el cifrado mediante la transformación D_{uv}, que sólo conoce el propietario de la

clave uv. De todas maneras establece las dos propiedades simultáneamente mediante la adición de algunos requisitos.

Sistemas de clave pública son los propuestos por RSA, Rabin, ElGamal, McEliece, Merkle.Hellman, Chor-Rivest, Goldwasser-Micali, o Blum-Goldwasser.

La utilización práctica de los sistemas de clave pública conlleva la necesidad de solucionar el suministro de claves, para que cada usuario pueda hacer la selección apropiada, lo que se lleva a cabo a través de protocolos de distribución.

La tendencia a emplear arquitecturas a base de sistemas abiertos, en vez de sistemas que sean propiedad exclusiva de determinados suministradores, facilita los ataques a la información.

2.3.1.- La gestión de claves.[84]

Una vez establecido el sistema de cifra, es determinante diseñar una protección adecuada de las claves, hasta el punto que, en caso de no hacerlo, de poco serviría la utilización de algoritmos de gran seguridad.

El proceso que comprende la generación, distribución, almacenamiento, utilización, archivo y destrucción de claves empleadas en un criptosistema, es conocido como *"gestión de claves"*.[85]

La fortaleza alcanzada por los algoritmos de cifrado, orienta las preocupaciones de seguridad y facilidades de uso, hacia el establecimiento y

desarrollo de procedimientos adecuados de gestión de claves, sobre todo en las grandes redes.

El método de cifrado determina el número de claves a gestionar.

En un criptosistema de clave privada o convencional, se requiere una clave para cada par de usuarios. Si se tiene que incluir algún nuevo usuario, el número de claves crece combinatoriamente, lo que viene a complicar las operaciones de generación y distribución de claves. En los sistemas de clave pública, el problema es mucho menor, al no tener la necesidad de intercambiar previamente claves y manejar un número de estas más reducido.

Los sistemas de clave pública se caracterizan por utilizar dos claves para cada participante, una sirve en general para la operación de cifrado y es pública, mientras que la clave de descifrado, es secreta, y es la única que puede recuperar la información cifrada.[86]

La generación de claves se realiza mediante algoritmos que generan claves pseudoaleatorias. El ideal es conseguir generadores automáticos de claves totalmente aleatorios.

Los fabricantes, en muchos casos, utilizan algoritmos inéditos de diseño propio.

Existen diversos procedimientos de generación de números aleatorios para usar como claves criptográficas (generadores aleatorios de bits, registros de desplazamiento de realimentación lineal... etc.).

En todo caso, la distribución de claves al más alto nivel ha de realizarse por medios extraordinariamente seguros.

El almacenamiento de claves viene determinado, en gran medidas, por el sistema criptográfico empleado, existiendo diferencias entre los sistemas de clave privada y los de clave pública.

En los modernos criptosistemas, se suelen utilizar varias claves, las claves de sesión se pueden distribuir de varias formas, jerarquía de claves, claves centralizadas, por intercambio mutuo, o utilizando un criptosistema de clave pública.

Un aspecto muy importante de las claves es el cambio periódico de las mismas, la frecuencia con que se efectúe afecta a la seguridad del criptosistema, así como las acciones a llevar a cabo cuando estas son reveladas o robadas.

Para incrementar la seguridad del criptosistema, como principio general, se recomienda el cambio de claves con cierta frecuencia.

Los criptosistemas de clave privada suelen utilizar claves generadas de forma aleatoria y distintas en cada sesión, incluso, distintas para el que cifra y para el que descifra el mensaje, y no reutilizables.

Ante situaciones comprometidas de la clave, se suele comunicar a todos los usuarios, en el menor tiempo posible y actuar en consecuencia. [87]

El establecimiento de un adecuado sistema de gestión de claves permitirá hacer realidad un determinado plan de seguridad de la información en todos sus aspectos.

2.4.- EL CRIPTOANÁLISIS.[88]

La lucha por desentrañar los contenidos de los mensajes cifrados es tan antigua como estos mismos.

Desde los primeros tiempos, cuando aparecía un procedimiento de comunicación secreta, se ha tratado por todos los medios, no solo de conocer el contenido de esa información,- que lo podían obtener, en algunos casos, por otros procedimientos-, sino de hacerse con el sistema utilizado, de forma que le permitiese un acceso a la información secreta cada vez que se utilizase.

Durante el siglo XVI, en pleno auge de la criptografía, comienza a desarrollarse el criptoanálisis, a lo que contribuyeron, de forma decidida, Sir Francis Walsinghaun, con importantes soluciones a la correspondencia entre Luis XIV y su embajador en Polonia, y Edward Silles, con una obra sobre criptoanálisis.

Los "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", se denomina criptoanálisis.[89]

Para explicar la tensión entre criptografía y criptoanálisis, se recurre a símiles como la flecha y el escudo o la coraza y el cañón.

La criptografía seria la coraza que, cuando es perforada por la bala de cañón -criptoanálisis positivo- , requiere un reforzamiento, lo que obliga a su vez a los atacantes a introducir una mayor potencia en el impacto para lograr su objetivo.

La criptografía tiene un carácter defensivo, mientras que el criptoanálisis, tiene un carácter eminentemente ofensivo.

Esa guerra silenciosa y constante, por procedimientos científicos, entre la protección criptográfica de la información y su quebranto, es lo que ha ido haciendo evolucionar los distintos sistemas criptológicos.

El *"scytalo"*, el sistema de Julio César, el cifrado de rotación ... ,son vulnerables a las técnicas criptoanalíticas más elementales, una de ellas es conocida como "búsqueda exhaustiva".

En el criptoanálisis existen técnicas mucho más sofisticadas que la búsqueda exhaustiva, a las que no se resisten ni siquiera los criptogramas cifrados con sistemas de elevado número de claves.

Los sistemas de cifrado de rotación utilizando todas las permutaciones del alfabeto, o sistemas de sustitución monoalfabética, son vulnerables como lo demostró el relato publicado en 1.843, "The gold-Bug", (El escarabajo de oro), por Edgar Allan Poe, que además de escritor era aficionado a la descriptación de códigos secretos.

El sistema descrito por Allan Poe, en el que un personaje del relato desentraña el cifrado del pirata Kidd, es un método estadístico basado en la frecuencia de las letras que componen un texto inglés, método que recibe el nombre de "principio de máxima verosimilitud".[90]

En "El escarabajo de oro", de Poe, interviene también la esteganografía, esto es, el arte de ocultar los mensajes recurriendo a tintas invisibles y otros trucos, de forma que pasen totalmente inadvertido. Poe facilita una serie de recetas para fabricar tintas simpáticas. Una técnica actual de tipo esteganográfico sería la miniaturización.

Francis Bacon, Vizconde de St. Albans y Lord Canciller de Inglaterra (1.561-1.626), recurrió al cifrado mixto cripto-esteganográfico.

Un sistema esteganográfico muy antiguo, consiste en ocultar un mensaje secreto incrustando las letras en un texto de apariencia inocente.

En la Revista TIEMPO, del 23 de noviembre de 1.992, página 41, sección Confidencial, leyendo de arriba hacia abajo las últimas letras de cada línea que llega hasta el final del margen derecho, se puede leer claramente la palabra *"s o l a n a"* . Si se tiene en cuenta la notoriedad del apellido y la alta responsabilidad política de Javier Solana, Ministro de Asuntos Exteriores, en esos momentos, cabe pensar que, tal vez, estemos en presencia de un mensaje esteganografiado.[91]

Los valores porcentuales obtenidos de textos extensos y representativos de cada idioma, tienden a manifestarse con cierta regularidad en todos los textos medianamente significativos de cada idioma.[92]

FRECUENCIAS INDIVIDUALES DE LETRAS (%)

ESPAÑOL	FRANCÉS	ALEMÁN	INGLES	ITALIANO
e 14,14	*e* 17,76	*e* 19,18	*e* 12,86	*i* 12.04
a 12,90	*s* 8,23	*n* 10,20	*t* 9,72	*e* 11,63
o 8,84	*a* 7,68	*y* 8,21	*a* 7,96	*a* 11,12
s 7,64	*n* 7,61	*s* 7,07	*i* 7,77	*o* 8,92

...

Las leyes estadísticas sirven de ayuda al criptoanálisis y, por consiguiente, tienen que ser sorteadas por los criptólogos.

Una de las formas sería utilizando un libro como el de Ernest V. Wright que, en 1.914, publica en Los Angeles un libro titulado "Gadsby, A Story of Over 50.000 Words Without Using the Letter E" (Gadsby, relato de más de 50.000 palabras en el que no se ha empleado la letra E).

Existen otros sistemas para engañar a las estadísticas.

A principio del siglo XV, el árabe Qalqashandi describió métodos estadísticos que anticipan y prefiguran el principio de máxima verosimilitud, atribuidos a su antecesor Ibn ad-Duraihim (1.312-1.361).

En Occidente, el primer tratado dedicado íntegramente al análisis criptográfico apareció en 1.474 y fue escrito por Cicco Simonetta, Secretario

de la Cancillería de los Sforza de Milán, en la misma época que Alberti, que también se plantea problemas de análisis criptográfico.

Es una exigencia de los criptólogos, evitar el análisis estadístico.

Los criptólogos de la corte de la reina Isabel de Inglaterra lograron violar el nomenclator utilizado por la reina de Escocia, María Estuardo, -prisionera en Chartley-, en su correspondencia con los aliados franceses. De esta forma probaron la conspiración contra los ingleses y la reina de Escocia, el 8 de febrero de 1.587 subió al patíbulo.

La actividad criptoanalítica, además de en Londres, florecía en otros lugares. Los servicios secretos de la Serenísima República de Venecia, gozaban de gran prestigio.

Las cortes de las grandes potencias europeas organizaron muy pronto sus correspondientes y expertos departamentos de criptoanálisis. Son famosos el *"Cabinet Noir"*, de París y el "Geheime Kabinets-Kanzley" de Viena, o el departamento criptoanalítico de Estados Unidos denominado M-18.

Durante tiempo se consideró que el cifrado de Vigenère era inexpugnable con métodos criptoanalíticos. Pero Friedrich Kasiski (1.805-1.881), oficial prusiano retirado, publicó en 1.863 en Berlín un tratado de criptología denominado "Geheimschriften und die Dechiffrierkunst" (La escritura secreta y el criptoanálisis), que sin tener un apoyo matemático sofisticado, resultó muy eficaz para desentrañar un

criptograma largo, en base a la observación de la repetición de grupos de letras y la frecuencia con que se produce esta repetición.

El cifrado de Vigenère es un ejemplo significativo de toda una gama de cifrados polialfabéticos. Las técnicas criptoanalíticas para la demolición de estos cifrados son las de Kasiski, aludida, o la del americano William Friedmann, uno de los más famosos criptoanalistas de nuestro siglo.

Otra variante débil del cifrado de Vigenère es el que se conoce como método Gronsfeld, que debe su fama no precisamente a las cualidades criptológicas de su sistema. En 1.892, las autoridades francesas detuvieron a un grupo de anarquistas que habían cifrado sus secretos con el método de Gronsfeld. Los criptogramas fueron resueltos por Etienne Bazeries, uno de los más famosos especialistas en criptografía de la época, que había desentrañado nomenclatores históricos utilizados por Francisco I, Francisco II y Enrique IV, por el diputado Mirabeau y por Napoleón.[93]

También se utiliza el criptoanálisis para desentrañar el significado de lenguas muertas, aunque en esta actividad se superpone el estudio de las lenguas y la criptografía.

Entre estos criptoanalistas hay que destacar a Jean François Champollion que, en 1.822, consiguió dar solución criptográfica a los jeroglíficos del egipcio arcaico, desentrañando las inscripciones de la piedra Rosetta, o, George Friedrich Grotefend y Henry Rawlinson, que en la primera mitad del siglo pasado lograron desentrañar los caracteres

cuneiformes con que se escribían las lenguas de los antiguos persas, de los asirios y de los babilonios. Michel Ventris, en 1.952 descifró el misterioso "lineal B" de Creta.

En el siglo XVII, el jesuita alemán Athanasius Kircher (1.601-1.680), se dedicó a descifrar jeroglíficos.

Kircher y Gaspar Schott (1.608-1.666), fueron grandes especialistas en "anamorfosis" (técnica pictórica de deformación de la imagen).

La guerra secreta entre la criptografía y el criptoanálisis es una constante en la historia. Algunos hechos de esta naturaleza consiguieron modificar su curso.

1.- Algunas referencias históricas.

a) Telegrama Zimmerman.

El telegrama Zimmerman trae a la memoria un conocido caso ocurrido en 1.917, durante la Primera Guerra Mundial, en uno de los episodios de la guerra sumergida entre criptólogos y criptoanalistas. Los protagonistas de esta historia son el servicio secreto del Almirantazgo británico, el ministro de exteriores alemán Arthur Zimmermann y, en el transfondo, el presidente americano Thomas Woodrow Wilson.[94]

En 1.915 y 1.916 América se hallaba en conflicto simultáneamente, y por las mismas razones, con Alemania y con Inglaterra, lo que en pura lógica hubiese llevado a declarar la guerra a las dos naciones.

En esos momentos, Alemania e Inglaterra eran dos potencias marítimas, la primera apoderándose del fondo y la segunda de la superficie, habían exclusivizado el dominio del mar, colocando al comercio y al tráfico mundial entre la agresión, el boicoteo y las listas negras.

Cuando los aliados impusieron a Alemania un bloqueo jamás conocido, los Imperios Centrales respondieron al golpe declarando el contra-bloqueo de las costas inglesas, y sus submarinos, -centrados antes solo en los barcos de guerra-, empezaron a hundir mercantes, contrabandistas y sospechosos. Las pequeñas potencias neutrales tuvieron que resignarse.

Pero Estados Unidos, sintiéndose más fuerte, se negaron a la aceptación de unas restricciones tan contrarias a su sentido de la libertad.

En estas circunstancias, durante el mes de abril de 1.915, el transatlántico inglés *"Lusitania"*, de 32.000 toneladas, era despachado para Inglaterra por las autoridades del puerto de Nueva York. El barco había cargado 173 toneladas de material bélico.

Era un reto mutuo. Alemania que no quería consentir por más tiempo la irritante conducta de Estados Unidos, y el de Norteamérica, que no quería interrumpir su mortífero y lucrativo negocio ni someterse a la determinación tomada por Alemania de bloquear a Inglaterra.[95]

El día 7 de mayo, el submarino alemán "U-20" lanzó un torpedo y hundió al *"Lusitania"*, arrastrando al fondo del mar a 1.195 vidas humanas.

La tormenta diplomática consiguiente se debatía en si el *"Lusitania"* iba o no armado con cañones y por tanto debía ser considerado como un crucero auxiliar.

Alemania comunica a Washington que trataría de impedir el tráfico en el Mediterráneo y en torno a las Islas Británicas por cuantos medios tuviese a su alcance; los barcos neutrales que surcaran esas aguas lo harían por su cuenta y riesgo; no obstante, se permitiría el transporte de pasajeros norteamericanos, siempre y cuando se hiciese a bordo de transatlánticos que siguiesen determinadas rutas, ostentasen ciertos distintivos y no transportasen contrabando. Estados Unidos replicó rompiendo relaciones con Alemania pero no con sus aliados y, posteriormente, el 6 de abril de 1.917, declaró la guerra a los Imperios Centrales, en base a que la guerra que hacían los submarinos "era una guerra contra la Humanidad".

Sin embargo, la razón fue al parecer otra.

En enero de 1.917, Zimmerman, ministro alemán de Asuntos Exteriores, envió dos telegramas a los embajadores de su país en Washington y Méjico. El servicio de escucha de los servicios secretos del Almirantazgo inglés, captó, criptoanalizó y obtuvo el texto en claro del primero, entregandolo al ministro inglés de Asuntos Exteriores, lord Balfour, quien lo entregó al embajador de Estados Unidos en Londres, el cual, a su vez, lo reexpidió a Washington.

El texto del telegrama venía a decir que Alemania pensaba iniciar, en febrero, una campaña submarina masiva y sin restricciones, y temía que al hacer pública esta resolución, Estados Unidos se decidiesen a declararle la guerra. Ante esta eventualidad, los Imperios Centrales estaban dispuestos a concertar una alianza con Méjico, ofreciendo a ese país por su cooperación, un concurso económico ilimitado y la garantía de recuperar los territorios perdidos de Nuevo Méjico, Tejas y Arizona. El embajador alemán en Washington debía entablar urgentes negociaciones en este sentido con el gobierno mejicano y actuar, a la vez, cerca del Japón para inducirle también a la lucha.

El texto del telegrama de Zimmerman, facilitado interesadamente por los servicios secretos británicos, dio a los Estados Unidos el sentimiento de frontera que no había tenido durante ciento cuarenta años de historia.

El cese del embajador alemán no modificó la posición de Alemania que, de nuevo, envía a su sustituto en Washington un telegrama en el que le indicaba que tomase en sus manos la cuestión de la alianza con Méjico, pero que no concluyese el Tratado, ya que éste dependía de la ruptura con Estados Unidos. Telegrama que igualmente fue criptoanalizado con éxito en Londres y enviado a Washington.[96]

La guerra submarina se llevó consigo al fondo del mar un total de 14.000 vidas humanas; la opinión pública americana apoyaba cada vez más

la entrada en guerra de Estados Unidos, junto a las potencias aliadas. Pero, a pesar de todo, el presidente Wilson contemporizaba.

Las distintas peripecias por las que atravesó el telegrama, unas criptográficas y otras con bastante menor contenido estadístico, hizo que su explosivo texto fuese conocido por Estados Unidos y fue la gota que colmó el vaso y convenció a América para que entrara en guerra contra Alemania.

b) La Enigma.

Con la máquina de cifrar "Enigma", todo parecía indicar que los alemanes habían descubierto un sistema impenetrable. Sin embargo, el nombre de Enigma se ha unido a uno de los mayores éxitos criptoanalíticos de los Aliados en la Segunda Guerra Mundial.

Al final fue forzada, entre otras cosas, por errores cometidos por los criptólogos alemanes, los servicios de algún espía de esa nacionalidad y, sobre todo, el genio de tres universitarios expertos matemáticos del Servicio Criptográfico Militar de Varsovia.

Sun Tzu, en "El arte de la guerra", decía que: "Existen cinco clases de espías: el espía nativo, el espía interno, el doble agente, el espía liquidable y el espía flotante. cuando están activos todos ellos, nadie conoce sus rutas: a esto se le llama genio organizativo, y se aplica al gobernante.- Los espías nativos se contratan entre los habitantes de una localidad. Los espías internos se contratan entre los funcionarios enemigos. Los agentes dobles se contratan entre los espías enemigos. Los espías liquidables

transmiten falsos datos a los espías enemigos. Los espías flotantes vuelven para traer sus informes",[97] de todo ello pudo haber entorno a la máquina Enigma.

Ya en el verano de 1.939 varios jefes de los Servicios Secretos francés y británicos se reunieron con sus homólogos polacos. Estos desvelaron que sus técnicos habían conseguido resolver la parte teórica del descifrado de Enigma.

Pero el éxito teórico, requería la tecnología adecuada para explotarlo. Los avances en criptografía de los británicos fue lo que permitió montar la máquina para explotar el logro criptoanalítico. Estas máquinas actuaban como cribadoras de cifrado.

Los ingleses -ayudados por polacos como Marian Rejewski, Henri Zigalski y Jerzy Rozicki- recurrieron a máquinas de cálculo gigantescas que recibieron varios nombres, entre ellos el de Bomba o el de Colosos.

Al grupo de contraespionaje británico pertenecía Alan Turing (1.912-1.954), uno de los más famosos matemáticos de nuestro siglo, que investigó sobre el concepto lógico matemático de calculabilidad.

El inglés Frederic Winterbotham, en 1.995, ha escrito The Ultra Secret, donde se explican la mayor parte de las victorias aliadas durante la Segunda Guerra Mundial. Según el libro "Ultra " era el nombre de la organización secreta británica, con mas de 10.000 personas entre civiles y militares, encargada de desmantelar el sistema de cifrado alemán y de explotarlo

para usos militares y políticos. Las redes alemanas quedaron al alcance aliado a partir de 1.941-42, a partir de entonces, los aliados pudieron conocer los planes del ejercito alemán.[98]

¿Por qué se mantuvo el secreto tanto tiempo?, porque las dos potencias, EE.UU. e Inglaterra, pretendían seguir aprovechándose de su acceso a la máquina de origen alemán, después de 1.945.

Para ello realizaron una verdadera siembra de ejemplares de Enigma en diversos países que, al emplearlas en sus cancillerías, convirtieron en transparentes sus comunicaciones diplomáticas. La URSS no llegó a utilizarla porque sus servicios le habían revelado la operación desde el principio.[99]

El resultado positivo del criptoanálisis efectuado sobre los mensajes alemanes se mantuvo en secreto hasta 1.976, con lo que, el hasta entonces primer ordenador de la Universidad de Pennsylvania, el ENIAC -Electronic Numerical Integrator and Calculator-, pasó a ser el número once, pues durante la guerra se construyeron diez Colossus.[100]

Estas máquinas utilizaron por primera vez células fotoeléctricas, papel continuo y válvulas electrónicas.

c) Pearl Harbour.

Durante la Segunda Guerra Mundial, el Código Secreto de la Marina Imperial Japonesa, también cayó en manos norteamericanas.

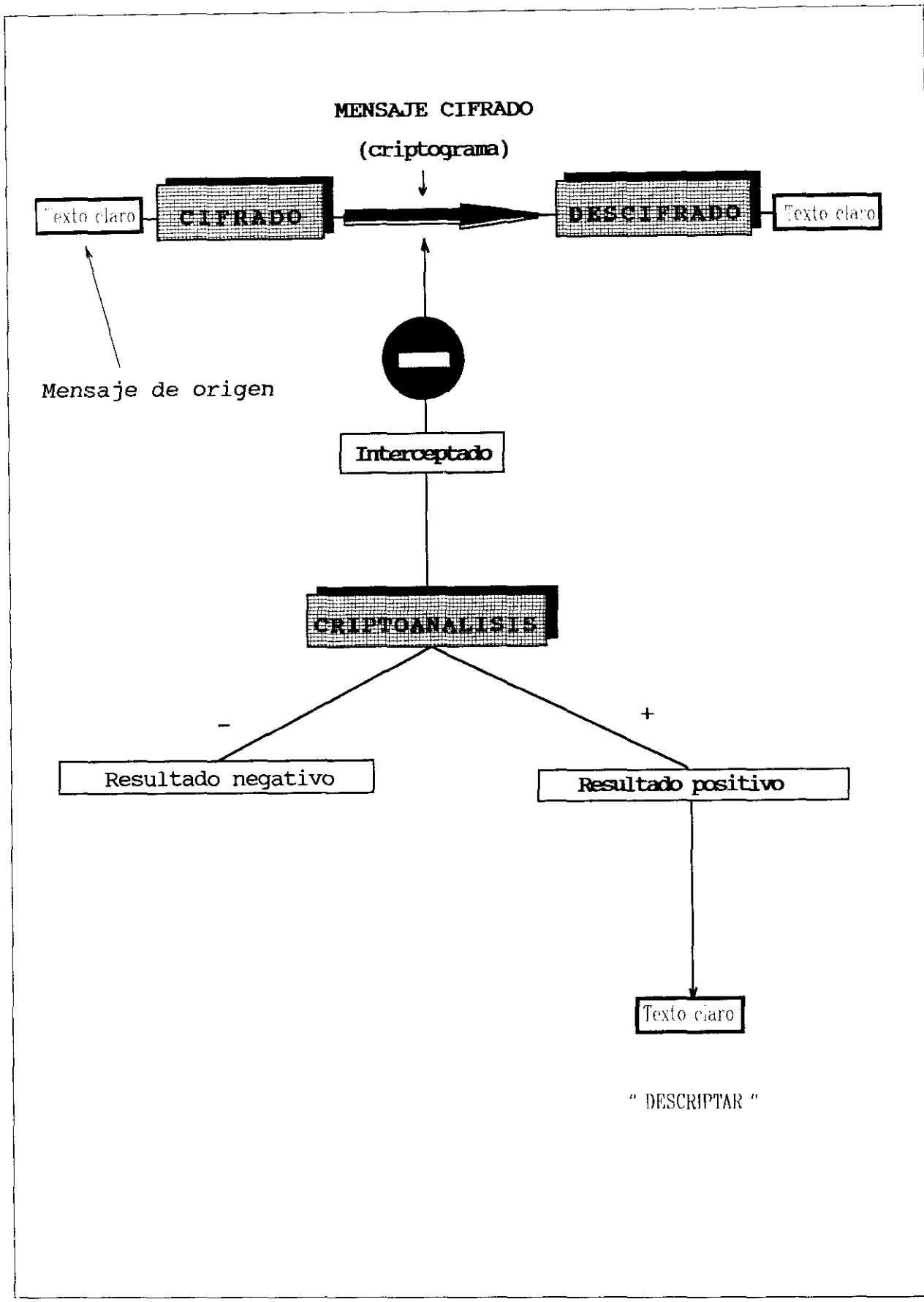
En mayo de 1.940, un tornado alcanzó en el mar de Behring a una embarcación japonesa que se dedicaba a la caza de focas, que junto con sus tripulantes se perdieron junto a las islas San Mateo. Tres días después, un ballenero noruego recogía el cadáver del capitán japonés.

Antes de arrojar el cuerpo del capitán al mar, los noruegos separaron algunos objetos que llevaba consigo, entre ellos un pequeño libro, con pastas de plomo, que más que para su protección, servían de peso que garantizase su hundimiento y salvarlo así de caer en manos indiscretas. Lo que en este caso no ocurrió, al sorprender posiblemente la muerte al capitán llevándolo colgado del cuello.

El libro fue entregado por el ballenero a un guardacostas norteamericano, su comandante se dio cuenta que tenía en sus manos el Código Secreto de la Marina Imperial Japonesa y ordenó poner rumbo a Dutch Harbour a toda máquina.

No ha de extrañar que tan importante hallazgo estuviese en manos de un cazador de focas, puesto que los japoneses solían dar el mando de sus pesqueros a excelentes oficiales de su Armada, los cuales se dedicaban sencillamente a tareas de espionaje.

Este hecho fue guardado en el más absoluto de los secretos por los norteamericanos, que disponían, desde 1.940, del código secreto con el que, posteriormente, fueron cifradas las órdenes preparatorias del ataque nipón a Pearl Harbour.


MENSAJE CIFRADO
(criptograma)
Texto claro
CIFRADO
DESCIFRADO
Texto claro
Mensaje de origen
Interceptado
CRIPTOANALISIS
-
+
Resultado negativo
Resultado positivo
Texto claro
" DESCRIPTAR "

Sin embargo, a principios de 1.943, algo debió sospechar Tokio, ya que comunicó a su flota la decisión de cambiar el código secreto. Esta medida, que en sí misma era acertada, fue comunicada por un radio que fue cifrado con el antiguo código, y en el que se advertía, además -y como colmo de errores- que la nueva clave se transportaría y distribuiría a bordo del *Tami Maru*, lo que dio lugar a que la aviación norteamericana le destruyese.[101]

Esta imposibilidad de cambiar el código secreto prolongó la utilización del antiguo y, el 17 de abril de 1.943 fue interceptado por las escuchas norteamericanas un mensaje cifrado japonés procedente de Truck y llevaba el indicativo de Yamamoto. Descifrado rápidamente gracias al código localizado al pesquero japonés, se conoció la existencia de una visita de inspección del Almirante Yamamoto a Bougainville, lo que dio lugar al ataque al avión que le transportaba, donde murió carbonizado.

Es difícil evaluar el provecho obtenido de estos éxitos criptoanalíticos, que proporcionaron a los aliados, un valioso conocimiento previo de las intenciones enemigas.

Menos brillantes, más silenciosos, pero no por ello de menor importancia, aunque generalmente desconocidos, son los éxitos diarios que la criptografía viene proporcionando durante siglos, precisamente para evitar que se tenga acceso a ese conocimiento previo. Es más que probable que los servicios de descriptación de los alemanes y japoneses estuvieran intentando

lo mismo, con respecto a los códigos aliados. Es un éxito aún de mayor importancia que el de los hechos relatados, el que los servicios de criptografía aliados lo impidieran.

2.- Ultima década.

Acontecimientos más recientes siguen manteniendo vigente la importancia de la batalla silenciosa de las comunicaciones.

Aunque rara vez transcienden, en la última década no faltan hechos de violaciones de comunicaciones gubernamentales dados a conocer a la opinión pública.

Durante la guerra de Las Malvinas, en 1.982, Argentina descubrió que sus códigos secretos de comunicaciones habían sido *"rotos"* por los británicos. Los equipos tenían origen europeo, y "para evitar la trampa", se apeló a métodos alternativos, según reveló en su momento Business Week. [102]

Con ocasión del bombardeo por la fuerza aérea norteamericana de objetivos libios, en 1.986, cuando todo estuvo a punto, desde las centrales de inteligencia occidentales pulverizaron las claves cifradas del gobierno de Trípoli, protegidas por equipos europeos del mismo origen que los utilizados por Argentina durante la guerra de Las Malvinas.

El Financial Times, de Londres publicó entonces que las comunicaciones libias eran transparentes, porque los equipos de origen europeo con que se protegían, podían ser *"penetrados"*, o se los había provisto de claves

cuyos algoritmos podían ser descubiertos a voluntad, por designios de su fabricante.[103]

Ya en la década de los noventa, el 3 de febrero de 1.994, el diario LA RAZON de Buenos Aires publica un artículo, a toda pagina, que titula "Confesiones del espía del siglo", sospechoso de vender equipos de cifrado que no ocultaban nada.

En este artículo se recoge la noticia, difundida en su día por los medios europeos, de la detención en Teherán, en marzo de 1.992,[104] de un ingeniero de la firma CRYPTO, A.G., que fundara el prestigioso criptólogo Boris Hagelin (1.892-1.983), en 1.952, dedicada a la fabricación de "aparatos de cifrado para la transmisión de información y suministra sus productos a más de 120 países".[105]

Se da la circunstancia, según Frank Garbely, periodista helvético, que Boris Hagelin formó parte del equipo que logró desentrañar las claves de las comunicaciones secretas de la célebre Enigma.[106]

Tras la salida de prisión, después de nueve meses en las cárceles de Teherán, el ingeniero fue despedido por su empresa,[107] y, en un reportaje a la televisión europea, en 1.994, viene a actualizar la discusión de, ¿hasta dónde son seguros los equipos de una empresa que deberían garantizar claves inviolables en las comunicaciones?.

Según publicó la revista española TIEMPO, el 29 de diciembre de 1.995, la empresa fundada por Boris Hagelin en 1.952, "estuvo

teledirigida desde su creación por norteamericanos y alemanes y que el secreto de las comunicaciones al más alto nivel ha sido una ilusión desde, al menos mediados de los años 50, cuando Hagelin puso en marcha su compañía. El sueco fue, por lo tanto, instrumento de una colosal misión de espionaje a largo plazo".[108]

F.L. Bauer considera que la desconfianza sentida por algunos ciudadanos o corporaciones contra el poder del estado no ha disminuido y, con respecto a los suministradores de productos criptológicos considera que el vendedor comercial es un tercero que está fuera del balanceo de los derechos constitucionales sobre privacidad y los derechos del estado como derecho imperativo, pero no se puede perder de vista su importancia económica.

El vendedor, en su propio interés, tiene buenas relaciones con ambos: el ciudadano como potencial cliente y el estado como supervisor y, a veces, también cliente.

Y textualmente dice: "En el mejor de los casos, el vendedor es un honesto intermediario entre estado y ciudadano. No obstante, este papel es dificultado por una cierta falta de honestidad derivada de la presión de las autoridades estatales sobre los vendedores para influir sobre sus negocios con clientes extranjeros que no hacen para sus negocios internos con el propio estado".[109]

En 1.957, hubo informaciones sobre estrechos contactos entre William F. Friedman -probablemente el más importante criptólogo de Estados Unidos en los tiempos modernos- y Boris Hagelin que levantaron sospechas.[110]

Por el momento, aún resulta difícil conocer exactamente lo ocurrido en CRYPTO A.G., sus causas y alcance, y menos aún, si estamos ante un caso de criptoanálisis o estamos ante un episodio del espionaje mundial, general e indiscriminado, en su versión más actualizada y futurista, que poco tendría que ver con la ciencia criptológica.

El hecho preocupó y desató gran polémica en Europa.

El artículo que apareció en LA RAZON de Buenos Aires, -al margen de las anécdotas del hombre- insinúa unos hechos que, de ser ciertos, tendrían consecuencias, de magnitud y alcance desconocidos:

1.- En el plano político internacional, puede suponer un escándalo a escala mundial con efectos muy negativos, fundamentalmente, para Alemania, EE.UU, Gran Bretaña y Francia y, eventualmente, el resto de los países occidentales, -en el caso de que fuese conocido y "tolerado" por sus gobiernos-, así como con incidencia en todo el sistema de valores que representan.

2.- En el plano criptológico, afectaría a la credibilidad de la criptología como instrumento eficaz para garantizar la seguridad de la infor-

mación y, aunque no parece probable, podría alentar el uso de formas alternativas de protección de información (clásicas o por descubrir),

3.- En el plano tecnológico, sería fundamental conocer el nivel tecnológico requerido para que las afirmaciones efectuadas sean realidades tangibles, así como saber quienes están en condiciones de poseer esa tecnología.

4.- Todo ello, podría dar lugar a pensar que tal vez habríamos asistido al acontecimiento histórico relacionado con la criptología de mayor importancia en los últimos tiempos, que pondría punto final a la política mundial de cifrado de la "guerra fría" y marcaría un antes y un después de la política criptológica, la cual necesita una redefinición que dé respuesta a las exigencias, de todo tipo, derivadas de una nueva configuración política mundial en el próximo siglo.

En 1.994, en la lista de productos y programas para cifrado, identificados por la SPA (Software Publishers Association) de fecha 22 de marzo, no aparece incluido ningún producto de la firma CRYPTO A.G.[111]

Otro acontecimiento que pone en evidencia la vulnerabilidad de comunicaciones gubernamentales es el que recoge el mes de marzo de 1.997, The New York Times, que informa acerca de que agentes secretos estadounidenses interceptaron en 1.996 las comunicaciones entre Pekín y los representantes diplomáticos de China en EE. UU. Los agentes pertenecían a la Agencia Nacional de Seguridad (NSA), que se dedica a proteger las

comunicaciones secretas norteamericanas y a localizar y descifrar las extranjeras.[112]

En todo caso, el gran problema no es solo que el criptoanálisis permita forzar, en un momento determinado, un algoritmo. Es mucho más importante para la organización que padece los efectos del criptoanálisis, conocer cuando se ha producido y, mejor aún, cuando se puede producir, para evitarlo. Y esto, ya no es tarea de la criptología sino, de los Servicios de Inteligencia.

En los modernos sistemas de cifrado se tiene en cuenta la "cripto-complejidad" para dar fortaleza al sistema.

Durante el diseño y estudio del sistema de cifrado se considera al oponente y las técnicas que este tiene a su disposición para violar los mensajes.

En el criptoanálisis se utilizan un conjunto de técnicas que van desde el análisis estadístico hasta las más sofisticadas técnicas computacionales.

El trabajo de criptoanálisis requiere obtener información cifrada, -lo que supone una vulneración del método de comunicación o almacena-miento-, sobre la cual aplica sus técnicas el criptoanalista.

Los diseñadores de sistemas criptográficos establecen un compromiso entre los costes de operaciones de cifrado y descifrado -que

deben ser sencillas- y las operaciones de criptoanálisis, que deben ser muy complejas y de coste muy elevado.

La meta de todo criptólogo, diseñador de un sistema de cifra, es que la tarea del criptoanalista no pueda ser realizada con los recursos de cálculo existentes.

El sistema que cumple estas condiciones es computacionalmente seguro.

Pero los recursos de cálculo al alcance del criptoanálisis no son indiferentes a las necesidades de tiempo de cálculo y de capacidad de memoria de ordenador que precisa para un análisis de un criptosistema. La combinación de ambos es lo que se conoce como compromisos entre tiempo y memoria.

El criptoanálisis permite cualquier punto intermedio entre el compromiso de tiempo y memoria y es fundamental estudiar las posibilidades que existen en el citado compromiso.[113]

Hay algunos sistemas de cifrado en los que se podría hacer un estudio exhaustivo de cifrado, mediante el uso de una máquina que podría realizar su trabajo en minutos, pero hay otros para los que se requeriría centenares o miles de años y, otros, en los que sería imposible la búsqueda por cualquier método conocido, en ellos se logra el ideal del diseño criptológico: un sistema computacionalmente seguro contra los ataques del criptoanálisis.

En todo caso, el criptoanálisis positivo de un equipo no suele ser conocido, al menos mientras está siendo útil a quienes la consiguen. Su beneficiario trata de mantenerla en secreto, para provecho propio o de tercero, el máximo tiempo posible.

Rara vez transciende y, generalmente, se haya muy próxima a las operaciones de inteligencia de los distintos países, no llegando a conocerse, en ocasiones, donde finaliza el criptoanálisis y dónde comienza la acción de inteligencia, cuando no, como es lo más usual, inteligencia y criptoanlisis aparecen unidos, completándose recíprocamente.

Con los antiguos procedimientos manuales y lentos de criptoanálisis, era suficiente una seguridad probable, pues en la mayoría de los casos, se lograba un resultado positivo cuando la información del documento había perdido toda validez.

Si el criptoanálisis tuvo éxitos de importancia histórica y social fue porque al igual que era lento el proceso de análisis, lo era también el cambio de claves.

En la actualidad, con el uso de ordenadores para el criptoanálisis, los sistemas criptográficos tienen que tener propiedades matemáticas que los hagan invulnerables, no solo en el presente, sino también en el futuro previsible, por lo que los sistemas criptográficos tienen que ser computacionalmente o incondicionalmente seguros.[114]

La potencia de los algoritmos, y las consiguientes dificultades y coste para obtener un criptoanálisis positivo, podría dar paso a una situación en la que se genere un gran mercado mundial de venta ilegal de información, con aumento de las acciones de inteligencia que poco o nada tienen que ver con la Criptología, en su dimensión científica.

Alvín Tolffler, en su libro titulado "Las guerras del futuro" -La supervivencia en el alba del siglo XXI-, publicado en 1.994, entre otras cosas dice:

"Es posible que llegue el día, si aún no se ha dado el caso, en el que se vendan armas de componentes suficientemente 'inteligentes' para limitar (o prevenir) su empleo bajo condiciones especificadas de antemano".

Los fabricantes de armas norteamericanos, franceses o rusos o de cualquier otro país de economía avanzada podrían, por ejemplo, introducir subrepticiamente chips autodestructivos en los aviones, las plataformas de cohetes, los carros de combate o los misiles que exporten, previendo la posibilidad de que el comprador se torne enemigo o venda el arma en cuestión a un adversario.

Unas instrucciones determinarían la expulsión del piloto de un caza o la explosión de la aeronave. Tecnologías futuras basada en datos de satélites de localización global serían verosímilmente capaces de programar un sistema de armas que fallase o un sistema de navegación que no funcio-

nara una vez que el vuelo superase los límites geográficos fijados de antemano.

¿Son especulaciones o simple ciencia ficción?. No lo cree así un destacado ejecutivo de la industria bélica. De hecho, nos dijo: 'Nosotros podríamos codificar todos los aviones que vendemos; podríamos incluir un identificador en todos los chips de aviones que exportamos a Oriente Próximo... En caso de acción hostil, nosotros seríamos capaces de establecer comunicación con ese *chip* y lograr que fallase. Esto ha de suceder de una forma o de otra'. Ese ejecutivo no fue el único en hacer referencia a semejante posibilidad.

¿Lograría encontrar el comprador el componente introducido, prestando gran atención a lo que compre? 'Es muy difícil -dicen los especialistas-, extremadamente difícil... casi imposible'.

De ser así, éste constituye un ejemplo de actividad bélica muy avanzada del conocimiento".[115]

Pero, de igual modo que los fabricantes de armas son capaces de trucar sus exportaciones, en base a la misma tecnología y en nombre de la paz, se podría acceder a los procesos de fabricación y reprogramar ciertos sistemas para que no funcionen nunca en combate.

¿Se podría aplicar toda esta tecnología a la criptología?... ¿por qué no?. Pero... ¿quien controlaría todo ese proceso?.

CRIPTOANÁLISIS
DE UN TEXTO CIFRADO POR EL SISTEMA "JULIO CESAR"

1.- Texto cifrado: JWXLQNLN

2.- Desarrollo alfabético de cada letra del texto cifrado:

J	**W**	**X**	**L**	**Q**	**N**	**L**	**N**
k	x	y	m	r	o	m	o
l	y	z	n	s	p	n	p
m	z	a	o	t	q	o	q
n	a	b	p	u	r	p	r
o	b	c	q	v	s	q	s
p	c	d	r	w	t	r	t
q	d	e	s	x	u	s	u
r	e	f	t	y	v	t	v
s	f	g	u	z	w	u	w
t	g	h	v	a	x	v	x
u	h	i	w	b	y	w	y
v	i	j	x	c	z	x	z
w	j	k	y	d	a	y	a
x	k	l	z	e	b	z	b
y	l	m	a	f	c	a	c
z	m	n	b	g	d	b	d
a	***n***	***o***	***c***	***h***	***e***	***c***	***e***
b	o	p	d	i	f	d	f
c	p	q	e	j	g	e	g
d	q	r	f	k	h	f	h
e	r	s	g	l	i	g	i
f	s	t	h	m	j	h	j
g	t	u	i	n	k	i	k
h	u	v	j	o	l	j	l
i	v	w	k	p	m	k	m

3.- Resultado positivo del criptoanálisis:
Texto en claro: ***ANOCHECE***

2.5.- LA CRIPTOLOGÍA COMO PARCELA DE LA REALIDAD.

Una de las formas tradicionales de protección de la información, una vez determinado qué ha de protegerse ,-mediante la delimitación de los ámbitos de confidencialidad-, y con qué niveles de seguridad, consiste en la aplicación de técnicas criptográficas.

La "protección criptológica" de la información, como parcela de la realidad, para su plenitud de funcionamiento requiere, además de su coherencia interna como sistema, considerar el campo de relaciones en que se desenvuelve, constituido por la realidad política, económica, tecnológica, social, cultural y administrativa de la organización a que se refiera, en todas sus dimensiones, tanto internas como externas, lo que exige el conocimiento de la propia organización y del medio en el que opera, tanto nacional como internacional y , además, actuar en coherencia con todo ello.

La viabilidad y vigencia de la "protección criptológica" está condicionada a su manifestación como sistema que, para que sea armónico, requiere concordancia entre el nivel de conciencia de su realidad (sociológica, jurídica, política, tecnológica, etc.), con los medios de que dispone y los problemas que tiene que afrontar, centrado, esencialmente, en la protección de la información.

La "protección criptológica" como toda realidad humana evoluciona y, a medida que cambian o se modifican los problemas, requiere una readaptación constante de conocimientos y medios para su tratamiento, lo

que conseguirá a través de la información, la investigación, el análisis; y los medios materiales, legales, tecnológicos, organizativos, humanos, etc.

En definitiva, el grado de eficacia del funcionamiento de la "protección criptológica" de la información, en su conjunto, vendrá determinado por el grado de coherencia alcanzado en la integración del conocimiento con los medios disponibles y los problemas a resolver.

La Criptología, como ciencia, -o la "protección criptológica", como consecuencia de la acción de la misma-, son realidades claramente diferenciadas y caracterizadas por su función.

La Criptología como toda parcela de la realidad con entidad propia, se manifiestan como un sistema y con ello tiene directa relación su vigencia, su viabilidad, su plenitud como tal. A su vez, la Criptología, es parte de otras parcelas de la realidad, de distinta naturaleza (empresarial, administrativa o política), de nivel superior y, junto a muchas otras, conforman los distintos niveles de la realidad nacional e internacional.

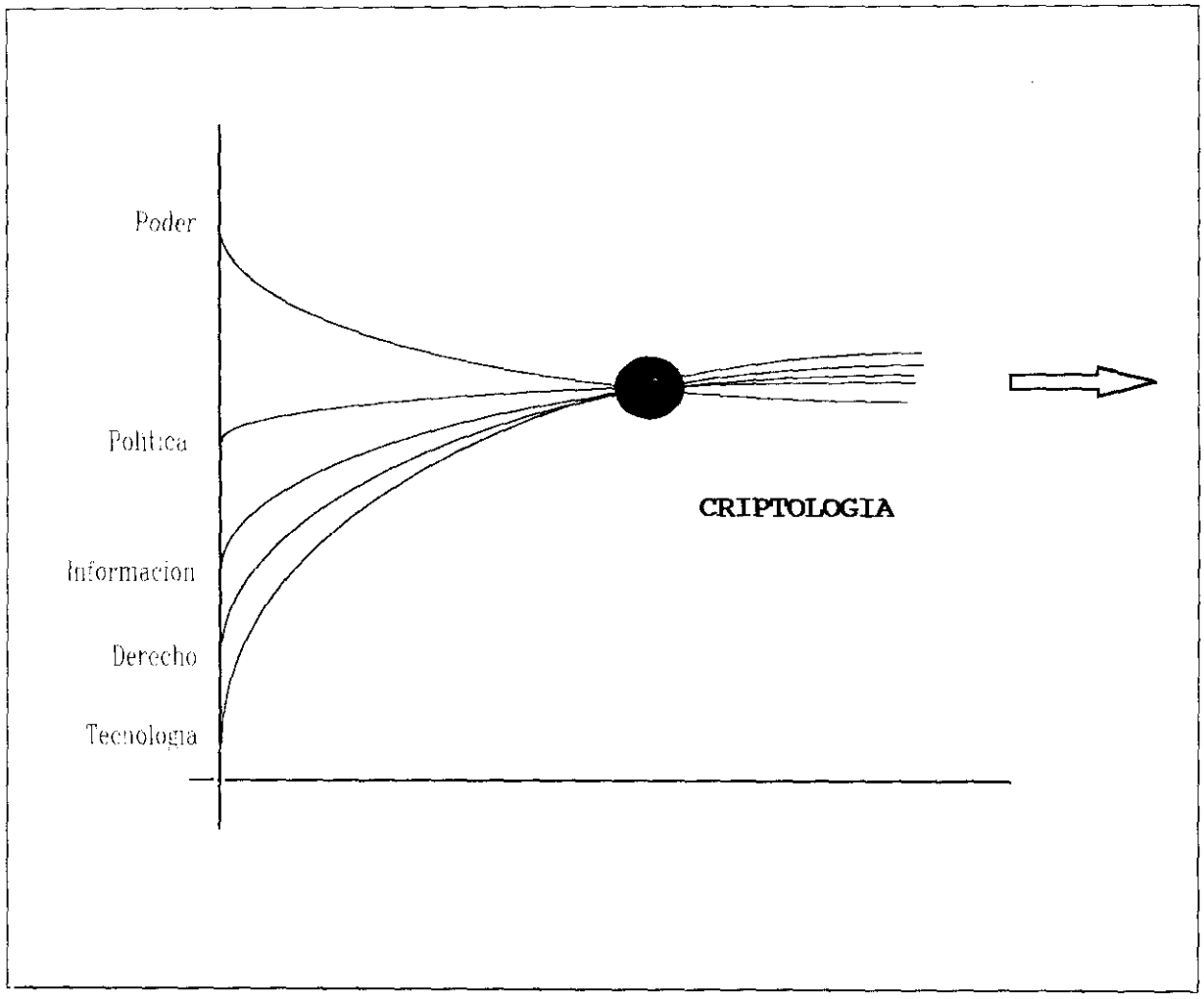
En todo este juego de círculos concéntricos, tangentes y secantes, en distintos planos, verticales, horizontales o inclinados, el ámbito de actuación consistente y completo, gobernado desde el nivel superior, que marca la estrategia y sentido de actuación del conjunto es el Estado y la sociedad, (las organizaciones supranacionales serían producto de la voluntad de los Estados y su existencia estaría subordinada a la voluntad de estos) en los que

la Criptología sería un instrumento, que tiene razón de ser en orden al cumplimiento de un fin, sin el cual, carecería de sentido.

La Criptología ha de responder, de modo directo, a un sentido de actuación marcado desde el nivel superior. Corresponde a los criptólogos el máximo aprovechamiento de los últimos desarrollos de esta ciencia para cumplir con eficacia el sentido de actuación marcado por el nivel superior. Si se logra, se habrá conseguido la protección efectiva de los intereses nacionales.[116]

El Estado como parcela de la realidad constituido por diversos niveles, implica la necesidad de un perfecto funcionamiento de los elementos que lo conforman y exige que cada uno se desenvuelva según su propia naturaleza.

FACTORES QUE CONVERGEN EN LA CRIPTOLOGIA



[1] Sgarro, A., "Códigos Secretos", Edit. Pirámide, 1.990.
[2] Pastor Franco, J, "Criptografía moderna, informática y sociedad", Seminario Universidad de Zaragoza, octubre 1.989, pág. 2.
[3] Real Academia Española, Diccionario de la Lengua, Tomo I, pág. 314, acepción primera.
[4] Pastor Franco, J., op. cit.
[5] Sgarro, A., op. cit.
[6] Centro Superior de Información de la Defensa, Glosario de término de Criptología, edición revisada, marzo de 1.993.
[7] Centro Superior de Información de la Defensa, op. cit.
[8] Rodríguez Prieto, A., "Protección de la Información", Paraninfo, Madrid, 1.996.
[9] Martínez Lage, S., "Breve Diccionario Diplomático", Ministerio de Asuntos Exteriores, Oficina de Información Diplomática, 1.982.
[10] Centro Superior de Información de la Defensa, op. cit.
[11] Martínez Lage, S., op. cit.
[12] Bauer, F.L., "Descrypted Secrets", Methods and Maxims of Cryptology. Springer Verlag, Berlín 1.997, Parte 1.
[13] Diccionario de la Lengua Española. Real Academia, vigésima edición, 1.984, tomo I, pág. 397.
[14] Sgarro, A., op. cit.
[15] Pastor Franco, J., op. cit.
[16] Centro Superior de Información de la Defensa, op. cit.
[17] Diccionario Básico Espasa, Séptima Edición, Espasa Calpe, Madrid 1.989, Tomo 2, pág. 1.550.
[18] Ribagorda Garnacho, A., "Glosario de Términos de Seguridad de las T.I.", Ediciones CODA, Madrid, 1.997.
[19] Centro Superior de Información de la Defensa, op. cit.
[20] Urquía Gómez, A., "Diccionario Técnico Militar, inglés-español, español-inglés, Ediciones Agulló, Madrid, 1.980, pág. 451.
[21] Centro Superior de Información de la Defensa, op. cit.
[22] Centro Superior de Información de la Defensa, op. cit.
[23] Centro Superior de Información de la Defensa,op. cit.
[24] Ribagorda Garnacho, A., op. cit.
[25] Centro Superior de Información de la Defensa, op. cit.
[26] Ribagorda Garnacho, A., op. cit.
[27] Molina Mateos, J.M., op. cit., pág. 51.
[28] Sgarro, A., op. cit.
[29] Ribagorda Garnacho,A., op. cit.
[30] Centro Superior de Información de la Defensa, op. cit.
[31] Centro Superior de Información de la Defensa, op. cit.
[32] Ribagorda Garnacho, A., op. cit.
[33] Diccionario de la Real Academia Española de la Lengua, op. cit.
[34] Centro Superior de Información de la Defensa, op. cit.
[35] Ribagorda Garnacho, A., op. cit.
[36] Bauer, F.L., op. cit.

[37] Ocasar y Vigil de Quiñones, J.L., "Los albores de la criptología", Criptosistemas nº 1, abril de 1.996, Revista de la Asociación Española de Criptología.
[38] Muñoz, J.L., "La Criptografía en anécdotas", Ediciones Ejército, Madrid, 1.955.
[39] Enciclopedia Universal Ilustrada, Espasa Calpe.
[40] Muñoz, J.L., op. cit.
[41] Drosnin, M. "El código secretode la Biblia", traducción de Andy Ehrenhaus, Edit. Planeta, Barcelona, 1.997.
[42] Rips, E, tomado de Drosnin, M., op. cit.
[43] Spes, Gran Consultor, Diccionario de Técnica y Tecnología, Edit. Bibliograf, Barcelona, 1.996, pág. 277.
[44] Drosnin, M., op. cit. pág. 24.
[45] Drosnin, M., op. cit. pág. 20.
[46] Drosnin, M., op. cit. pág. 21
[47] Drosnin, M., op. cit. pág. 21.
[48] Drosnin, M., op. cit. pág. 231.
[49] Muñoz, J.L., op. cit.
[50] Sgarro, A., op. cit.
[51] Muñoz, J.L., op. cit.
[52] Muñoz, J.L., op. cit.
[53] Rodriguez Prieto, op. cit.
[54] Moreyra, C.A., "Los Criptogramas de Sta. Teresa", Dean Funes, Córdoba, Argentina, 1.964.
[55] Sgarro, A., op. cit.
[56] Bauer, F.L., op. cit.
[57] Centro Superior de Información de la Defensa, op. cit.
[58] Centro Superior de Información de la Defensa, op. cit.
[59] Sgarro, A., op. cit., pág. 75.
[60] Centro Superior de Información de la Defensa, op. cit.
[61] Sgarro, A., op. cit.
[62] Lozano Bartoluzzi, P., "Estructura dinámica de las relaciones internacionales", Edit. Mitre, Barcelona, 1.,987, pág. 99.
[63] Lozano Bertoluzzi, P., op. cit.
[64] Kissinger, H., "Diplomacia"Ediciones B, 1.996, págs. 24,26,28,34,41 y 498.
[65] Revenga Sánchez, M., "El imperio de la política", Edit. Ariel, 1.995, pág. 89.
[66] Revenga Sánchez, M., op. cit.
[67] Pastor Franco, J., op. cit.
[68] Sgarro, A., op. cit.
[69] Rodríguez Prieto, A., op. cit.
[70] Rodríguez Prieto, A., op. cit.
[71] Morant Ramón, J.L., op. cit.
[72] Morant Ramón, J.L., op. cit.
[73] Morant Ramón, J.L., op. cit.
[74] Rodríguez Prieto, A., op. cit., pág. 210.

[75] Bauer, F.L., op. cit.
[76] Bauer, F.L., op. cit.
[77] Pastor Franco, J., op. cit.
[78] OMNISEC, A.G., firma suiza dedicada a la Criptología (fondo documental), 1.994.
[79] Toffler, A. y H., op. cit. pág. 206.
[80] OMNISEC, A.G., Regensdorf, fondo documental, Suiza, 1.994.
[81] Molina Mateos, J.M., op. cit., pág. 58.
[82] Rodríguez Prieto, A., op. cit.
[83] Rodríguez Prieto, A., op. cit.
[84] Bauer, F.L., op. cit., pág. 146.
[85] Centro Superior de Información de la Defensa, op. cit.
[86] Morant Ramón, J.L., op. cit.
[87] Morant Ramón, J.L., op. cit.
[88] Bauer, F.L., op. cit. Part. II-
[89] Centro Superior de Información de la Defensa, op. cit.
[90] Sgarro, A., op. cit.
[91] Tiempo, revista semanal.
[92] Muñoz, J.L., op. cit. pág. 15.
[93] Sgarro, A., op. cit.
[94] Sgarro, A., op. cit.
[95] Ferrero, G., "La unidad del mundo", tomado de Muñoz, J.L, op. cit.
[96] Muñoz, J.L., op. cit.
[97] Tzu, S., "El arte de la guerra", Oxford, 1.963.
[98] El Mundo, 26 de febrero de 1.995.
[99] El Mundo, 26 de febrero de 1.995. Ediciones B, 1.996.
[100] Pastor Franco, J., op. cit.
[101] Muñoz, J.L., op. cit.
[102] La Razón de Buenos Aires, de 3 de febrero de 1.994.
[103] La Razón de Buenos Aires, de 3 de febrero de 1.994.
[104] Revista Tiempo, 23 de noviembre de 1.992, pag. 41.
[105] Zn Zuger Nachrichten, 11 de marzo de 1.993, nº 58.
[106] Garbely, F., Revista Tiempo, 29 de diciembre de 1.995.
[107] Zeitung, 14 de marzo de 1.993.
[108] Revista Tiempo, 29 de diciembre de 1.995, nº 713, pags. 17,18 y 19.
[109] Bauer, F.L., op. cit. pag. 204.
[110] Bauer, F.L., op. cit. 1.997, pág. 204.
[111] Hoffman, L.J., op. cit. pag. 489-495.
[112] El País, 14 de marzo de 1.997.
[113] Rodríguez Prieto, A., op. cit., pag. 221.
[114] Pastor Franco, J., op. cit.
[115] Toffler, A. y H., op. cit., pags. 325 y 326.
[116] Molina Mateos, op. cit.

CAPITULO III

LA PROTECCIÓN CRIPTOLÓGICA

3.1.- APLICACIÓN DE LA CRIPTOLOGÍA.

Dadas las características de la información y el conocimiento, y el uso de las nuevas tecnologías para su almacenamiento y transmisión, ante la vulneración de la norma, la sanción jurídica es insuficiente, -incluso apelando a la sanción penal-, al no hacer reversible el daño causado.

Las medidas legales son medidas de protección que actúan *"a posteriori"*, y en un entorno tecnológico con grandes dificultades de prueba.

El alto valor de la información y los graves efectos de su violación, de consecuencias imprevisibles e irreparables, en muchos casos, hacen necesario la utilización de medidas de prevención que, *"a priori"*, eviten de forma eficaz que la violación se produzca, e impidan el éxito de eventuales amenazas.[1]

Entre las medidas de prevención para garantizar el secreto de la información y las comunicaciones destacan por su importancia aquellas que permiten la ocultación, disimulación o cifrado de la información y son objeto de la Criptología.

La aplicación de técnicas criptográficas es la solución universalmente aceptada para evitar los actos que puedan vulnerar la información y las comunicaciones -y, en general, evitar cualquier utilización no autorizada-,[2] y es la forma tradicional de preservar la confidencialidad de una red de comunicaciones.

Las medidas criptológicas, son un mero instrumento para la realización efectiva de la protección, que requiere una decisión previa sobre qué ha de protegerse y con qué niveles de seguridad, en el contexto de un sistema de información.

Ante los avances tecnológicos que permiten el acceso a las bases de datos y la interceptación de las transmisiones de todo tipo, efectuadas por cualquier medio, se incrementa la necesidad de uso de aplicaciones criptológicas al nivel adecuado, hasta el extremo de resultar imprescindibles.

La Criptología -o criptografía- ha sido utilizada fundamentalmente en los ámbitos militar, diplomático y empresarial, constituyendo la trilogía clásica de *"cifra militar"*, *"cifra diplomática"* y *"cifra comercial"*.

Actualmente se les podrían añadir muchos otros ámbitos: policial, fiscal, judicial, notarial, sanitario, etc., cuya enumeración, por extensa, tal vez carezca de utilidad, pero de los que sí destacaríamos, por su singularidad e importancia, el destinado a preservar la privacidad del individuo, cuya denominación no alcanzamos a determinar, y bien podría ser el de *"cifra cívica"*, que puede constituir una cifra básica o general, todo ello sin entrar en las múltiples aplicaciones de la criptología en la cotidianeidad, en relación con la protección de información de todo tipo, que ha llevado al uso de expresiones como la de *"criptología de consumo"*.

Pero referirse a protección criptológica es referirse a una amplia gama de posibilidades de protección de distintos niveles e intensidades, por

lo que, solo la decisión de proteger criptológicamente, no es suficiente. Se requiere, además, determinar el nivel de protección dentro de las múltiples opciones que ofrece la Criptología.

La protección criptológica de la información se encuentra sometida a una doble tensión, con tendencia ascendente hacia los máximos niveles de impenetrabilidad cuando se refiere a los altos intereses de la sociedad y del Estado y, orientada hacia niveles de impenetrabilidad relativa, en otros casos y que, básicamente, se corresponden con los dos grandes bloques en que se encuentra agrupada la información: el destinado a garantizar el secreto de las comunicaciones privadas y el constituido por la protección de la información pública.

Sin embargo, en el ámbito de las comunicaciones, con la tecnología actual, y con aplicación de la Criptología, se pueden crear condiciones para que exista un secreto de las comunicaciones sea real y efectivo, a niveles suficientes. Corresponde a los poderes públicos esta responsabilidad.

3.1.1.- CIFRA DIPLOMÁTICA.

La institucionalización de la diplomacia a base de la creación de legaciones permanentes se inicia, según la doctrina, en la república de Venecia durante la segunda mitad del siglo XV. La práctica es seguida por el resto de los Estados italianos, y Fernando el Católico lo introduce en sus

reinos llegando a alcanzar un uso generalizado en Europa en el Siglo XVI. [3]

Los elementos que constituyen el sistema internacional no son homogéneos y aunque teóricamente, hoy, las unidades políticas que le integran son soberanas e iguales jurídicamente, son diferentes en tamaño y en poder.

El medio internacional presenta según Merle las siguientes características:

"1.- Instantaneidad de la transmisión de las informaciones entre los diferentes puntos del sistema.

2.- Aceleración de la rapidez y del volumen de las comunicaciones y del desplazamiento de las personas.

3.- Aumento del volumen de las transacciones monetarias y comerciales.

4.- Advenimiento de una red de instituciones internacionales dotadas de permanencia, universalidad y colegialidad" [4].

Las interacciones provocadas por la combinación de estos factores, se ordenarán en torno a una creciente interdependencia y a un crecimiento de tensiones.

En las relaciones entre los Estados no solo se manifiestan solidaridades o antagonismos externos, sino, también, las alteraciones en el orden

político interno, lo que viene a desdibujar la distinción tradicional entre política interior y política exterior.

El estrechamiento del mundo refuerza la interdependencia de los Estados, pero también contribuye a renovar las tensiones en el interior del sistema internacional, que como todo sistema de relaciones sociales implica una dosis de conflictividad.

El Estado se sitúa como mediador entre las sociedades cerradas que aún son las naciones y la sociedad global que emerge impulsada por factores que escapan al control del Estado.

En este contexto internacional opera actualmente la diplomacia, en el que las nuevas tecnologías están alterando los objetivos nacionales en política exterior, así como influyen directamente en los modos de alcanzarlos.

La red diplomática como medio de comunicación entre gobiernos, para la información y la negociación, se está viendo modificada por el auge de los medios de transporte -especialmente la aviación- y el desarrollo de las comunicaciones.

La importancia creciente de la información en la vida internacional hace que el servicio diplomático de un país sea sus *"ojos y oídos"* en el exterior.

La administración exterior es, en estas circunstancias, agente ejecutivo de una política elaborada por instancias gubernamentales. Para

cuyo diseño y toma de decisiones resulta determinante el conocimiento de las condiciones de evolución de los acontecimientos del Estado receptor, donde se encuentra acreditada, y cuya información al gobierno del Estado al que representan, constituye una de sus principales funciones.

La comunicación de este flujo de información -junto a otros derivados de las relaciones normales entre las misiones diplomáticas y los órganos de la Administración Central- integran el caudal de información selectiva que ha de ser transmitido de forma que sea conocido solamente por los destinatarios, los cuales, en función de criterios preestablecidos, pueden dar un tratamiento que va desde la más amplia difusión hasta la máxima restricción.

El que toda información transmitida por circuitos diplomáticos sea, en principio, selectiva y, fundamentalmente, cuando la información es relativa a intereses de gran valor; ha requerido secularmente el uso de procedimientos que aseguren el carácter restringido o secreto de lo que se comunica; que han evolucionado a lo largo de la historia desde mensajeros, hasta los más modernos desarrollos informáticos y de telecomunicaciones, con la Criptología y la seguridad como elementos prioritarios y determinantes.

Todo ello ha configurado lo que se ha dado en llamar *"cifra diplomática"*, que opera en un contexto constituido por el entorno internacional, en el que la información transmitida puede ser de gran interés para el

estado receptor o para terceros, lo que viene a reforzar que la seguridad de la información sea elemento prioritario de una red de comunicaciones diplomáticas.[5]

Los ámbitos de defensa, política exterior y servicios de inteligencia tradicionalmente han sido, y siguen siendo, generadores de secretos de Estado en su más alto grado y, consiguientemente son usuarios de la protección criptológica en sus más altos niveles.

3.1.1.1.- Real Decreto 632/1.987, de 8 de mayo sobre organización del Estado en el exterior.

El Real Decreto 632/1.987 regula la organización del Estado en el Exterior, tras indicar que a la Administración del Estado en el exterior le corresponde ejecutar la política exterior del Gobierno, señala como rasgo específico de esta Administración el hecho de desarrollar su actividad en el marco del ordenamiento jurídico español, el ordenamiento jurídico internacional y el ordenamiento jurídico interno de cada uno de los países donde ejerce su actividad.

Subraya como objetivo, la necesidad de conseguir una mayor coordinación y eficacia en el Servicio Exterior y concretar y reforzar el principio de unidad de acción exterior; potencia la figura del Jefe de Misión que representa a España y ostenta la máxima autoridad del Estado español ante el estado u Organismo internacional en el que esté acreditado y ejerce la jefatura superior de todo el personal de la Misión.

Para asegurar la eficaz coordinación de la Administración del Estado en el Exterior, el Real Decreto regula también el sistema de comunicaciones oficiales entre los Organismos que la componen y la Administración central, configurándose el Ministerio de Asuntos Exteriores como cauce y agente coordinador y en su artículo 10° dice:

"1.- Las comunicaciones entre las Misiones Diplomáticas, Representaciones Permanentes o Delegaciones y los órganos de la Administración central se canalizarán a través del Ministerio de Asuntos Exteriores. No obstante, por razones de celeridad y eficacia en la gestión, las Consejerías y Agregadurías sectoriales podrán comunicarse directamente con los Departamentos Ministeriales de los que dependan funcionalmente, o con los competentes en la materia de que se trate, y éstos con aquéllas, debiendo en tales casos trasladarse simultáneamente la comunicación de que se trate al Jefe de la Misión diplomática, de la Representación Permanente o Delegación.

2.- Los Servicios e Instituciones de la Administración en el exterior dependientes funcionalmente de otros Ministerios de la Administración del Estado, y que no tengan condición de Oficina Diplomática, se comunicarán directamente con ellos. No obstante, el Ministerio de Asuntos Exteriores y el Jefe de la Misión diplomática podrán recabar la información que estimen oportuna de estos Servicios e Instituciones".

El Real Decreto hace referencia de forma genérica a "las comunicaciones", sin distinguir, por lo que se ha de entender que se refiere a todas.

Las características de la Administración del Estado en el exterior y la creciente internacionalización hace recaer sobre los sistemas de comunicaciones diplomáticas y, consiguientemente, sobre los sistemas criptológicos que eventualmente las protejan, la responsabilidad de disponer de la estructura adecuada de forma que estén en condiciones de dar respuesta satisfactoria a la canalización de las comunicaciones de las Misiones,

Representaciones o Delegaciones y los órganos de la Administración Central.

Incluso la posibilidad de una comunicación directa entre consejerías y Agregadurías con los Departamentos Ministeriales de los que dependen funcionalmente es una posibilidad basada en "razones de celeridad y eficacia en la gestión", por lo que la canalización de estas comunicaciones a través del Ministerio de Asuntos Exteriores sería la norma y el hecho de que se efectúen directamente, sería la excepción, lo que exige a la red diplomática disponer de la estructura adecuada.

Esta interpretación llevaría a consideraciones sobre la "cifra diplomática" que rebasan el ámbito sectorial o departamental y además de las razones derivadas de su propia naturaleza, la sitúan en los niveles de exigencia de un sistema criptológico de Estado, que requeriría estar en condiciones de dar satisfacción, -a través de la extensa red de representaciones diplomáticas y consulares en todo el mundo-, a las necesidades de comunicaciones seguras que los intereses del Estado en el exterior. demandan.

3.1.2.- CIFRA MILITAR.

El fin de la guerra fría ha cambiado los parámetros estratégicos que han imperado en el mundo durante su vigencia.

Los propios conceptos de seguridad nacional están sufriendo fuertes transformaciones y han ido evolucionando hacia concepciones no agresivas, dando entrada a nuevos actores como los económicos, los recursos naturales, la protección ecológica, las migraciones, la información y el conocimiento con la revolución informática y de las comunicaciones, el incierto futuro del Estado-nación y de las instituciones multilaterales y supranacionales como base del sistema político internacional.

A partir de lo cual, cada país debe elaborar su propia doctrina estratégica de acuerdo con sus circunstancias, lo que supone un verdadero esfuerzo creativo en la localización de las variables esenciales para la definición de la mejor estrategia de seguridad nacional, para lo que resulta inprescindible la percepción clara, el sentido y el alcance de los cambios y transformaciones en que estamos inmersos y la previsión de los acontecimientos derivados de ellos.

Es vital para el desarrollo histórico de cada país el conocimiento exacto de sus posibilidades y limitaciones, para poder diseñar las estrategias más adecuadas en cada momento y alcanzar las metas que cada sociedad se ha marcado, así como prever escenarios futuros.

Decía Sun Tzu, en su "Arte de la guerra", que "lo que posibilita a un gobierno inteligente y a un mando militar sabio vencer a los demás y lograr triunfos extraordinarios es la información previa"[6].

Para hacer frente a estos retos es necesario ir elaborando un nuevo modelo de seguridad nacional adecuado a los intereses y circunstancias y el papel del país en el entorno internacional.

La España democrática, continuando la tendencia iniciada en 1.953, ha buscado su seguridad a través de la Alianza Atlántica y, dentro de ella, en la Unión Europea Occidental y mediante la alianza con los Estados Unidos[7].

Pero hoy la planificación estratégica debe tener en cuenta cada vez más, factores que no son estrictamente militares, tales como los económicos, los ecológicos, los tecnológicos, políticos, diplomáticos, históricos, culturales, sociales o los institucionales, y, en todo caso, los factores relacionados con la información y el conocimiento aplicado a todo ello, sin que esto suponga que los factores estrictamente militares no sigan siendo imprescindibles.

Un concepto amplio de seguridad nacional ha de tener en cuenta todos los factores indicados para lo que resulta absolutamente necesario un esfuerzo conjunto de instancias públicas y privadas.

En términos económicos se trata de no perder competitividad, en términos sociales de modernizar nuestra estructura y hábitos sociales, en términos psicosociales de reforzar la identidad nacional y enriquecer la fuerza cultural del país y su proyección externa, sin olvidarnos de la protección ecológica de nuestros recursos naturales, el fomento de la investigación

y la ciencia, con especial interés en la información y las comunicaciones y, en general, el conocimiento. En términos políticos en fortalecer las instituciones y propiciar la cohesión interna.

La seguridad nacional busca la efectividad en un contexto de incertidumbre controlable, aunque de todos los factores que inciden en ella, en sentido amplio, algunos son de más difícil planificación que otros.

La construcción de un nuevo modelo de seguridad nacional ha de pasar por un debate constructivo y permanente, alejado de convencionalismos y ceñido a la realidad española en su dimensión nacional e internacional.

La posición geográfica de España la convierte en factor decisivo de la posición europea por su entrada en el Mediterráneo y como frente occidental.

España es, por su geografía, economía y demografía, una potencia de grado medio, con intereses y responsabilidades regionales en el sur de Europa. Pero a quien la historia, la lengua y la geoestrategia permiten influir en la política global, que es lo propio de una gran potencia. Este valor indiscutible nos genera unas responsabilidades.

La cultura permite trascender los límites que impone la naturaleza. Así ocurre en cuatro dimensiones clave de la política exterior española: la seguridad, la construcción europea, la cooperación y la proyección iberoamericana.[8]

Con amenazas previsibles procedentes de países de nivel inferior, correspondientes a escenarios de crisis que, probablemente, se situarán en el Tercer Mundo, o en sus bordes, con países que, aunque con menores niveles en el plano tecnológico, tienen acceso a los mercados internacionales.

En reciente estudio sobre armas de destrucción masiva titulado "Proliferación en la cuenca del Mediterráneo", la CIA anuncia un cambio profundo del equilibrio estratégico en el Mediterráneo, a medida que se confirman las intenciones de adquisición de armamento nuclear, químico y bacteriológico por parte de los regímenes del norte de África y de Oriente Próximo.

La CIA analiza extensamente tanto las actuales motivaciones como las posibilidades técnicas y concluye que, en 10 años, todas las capitales del sur de Europa estarán al alcance de misiles balísticos con base en el norte de África. La adquisición de estos armamentos, cuyo objetivo esencial sería ganar peso específico frente a los vecinos y frente al mundo occidental, se acelerará debido a los problemas políticos y a la inestabilidad en la región.

No obstante, expertos en Defensa restan importancia e inmediatez a las conclusiones de este informe y señalan que en el norte de África sólo Libia posee una capacidad mínima de misiles balísticos y que ningún país cuenta con misiles de crucero de largo alcance. Además, el único medio para llevar un arma de destrucción masiva a cierta distancia es la aviación, y

el número de aviones disponibles para poder ejecutar este tipo de ataques es muy reducido. Un cambio cualitativo de esta situación exigiría un aumento de la inversión militar, lo que no parece probable, o una mayor cooperación por parte de países como China o Corea del Norte, algo fácilmente detectable.[9]

Ello sin eliminar los conflictos con otras potencias, de carácter fundamentalmente económico, pero que resulta razonable estimar que se conducirán a través de tensiones con menor nivel y ciertas probabilidades de salida consensuada.

Estas reflexiones nos llevan a la conclusión de que hemos de reforzar nuestra inteligencia, información y comunicaciones, como parte de un conjunto de estrategias orientadas a asegurar nuestra posición internacional y poder prevenir y hacer frente, en su caso, a eventuales conflictos.

Ante la evolución internacional descrita ¿estamos en condiciones de abordar las nuevas misiones?. ¿Son los sistemas de información y comunicaciones aptos para hacer frente a las exigencias internacionales de comunicación y seguridad?. ¿Se ha previsto la adquisición del material necesario para poder cumplirlas? ¿Tenemos organización, equipos y sistemas capaces de proporcionar y garantizar de forma efectiva y prolongada en el tiempo unas comunicaciones seguras?.

De todo ello surge un debate, donde juegan un importante papel los factores tecnológicos y económicos, pero sobre todo organizativos,

políticos e intelectuales que permitan una toma de conciencia de la importancia de la información y el conocimiento, su transmisión y protección, en el nuevo escenario internacional.

La seguridad nacional es un concepto demasiado importante para confundir la reserva y el necesario secreto con el oscurantismo y el aislamiento intelectual.[10]

Entre otros temas no debemos olvidar qué modelo de industrias nacionales de tecnologías de la información y las comunicaciones y de criptología se quiere, el alcance de la protección OTAN-UEO, los beneficios en este aspecto derivados de nuestra pertenencia a la Unión Europea.

Los recursos no son ilimitados, pero en información y comunicaciones, así como en la seguridad de las mismas, no todo es cuestión de recursos; en todo caso el acierto en este sentido dependerá de las prioridades que se le dé a la hora de invertir los recursos disponibles.

Por consiguiente, parece adecuado hacer los esfuerzos necesarios en recursos humanos, materiales, organizativos o de planeamiento para atender a uno de los vectores esenciales de cualquier estrategia nacional: la información y el conocimiento.

En el juego de relaciones internacionales, cada nación persigue de forma prioritaria, consolidar su seguridad, que no es otra cosa, que procurar su propia existencia y soberanía, como sociedad y como estado, que constituye la meta tradicional de toda política exterior.

Aunque el concepto de seguridad nacional, hoy, rebasa los componentes militares y se extiende a toda una gama de factores e índole económico, político, sociológico...etc., la defensa militar sigue siendo imprescindible.

Y en las actuales circunstancias internacionales, tras la guerra fría, estamos en una estructura multipolar, más flexible y con posibilidades de cambio, pero, también, con más riesgos de enfrentamiento.

El sistema internacional, como todo sistema implica una cierta dosis de conflictividad, por lo que, la existencia de tensiones y enfrentamiento -no siendo deseables- es algo que no debe sorprender y, aunque el recurso a la violencia como solución no sea otra cosa que una manifestación patológica del funcionamiento del propio sistema, al ser una posibilidad, hay que contemplarla.

En las actuales circunstancias no se da una jerarquía de fuerzas capaces, por sí solas, de disponer de un poder de intervención coherente y duradero.

Se camina en la dirección de ejércitos eminentemente defensivos, más reducidos, muy operativos y con un alto grado de preparación técnica, bien dotados, versátiles y aptos para, llegado el caso, integrarse en una defensa supranacional,[11]l en los que la información y las comunicaciones son factores de primera magnitud y vitales, para su operatividad y eficacia y,

podríamos decir, que alcanzan el rango de elementos constitutivos de su propia esencia en un ejército del siglo XXI.

En la guerra moderna lo más importante es la Inteligencia y los sistemas de control y comunicaciones, que proporcionan las condiciones previas necesarias para una efectiva coordinación de las tropas y suministros.

Los ejércitos han de estar preparados para la guerra y, en la actualidad, los hechos se aceleran de tal modo que exigen decisiones rápidas con comunicaciones y respuestas instantáneas.

Las modernas doctrinas exigen un alto grado de coordinación para aunar las fuerzas de tierra, mar y aire, el apoyo espacial y los sistemas centralizados, así como poder integrar adecuadamente la acción.

Los ejércitos modernos son sistemas pensantes, con capacidad de comunicación y ajuste autorregulador, con una extrema especialización de sus efectivos, integrados a través de las comunicaciones en el control de la dirección de la batalla.

En todo este proceso es determinante la información, cuya captación, almacenamiento, procesado, distribución y protección, son vitales.

La informática y las telecomunicaciones han alterado las reglas de la guerra y a los tradicionales escenarios de tierra, mar y aire, se añadirán "los campos de batalla" de las redes informáticas y el espacio.

La guerra informática tratará de destruir o confundir los sistemas de información enemigos y proteger los propios. En este contexto, los sistemas informáticos y las claves criptográficas para comunicaciones, se convierten en objetivos prioritarios de cualquier ataque.[12]

En la información militar, la seguridad de la información y la Criptología en sus distintos niveles, siempre han estado presente pero, actualmente, junto a las comunicaciones ejercen un papel de dimensión estratégica.

3.1.3.- CIFRA COMERCIAL.

La importancia de la economía a lo largo y ancho de la historia no parece ofrecer la menor duda. Forma parte esencial de las relaciones internacionales y es frecuente la confusión con la estrategia de los actores para los que constituye tanto un medio como un objetivo.

La economía depende de una parte de los recursos y de otra de la capacidad de explotarlos (aportaciones cuantitativas y cualitativas, grado de perfeccionamiento del equipaamiento tecnológico, etc.)

La combinación de todos estos factores establecerá la jerarquía de las ganancias o de las oportunidades entre las diversas colectividades políticas, en cuyo resultado final desarrollará un papel central la competitividad de cada una de ellas.

La competitividad como capacidad para luchar favorablemente en el mercado, se traduce en la obtención y desarrollo de ventajas respecto a los competidores, lo que, en última instancia desemboca en una situación en la que se percibe que resulta de mayor interés adquirir unos productos y servicios en lugar de otros.

De las diversas formas de obtener ventajas competitivas, las nuevas Tecnologías de la Información han venido tradicionalmente aportando ventajas basadas esencialmente en la automatización de operaciones.

Con su implantación y desarrollo generalizado estas nuevas tecnologías dejan de aportar singularidad entre los usuarios de las mismas. En estas circunstancias pierden su dimensión estratégica y se convierten en una exigencia más de las reglas del juego.

Lo que determina la competitividad no es sólo la capacidad de manejar de forma eficaz las operaciones internas -exigencia que obviamente hay que cumplir- sino que se requiere, además, la capacidad de conexión y adaptación al entorno.

En este escenario de competencia, muy extendido actualmente, resulta imprescindible tener capacidad para captar las necesidades del mercado y desarrollar de forma rápida un producto o servicio que dé respuesta a estas necesidades, lo que exige captación de información sobre

el entorno, agilizar sus flujos, promover innovación, facilitar la comunicación, aumentar la coordinación... etc.

En definitiva, el nuevo escenario de competencia, convierte el manejo de la información en un tema crítico, al hacer posible la mejora de la capacidad de respuesta a las exigencias del mercado.

Un componente esencial, que a la vez posibilita estas nuevas estrategias, consiste en el aprovechamiento de las tecnologías de la información y las comunicaciones.

Pero no a todos les afecta por igual las ventajas competitivas obtenidas de la aplicación de las tecnologías de la información.

Resulta evidente que los sectores en los que se manejan grandes volúmenes de información y en general, los que experimenten presión competitiva creciente, la utilización de las tecnologías de la información permite dar respuesta inmediata y obtener un buen posicionamiento respecto a las nuevas exigencias del mercado, lo que puede convertir a estas tecnologías en clave de su competitividad. Pero sin olvidar que la primera exigencia para utilizar con éxito las tecnologías de la información como parte integrante de la estrategia competitiva radica en la toma de conciencia de su importancia y efectos en la competitividad.

En la época de la globalización de la economía con rápidas mutaciones en los mercados, es cuando más se aprecia la importancia de la información y su explotación inteligente.

En este entorno, para lograr una posición óptima de competitividad, se tratará de saberlo todo acerca de los competidores mientras se evitará que estos conozcan datos, en los aspectos que interesa preservar, alterando, en beneficio propio, el equilibrio de información y conocimiento. Lo que se lograría de una forma más eficaz, armónica y completa si lograse dar lo que parece ser el paso definitivo en esta progresión con la formulación de un concepto sistemático y estructurado de la estrategia del conocimiento.[13]

En todo caso, cualquier organización tiene claro que con respecto al conocimiento tiene que desempeñar, al menos, cuatro funciones: adquirir, procesar, distribuir y proteger la información, mientras selectivamente la niega o la distribuye a sus competidores.

La importancia del conocimiento como factor de competitividad exige, obviamente, una defensa del activo del propio conocimiento frente a los competidores, lo que demanda incorporar la seguridad como parte de la dimensión estratégica de la información.[14]

Las aplicaciones criptológicas destinadas a usos comerciales están experimentando un crecimiento de una magnitud inimaginable hace unos años.

El aumento de las transacciones telemáticas y el uso masivo de las nuevas tecnologías de la información y las comunicaciones convierten al mercado de la criptología para usos civiles y comerciales, a nivel mundial,

en una magnitud dos veces superior al mercado clásico de criptología para usos militares.

En número de unidades, según una estimación francesa las necesidades del mercado mundial para 1.997 estaría en 600 millones de unidades criptológicas para usos civiles y comerciales.[15]

Cada día son más las empresas que empiezan a depender de forma esencial de la Criptología.

3.1.4.- Cifra Cívica.

Entre los grandes efectos producidos por las nuevas tecnologías de la información y las comunicaciones y su utilización masiva, está la posición de vulnerabilidad en que sitúa al ciudadano y las organizaciones en las que se integran.

Los ordenamientos jurídicos responden con figuras como el secreto de las comunicaciones, pero una efectiva protección requiere, además, medidas preventivas constituidas por la seguridad de la información, en la que juega un papel destacado la Criptología.[16]

Además de los ámbitos clásicos de protección criptológica, actualmente se ha de añadir, por su importancia y presencia en las más diversas actividades de la actividad cotidiana, el destinado a preservar la privacidad del individuo, que hemos denominado como *"cifra cívica"*, que puede constituir una cifra básica o general

Aunque con respecto a las nuevas tecnologías, no parece conveniente establecer una nueva generación de derechos, sí parece necesario adecuar los planteamientos jurídico-normativos a las nuevas necesidades sociales.

Las violaciones de la legalidad están vigentes desde que el hombre lo es. Lo que ha evolucionado son 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 se puede obviar que 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.

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

Algunos sectores de la doctrina consideran a la informática como una posibilidad nueva de agresión de los derechos del hombre, de naturaleza jurídica distinta. Incluso se habla de "delito informático", como

tipo específico,[17] sobre lo cual compartimos lo dicho por Javoleno Prisco *"omnis definitio, in iure civile, periculosa est"*. [18]

Por nuestra parte consideramos que los nuevos medios técnicos establecen nuevos mecanismos de lesión o violación, pero en el fondo, la naturaleza jurídica de la agresión, tiene los mismos fundamentos.

Los problemas que plantea la informática y el posicionamiento del Estado, con relación 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.

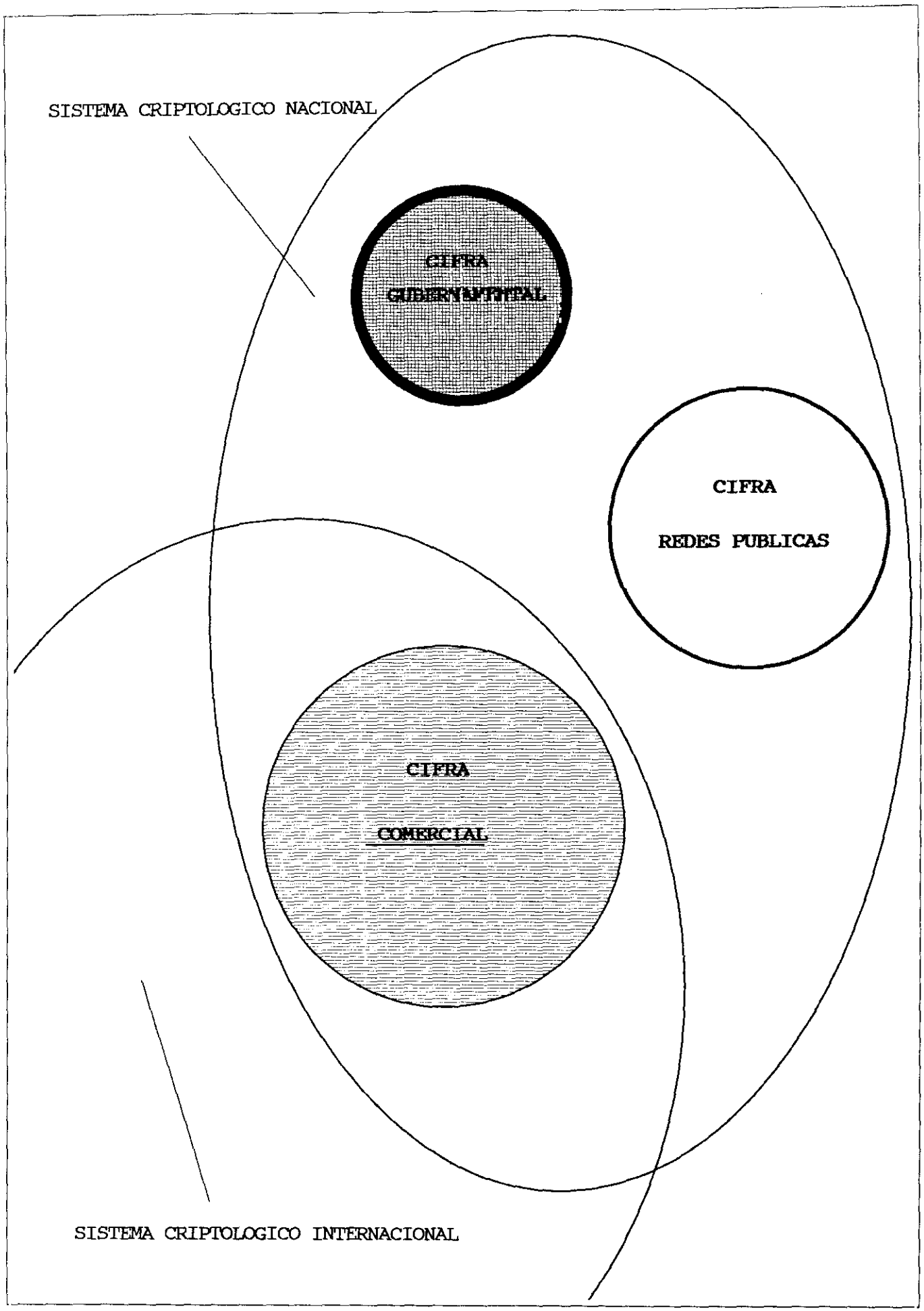
La Criptología viene a ser un método, una técnica secular, aplicada a algo reconocido históricamente y que ha evolucionado en sus manifestaciones concretas, al ser utilizada en la aplicación de las nuevas tecnologías de la información y las comunicaciones, y cuya expansión en los niveles de implantación corre en paralelo a la vulnerabilidad de la propia tecnología y mayor desarrollo de la sensibilidad jurídica y social, esencialmente en lo referido a los derechos fundamentales.

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 de forma 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).

La *"cifra cívica"* podría ser considerada como la protección criptológica orientada a que la seguridad de los datos derivados del individuo y sus relaciones cívico-sociales sean una realidad efectiva.


SISTEMA CRIPTOLOGICO NACIONAL
CIFRA
GUBERNAMENTAL
CIFRA
REDES PUBLICAS
CIFRA
COMERCIAL
SISTEMA CRIPTOLOGICO INTERNACIONAL

3.2.- PROTECCIÓN CRIPTOLÓGICA Y SERVICIOS DE INTELIGENCIA.[19]

El filósofo guerrero chino Sun Tzu, en "El arte de la guerra", recopilado hace más de dos mil años, al referirse a la importancia de la información previa decía que esta "no puede obtenerse de fantasmas ni espíritus, ni se puede tener por analogía, ni descubrir mediante cálculos. Debe obtenerse de personas; personas que conozcan la situación del enemigo".[20]

El arte de la guerra, escrito hace más de dos mil años, "tal vez sea, todavía hoy, el libro de estrategia más prestigioso e influyente del mundo, y es estudiado en Asia por los políticos y ejecutivos actuales con el mismo ahínco con el que lo han estudiado los líderes y estrategas militares durante más de dos milenios.

En Japón, país en el que se ha pasado directamente a una cultura empresarial a partir de una cultura feudal prácticamente de la noche a la mañana, los estudiantes contemporáneos de "El arte de la guerra," han aplicado con la misma presteza la estrategia de este antiguo texto clásico a la política y al mundo empresarial. Por cierto, que algunas personas ven en los éxitos del Japón de posguerra un ejemplo de la máxima clásica de Sun Tzu: *"Es mejor ganar sin luchar"*.

Como estudio de la anatomía de las organizaciones en conflicto, "El arte de la guerra" puede aplicarse a las rivalidades y conflictos en

general en todos los niveles de las relaciones, desde el nivel interpersonal hasta el internacional. Su objetivo es la invencibilidad, la victoria sin batalla, y la fortaleza inexpugnable mediante la comprensión de los aspectos físicos, políticos y psicológicos del conflicto.

Esta traducción de "El arte de la guerra" presenta el texto clásico desde la perspectiva de su inclusión en el contexto general de la gran tradición espiritual del taoísmo. Tal vez, lo más característico de "El arte de la guerra" -hasta el punto de seguir teniendo valor por sí mismo en nuestra época- es la manera en la que el poder se halla continuamente moderado por una profunda corriente subterránea de humanismo. El arte de la guerra no es, pues, solamente un libro que trata de la guerra, sino que también es un libro sobre la paz, y, sobre todo, es un instrumento para comprender las verdaderas raíces del conflicto y de su resolución".

Las artes de la *curación* y las artes *marciales* quizá constituyan un mundo aparte en cuanto a su utilización ordinaria, pero tienen paralelismo en varios sentidos: en el de reconocer, como cuenta la vieja historia, que cuanto menos se necesita algo o a alguien, tanto mejor; en el sentido de que ambos grupos de artes requieren la estrategia para tratar la ausencia de armonía; y en el sentido de que para ambos el conocimiento del problema es la clave de la solución.

Como en la historia de los antiguos sanadores, en la filosofía de Sun Tzu la eficiencia máxima del conocimiento y de la estrategia es hacer que el conflicto sea totalmente innecesario.

Sun Tzu explica todos los grados de las artes marciales: la mejor técnica militar es la que frustra los complots de los enemigos; a continuación, lo mejor es deshacer sus alianzas; después, atacar sus fuerzas armadas; y lo peor es sitiar sus ciudades.

Esta estrategia ideal, mediante la que es posible ganar sin luchar, y que consigue el máximo haciendo lo mínimo, lleva la impronta característica del taoísmo, la antigua tradición del conocimiento que alimentó tanto las artes de la curación como las artes marciales chinas.

Es posible que la paradoja de "El arte de la guerra" resida en su oposición a la guerra. Y la manera en que "El arte de la guerra" lucha contra la guerra es mediante los propios principios de la guerra: infiltra las líneas enemigas, descubre los secretos del adversario y hace cambiar los corazones de las tropas contrarias. Esta filosofía podría estar en la base de los servicios de inteligencia.

Uno de los primeros sistemas de inteligencia militar desarrollados en Occidente se debió a Sir Francis Walshingham, Secretario de Estado de la Reina Isabel de Inglaterra en el siglo XVI, quien no sólo urdió una red de espías como la mayoría de sus contemporáneos, sino que redactó un plan para la obtención y análisis sistemáticos de información sobre el desarrollo

de la Armada Invencible española, lo que, según algunos historiadores contribuyó de manera fundamental a la victoria de los británicos.

En 1.588, las señales ópticas, hicieron llegar a Londres, desde centenares de kilómetros, la noticia de que la Armada Invencible española había sido avistada en el Canal de la Mancha, a la altura de Plymouth: una cadena de fogatas encendidas en lo alto de colinas y campanarios, a una distancia aproximada entre ellas de cinco millas, transmitió la noticia en menos de 20 minutos.

Este sistema de transmisión se solía combinar con el código casi criptográfico basado en el "Damero de Polibio", que codificaba un mensaje sustituyendo cada letra por una pareja de cifras.[21]

El caso de Walshingham es comparable al de muchos otros servicios de inteligencia surgidos con objetivos militares o políticos, como los de Richelieu, Cromwell, Gengis-Kan o Clausewitz.[22]

Lo que diferenció a los casos citados de sus contemporáneos fue la explotación inteligente de los instrumentos de obtención y transmisión de información existentes en la época, bien se tratara de espías, cartas manuscritas o palomas mensajeras. Tanto ellos como sus coetáneos tenían acceso a estas "tecnologías", pero sólo ellos acertaron a aplicarlas a la obtención de información estratégica. La idea puede ser extrapolada a la situación actual, en la que las tecnologías de la información posibilitan la obtención, análisis y transmisión de información en formas altamente sofisticadas. La

tecnología por sí sola no basta, se requiere una planificación detallada, una cierta sistematización, así como el empeño de todos los miembros de la organización.

De la información previa a la que se refería Sun Tzu, pasando por la expresión comteana de *"Savoir pour pouvoir pour prévoir"*, se deriva la necesidad no solo de predecir el porvenir, sino de actuar para prevenir. [23]

Para el Presidente de la República Francesa, Jacques Chirac, "...La prevención es, en primer lugar, una cuestión de información y confirmo la prioridad dada a la adquisición de medios espaciales y al reforzamiento de los servicios especializados. La comprensión de las situaciones y el control de la información condicionan la autonomía de decisión. La construcción junto con nuestros aliados de estos medios tan costosos concurre con la emergencia progresiva de una Europa que deseamos que controle su información, compromisos y, finalmente, su destino...".

A medida que la sociedad avanza hacia un nuevo sistema de creación de riqueza en el que cada vez interviene más la información y el conocimiento, las funciones informativas de los gobiernos aumentan vertiginosamente.

No se puede negar que la información anticipada, producto de la recogida, análisis y elaboración de la misma, sigue siendo un instrumento de primera magnitud y eficacia para prevenir las eventuales desestabilizaciones

de la convivencia pacífica, siendo, en ultima instancia, una garantía de la seguridad nacional.

Los fenómenos como la transferencia de tecnología, equipos y conocimientos de aplicación militar, la radicalización de conflictos nacionalistas, religiosos o étnicos, o la expansión internacional del crimen organizado, no sólo exigen el mantenimiento, sino el aumento de la tensión de la vigilancia de los Estados de derecho para preservar su mantenimiento como regímenes de garantías y salvaguarda de libertades individuales y colectivas. [24]

En diciembre de 1.996, los jueces europeos han lanzado desde Ginebra una llamada angustiosa contra la progresiva penetración del crimen organizado en todos los sectores de la economía mundial. Particularmente en las finanzas y en los negocios. En Rusia se estima que la mafia controla ya el 40% de la economía.[25]

En unas declaraciones realizadas ante la Comisión de Relaciones Exteriores del Senado, Madeleine Albright, Secretaria de Estado norteamericana, compara el narcotráfico con la amenaza nuclear.[26]

Por todo ello, no sólo se exige el mantenimiento, sino el aumento de la tensión de la vigilancia de los Estados de derecho para preservar su mantenimiento como regímenes de garantía y salvaguarda de libertades individuales y colectivas.[27]

El poder de la información es un multiplicador de fuerza, incluido el *"poder suave"* (soft power) como capacidad de conseguir los resultados deseados en asuntos internacionales mediante la atracción en lugar de la coerción.

"La belleza de la información como un recurso de poder es que, aunque pueda potenciar la efectividad de la potencia militar en sí, inevitablemente democratiza las sociedades".[28]

Si el Estado consigue establecer instituciones internacionales que instiguen a otros a canalizar o limitar sus actividades puede que necesite emplear menos recursos económicos o militares.[29]

La revolución industrial transformó la guerra y también el espionaje, que se hizo más sistemático y burocrático, se crearon escuelas de inteligencia y los agentes empezaron a recibir formación profesional.

La Segunda Guerra Mundial propició la aparición de notables descubrimientos tecnológicos que sentaron las bases para una producción masiva de información, a la que contribuye no solo el avance en las comunicaciones y los progresos informáticos en el campo de la criptografía, sino la información que se incorpora de fuentes abiertas, como la prensa, los medios de comunicación en general, las estadísticas oficiales o los congresos científicos, lo que se viene a sumar a las clásicas fuentes secretas.

Los cambios que se están produciendo en las relaciones internacionales revelan la necesidad de redefinir el modelo de servicio de inteligencia vigente durante los años de la guerra fría.

Los organismos de información secreta no tienen porqué continuar siendo reliquias del pasado, sino utilizarse como instrumentos que pueden ser más poderosos, rentables y flexibles.[30]

La aparición de fenómenos, como el narcotráfico, introducen nuevas prioridades de información anticipada para la toma de decisiones políticas; los nuevos perfiles del terrorismo demandan mayor especialización y mejor coordinación y la complejidad de los nuevos conflictos internacionales exige un esfuerzo de especialización profesional y madurez intelectual que permita una completa comprensión de situaciones con implicaciones multidireccionales.[31]

Una Comisión Especial del Congreso de Estados Unidos sobre diversas agencias de inteligencia encargadas de velar por la seguridad nacional, ha dicho que "Carecen de análisis profundo, amplitud de miras, habilidad para estudiar las tendencias políticas, económicas y militares en todo el mundo" y pone igualmente en evidencia la capacidad para conectar "inteligencia humana" en todo el mundo.[32]

La información realizada por humanos -Humint- vuelve a recobrar posiciones, tras años de ser desplazada por poderosos, sofisticados y costosos sistemas.

El paso al sistema de información de la tercera ola supone paradójicamente un mayor énfasis en el espía humano, el único tipo disponible en el mundo de la primera ola. Pero en el presente, los espías de la primera ola se presentan armados con las tecnologías complejas de la tercera.[33]

Hoy se podría decir que en el escenario previsible, hombres y máquinas, ocuparán cada uno su lugar, complementándose, pero en modo alguno, sustituyéndose.

La obtención de información anticipada sobre tendencias económicas y tecnológicas, proyectos de inversión, actividades competitivas, investigación y desarrollos concretos, serán objeto de atención creciente por los servicios de inteligencia.

Además, las relaciones internacionales de las próximas décadas van a ser fundamentalmente relaciones económicas y no sólo por lo que respecta al libre comercio o disputas por los mercados, sino por lo que se relaciona con las repercusiones políticas, nacionales y de lucha de poder dentro del sistema internacional que puede llevar aparejada toda expansión de la influencia nacional por vía económica fuera de las propias fronteras. Hoy, los intereses de seguridad nacional están inextrincablemente ligados a los intereses económicos.[34]

En la situación presente, las organizaciones burocratizadas resultan demasiado lentas, se está abandonando la producción en serie y se da paso a una *"producción flexible"* adaptada a las necesidades del *"cliente"*.

La adaptación a los rápidos cambios exige olvidarse de los organigramas piramidales, buscándose en la actualidad formas nuevas de organización, entre las que destacan las que se realizan en torno a procesos y no a mercados o especialidades parceladas, a través de organizaciones matrices, equipos de proyectos específicos y diversidad de alianzas y consorcios. Al cambiar las situaciones constantemente, es menos importante la posición que la flexibilidad y la capacidad de maniobra.[35]

La captación de información masiva produce tal cúmulo que provoca una paralización del análisis, trasladándose el problema de la captación, que ha sido el anhelo tradicional de todo servicio de inteligencia, al análisis, volviendo a situar en posición destacada al factor humano. La frase atribuida a Donoso Cortés,para el que *"Lo importante no es escuchar lo que se dice sino averiguar lo que se piensa"* [36], adquiere gran actualidad.

El avance del mundo hacia un sistema basado en la información y el conocimiento producirá en los servicios de inteligencia una crisis similar a la que está produciendo en la economía.

En el sector de la inteligencia, como en el ámbito empresarial o industrial, hay unas cuantas organizaciones gigantescas y muchas otras pequeñas.

Estados Unidos, como en tantas otras actividades, figura a la cabeza, y donde además de la conocida Agencia Central de Inteligencia (CIA), conocida comunmente como "la Compañía", existe la Agencia de Inteligencia de la Defensa del Pentágono y, por encima de todo, la Agencia de Seguridad Nacional (NSA) [37] y la Oficina de Reconocimiento Nacional, además de las unidades militares de información especializadas y las pequeñas unidades existentes en el Departamento de Estado, Departamento de Energía, Tesoro, Departamento de Comercio y otros organismos gubernamentales, con frecuencia integradas por personal de la CIA.

El éxito de la NSA en el criptoanálisis de claves constituye uno de los secretos más celosamente guardados. Continúa diciendo el autor , que los ordenadores pueden generar claves al azar que otros ordenadores no pueden descifrar. El continuo miedo de la NSA es que un país cambie de un código simple a otro más complejo. Si una nación adopta uno de los sistemas de clave virtualmente indescifrables, la NSA tiene que acudir a la CIA o al FBI para que realicen un trabajo sucio, penetrar en los cuarteles del objetivo para robar su código.

Los ordenadores de la NSA realizan otra serie de operaciones además de descifrar códigos, como la interceptación de cables a alta velocidad, o el análisis de tráfico, que consiste en cribar grandes cantidades de mensajes en clave. En este breve resumen -año 1.982- se dice que trabajaban para la NSA más de 10.000 civiles y que este número se ve reforzado por

casi 45.000 soldados de los ejércitos de tierra, mar y aire, que operan los puestos de escucha, que van abriéndose y cerrándose dependiendo de los cambios en la política exterior norteamerica. También se instalan equipos de escucha en barcos de guerra.

Según un reportaje publicado en España, por la revista TIEMPO, el 28 de abril de 1.986, por Eric Laurent (Le Figaró Magazine), la National Security Agency (NSA), es la más grande, poderosa y secreta de todas, se creó por Truman, el 4 de noviembre de 1.952, de una decisión secreta de la Presidencia, la orden número seis del Consejo Nacional de Seguridad, cuyo texto continuaba siendo secreto. Durante los primeros ocho años su existencia no fue conocida ni por los propios legisladores norteamericanos, hasta que en 1.960 y debido a la fuga de dos criptólogos, se supo que la NSA interceptaba y revelaba comunicaciones secretas, entre ellas las del Estado español.

Señalaba el reportaje que no existía siquiera una ley ordenando o confirmando su creación, existiendo sólo textos destinados a protegerla. Considerada como centro nervioso de la implacable guerra de la información entablada contra la URSS. A través de la oficina de protección, el más importante de los tres sectores de actividad de la agencia, los ordenadores son utilizados para descriptar, a gran velocidad, gracias a la frecuencia de las letras, las decenas de millares de palabras usuales, las reglas gramaticales almacenadas en su memoria y los textos codificados más difíciles.

En 1.986, época del reportaje, estos ordenadores eran capaces de transferir 320 millones de palabras por segundo (equivalente a unos 2.500 libros de trescientas páginas cada uno), y estaban en conexión con más de tres mil especialistas de la NSA que trabajaban en bases instaladas en todo el mundo.

La NSA puede considerarse capaz de describir todo lo que pasa en el conjunto del planeta.

Matemáticos y especialistas en descifrar mensajes, ingenieros en informática, especialistas en radar y electrónica, expertos en comunicación y lingüistica, constituyen la elite de ese cuerpo gigantesco que utiliza métodos auxiliados por la más moderna tecnología, incluyendo el uso de satélites espías.

En 1.984, la NSA interceptó 23.467.587 comunicaciones provenientes de todos los rincones del globo, muchas de ellas "ultradelicadas" y "estratégicas", para lo cual tuvo que desentrañar los sistemas de codificación utilizados.

Finaliza el reportaje afirmando que *"No es exagerado afirmar que la NSA puede poner bajo escucha al mundo entero".*

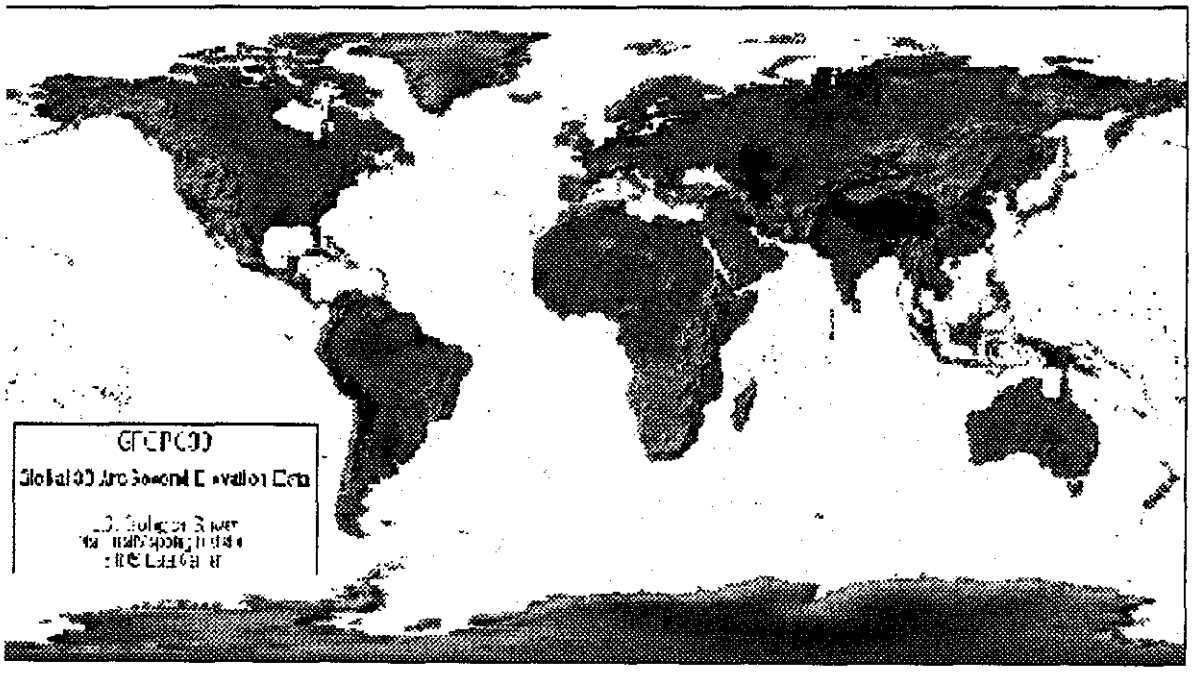
Una confirmación actualizada de lo dicho la tenemos en el conocido como sistema *Echelon,* el producto tecnológicamente más avanzado del Ukusa Security Agreement, al que nos referimos en el Capítulo I de esta tesis.

Desde 1.948, el pacto secreto para compartir información conocido como Acuerdo de Seguridad UKUSA, ha vinculado a la NSA estadounidense, la GCHQ (Cuartel General de Comunicaciones) británica y sus homólogos de Canadá, Australia y Nueva Zelanda. Más tarde se unió al pacto la OTAN.

-En 1.986 Nueva Zelanda fue excluida por prohibir la entrada en sus puertos de los barcos estadounidenses que portasen armas nucleares-. [38]

Los soviéticos dependían del KGB para la información extranjera y del GRU especializado en temas militares y tecnológicos; los británicos dependen del Servicio de Información Secreto MI6 y del Cuartel General de Comunicaciones del Gobierno; los franceses cuentan con la DSGE, conocida como *"la Piscina"*, complementada por la Agrupación de Controles Radioeléctricos. El Mossad israelí, conocido como *"el Instituto"*, y el Bundesnachtendienst alemán, junto con los tres servicios japoneses, son también importantes productores de información.

En España, el Centro Superior de Información de la Defensa (CESID), comúnmente conocido como "La Casa", *"es el órgano de información del Presidente del Gobierno, para el ejercicio de sus funciones de dirección de la política de defensa y de coordinación de la acción del Gobierno en la defensa del Estado, y del Ministro de Defensa, en el ejerci-*


GTOPO30

cio de las funciones que le corresponden en materia de defensa y de política militar." (Art. 5 del Real D. 1.883/1.996, de 1 de enero).

En general, con mayor o menor dimensión, casi todos los países tienen algo parecido a una agencia de inteligencia para la recogida de información exterior, constituyendo estas organizaciones uno de los mayores sectores de servicio de todo el mundo, y donde se reflejan los cambios de poder y las nuevas correlaciones de fuerza.

A medida que un país asume mayores papeles en el campo diplomático, político y militar, en consonancia con su poder económico, es de esperar que se aumenten sus actividades de inteligencia; lo que a su vez incrementará las actividades de inteligencia y contrainteligencia entre vecinos, socios comerciales, aliados y adversarios.

En Alemania, en la época del nazismo, la Gestapo asumía al mismo tiempo funciones de servicio secreto y policía, por ello Bonn se ha esforzado por trazar una línea divisoria clara entre ambas funciones y hoy, los servicios secretos alemanes sólo están autorizados para reunir información en su ámbito de actuación, pero sin cumplir tareas policiales.

La Oficina Federal de Defensa de la Constitución (BFV), dependiendo del Ministerio del Interior reúne información sobre actividades terroristas y extremistas, labores de contraespionaje y observación de extranjeros que constituyan un peligro para la seguridad y el orden constitucional.

El Servicio de Protección Militar (MAD), depende del Ministerio de Defensa y tiene como misión proteger la seguridad del ejército. El Servicio Federal de Información (BND), depende de lo que sería en España el Ministerio de Asuntos Exteriores y tiene encomendada tareas de espionaje en el extranjero.

Para coordinar estos tres servicios (exterior, interior y ejército) existe en la cancillería federal un ministro de Estado con esta función.

En Gran Bretaña, los servicios de seguridad y espionaje se estructuran en tres agencias: El Servicio de Seguridad, conocido como MI5, dependiente de Interior, es responsable en defensa nacional; el Servicio Secreto de Inteligencia, SIS ó MI6, se dedica al extranjero, y el Centro Gubernamental de Comunicaciones, GCHQ, ambos dependientes de Exteriores.

En Francia, los servicios de espionaje son varios. La Dirección Central de Informaciones Generales es el cuerpo más básico del Ministerio del Interior, del que también depende la Dirección de Seguridad del Territorio, dedicado al contraespionaje. El Ministerio de Defensa dispone de la Dirección y Protección de la Seguridad del Territorio, dedicado a informaciones militares.

Las tareas más delicadas corresponden a dos servicios dependientes directamente del presidente, la Dirección General de la Seguridad

Exterior, para intervenciones militares clandestinas y el Secretariado General de la Defensa Nacional, para asuntos estratégicos y nucleares.

En Italia en 1.925 nace el Servicio de Informaciones Militares (SIM) que fue desmantelado por los aliados. Tras cuatro años de prohibición de los servicios secretos, cuando en 1.949 ingresó en la OTAN, se reanudaron las actividades de inteligencia con el Servicio de Informaciones de las Fuerzas Armadas (SIFAR), que, en 1.965 fue reconvertido en Servicio de Información de la Defensa (SID).

Reformados en 1.977, los servicios secretos italianos se dividen en una rama militar denominada Servicio para la Información y la Seguridad Militar (SISMI), que depende de Defensa, y otra civil, denominada Servicio para las Informaciones y la Seguridad Democrática (SISDE), dependiente de Interior, sobre ambos el Presidente tiene función de vigilancia a través del comité de coordinación (CESIS).[39]

El Gobierno italiano pretende terminar con lo que consideran viejos organismos -CESIS, SISMI y SISDE- fundados por ley en 1.977, para crear en su lugar el AISE, dedicado a la seguridad exterior y el AISI, encargadode la seguridad interna, ambos dependientes del DGS, departamento gubernamental para la seguridad, el cual a su vez será controlado directamente por el nuevo Ministerio de la Información para la Seguridad que se creará al efecto.

Con esta reforma se pretende poner fin a la multiplicidad de servicios secretos, y los nuevos organismos que eventualmente se crearán absorberán funciones que actualmente cumplen los servicios secretos de los carabineros (ROS), el SCICO y el GICO, de la Guardia de Finanzas, Policía Judicial, el SCO, de la Policía del Estado, y otros.

A esta conclusión ha llegado el Gobierno italiano tras el estudio de un informe elaborado durante siete meses de trabajo por la comisión Jucci, nombrada por el Primer Ministro y compuesta por militares, magistrados, juristas y veteranos agentes de los servicios secretos.[40]

Los nuevos sistemas de creación de riqueza trastocan las prioridades de los principales servicios de inteligencia que, en el futuro prestarán la máxima atención a los campos económico, tecnológico y ecológico.

Las agencias de inteligencia, al igual que las empresas, están vinculadas por medio de consorcios y alianzas, lo que no quiere decir que sean relaciones tranquilas, estando a menudo salpicadas por acusaciones recíprocas.

En muchos países los cambios de régimen político o simplemente, el cambio de partido en el gobierno, suele ser utilizado para tomar una de las decisiones de mayor transcendencia, consistente en la elección de un "mayorista" que le provea de información secreta.

Tras la finalización de la "guerra fría" y la creciente mundialización de los sistema de creación de riqueza, con el aumento del número de

empresas con intereses en el extranjero, las principales agencias de inteligencia orientan sus esfuerzos hacia el sector económico.

Cada día con mayor determinación, los países occidentales recurren a la utilización de su capacidad de influencia política en apoyo de sus intereses económicos y comerciales. ¿Está preparada España para el reto que supone la nueva era de la diplomacia comercial?.

La utilización de la capacidad de influencia política de los Estados en favor de sus intereses económicos en los mercados internacionales, constituye la diplomacia comercial.

Los Estados Unidos han involucrado a la CIA en operaciones comerciales en las que participan empresas norteamericanas, con el fin de obtener información acerca de los movimientos de sus competidores. [41]

La nueva economía es cada vez más dependiente de la electrónica y las comunicaciones; redes de ordenadores permiten flujos transnacionales de delicada información económica, con lo que todo el sistema empresarial se hace más vulnerable a la penetración de las agencias de inteligencia, al ofrecer un amplio campo de actuación para sus actividades.

La inteligencia se verá obligada a intervenir en apoyo no sólo de los objetivos gubernamentales, sino en apoyo de las propias estrategias empresariales, industriales o científicas, en base al supuesto de que estos ámbitos de poder contribuyen al poder nacional.

En el año 1.998, Estados Unidos invertirá en inteligencia 3,99 billones de pesetas. La parte más importante, 900.000 millones, se los llevará la agencia encargada de los satélites de espionaje. En interceptación de comunicaciones se gastarán 600.000 millones y en la CIA, 450.000 millones. La inteligencia táctica, -Defensa, Fuerzas Aérea y Armada- recibirá 1,5 billones y la inteligencia interior, -FBI, Comisión de Energía Atómica, Departamento del Tesoro, seguridad de altos cargos-, 450.000 millones de pesetas.

Pero en la historia de los servicios de inteligencia no han faltado las aplicaciones económicas y financieras.

En el siglo XVI la familia Fuggers, banqueros privados de la Casa de Habsburgo e iniciadores de la banca internacional, fueron pioneros en el concepto de informe comercial, ya que enviaban cartas manuscritas con información política y comercial a sus diferentes agentes situados en las distintas capitales europeas.

Dentro de éste ámbito es también conocido el caso del banquero Nathan Rothschild que construyó una red de agentes en toda Europa con los que se comunicaba mediante palomas mensajeras. Esta red le permitió ser en Londres el primero en conocer la derrota de Napoleón en Waterloo, antes incluso que el gobierno británico.

Disponiendo de esa ventaja, procedió a la venta masiva de bonos de Tesoro en la Bolsa de Londres, acción en la que fue imitado por todos los

que, conocedores de las fuentes de información de Rothschild, concluyeron que ello significaba que los británicos habían perdido la batalla. Cuando el precio bajó suficientemente, Rotschild pasó a la compra masiva, con lo que protagonizó uno de los primeros ejemplos de lo que hoy se conoce como utilización de "información privilegiada".[42]

Quienes parecen dominar a la perfección el arte de la "succión" de información del entorno son los japoneses, hasta el extremo que hay quien dice que su habilidad para aspirar datos, información y conocimientos ha constituido la pieza clave de su desarrollo tecnológico y comercial.

Alfonso Cornella se refiere a una serie de ejemplos que pueden ayudar a comprender hasta qué punto las empresas japonesas se toman en serio la información.

"- En cualquier feria europea o norteamericana es fácil encontrar un grupo de trabajo japonés que literalmente "peina" la muestra en búsqueda de nuevos desarrollos. Por regla general, estos grupos están perfectamente organizados, ya que cada miembro tiene una función muy concreta (establecer el contacto, tomar notas, tomar imágenes en vídeo, etc.) (Goodman, 1.990).

- Durante años, los ingenieros japoneses se han caracterizado por su habilidad en desentrañar los secretos de los productos occidentales mediante técnicas de "ingeniería inversa" (abrir un producto para ver qué contiene) (Villain, 1.989).

- Los directivos japoneses han desarrollado una especial habilidad para las negociaciones industriales y para la captura de know-how mediante joint-ventures o acuerdos estratégicos, a través de lo que Badaracco (1.991) ha denominado knowledge-links.

- Según la OCDE, mientras que Europa produjo en 1.990 el 40 por 100 de las patentes mundiales, los Estados Unidos el 39 por 100 y Japón el 15 por 100, son las empresas japonesas las que sorprenden cada vez más por su habilidad innovadora. Cerca del 72 por 100 de las demandas de utilización de patentes en el mundo en ese año correspondieron a patentes europeas (Le Nouvel Economist, 18-12.1.992).

- A diferencia de las empresas norteamericanas, en las que reina el denominado "síndrome de no-inventado-aquí" (que lleva a los técnicos de las empresas a desconfiar de las innovaciones procedentes del exterior de la empresa), las empresas japonesas manifiestan un gran interés por los productos o tecnologías que ya disponen de un mercado en el extranjero, ya que ello les permite ahorrar esfuerzos (el producto ya ha demostrado sus posibilidades) y maximizar su valor añadido (Bayenb, 1.989).

- Algunos de los casos más sonados de espionaje industrial en los últimos años han tenido por protagonistas a empresas japonesas y por víctimas a empresas norteamericanas.

- Se ha sugerido que la división de inteligencia industrial de la

Mitsui Corporation supera a la misma CIA norteamericana en lo que respecta a la obtención de información (Cronin, 1.990).

- La Mitsubishi Corporation dispone de dos plantas de un edificio en Nueva York donde un pequeño ejército se dedica a analizar centenares de revistas generales, económicas o técnicas, prospectos y catálogos de los competidores internacionales, anuncios, ponencias en congresos y conferencias, e incluso rumores, y posteriormente envía las correspondientes síntesis a la sede de la empresa en Japón, donde esta información es utilizada para identificar nuevos productos, procesos, es decir, nuevos retos y oportunidades (Villain, 1.989; Meyer, 1.987). Así, las delegaciones de las empresas japonesas en el extranjero actúan como verdaderas "aspiradoras de información". Lo más destacable es que llevan a cabo esta tarea de manera escrupulosa y sistemática, a diferencia de la mayoría de empresas norteamericanas y europeas que no disponen de un servicio de inteligencia industrial formalmente organizado (Meyer, 1.987).

- Se estima que hay más de diez mil especialistas en la obtención de información industrial para las empresas japonesas. Sólo en Tokio hay unas cuatrocientas agencias privadas de búsqueda de información para empresas (brokers de información) (Bayen, 1.989)."

El ejemplo más representativo de las empresas japonesas en la información lo constituyen las Sogo Shoshas, o sociedades de comercio. Son conglomerados de empresas que aseguran a sus miembros el acceso a los

recursos necesarios para la distribución de sus productos a escala mundial, incluido mercados financieros, información, etc.

A través de sus misiones comerciales en todo el mundo, recogen información sobre los productos fabricados en el extranjero, las novedades tecnológicas y las oportunidades comerciales, y la difunden de forma gratuita a los fabricantes que les han confiado la distribución de sus productos (Bayen 1.989).

Se estima que una Sogo Shosha típica dispone de unos diez mil empleados, repartidos por unas ciento ochenta oficinas en el extranjero, que pueden enviar cien mil mensajes diarios a la sede en Japón (Goodman, 1.990).

El mantenimiento de tales redes implica inversiones considerables en sistemas de información-telecomunicación que cubran todo el globo. "Las Sogo Shoshas son, de hecho, industrias de la información" (Goodman, 1.990).[43]

El Congreso de los Estados Unidos prepara una ley para combatir el problema del espionaje industrial, consciente de las millonarias pérdidas económicas que causa a las empresas.

Los congresistas han decidió actuar así debido a que, según las quejas recibidas, cada vez hay más gobiernos extranjeros que intentan obtener información confidencial sobre aspectos financieros, técnicos,

científicos o de ingeniería de empresas de EE.UU. para actuar en su propio beneficio.

La Sociedad Americana de Seguridad Industrial calcula que las pérdidas anuales de las empresas norteamericanas debido al espionaje industrial asciende a 20.000 millones de dólares anuales (2,5 billones de pesetas) y que afectan sobre todo a las empresas de ordenadores y telecomunicaciones.[44]

Toda esta situación es previsible que produzca un auge de la criptografía.

Si las organizaciones de inteligencia, que siempre resultan difíciles de controlar por los parlamentos, llegaran a entrelazarse con las actividades cotidianas de la sociedad de forma que hicieran imposible su control efectivo, la democracia peligraría.

Pero mientras el mundo sea mundo, las democracias necesitan las organizaciones de inteligencia para subsistir.

La forma en la que se maneje la información y el conocimiento en general, y dentro de él, la forma en la que se delimite, proteja y administre el secreto, así como los servicios con él relacionados, es y será uno de los temas políticos esenciales.[45]

Al ser la información y el conocimiento un elemento constitutivo del poder nacional, tanto su obtención como su protección forman parte del

mismo y, consiguientemente, han de ser -y de hecho lo son- objeto de atención preferente de los servicios de inteligencia de todo el mundo.

Por lo que se refiere a la criptografía, además de ser de uso tradicional en el ámbito de la inteligencia, es una faceta de su actividad a la que todos los servicios y agencias dedican especial atención.

En España, entre los órganos que integran el Centro Superior de Información de la Defensa, están las Divisiones de Inteligencia Exterior, Contrainteligencia, Inteligencia Interior, y Economía y Tecnología.

La División de Economía y Tecnología es a la que le corresponde, *"obtener, evaluar y difundir la información necesaria para prevenir cualquier peligro, amenaza o agresión exterior contra la industria y el comercio español de armamento y material de guerra y para asegurar los intereses nacionales en los campos de la economía y la tecnología de interés específico para la Defensa, así como velar por la seguridad de la información, tecnología, procedimientos, objetivos e instalaciones de interés para la Defensa, tanto propios como de los países aliados de España". (art. 7º del Real Decreto núm. 2632/85, de 27 de diciembre de 1.985).*

Al CESID le corresponde, además, *"coordinar la acción de los distintos organismos que utilicen medios o procedimientos de cifra, garantizar la seguridad criptográfica, promover la adquisición coordinada de*

material y formar al personal especialista". (Art. 5 del Real Decreto 1.883/1.996, de 2 de Agosto).

En lo referido a la función de coordinación de los distintos organismos que utilizan medios o procedimientos de cifra y a la facultad de promover adquisiciones coordinadas de material, tal vez el nudo gordiano de las posibilidades reales de llevarlas a cabo radique en el contenido jurídico-administrativo del concepto "organismo", su significado y alcance.

En este sentido García de Enterría, considera que no afecta en nada a la Administración del Estado el hecho de que en el seno de la misma puedan distinguirse diversos órganos. Todos los órganos de la Administración del Estado -los distintos Departamentos ministeriales y, dentro de éstos, las diferentes Direcciones Generales y servicios- son sólo simples órganos de una sola persona jurídica a la que imputan sus respectivas actividades.

La personalidad jurídica única no es óbice para que se traduzca en una pluralidad de capacidades, la competencia de los distintos órganos que componen esa persona jurídica única se ve compartida con frecuencia con la de otros que no pueden ignorar las atribuciones que las disposiciones en vigor pueden conceder o reconocer a los demás.

Recientemente, la Ley 6/1.997, de 14 de abril, de Organización y funcionamiento de la Administración General del Estado, en el artículo 1, al referir al ámbito de aplicación, indica que los Organismos públicos son las Entidades de Derecho público que desarrollan actividades derivadas de la

propia Administración General del Estado, en calidad de organizaciones instrumentales diferenciadas y dependientes de ésta.

En todo caso, y por lo que se refiere a la necesaria acción coordinada en relación con la Criptología, sería conveniente mayores precisiones normativas aprovechando las eventuales nueva ley de secretos oficiales, y ley de los servicios de inteligencia, así como sus normas de desarrollo.

Por lo que se refiere a la formación de especialistas en criptología, el CESID, anualmente, suele desarrollar un curso de Especialidades Criptológicas, para la obtención del título de Especialista Criptólogo.

Por Resolución 453/38604/1.997, de 28 de mayo, de la Dirección General de Reclutamiento y Enseñanza Militar del Ministerio de Defensa, (B.O.E. nº 146 de 19 de junio de 1.997),[46] se convocó el XII Curso de Especialidades Criptológicas, cuya finalidad es "Especializar en la protección de información mediante el empleo de técnicas criptológicas y capacitar para la dirección de una red de cifra".

El curso al que se accede tras superar un examen previo, tiene una duración de siete meses y va dirigido al personal militar perteneciente a la Escala Superior y al personal civil, funcionario del grupo A y no funcionario con categoría laboral de Técnicos titulados superiores que ocupen destinos que requieran especialización en el campo de protección de la información mediante el empleo de técnicas criptológicas; una vez superado con aprovechamiento se obtiene el título de "Especialista Criptólogo".

En el marco general de los objetivos de la inteligencia tecnológica donde se sitúa hoy todo lo relacionado con la criptología, los servicios de inteligencia suelen tener departamentos específicos que cubren las tareas tanto de criptografía como de criptoanálisis.

La información tecnológica o Techint, incluye: Información Sigint, que comprende a su vez comunicaciones, electrónica y telemetría; Radint, que barre las señales enviadas por los radares o a ellos, e Imaging, que incluye fotografía, infrarrojos y otros medios de detección.

Expresiones como "la guerra etérea", "la guerra electrónica" ó "la guerra de radio", son expresiones de una actividad que siempre existe, tanto en paz como en guerra, que es realizada en diferentes formas, de las que el servicio de información de señales o inteligencia de señales (SIGINT) y la seguridad de señales, son las significativas.

El SIGINT más extenso y calificado es realizado por naciones o grupos de países dentro de organismos internacionales. En tiempo de paz el propósito principal es obtener información diplomática y estratégica.

La interceptación y recopilación de señales tiene varios propósitos, tales como descubrir la formación de redes de comunicaciones, intensidad de tráfico etc. Mediante el análisis, complementado con otro tipo de información, se puede llegar a descubrir organizaciones, probables actividades u otros hechos, o funcionamiento de telesistemas.

Pero la parte de mayor interés del análisis es la que pasa por el texto del mensaje. Conocido como "criptoanálisis", tiene el propósito de desentrañar el sistema de cifrado usado, para poder leer la información secreta. El sigilo sobre los éxitos de este tipo de operaciones suele ser muy grande y rara vez se mencionan antes de que hayan pasado a ser historia, por una razón obvia, nadie desea cortar una corriente de información.

Junto con la actividad dirigida hacia actividades diplomáticas y militares, también hay una "guerra de señales" en menor escala, como puede ser la sistemática sintonización de las transmisiones de radio de la Policía, en la que estarían interesados los delincuentes.

El creciente uso de las computadoras para la transmisión aumenta los riesgos de que personas no autorizadas puedan intervenir en las comunicaciones. No son sólo las representaciones diplomáticas y la Defensa Nacional las que necesitan protección.

La protección del contenido del mensaje se lleva a cabo por la seguridad criptográfica (CRYPTSEC), hoy totalmente automatizados y que no sólo se orienta a la protección de mensajes escritos, sino de voz, imágenes, o datos.[47]

Y es precisamente en esa pugna clásica entre criptografía y descriptación donde adquiere especial relevancia una de sus misiones, que obliga a las agencias correspondientes a disponer de la información previa necesaria sobre criptología, a nivel internacional, que permita conocer en

qué momento los equipos y sistemas de protección criptológica utilizados por su país pueden ser rebasados por el criptoanálisis para, en su caso, y con carácter previo, aconsejar la utilización de mayores niveles criptológicos en la protección de las comunicaciones, que eviten su criptoanálisis por otras potencias, y, en definitiva, estar protegido a los niveles criptológicos internacionales más avanzados para poder neutralizar las amenazas procedentes de los modernos desarrollos electrónicos.[48]

Adscrito al Centro Superior de Información de la Defensa, está el Centro Criptológico Nacional, de reciente creación.[49]

Todo ello exige un indudable esfuerzo económico, tecnológico y de conocimiento, solo justificado por el alto valor de lo que se protege: la información.

De igual forma, los servicios de inteligencia han de proyectar sus capacidades criptológicas en el criptoanálisis, de forma que les permita estar en condiciones técnicas para criptoanalizar cualquier mensaje cifrado y poder dar cumplimiento efectivo a eventuales requerimientos en este sentido.

Por lo que se refiere al criptoanálisis, corresponde al Centro Superior de Información de la Defensa, a través de la Jefatura de Apoyo Operativo, *"criptoanalizar y descriptar por procedimientos manuales, medios electrónicos y criptofonía, así como realizar investigaciones tecno-*

lógico-criptográficas y formar al personal especializado en criptología". (art. 11.1, último párrafo, del Real Decreto 2632/85 de 27 de diciembre).

El criptoanálisis, como vimos en el Capítulo II, requiere la aprehensión previa del soporte del mensaje, -el criptograma-, sobre el que trabaja, lo que, de acuerdo con la Sentencia del Tribunal Constitucional 114/1.984, de 29 de noviembre, sería inconstitucional, y requeriría la correspondiente resolución judicial motivada -artículo 18.3 de la Constitución- que dé soporte legal a esta excepción del secreto de las comunicaciones.

La STC 114/1.984 afirma que "el derecho fundamental (del art. 18.3 CE) consagra la libertad de las comunicaciones, implícitamente, y, de modo expreso, su secreto, estableciendo en este último sentido la interdicción de la interceptación o el conocimiento antijurídico de las comunicaciones ajenas. El bien constitucionalmente protegido es así -a través de la imposición a todos del "secreto"- la libertad de comunicaciones, siendo cierto que el derecho puede conculcarse tanto por la interceptación en sentido estricto (que suponga aprehensión física del soporte del mensaje-con conocimiento o no del mismo- o captación, de otra forma, del proceso de comunicación) como por el simple conocimiento antijurídico de lo comunicado".

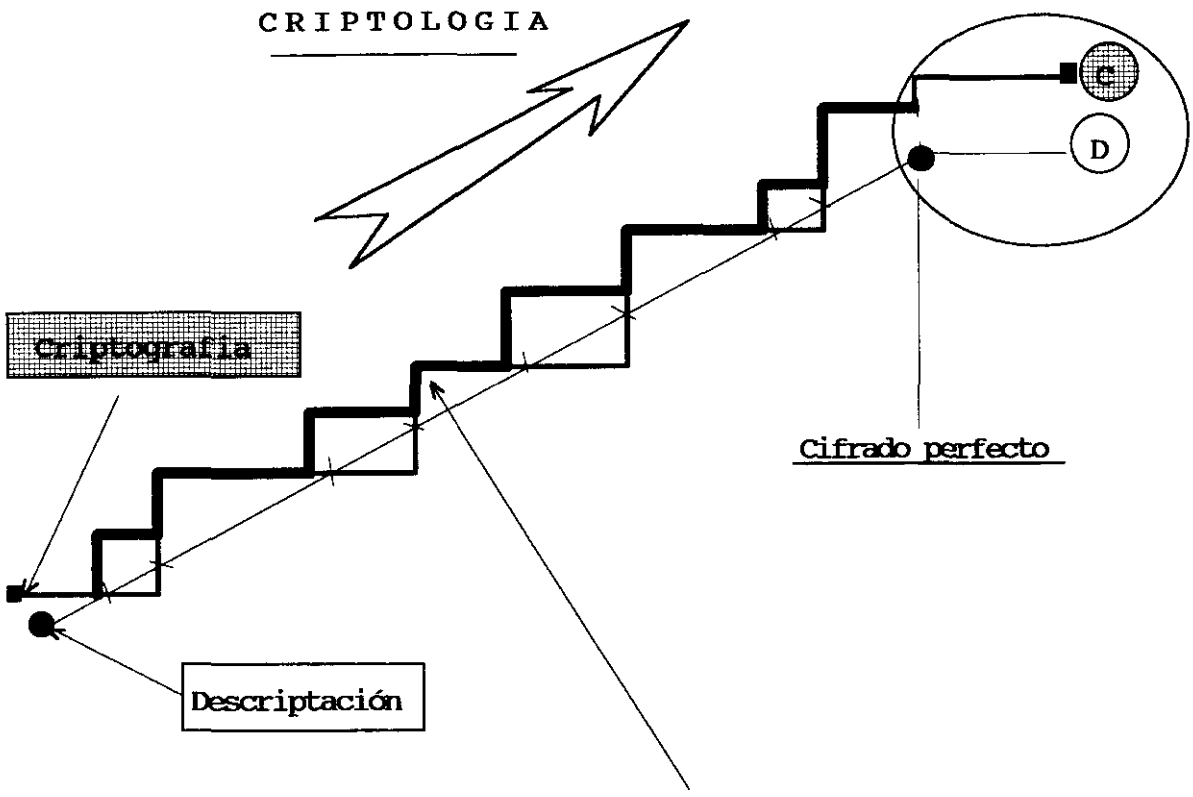
Todo ello nos podría llevar a las formas de control de los servicios de inteligencia que, con independencia de como se establezca al efecto en cada caso, -y comenzando por el rango legal de la norma reguladora de

estos servicios-, por lo que se refiere a la criptología, debería tener un componente judicial, que con ponderación de las circunstancias concurrentes y los intereses en juego, autorice o deniegue, en su caso, aquellas acciones en las que se excepcionen derechos y libertades fundamentales.

Según INFORME SEMANAL de Política Exterior nº 71 del 14 de abril de 1.997, se podría estar a las puertas de una nueva etapa en la inteligencia española, lo que eventualmente se llevaría a cabo al hilo de la nueva Ley de Secretos Oficiales, y comportaría la articulación de un nuevo marco legal que la ampare, limite y controle, contemplándose, incluso, la posibilidad de un cambio de denominación entre las que estaría la de Servicio Español de Inteligencia Secreta (S.E.I.S.).

En esta nueva etapa tal vez los servicios de inteligencia encuentren articulación legal en una ley específica.[50]

E V O L U C I O N



NIVELES CRIPTOLOGICOS TRAS PREVISIONES DE INTELIGENCIA

[1] Molina Mateos, J.M., "Seguridad, información y poder", Edit. Incipit, Madrid, 1.994

[2] Rodriguez Prieto, A., "Protección de la información", Edit. Paraninfo, Madrid, 1.985.

[3] Díez de Velasco, M., "Instituciones de Derecho Internacional Público", Tomo y, Editorial Tecnos, 1.976, pág. 385.

[4] Merle, M., "Sociología de las relaciones internacionales", Alianza Universidad, Madrid, 1.984.

[5] Molina Mateos, J.M., "Seguridad, información y poder", Edit. Incipit, Madrid, 1.994.

[6] Sun Tzu, "The Art of The War", The Clarenton Press, Oxford, 1.963.

[7] Herrero de Miñón, M., "Entre dos siglos. Reflexiones sobre la democracia española", Alianza Editorial, Madrid, 1.996, pág. 3.

[8] Herrero de Miñón, M., op. cit., pág. 3

[9] Informe Semanal de Política Exterior, nº 46, octubre de 1.996.

[10] Olivares Solina, y., "Nuevos retos para la seguridad nacional", Revista Española de Defensa, número 101-102, julio-agosto de 1.996.

[11] Molina Mateos, J.M., "Marco de referencia para un modelo de servicio militar", comunicación presentada en el Panel de Expertos sobre "El servicio militar en Europa", organizado por la Fundación Ciencia, Democracia y Sociedad, Madrid, diciembre, 1.990.

[12] The Economist, marzo 1.997.

[13] Cornella, A., "Los recursos de información", Serie McGraw-Hill de Management, ESADE, Madrid, 1.994.

[14] Ortega García, R., "Control interno, auditoria y seguridad informática",EXPANSIÓN, Madrid, 1.996.

[15] Dávila, J., Morant, J.L. y Sancho, J., "Control gubernamental en la protección de datos: Proyecto Clipper". Universidad Pontificia Comillas. Madrid. Aranzadi, 1.997.

[16] Bauer, F.L., "Dcrypted secrets", Springer Verlag, Berlin, 1.997, pág. 200.

[17] Julio Téllez Valdes, Carlos Sarzana, Nidia Callegari, Rafael Fernández Calvo, Maria de la Luz Lima, en "Concepto de 'delitos informáticos'", Delitos informaticos: Definición, *http://tiny.uasnet.mx/prof/cln/der/silvia/define.htm*

[18] Digesto, Libro 50, Texto 17, Par. 202.

[19] Servicio de inteligencia: "Conjunto de órganos de inteligencia que sirven a un determinado nivel de decisión". (Fernando Rueda, "LA CASA", Edit. temas de Hoy, 1.993, y Manual de Inteligencia , publicado por la revista TIEMPO, julio de 1.995).

[20] Prefacio de "El arte de la guerra", de Sun Tzu, en la versión de Thomas Cleary, ha sido editado en España en 1.993 por Ediciones Tiempo, S.A., en edición especial parala revista Dinero.

[21] Sgarro, A., op. cit. pág. 84.

[22] Cornella, A., op. cit. pág. 80.

[23] Chirac, J., Presidente de la República Francesa, discurso sobre profesionalización completa de las Fuerzas Armadas, Escuela Militar de París, 23 de febrero de 1.996.

[24] Cachinero, J., y Trujillo, J., "La guerra silenciosa: el futuro de los servicios de inteligencia". Política Exterior, número 34. (verano 1.993).
[25] Le Monde Diplomatique, Diciembre, 1.996.
[26] Reuter-El Mundo, 10 enero 1.997.
[27] Cachinero, J., y Trunillo, J., op. cit.
[28] Nyer, J. y Owens,W.A., "Estados Unidos y el poder de la información", Política Exterior, núm. 51, mayo-jnio, 1.996.
[29] Nyer, J. y Owens, W.A., op. cit.
[30] Nyer, J. y Owens, W.A., op. cit.
[31] Cachinero, J., y Trujillo, J., op. cit.
[32] El Mundo, 21 de junio de 1.997.
[33] Toffler, A. y H., "Las Guerras del Futuro", op. cit.
[34] Brown, R., Secretario de Comercio de Estados Unidos.
[35] Toffler, A. y H., "La creación de una nueva civilización", Editorial Plaza & Janes, Barcelona, 1.995, pág. 55.
[36] Expresión incluida en el comunicado enviado por Donoso Cortés al Ministerio de Asuntos Exteriores, siendo Embajador en París, el 24 de febrero de 1.853.
[37] Amford, J., "The puzzle pace", breve resumen sobre la Agencia Nacional de Seguridad, publicado en El País, 26 de septiembre de 1.982.
[38] Toffler, A., "El cambio del poder", Plaza & Janes, Barcelona, 1.990, pág. 351.
[39] Comas, J., Gómez, L., González, E. y Egurbide, P., "Los espías de la Unión", el País, 2 de junio de 1.996.
[40] El Mundo, domingo, 7 de diciembre de 1.997.
[41] Editorial de "Economía Exterior", suplemento de Política Exterior, sobre internacionalización de la Economía Española, 1.995/1.996 (nº 48 de Política Exterior).
[42] Cornella, A., op. cit. pág. 81.
[43] Cornella, A., op. cit., pág. 82.
[44] El Mundo, 10 de agosto de 1.996.
[45] Toffler, A., "El cambio del poder", op. cit., pags. 344 y ss.
[46] Boletín Oficial del Estado, nº 146, de 19 de junio de 1.997.
[47] Gerente General de AB Transvertex, discurso de 10 de septiembre de 1.976.
[48] Molina Mateos, J.M., op. cit. pág. 54.
[49] Jimenez, L, "La Criptología: principios básicos", Jornadas de la Abogacía y las Nuevas Tecnologías de la información y la comunicación, 15-18 de octubre de 1.996, organizadas por el Ilustre Colegio de Abogados de Madrid.
[50] Informe Semanal de Política Exterior, nº 121 de 27 de abril de 1.998, reitera la necesidad de una ley para los servicios secretos.

C A P I T U L O IV

PERSPECTIVA JURÍDICA
DE LA
PROTECCIÓN CRIPTOLÓGICA

4.1.- CRIPTOLOGÍA Y DERECHO.

El valor de la información y, consiguientemente, su poder, requiere que, en ocasiones, se utilicen instrumentos para asegurarla.

En este sentido, la seguridad de la información y la criptología como elemento esencial de la misma, actúan como coadyuvantes y, en cierto modo vienen a ser depositarios de dicho poder y como tales, participan de las características intrínsecas del mismo.

Pero mientras el poder pertenece a la esfera de lo fáctico, el derecho pertenece a la esfera del deber ser. Las relaciones entre Criptología y Derecho, nos llevan, en cierto modo, y en última instancia, a las relaciones de Derecho y Poder.

El derecho regula las relaciones interhumanas y limita tanto el poder del individuo como el de la sociedad, y tiene la doble función de regular la vida de relación y garantizarla.

En una moderna sociedad democrática, la autoridad del Estado no exige la exclusividad, pero sí requiere la hegemonía para poder garantizar la paz interior y exterior y, garantizar los derechos y libertades individuales, en definitiva, tiene el deber de defender la sociedad y su democrático funcionamiento.

En este proceso, el individuo cede parcelas de su poder a la comunidad y lo recupera en garantías de derechos y libertades individuales.

Tanto el derecho como el poder son principios reguladores de la acción social y ambos son interdependientes y complementarios. La armónica combinación de ambos elementos de ordenación social constituye en esencia lo que se ha dado en llamar el *"arte de la política"*.

La paz, la estabilidad, o simplemente los intereses del Estado, o de una organización, puede verse amenazados por egoísmos individuales, egoísmos de grupos, o por egoísmos de otros estados u organizaciones competidoras, en muchos grados y con distinta intensidad. Y estas amenazas se producen, actualmente, en una proporción elevada en el entorno de la información, por lo que para neutralizarlas se demanda, cada vez más, su protección cuyo instrumento fundamental es la criptología.

Por todo ello nos parece evidente el nexo de unión entre Criptología, Poder y Derecho. Desde esta concepción y teniendo en cuenta esta relación es como se puede abordar una reflexión sobre la Criptología desde una perspectiva jurídica.

La Criptología es un instrumento para lograr el ejercicio efectivo de determinados derechos. Derechos que no son otra cosa que manifestaciones de poder en sus distintos grados.

A la vez, la Criptología cuya misión es ser eficaz, también comporta una eficacia en la sustracción de informaciones al conocimiento público, con todo lo que ello implica para las libertades de expresión es información.[1]

Todo ello genera una complejidad que aconseja tratar el tema desde los más diversos ángulos.

En la base de toda protección criptológica está la necesidad de garantizar la confidencialidad de un ámbito de información, por lo que su delimitación resulta un presupuesto básico para poder alcanzar una protección real y efectiva.

4.2.- ÁMBITOS DE CONFIDENCIALIDAD.

El sustantivo "confidencialidad", proviene de "*confidencial*", adjetivo aplicable a lo *"que se hace o se dice en confianza o con seguridad recíproca entre dos o mas personas"*, derivado de *"confidencia: Revelación secreta, noticia reservada"*, y que mucho tiene que ver con el concepto de *"secreto"*.[2]

Por virtud de la confidencialidad un sistema de información sólo permite el conocimiento de la misma a quienes estén autorizados, lo que sería una forma de preservar la naturaleza del "secreto", considerado en abstracto, como *"conocimiento de objetiva relevancia que voluntariamente se oculta a una o más personas."* [3]

El secreto es de naturaleza deóntica antes que cognitiva, pues se establece por la prohibición de divulgar y no por la imposibilidad de saber -como ocurre con el misterio-.[4]

La palabra secreto aparece en el Diccionario de la Real Academia de la Lengua Española dos veces. En la primera, señala la procedencia

de la palabra latina *secretum* y, en su acepción 1 indica que es "Lo que cuidadosamente se tiene reservado y oculto" y, en la acepción 2 "Reserva, sigilo".

La segunda vez que aparece la palabra secreto en el Diccionario de la Real Academia, lo hace como adjetivo e indica la procedencia del latín *secretus*, (participio de *scernere*, segregar) y en su acepción 1 señala que es lo "Oculto, ignorado, escondido y separado de la vista o del conocimiento de los demás".

De la definición gramatical se puede desprender que lo secreto además de ser algo separado o segregado debe ser, también, oculto.

Secreto, por consiguiente, como instrumento de paz y armonía, donde encuentra su justificación, y cuya eficacia en el ámbito comunicativo se vería garantizada, entre otros, por la aplicación del lenguaje criptológico, en el que opera una recodificación, cuya singularidad está en subrayar el ámbito restringido y excluyente de los grupos que intercomunica.

Para Arturo Ribagorda, confidencialidad es: "1.- Propiedad de la información que impide que ésta esté disponible o sea revelada a individuos, entidades o procesos no autorizados (ISO 7498-2). Según esta norma la confidencialidad es un servicio de seguridad.

2.- Prevención de la revelación no autorizada de información (ITSEC).

3.- Característica de los datos e informaciones que son revelados sólo a los usuarios, entidades o procesos en el tiempo y forma autorizados (OCDE).

El mantenimiento de la confidencialidad, junto con el de la integridad y disponibilidad, constituye el objetivo de la seguridad de la información".[5]

No toda la información manejada por una organización incide del mismo modo en su funcionamiento y logro de sus objetivos. Existen informaciones que por su importancia vital para la organización constituyen un activo estratégico, y cuya pérdida puede llegar a ser gravemente perjudicial, e incluso letal, para la misma, mientras que otras, aún manteniendo el valor intrínseco atribuible a toda información en un sentido genérico, incorporan un valor de menor entidad cuya pérdida produce efectos o perjuicios de efectos menos significativos.

En medio de ambas clases de informaciones existe toda una gama de grupos y grados de interés intermedios.

Por ello, la información, como activo de cualquier organización, ha de ser clasificada según el grado de sensibilidad e importancia para la misma y, en base a ello, poder definir la que debe ser protegida y con qué niveles.

El control de la totalidad de la información que fluye por una organización es difícil y costoso, no obstante puede haber casos en que así

se requiera, pero generalmente, junto a las informaciones que han de ser preservadas, existen otras que requieren ser difundidas y por tanto no necesitan ser protegidas.

Por ello, en primer lugar, es necesario distinguir la información que merece ser controlada del resto.

Y dentro del primer grupo, la que es vital para su funcionamiento y altamente sensible por su grado de confidencialidad y susceptibilidad de revelación, riesgo de modificación, o destrucción.

Pero la delimitación de estos ámbitos de confidencialidad y su protección, no es pacífica, llegando a constituir uno de los temas políticos esenciales a nivel mundial en las países con sistemas democráticos.

En 1.974, tras los años de Vietnam y Watergate, el juez Warren, que fue gobernador del estado de California y ex presidente del Tribunal Supremo de los EE.UU., decía que "el nivel de secreto admisible, tanto en los ámbitos gubernamentales más elevados como en los más bajo, debería definirse mediante ley..." y en base al consenso de periodistas, juristas, politólogos junto a los representantes federales y estatales ponerse de acuerdo sobre la definición de un ámbito esencial de confidencialidad dejando el resto abierto al control público.

Esta solución omnicomprensiva propuesta por Warren sigue siendo necesaria hoy. Pero la delimitación de ámbitos y niveles de confidencialidad es insuficiente. Su protección real y efectiva en la era de la

información añade exigencias que demandan ampliar el consenso, con la incorporación de tecnólogos y expertos en criptología y, entre todos, sentar las bases para una solución integral,[6] en un clima de confianza de toda la sociedad.

Muchas son las clases de secreto y, diferente son, por tanto, los ámbitos de confidencialidad.

1.- *Secretos públicos y secretos privados*:[7] Los secretos públicos se subdividen en secreto de Estado que es aquel que tiene como elemento objetivo la seguridad y defensa del Estado, entendida en un sentido amplio, incluyendo aspectos políticos, económicos, militares, diplomáticos, científicos, industriales etc., "pues todos ellos tienen relación muy directa con la supervivencia del Estado."[8], y, secretos funcionariales que garantizan el normal funcionamiento de la Administración pública.

Los secretos privados incluyen los referidos a la personalidad, a la intimidad personal o familiar y a los de contenido patrimonial.

2.- Por razón del objeto se pueden distinguir por su *legalidad o ilegalidad* y, por razón de la materia.

3.- Por razón del carácter oculto del conocimiento se atiende fundamentalmente a la intensidad de la ocultación del mismo. Estando en un extremo el *conocimiento público* que, al no estar oculto, no cabe hablar de secreto. Sáinz Moreno entiende que "La intensidad con la que cada secreto constituye un saber oculto frente a los demás, puede ser *absoluta* (se oculta,

incluso, la existencia misma del secreto) o *relativa* (se reconoce la existencia de un secreto sobre cierta materia, pero se oculta su contenido, o su alcance o sus causas, etc.). A veces el secreto se cubre mediante informaciones falsas, inexactas o incompletas".[9]

4.- Por razón del elemento subjetivo pueden ser *secretos voluntarios y accidentales y secretos con voluntad expresa y tácita.*

5.- Por razón del elemento objetivo, en función de la naturaleza puede ser *un interés, un bien, jurídico o no, e incluso un bien jurídico protegido penalmente.* También se pueden clasificar por su unidad o pluralidad y en función de su temática.

6.- Por razón de los sujetos, la primera clasificación es por la existencia o no de los sujetos, en base a lo cual se podrían distinguir *secretos absolutos y secretos relativos*. Los primeros, esto es, los secretos absolutos serian aquellos que nadie conoce por lo que al faltarle uno de los elementos estructurales se podría considerar que no se trata de un secreto (tal vez sería un misterio).

Por razón del sujeto activo se puede distinguir entre *sujeto titular y depositario*. El primero decidiría si el conocimiento ha de permanecer oculto o no y en qué condiciones. El segundo es un sujeto que por cualquier motivo, accede legítimamente al conocimiento pero sin poder decidir sobre él.

También, por razón del sujeto activo se puede distinguir entre persona física y persona jurídica y dentro de ésta, pública y privada.

De igual modo cabe diferenciar entre sujeto individual y plural.

7.- Por razón de la regulación cabría distinguir entre *secreto jurídico y no jurídico.*

De donde se derivan diferentes y variados ámbitos de confidencialidad: el *secreto de Estado, secreto militar, secreto diplomático, el secreto fiscal, el secreto médico, secreto notarial, el secreto sumarial, el secreto profesional, el secreto comercial, secreto industrial* ... etc.

En el ámbito empresarial se suele distinguir entre información clasificada y no clasificada. Dentro del primer grupo, Confidencial, Restringida o Reservada, y de uso interno.

Con independencia de las clasificaciones a que se pueda llegar que es algo susceptible de ser abordado desde multiples enfoques, sí existe una primera y gran clasificación de ámbitos de confidencialidad en cuyo seno se engloban todas las demás: ámbitos públicos y ámbitos privados, que se vienen a corresponder con los reductos de confidencialidad aplicables a la información pública y a la información privada, como los dos grandes bloques en que podría estar agrupada la información y que así son, incluso, objeto de trato constitucional, en el artículo 20 de la C.E. referido a la información pública y el 18 de la C.E. referido a la información privada.

La delimitación del ámbito de confidencialidad es el paso previo para una protección efectiva adecuada.[10]

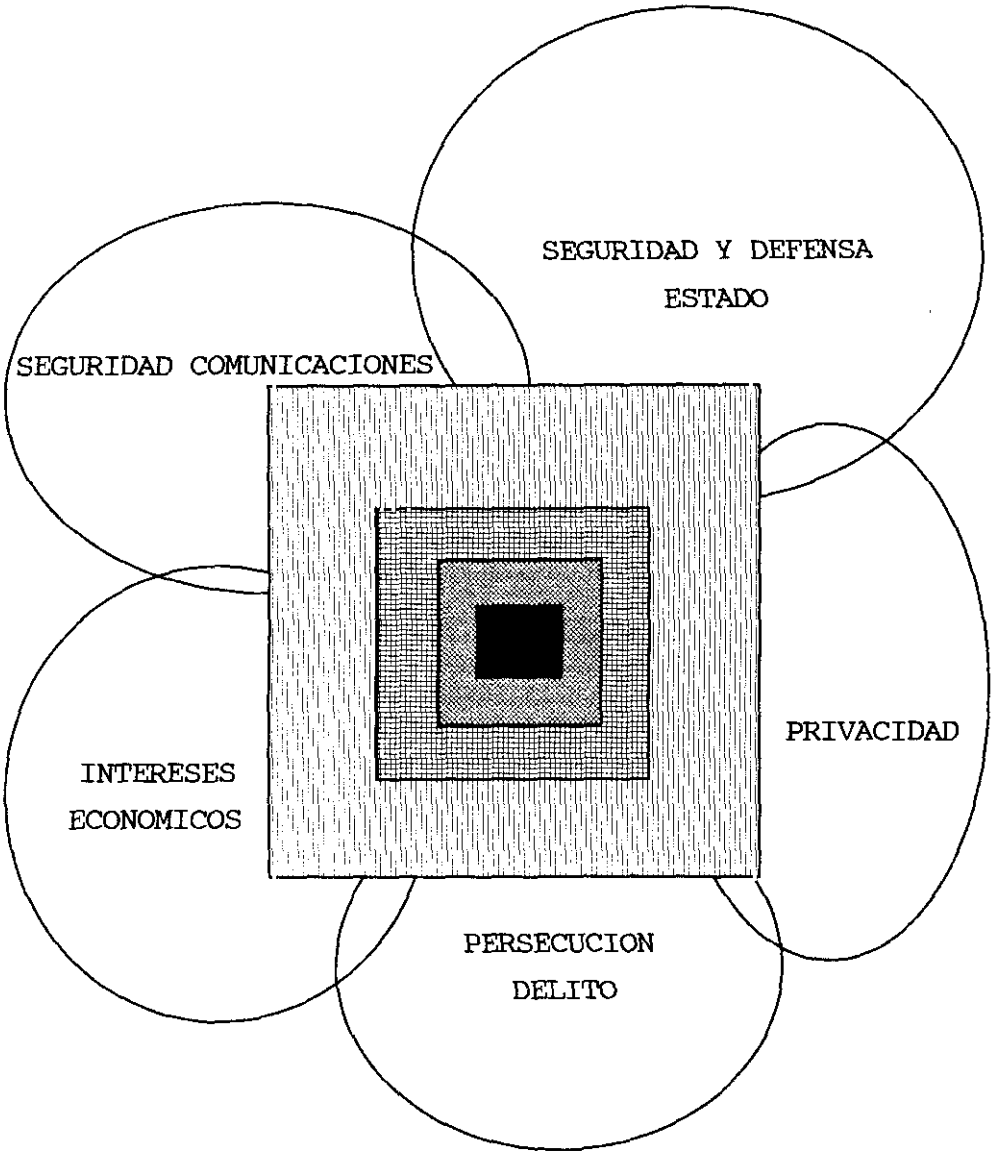
4.2.1.- DELIMITACIÓN DE ÁMBITOS PÚBLICOS DE CONFIDENCIALIDAD.

La Exposición de Motivos de la Ley 9/1.968, de 5 de abril sobre Secretos Oficiales proclama como principio general la publicidad de la actividad de los órganos del Estado, porque las cosas que a todos interesan pueden y deben ser conocidas por todos.[11] Es lo deseable en aras a la participación, considerada en la actualidad derecho fundamental.[12]

El carácter de generalidad -y no de universalidad- atribuido al principio de publicidad, lleva de forma inmediata a admitir que, por definición, permite excepciones.

Para un sector de la doctrina, los secretos oficiales existen en su calidad de excepción al principio de difusión general que caracteriza al Derecho de los Mensajes, una parte muy específica del Derecho de la Información, entendido como Ciencia y como Micro-Ordenamiento.[13]

Aunque la aceptación del secreto viene a suponer, en cierto modo, una renuncia a las exigencias de la democracia, la transparencia no implica la inexistencia de reductos de confidencialidad que, con la debida justificación y garantía, constituyen una excepción al régimen general de la información pública y que adoptan la forma de *"secreto oficial"*.



AMBITOS DE CONFIDENCIALIDAD

4.2.1.1.- TRANSPARENCIA DE "LO PÚBLICO".

La justificación del principio de publicidad se basa en el fundamental derecho ciudadano a participar en los asuntos públicos con la máxima información posible, que hoy se encuentra amparado por el artículo 23.1 de la Constitución que dice: *"Los ciudadanos tienen el derecho a participar en los asuntos públicos, directamente o por medio de representantes, libremente elegidos en elecciones periódicas por sufragio universal"*.

La información de que se disfruta modulará las opiniones y decisiones de los ciudadanos en un sentido u otro.[14]

La transparencia en los asuntos públicos es consustancial con los regímenes democráticos.[15] En el plano socio-político existe una profunda vinculación entre el principio de publicidad de las decisiones gubernamentales y los propios fundamentos de la democracia que, como forma de gobierno, excluye por principio la opacidad de las decisiones.

En el ámbito administrativo, el artículo 105, b) de la Constitución señala que la Ley regulará *"El acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas"*.

La Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (Ley 30/1.992, de 26 de noviembre, recoge en su Exposición de Motivos una referencia a las nuevas corrientes de la ciencia de la organización que *"aportan un enfoque adicional en*

cuanto mecanismo para garantizar la calidad y transparencia de actuación administrativa, que configuran diferencias sustanciales entre los escenarios de 1.958 y 1.992..."

El término transparencia ha venido a sustituir al término publicidad y tiene que ver con la facultad de investigar del particular, de acceder a datos o fuentes de información.[16]

En el ámbito del poder legislativo, también existe una cierta regulación del principio de publicidad respecto a las actuaciones de las Cortes. Los Reglamentos del Congreso en sus artículos 63 y 64 y del Senado en los artículos 72 y 75, así lo señalan, con sus excepciones.

Por lo que se refiere a la publicidad judicial, el artículo 24 de la Constitución señala que: *"...Todas las personas tienen ...derecho a... ser informados de la acusación formulada contra ellos, a un proceso público sin dilaciones indebidas y con todas las garantías...".*

Sin embargo, el artículo 105, b) , antes citado, excluye del acceso ciudadano a los archivos de la Administración cuando afecte a la averiguación de los delitos.

Por su parte, el artículo 120 de la Constitución dispone que: *"Las actuaciones judiciales serán públicas, con las excepciones que prevean las leyes de procedimiento"* y *"las sentencias serán siempre motivadas y se pronunciarán en audiencia pública".*

En el mismo sentido, el artículo 232 de la Ley Orgánica del Poder Judicial, reitera esta publicidad en su apartado 1 y, añade en el apartado 2 *"Excepcionalmente, por razones de orden público y de protección de los derechos y libertades, los Jueces y Tribunales, mediante resolución motivada, podrán limitar el ámbito de la publicidad y acordar el carácter secreto de todas o parte de las actuaciones"*.

De otra parte, el artículo 7 de la Ley de Prensa (L. 14/1.966, de 18 de marzo), considerado vigente por parte de la doctrina iusinformativa, regula el derecho a obtener información oficial de la siguiente manera: *"1.- El gobierno, la Administración y las Entidades públicas deberán facilitar información sobre sus actos a todas las publicaciones periódicas y agencias informativas en la forma que legal o reglamentariamente se determine. 2. La actividad de los expresados órganos y de la Administración de justicia será reservada cuando por precepto de la Ley o por su propia naturaleza sus actuaciones, disposiciones o acuerdos no sean públicos o cuando los documentos o actos en que se formalicen sean declarados reservados"*.

La transparencia de lo público se complementa y potencia con las libertades de expresión e información recogidas en el artículo 20 de nuestra Constitución, que legitiman el funcionamiento del sistema democrático y la eficacia de sus instituciones.[17]

La transparencia es un valor fundamental que sólo excepcionalmente y con muy fundadas razones, cabe marginar.

La ocultación de las decisiones y los motivos que la fundamentan, se suele considerar como radicalmente incompatible con el principio democrático que debe inspirar toda actividad pública.

Es generalmente admitido que junto a las proclamas de una transparencia ilimitada para los asuntos de gobierno, existan restricciones justificadas, dirigidas a la preservación de los intereses generales.

En todo caso, la consideración y el análisis pormenorizado de estos principios, y sus límites, ha de hacerse con grandes cautelas. Porque una formulación incondicionada del principio de publicidad -con eliminación total del secreto- podría poner en peligro importantes fundamentos del propio régimen democrático, los derechos fundamentales e, incluso, la existencia del propio Estado que los sustentan.

Se trata de una tensión para cuya óptima solución no son válidos postulados románticos en defensa de una trasnsparencia incondicionada e ingénua ni, tampoco, el atrincheramiento en el ocultismo y la opacidad. El resultado ideal debería ser el punto crítico y objetivo de equilibrio entre la publicidad o transparencia como norma general y el imprescindible secreto en determinados casos y asuntos concretos.

Los principios y valores que recoge nuestro texto constitucional son incompatibles con las interpretaciones restrictivas de la transparencia y publicidad de las acciones gubernamentales. Las disposiciones constitucionales y la normativa de desarrollo, ofrecen buenas perspectivas para la tutela

del principio de transparencia de las acciones administrativas y consiguiente relegación del secreto.

Desantes Guanter establece un principio básico para la resolución de los casos concretos, la regla general es el principio de publicidad, que siempre se ha de interpretar de manera favorable y extensiva. La excepción es la reserva y el secreto que se deberá interpretar restrictivamente[18]

Como sostiene Jorge de Esteban, "las verdaderas democracias se caracterizan por la publicidad de lo público y el secreto de lo privado, el totalitarismo se define, en sentido contrario, por la publicidad de lo privado y el secreto de todo lo público".[19]

En línea con la transparencia de los asuntos públicos va el "Libro Blanco" para eliminar la enraizada cultura del secreto, anunciado por Tony Blair, Primer Ministro de Gran Bretaña, durante el mes de diciembre de 1.997.

Según este plan cualquier ciudadano puede conocer las prioridades de las inversiones gubernamentales, cómo funcionan los mecanismos de la BBC, tener acceso a los archivos históricos, información sobre sistemas educativos, e incluso, hasta conseguir datos limitados de las Fuerzas Armadas, todo ello siempre que la información de que se trate no cause "daño sustancial" al interés público.

Lo que el Libro Blanco propone es el concepto de que el pueblo tiene pleno derecho a saber lo que el Gobierno hace en su nombre y se

podría considerar como decisivo en la busqueda de un Gobierno abierto, a la vez que pone en cuestión el "secreto administrativo" de larga tradición británica, cuyos orígenes se remontan al año 1.250, cuando se instauró en los consejos aldeanos el juramento a no divulgar confidencias relacionadas con la función de la autoridad.

Las cuestiones de seguridad nacional, los temas de Defensa, Inteligencia, los servicios de Policía, la privacidad personal, la confidencialidad en el mundo del comercio, la seguridad pública y el medio ambiente y, el amplio ámbito de la información suministrada confidencialmente, estarán protegidos dentro del plan propuesto.[20]

4.2.1.1.1.- LÍMITES A LA TRANSPARENCIA DE "LO PÚBLICO": EL SECRETO OFICIAL.

Como se ha indicado en el epígrafe anterior, junto al principio general de transparencia en las diferentes esferas de poder, existen restricciones, limitaciones o excepciones fundadas en intereses generales de la colectividad, y que vienen consagradas no solo en la doctrina española, sino a nivel internacional

Junto al principio de difusión general de la información administrativa, el legislador proclama que existen limitaciones al mismo, cuando se pueda perjudicar la "causa pública, la seguridad del Estado o los intereses de la colectividad nacional", y sitúa en este contexto las cuestiones "cuyo

conocimiento por personas no autorizadas pueda dañar o ponga en riesgo la seguridad del Estado o los intereses fundamentales de la nación y que constituyen los verdaderos *secretos oficiales...*",[21] que vienen a configurar el principal ámbito público de confidencialidad.

Desde el principio el secreto oficial queda vinculado al interés esencial del Estado y a su seguridad. Aunque, al mismo tiempo, el legislador da a entender que pueden existir otros secretos oficiales que no afecten al mismo.[22]

En lo que se refiere a la información y las comunicaciones, la transparencia de lo público tiene su articulación constitucional en el artículo 20 de la Constitución donde se amparan las libertades de expresión e información.

Mientras que la información es un fin en sí misma, cuando se identifica con la acepción dinámica de comunicación, los secretos oficiales tienen la naturaleza de medios o instrumentos para la consecución de un fin.

Para Pilar Cousido, los secretos oficiales se hallan al servicio de otro derecho, el derecho a la paz, que es un elemento final. "El derecho a la Información, a la comunicación, en el fondo es también el derecho a la comunidad y a la paz. Sin comunicación no hay paz y sin paz no hay comunicación. Puesto que la interrelación se manifiesta simbiótica, carece de sentido enfrentar dos instituciones que se pueden necesitar y además, formalmente, es inoportuno si se tiene en cuenta la naturaleza instrumental

de una de ellas -los secretos oficiales- y la naturaleza final de otra -la comunicación-".[23]

En la medida en que la paz de una comunidad depende de cuestiones tales como la seguridad, los secretos oficiales pueden ser el instrumento para garantizar ambas.

El derecho a la Información y a la comunicación, es también el derecho a la comunidad y a la paz, por lo que, los secretos oficiales -y las medidas para su protección efectiva-, como instrumentos para conseguirlo, forman parte de estos derechos.

En una sociedad lo que garantiza la seguridad y la defensa es la paz. La clasificación de materias es un instrumento para lograr esa seguridad y, por tanto, la paz.

A su vez, la garantía y protección de la información es la garantía y la protección de la propia comunidad.

La investigación, la difusión y la recepción de mensajes son instrumento para lograr la información, realizados al amparo del ejercicio legítimo de los derechos y libertades de expresión e información, que a su vez contribuyen a la formación de una opinión pública libre, elemento básico de un régimen democrático. Solo cuando la difusión de determinados mensajes pudiera alterar la paz de un Estado estaría justificado obstaculizar el libre ejercicio de estos derechos y libertades. Derecho y, consecuentemente, la efectividad de las libertades públicas.

Como única justificación del secreto estaría la prueba del daño directo e inminente que se cierne sobre el Estado o el pueblo.[24]

Para Pilar Cousido, la expresión *"secreto oficial"* podría suscitar la duda de si se trata de una *"contraditio in terminis"*, puesto que lo que es oficial no puede ser secreto, ya que no sólo es conocido sino que es oficialmente informado. La calificación de oficial tiene carácter formal y no material, lo oficial no es el contenido sino la forma que adquiere el secreto. [25]

No existe una delimitación precisa del concepto de "secreto oficial", ni en la ley ni en la doctrina.

Según la Ley 9/1.968, de 5 de abril, sobre secretos oficiales, modificada por Ley 48/1.978, de 7 de octubre, "*Los órganos del Estado estarán sometidos en su actividad al principio de publicidad, de acuerdo con las normas que rijan su actuación, salvo los casos en que por la naturaleza de la materia sea ésta declarada expresamente "clasificada", cuyo secreto o limitado conocimiento queda amparado por la presente Ley.*

Tendrán carácter secreto, sin necesidad de previa clasificación, las materias así declaradas por Ley". (art. 1).

A los efectos de esta ley podrán ser declaradas "materias clasificadas" los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas pueda dañar o poner en riesgo la seguridad y defensa del Estado. (art. 2).

El secreto oficial conceptualmente abarca un espacio más amplio que el correspondiente al secreto de Estado, dentro del cual, éste queda amparado.

Igualmente, la terminología sobre el secreto de Estado no es pacífica, sin que exista un concepto ni doctrinal ni legal unánime, no obstante se puede decir que secreto de Estado es aquel que tiene como elemento objetivo la seguridad y defensa del Estado, entendida en un sentido amplio, de forma que incluya tanto aspectos políticos y militares como diplomáticos, científicos, industriales o económicos, y todos los que tienen una relación directa con la supervivencia del Estado.[26]

En este sentido, la Sentencia del Tribunal Central Militar de 11 de julio de 1.989, señala que el concepto de Defensa Nacional "supera la dimensión de la defensa militar estricta para integrarse en la política general del Estado, teniendo en cuenta las exigencias militares, internacionales, socioeconómicas e, incluso científicas, la protección de los secretos de Estado comprende no solo los circunscritos al orden militar sino todos aquellos que pueden afectar a la seguridad de la nación, aunque sean de índole política, diplomática o meramente económica".

En un Estado democrático se puede admitir la existencia de secretos oficiales, pero restringiendo al máximo su aplicación.

La publicidad de los actos del Estado ha de ser el principio general y la limitación como excepción, lo que requiere:

1.- Concreción del ámbito material del secreto oficial, reduciéndolo a los casos que puedan comprometer la seguridad y defensa del Estado, fundamentalmente en su dimensión exterior.

2.- Delimitación clara de las conductas que atentan contra la seguridad y defensa del Estado.

3.- Distinción entre la conducta exigible al funcionario para su protección y custodia, de la de los medios de comunicación por su publicación.

4.- Intervención parlamentaria a través de comisiones especiales y sesiones no públicas.

5.- Control judicial.[27]

4.2.1.1.1.1.- LEY 9/1.968, DE 5 DE ABRIL, SOBRE SECRETOS OFICIALES.

MODIFICADA POR LA LEY 48/1.978, DE 7 DE OCTUBRE.

La Ley de Secretos Oficiales de 1.968, en su exposición de motivos, dice que la publicidad de la actividad de los Órganos del Estado es el principio general, porque las cosas públicas que a todos interesan puede y deben ser conocidas por todos, no obstante es innegable la necesidad de imponer limitaciones, cuando precisamente de esa publicidad puede derivarse perjuicio para la causa pública, la seguridad del mismo Estado o los intereses de la colectividad nacional.

Destacan por su importancia aquellas cuestiones cuyo conocimiento por personas no autorizadas pueda dañar o ponga en riesgo la

seguridad del Estado o los intereses fundamentales de la Nación y que constituyen los verdaderos "secretos oficiales", protegidos por sanciones penales que alcanzan penas de la máxima severidad. Pero esta sanción penal, especialmente represiva, sólo de una manera indirecta, por medio de la intimidación, protege el descubrimiento o revelación de secretos. Las medidas de protección eficaces son las que la propia administración ha de establecer para garantizar que los documentos o materiales en que físicamente se reflejan los secretos no puedan ser conocidos más que por aquellas personas que, por razón de su cometido, estén autorizadas para ello.

En este aspecto -continúa diciendo la exposición de motivos- existe una laguna en nuestra legislación que, al contrario de lo que ocurre en los Estados caracterizados por la mayor libertad de información, no prevé una regulación de las medidas protectoras de los secretos oficiales.

Con la denominación de *"materias clasificadas"* se comprenden los dos grados de secretos oficiales generalmente admitidos, la determinación de las Autoridades que pueden otorgar estas calificaciones, sus efectos y las líneas generales de las medidas protectoras que habrán de desarrollarse reglamentariamente y con carácter uniforme por todos los servicios afectados. La Ley se completa con un sistema de protección así como la referencia de las responsabilidades.

En el artículo primero, declara expresamente que los Órganos del Estado estarán sometidos en su actividad al principio de publicidad salvo los casos que sean declarada secreta.

En el artículo segundo[28] se dice que "A los efectos de esta Ley podrán ser declaradas "materias clasificadas" los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas pueda dañar o poner en riesgo la seguridad y defensa del Estado".

Los efectos de las calificaciones de secreto o reservado, determinarán, entre otros, los siguientes efectos según se establece en el artículo octavo:

"A) Solamente podrán tener conocimiento de las "materias clasificadas" las personas debidamente facultadas para ello y con las formalidades y limitaciones que en cada caso se determinen.

B) La prohibición de acceso y las limitaciones de circulación a personas no autorizadas en locales, lugares o zonas en que radiquen las "materias clasificadas".

En el artículo once, uno, se establece que "Las personas facultadas para tener acceso a una "materia clasificada" quedarán obligadas a cumplir con las medidas y prevenciones de protección que reglamentariamente se determinen, así como las particulares que para cada caso concreto puedan establecerse".

En el artículo doce [29], se sigue hablando de los sistemas de protección al decir "Los órganos referidos en el artículo cuarto [30] (Consejo de Ministros y Junta de Jefes de Estado Mayor) atenderán al mantenimiento y mejora de los sistemas de protección y velarán por el efectivo cumplimiento de cuanto se dispone en la presente Ley..."

La Ley vino a configurar el ámbito de confidencialidad del secreto oficial cuando una ley declare que determinadas materias, asuntos, actos, documentos, informaciones, datos y objetos, tengan carácter secreto y, cuando, mediante un acto formal y con los requisitos que reglamentariamente se determinen, lo decidan los órganos estatales competentes.

En relación con los asuntos clasificados por aplicación de la ley, lo están, como secreto, *"las claves y material criptográfico"*.[31]

Las personas facultadas para tener acceso a una materia clasificada quedarán obligadas a cumplir con las medidas y prevenciones de protección que reglamentariamente se determinen (artículo 11°).

El efecto principal de estas declaraciones es que las materias no podrán ser comunicadas, difundidas ni publicadas, ni utilizado su contenido fuera de los límites establecidos por la ley (art. 13°).

Los órganos con facultades de calificación atenderán *"mantenimiento y mejora de los sistemas de protección y velarán por su efectivo cumplimiento..."* (art. 12).

Además del "efectivo cumplimiento" de la ley, esta se refiere a las medidas represivas de carácter penal o administrativo. Pero una vez que ha sido revelado el secreto ya se ha producido el daño a la seguridad del Estado, por consiguiente para el cumplimiento efectivo de la protección se deben aplicar medidas preventivas.

Estas medidas protectoras de carácter preventivo operan "a priori", antes de -y precisamente para evitar- que el descubrimiento del secreto se produzca, y constituyen una forma de protección real y efectiva.

Es precisamente en este terreno de las medidas preventivas donde se detectan lagunas.[32]

Según la Disposición Final de la Ley, *"En Reglamento único, de aplicación general a toda la Administración del Estado y a las Fuerzas Armadas, se regularán los procedimientos y medidas necesarios para la aplicación de la presente Ley y protección de las "materias clasificadas".*

Se determinará igualmente con todo el detalle necesario y con especificación de las medidas técnicas precisas el régimen de custodia, traslado, registro, archivo, examen y destrucción de las "materias clasificadas", así como la elaboración de copias o duplicados de tales materias.

También se dispondrá lo necesario para el personal de la Administración Civil del Estado y de las Fuerzas Armadas en cuestiones de seguridad y protección de secretos".

Pero las facultades de la Administración para clasificar son una verdadera cláusula general que hace muy difícil la concreción, por lo que esta gran amplitud, su obsolescencia en la regulación de la protección y, su carácter preconstitucional, entre otras consideraciones, aconsejan su modificación.

4.2.1.1.1.2.- DECRETO 242/69, DE 20 DE FEBRERO, POR EL QUE SE DESARROLLA EL REGLAMENTO DE SECRETOS OFICIALES.

La Ley de Secretos Oficiales fue desarrollada por el Decreto 242/69, de 20 de febrero que da contenido al Reglamento de Secretos Oficiales, el cual, en su exposición de motivos, tras reiterar la disposición final de la Ley, continúa diciendo que *"para lograr una unificación normativa internacional y obtener el mismo grado de protección a las materias clasificadas en los distintos países parece aconsejable utilizar las enseñanzas del derecho comparado, en especial el de las naciones muy industrializadas con mayor experiencia en la información tecnológica"*.

Y, en base a ello, se recoge en el Reglamento lo relativo a definiciones, materias clasificadas, violaciones de su protección, Servicio de Protección de Materias Clasificadas y otros aspectos para la aplicación de la Ley.

En el Artículo Primero, el Reglamento vuelve a reiterar el principio de publicidad a que estarán sometidos los Órganos del Estado, ya indicado en la Ley.

Por cuanto se refiere a definiciones, podrá entenderse:

-Por *asuntos*, todos los temas que se refieran a las materias que en el mismo se especifican.

-Por *acto*, cualquier manifestación o acuerdo de la vida político-administrativa tendente a la obtención de fines específicos.

-Por *documentos*, cualquier constancia gráfica o de cualquier otra naturaleza.

-Por *informaciones*, los conocimientos de cualquier clase de asuntos o los comprendidos como materias clasificadas en el citado artículo segundo de la Ley.

-Por *datos y objetos*, los antecedentes necesarios para el conocimiento completo o incompleto de las materias clasificadas, las patentes, las materias primas y los productos elaborados, el utillaje, cuños, matrices y sellos de todas clases, así como los lugares, obras, edificios e instalaciones de interés para la defensa nacional o la investigación científica, y se entenderá también como materias propias de este Decreto, todas aquellas que, sin estar enumeradas en el presente artículo, por su naturaleza, puedan ser calificadas de asunto, acto, documento, información, dato u objeto, de acuerdo con lo dispuesto en el artículo dos de la Ley, (art. 2).

Especialmente considera que se entenderá por documento:

a) Los impresos, manuscritos, papeles mecanografiados o taquigrafiados y las copias de los mismos, cualesquiera que sean los

procedimientos empleados para su reproducción; los planos, proyectos, esquemas, esbozos, diseños, bocetos, diagramas, cartas, croquis y mapas de cualquier índole, ya lo sean en su totalidad, ya las partes o fragmentos de los mismos.

b) Las fotografías y sus negativos, las diapositivas, los positivos y negativos de película, impresionable por medio de cámaras cinematográficas y sus reproducciones.

c) Las grabaciones sonoras de todas clases.

d) Las planchas, moldes, matrices, composiciones tipográficas, piedras litográficas, grabados en película cinematográfica, bandas escritas o perforadas, la memoria transistorizada de un cerebro electrónico y cualquier otro material usado para reproducir documentos.

Las materias clasificadas se dividen en "secreto" y de "reservado".

La clasificación de secreto se aplicará a todas las materias que precisen del más alto grado de protección por su excepcional importancia y cuya revelación no autorizada, pudiera dar lugar a riesgos o perjuicios de la seguridad del Estado en materias referentes a la defensa nacional, la paz exterior o el orden constitucional.

La clasificación de reservado se aplicará a los asuntos, actos, documentos, informaciones, datos y objetos no calificados de secreto, por su menor importancia, pero cuyo conocimiento o divulgación pudiera afectar a

la seguridad del Estado, la defensa nacional, la paz exterior o el orden constitucional. (Artículo Tercero).

En los casos de revelación no autorizada o el extravío de documentos o material, se deberá proceder a las averiguaciones pertinentes, así como a la recuperación de los documentos o material extraviado.

El Servicio de Protección de Materias Clasificadas, de cada Departamento ministerial, tiene asignadas las funciones de:

"a) Asegurar el adecuado tratamiento de las materias clasificadas, tanto si se han producido en el departamento como si se han recibido en el mismo procedentes de otras dependencias de la Administración.

b) Instruir convenientemente respecto de las normas de protección al personal que tenga acceso, fehacientemente autorizado, al material clasificado.

c) Elaborar las condiciones de seguridad privativas del Ministerio, de las cuales deberán tener constancia, junto con las disposiciones necesarias para asegurar el perfecto cumplimiento de lo establecido en este Decreto, las Entidades y personas del propio Ministerio con competencia para la declaración de materias clasificables, según se dispone en el artículo cuarto de la ley.

d) Responder en todo tiempo, de la mejor protección del material clasificado que se le entregue para su custodia y, especialmente, de cerrar bajo seguro el material calificado de "secreto" en instalación de

seguridad apropiada, siempre que la misma no esté en uso o bajo supervisión directa de funcionarios autorizados.

e) Establecer procedimientos adecuados tendentes a evitar que personas no autorizadas puedan tener acceso, sea visual, sea auditivo, a información o material secreto, no discutiendose con o en presencia de personas no autorizadas, el contenido de aquellos.

f) Mantener el control o registro de las materias clasificadas".

(Art. Noveno).

La posesión o uso de información o material clasificado como secreto estará limitada a lugares donde se disponga de instalaciones para su almacenaje y segura protección, y a los cuales no pueden tener acceso otras personas que no sean las que, de manera fehaciente, hayan sido autorizadas para ello por las autoridades señaladas en el artículo cuarto de la Ley, (art. doce).

La custodia y transmisión del material clasificado, se recoge en el Decreto.

"La transmisión del material secreto se llevará a cabo, preferiblemente, por medio de contacto directo de los funcionarios a quienes tal función corresponda, o por personal específicamente designado, valija diplomática, por un sistema de correos creado expresamente para este fin o por medios de transmisión en forma cifrada". (Artículo Veinte).

"La transmisión de material reservado se llevará a cabo de la misma manera que la expuesta para el secreto en el artículo anterior o por medio de los comandantes de aeronaves o navíos con categoría de oficial o correo certificado si no fuere practicable ninguno de los procedimientos anteriores, cifrándose los textos siempre que sea posible". (Artículo Veintiuno).

"Si la transmisión de material clasificado se llevase a cabo dentro del órgano de origen, se regirá por las normas que elabore el Servicio de Protección de Materias Clasificadas correspondiente, las cuales deberán garantizar un grado de seguridad equivalente al indicado para transmisión fuera del mismo". (Artículo Veintidós).

Según el Reglamento, está prohibida la transmisión de información por teléfono, salvo que cuenten con la protección adecuada y, expresamente establece:

"La información clasificada no podrá ser transmitida o revelada por medio del teléfono, excepto en los casos en que así se disponga, expresamente, por medio de determinados circuitos tanto civiles como militares". (Articulo Veinticuatro).

Por lo que ha de interpretarse como circuitos adecuadamente protegidos que, actualmente, implicarían protección con sistemas para el cifrado de la voz.

Siempre que la Autoridad encargada de la calificación juzgare que el material clasificado resultare ya inservible será destruido por medio del fuego, procedimientos químicos o, cuando tales medios no existan, por medio de artefactos que los reduzcan a pulpa o fragmentos tan minúsculos que imposibiliten su reconstrucción. (Art. Veintinueve).

Sin perjuicio de lo dispuesto en el Reglamento de Secretos Oficiales y teniendo en cuenta las características de todo orden que concurren en el normal desenvolvimiento de la función de las Fuerzas Armadas, podrán elaborar normas específicas de régimen interior.

De igual modo, y en atención a las peculiaridades del servicio diplomático y a las circunstancias en que éste desarrolla sus funciones fuera del territorio nacional, el Ministerio de Asuntos Exteriores podrá elaborar normas específicas de régimen interior para sus oficinas en el extranjero, sin perjuicio de las normas de carácter general contenidas en el Reglamento. (Disposición Adicional).

4.2.1.1.1.3.- PROYECTO DE LEY DE SECRETOS OFICIALES.

El Consejo de Ministros en su reunión del 23 de agosto de 1.996, aprobó el anteproyecto de Ley Orgánica Reguladora de Secretos Oficiales, que vendría a sustituir a la vigente Ley de Secretos Oficiales de 1.968, reformada en 1.978, tras la superación de los distintos trámites parlamentarios.

Con independencia de la fase en que en estos momentos se encuentre, tras la emisión del dictamen del Consejo General del Poder

Judicial, consideramos de interés abordar algunos aspectos significativos del texto [33] por su relación con el tema central de esta .

Para el Anteproyecto son secretos oficiales: "... *los actos, documentos y medios materiales, cualquiera que sea su naturaleza, cuya difusión y conocimiento por personas no autorizadas pueda ocasionar daños, o entrañar riesgos, para los siguientes intereses, instituciones o actividades del Estado:*

a) La soberanía, la independencia y la integridad territorial de España.

b) El ordenamiento constitucional y el funcionamiento regular de sus instituciones.

c) Los criterios, medios materiales y actuaciones esenciales para la defensa militar de España.

d) Los intereses fundamentales de España en el exterior.

e) Los aspectos esenciales de la organización y funcionamiento de los servicios de inteligencia del Estado, especialmente en lo relativo al carácter anónimo de sus agentes o colaboradores y a la confidencialidad de las fuentes de información.

f) Los intereses fundamentales del Estado en materia económica, industrial, tecnológica o científica.

g) Aquellas otras actividades básicas relacionadas con la seguridad y la defensa del Estado no comprendidas en los apartados anteriores.

2.- Tendrán asimismo la consideración de secreto oficial las materias así clasificadas por ley y aquellas otras que tengan este carácter en virtud de los tratados internacionales celebrados por España...". (Artículo 1).

El secreto de Estado es aquel que tiene como elemento objetivo la seguridad y defensa del Estado, entendida en su sentido amplio, incluyendo aspectos políticos, económicos, militares, diplomáticos, científicos, industriales, etc., "pues todos ellos tienen relación muy directa con la supervivencia del Estado".[34]

El secreto funcionarial sería el que garantiza el normal funcionamiento de la Administración pública.

La definición de secreto de Estado que recoge el anteproyecto incorpora toda una gama de aspectos que se refieren a la más moderna concepción de defensa del Estado. Se incluyen los intereses fundamentales del Estado en materia económica, industrial, tecnológica o científica, recogiendo la corriente surgida en la I Guerra Mundial donde se puso de relieve la importancia de las cuestiones industriales y económicas para la defensa nacional a los que se han incorporado la tecnología y la ciencia, de donde se deriva la necesidad de extender la protección a dichas materias.

Las relaciones entre Estados han estado siempre presididas por una cierta discreción que, en ocasiones, lleva a pactos expresos de secreto sobre determinadas materias. La insuficiencia del Estado en la vida

internacional y su actuación en el marco de la supranacionalidad, lleva a compartir secretos entre Estados y surge lo que se ha denominado como secreto aliado.

Ejemplos de secreto aliado podrían ser el Acuerdo y Protocolo de 17 de junio de 1.986 entre España y Noruega sobre protección de información clasificada; el Acuerdo de 22 de febrero de 1.989 con Francia para la protección de la información clasificada, el Acuerdo con Italia de 2 de diciembre de 1.983 sobre protección de la información clasificada de interés para la defensa; el Acuerdo con la República Helena de 25 de enero de 1.992 para garantizar la seguridad de las informaciones de interés para la defensa o el acuerdo de la OTAN para la salvaguardia mutua del secreto de invenciones relativas a la defensa.

El anteproyecto introduce en su artículo 2, una novedad en cuanto a las categorías de clasificación y frente a las de secreto y reservado que operan en la Ley de Secretos Oficiales vigente, introduce las de "Alto secreto", "Secreto" y "Confidencial".[35]

"La clasificación de ***"alto secreto"*** *se reserva para los asuntos que exijan el máximo nivel de protección y cuya publicidad o conocimiento por personas no autorizadas pueda ocasionar daños a las instituciones y actividades esenciales del Estado a que se refieren los apartados a), b) y c) del artículo 1.1. de esta Ley.*

La clasificación de ***"secreto"*** *se aplicará a los asuntos cuya publicidad o conocimiento por personas no autorizadas pueda ocasionar daños a los intereses o actividades del Estado a que se refieren los apartados d) y e) del artículo 1.1 de esta Ley.*

La clasificación de ***"confidencial"*** *se aplicará a los asuntos cuya divulgación pueda causar perjuicio o menoscabo a los intereses y actividades del Estado a los que se refieren los apartados f) y g) del artículo 1.1. de esta Ley".*

Por cuanto se refiere a la protección, el propio acto de clasificación deberá indicar los lugares en que deban ser custodiados los documentos o medios materiales clasificados. (art. 4.1.d).

El Anteproyecto introduce una novedad al crear la Autoridad Nacional de Seguridad y Registro Central.

"1. La competencia para asegurar la protección de las materias clasificadas y el cumplimiento de los compromisos contraídos por España en razón a su pertenencia a Organizaciones Internacionales, o como consecuencia de la firma de convenios o tratados internacionales, así como la relación con las autoridades competentes en materia de secretos oficiales de otros países u Organizaciones Internacionales, será ejercida por la Autoridad Nacional de Seguridad. El nombramiento recaerá en un miembro del Gobierno.

2. Con dependencia funcional de la Autoridad Nacional de Seguridad, se nombrará una Autoridad Nacional de Seguridad Delegada que tendrá a su cargo el Registro Central de materias clasificadas en el que figurarán todos los documentos originales de los acuerdos de clasificación". (Artículo 9).

Entre las obligaciones de las Autoridades responsables de la protección de secretos oficiales recogidas en el artículo 10, por lo que se refiere a esta destacamos:

"a) Mantener y mejorar los sistemas y procedimientos de protección y control.

b) Velar por el cumplimiento de las disposiciones contenidas en la presente Ley y en su Reglamento de desarrollo. ...

e) Adoptar las medidas necesarias para la instrucción y perfeccionamiento del personal en materias de protección y seguridad".

Según el Anteproyecto, constituyen infracciones administrativas, con independencia de la responsabilidad penal en la que en su caso pudiera incurrirse, los siguientes actos:

"... b) El incumplimiento de las medidas de protección de secretos oficiales por parte de las personas legalmente obligadas a adoptarlas".

... e) La falsificación, destrucción o inutilización por cualquier medio de secretos oficiales". (Art. 11.1).

De especial mención es la Disposición final Primera, según la cual, el Gobierno, en el plazo de un año a partir de la promulgación de la presente Ley, dictará el Reglamento General para el desarrollo y aplicación de la misma.

Dicho Reglamento regulará las siguientes cuestiones:

"a) El miembro del gobierno que sea designado como Autoridad Nacional de Seguridad y sus relaciones con los diferentes servicios del Estado con atribuciones y competencias en materia de secretos oficiales.

b) Las normas generales sobre protección, control, anotación e identificación de los documentos y medios materiales clasificados.

c) Los procedimientos de comunicación en materia de secretos oficiales.

d) Las normas relativas al archivo, registro, traslado, revisión y destrucción de los documentos y medios materiales clasificados".

El Proyecto de Ley aborda aspectos considerados esenciales pero más determinante será su normativa de desarrollo.

4.2.1.1.1.4.- RESERVA DE LEY ORGÁNICA.

La participación en los asuntos públicos, y el principio general de transparencia de lo público y las libertades de expresión e información para lograrlo, en una sociedad democrática, son derechos fundamentales.

La configuración de ámbitos de confidencialidad en la esfera pública y la protección técnica de la información y las comunicaciones a ellos referidas incide de forma directa en el ejercicio de estos derechos.

De acuerdo con el artículo 53 de la Constitución, los derechos fundamentales vinculan a todos los poderes públicos y sólo por ley podrá regularse su ejercicio, que se tutelarán de según lo previsto en el artículo 161.1, a) de la C.E.

De otra parte, el artículo 81 de la Constitución establece que :"*Son leyes orgánicas las relativas al desarrollo de los derechos fundamentales y de las libertades públicas, ...*". Lo que significa que sólo por ley orgánica, que en todo caso deberá respetar el contenido esencial de los derechos fundamentales y las libertades públicas a que se refieran, podrá regularse el ejercicio de aquellos derechos y libertades que recogen los artículos 14 al 29 de la Constitución.

La reserva de Ley Orgánica implica que sólo es posible regular el ejercicio con respecto al contenido esencial de los derechos y libertades, y que la regulación legal del ejercicio podrá referirse a las condiciones o requisitos considerados formales, imprescindibles para que los ciudadanos titulares del derecho o libertad, los ejerciten, pero no a las formas o maneras de entenderlos.

El respeto del contenido esencial significa que la norma no puede desfigurarlo. Contenido esencial es "aquella parte del contenido de un

derecho sin la cual éste pierde su peculiaridad" (Sentencia del Tribunal Constitucional de 8 de abril de 1.981).

Estas garantías están incluidas por los límites que, según consolidada doctrina, cabe concebir desde la interpretación de condiciones permitidas en textos internacionales.

La falta de promulgación de leyes orgánicas sobre el desarrollo de determinados derechos y libertades, puede ser suplida por la legislación ordinaria preconstitucional[36], salvo las disposiciones incompatibles con su contenido esencial, puesto que los vacíos legislativos, según el Tribunal Constitucional, han de cubrirse aplicando la ley válida en el anterior sistema de fuentes, si la hubiera.

El que la regulación a que nos referimos sólo se pueda llevar a cabo por Ley Orgánica, excluye ordenaciones contenidas en leyes ordinarias, tanto estatales como autonómicas, de forma que la reserva de Ley Orgánica sólo puede ser cumplimentada por el Estado. Exigencia que ha sido flexibilizada por el Tribunal Constitucional, al justificar ciertas ordenaciones introducidas por vía reglamentaria para regular el ejercicio de determinados derechos.

La Declaración Universal de Derechos Humanos,[37] en su artículo 29 establece que: *"Toda persona tiene deberes respecto a la comunidad, puesto que sólo en ella puede desarrollar libre y plenamente su personalidad.*

2.- 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.

3.- Estos derechos y libertades no podrán en ningún caso ser ejercidos en oposición a los propósitos y principios de las Naciones Unidas."

De otra parte, según el Pacto Internacional de Derechos Civiles y Políticos.[38] *"Nadie podrá ser molestado a causa de sus opiniones.*

Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.

El ejercicio del derecho previsto en el párrafo 2 de este artículo 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." (art. 19).

De igual modo, el Convenio Europeo para la Protección de Derechos Humanos y Libertades Fundamentales, artículo 10, dice que:[39] *"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. El presente artículo no impide que los Estados sometan las empresas de radiodifusión, de cinematografía o de televisión a un régimen de autorización previa.*

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 constituyen medidas necesarias, en una sociedad democrática, para la seguridad nacional, la 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 del poder judicial".

Todos estos textos han sido suscritos y ratificados por España y, por tanto, son utilizables como parámetros hermenéuticos para los derechos y libertades fundamentales, de acuerdo con lo previsto en el artículo 10.2 de

la Constitución y, por consiguiente, para las libertades de expresión e información.

La amplitud de finalidades justificativas obliga al intérprete a un análisis casuístico, ante la inconveniencia de considerar estos límites como intrínsecos y compatibles con la naturaleza de las libertades a las que se refieren.

El Tribunal Constitucional recurre al principio de proporcionalidad para examinar determinadas medidas restrictivas que supongan una limitación de la garantía esencial de las libertades e expresión e información, lo que no es otra cosa que la forma de preservar valores considerados temporalmente superiores.

Estas medidas serían por tanto excepcionales, con tendencia a la desaparición cuando se den las condiciones para ello.

Tanto el artículo 10.2 del Convenio de Roma, como el artículo 19.3 del Pacto de Nueva York, disponen que las restricciones deberán estar expresamente fijadas por la ley, lo que viene a suponer que únicamente reconoce potestad restrictiva de las libertades al legislador nacional que es quien debe valorar el criterio de *"necesidad"* de la limitación.

Cualquier limitación de la libertad de expresión e información sólo es válida en cuanto hecha por ley, y no sólo en base a la exigencia de los pactos internacionales suscritos y ratificados por España, sino porque así

lo impone la propia Constitución que exige para estas medidas limitativas que adopten la forma de ley orgánica.

Por tanto, sólo el legislador ordinario, a través de la forma de ley orgánica, es el que está legitimado para establecer hasta dónde puede llegar la difusión de opiniones, juicios de valor e informaciones de todo tipo. Cualquier límite no consagrado expresamente en un texto legal de estas características se debe tener por inexistente.

Parece evidente que los derechos fundamentales no son derechos ilimitados. El Tribunal Constitucional en su Sentencia 91/83, de 7 de noviembre, dice que "Los derechos fundamentales reconocidos en la Constitución..., no son derechos ilimitados, sino que encuentran sus límites en el derecho de los demás (art. 10 de la Constitución) y, en general, en otros bienes y derechos constitucionalmente protegidos.

Luis Prieto habla de resistencia: "desde la perspectiva del Derecho positivo, los derechos se muestran tan solo resistentes, que es un concepto gradual o relativo. La fundamentalidad no es una etiqueta que se tiene o no se tiene; es una escala que admite distintos grados, de modo que algunos derechos serán más fundamentales que otros, es decir, más resistentes en presencia de otras decisiones políticas. Lo que no serían en ningún caso es absolutos, pues ello equivaldría a reconocer derechos ilimitados.[40]

El reconocimiento y protección de la libertad de expresión y del derecho a la información garantiza el derecho individual del ciudadano

contra el secreto, pero a la vez es condición indispensable para una efectiva operatividad del principio de transparencia mediante el instrumento de los medios de comunicación social.

Las eventuales limitaciones establecidas sobre estas libertades, tanto en la faceta de recibir información veraz, como en la de expresarse acerca de algunos asuntos y comunicar su existencia, constituyen recortes absolutamente incompatibles con su contenido esencial que resulta imprescindible justificar.

4.2.1.2.- ÁMBITO DE CONFIDENCIALIDAD DIPLOMÁTICO.

La especificidad de la función diplomática ha llevado a la comunidad internacional a un reconocimiento jurídico de un estatuto propio para personas e instalaciones que hayan sido acreditados como tales.

En esta regulación jurídica especial, plasmada esencialmente en los Convenios de Viena, se configura un ámbito de confidencialidad diplomático propio, de dimensión internacional, justificado por la función que realizan, con previsiones expresas de protección efectiva en lo referido a la transmisión de información, al contemplar la utilización de valijas, o comunicaciones *"en clave o en cifra"*.

a) Relaciones diplomáticas.

Las normas reguladoras de la función diplomática y de los privilegios y garantías de sus miembros son en su mayor parte de origen

consuetudinario. Algunas de ellas se recogieron en el Reglamento adoptado por el Congreso de Viena de 19 de marzo de 1.815.

La Comisión de Derecho Internacional de las Naciones Unidas convocaron una Conferencia en Viena, fruto de la cual fue la "Convención de Viena sobre relaciones diplomáticas", de 18 de abril de 1.961, a la cual se adhirió España el 21 de noviembre de 1.967 (B.O.E. de 24 de enero de 1.968).

Según el Breve Diccionario Diplomático, de Santiago Martínez Lage [41], el término *"Relaciones Diplomáticas"* tiene varios significados.

En sentido formal, son las que mantienen entre sí los Estados -y otros sujetos de Derecho internacional- que se autorizan el ejercicio recíproco de funciones diplomáticas, normalmente a través de Misiones Diplomáticas. Se habla, así, de establecimiento, mantenimiento y ruptura de relaciones diplomáticas.

Con cierta frecuencia, se emplea el término como equivalente de la totalidad de relaciones entre dos Estados, incluyendo los aspectos puramente políticos, los militares, los comerciales, los culturales, los migratorios, etc., y así, por ejemplo, se califican determinadas relaciones diplomáticas, globalmente, de buenas, malas, intensas, tibias, etc.

Con mayor frecuencia, se utiliza el término para referirse a aquella parcela de las relaciones entre Estados que afectan más directamente al ejercicio del poder y a la soberanía nacional (los aspectos políticos,

territoriales, militares, etc.) por contraste con aquellas otras parcelas que aún siendo de la mayor importancia están más alejadas de aquellos : relaciones comerciales, culturales, de cooperación técnica, etc. Así, por ejemplo, pueden contraponerse unas relaciones diplomáticas intensas y excelentes a unas relaciones diplomáticas escasas y conflictivas (o viceversa). Pero no debe olvidarse que cualquier conflicto surgido en estas segundas es susceptible de influir decisivamente en las primeras porque las relaciones son, en definitiva, un todo.[42]

Las funciones de una misión diplomática, según establece el artículo 3° de la Convención de Viena son, entre otras, las de *"... enterarse por todos los medios lícitos de las condiciones y de la evolución de los acontecimientos en el Estado receptor e informar sobre ello al gobierno del Estado acreditante".*

Sus archivos y documentos son siempre inviolables, dondequiera que se hallen.

Y, por lo que se refiere a las comunicaciones, el artículo 27 del Convenio de Viena, establece que*: "1.- El Estado receptor permitirá y protegerá la libre comunicación de la misión para todos los fines oficiales. Para comunicarse con el gobierno y con las demás misiones y consulados del Estado acreditante, dondequiera que radiquen, la misión podrá emplear todos los medios de comunicación adecuados, entre ellos los correos diplomáticos [43] y los mensajes en clave o en cifra. Sin embargo, únicamente*

con el consentimiento del Estado receptor podrá la misión instalar y utilizar una emisora de radio.

2.- La correspondencia oficial de la misión es inviolable. Por correspondencia oficial se entiende toda correspondencia concerniente a la misión y a sus funciones.

3.- La valija diplomática no podrá ser abierta ni retenida".[44]

b) Relaciones consulares.

De la institución consular se encuentran precedentes en los orígenes de la Grecia Antigua, sin embargo no será hasta la Edad Media cuando esta institución adquiera un amplio desarrollo.

Los comerciantes extranjeros solían organizar pequeñas comunidades a las que se les otorgaba cierta autonomía entre ellas la de tener unos Magistrados especiales. El principio de personalidad de las leyes contribuyó a esta realidad.

Estos Jueces especiales en el siglo XII toman el nombre de Cónsules, con funciones cada vez más amplias en épocas posteriores que se extienden hacia la protección de los intereses de su Estado de origen y la de los nacionales de este, llegando en el siglo XVI a ejercer una cierta representación oficial del Estado.

En el Siglo XVIII desaparecen las funciones consulares en lo relativo a la jurisdicción civil y penal y se amplían las funciones comerciales y en materia de navegación.

La reglamentación internacional de la función consular y de sus privilegios e inmunidades ha sido objeto de un gran número de tratados bilaterales y de algún tratado multilateral, como el de 20 de febrero de 1.928, firmado en La Habana.

Hoy se encuentra reglamentado por la Convención de Viena para las relaciones consulares. España se adhirió a esta Convención el 3 de febrero de 1.970 (B.O.E. de 6 de marzo de 1.970). [45]

Las funciones consulares están establecidas en el artículo 5 del Convenio y, entre otras, consistirán en "... *Informarse por todos los medios lícitos de las condiciones y de la evolución de la vida comercial, económica, cultural y científica del Estado receptor, informar al respecto al gobierno del Estado que envía y proporcionar datos a las personas interesadas*".

Por cuanto se refiere a la protección de los locales y archivos consulares y de los intereses del Estado que envía en circunstancias excepcionales, el artículo 27 del Convenio establece en su punto 1, que en caso de ruptura de las relaciones consulares entre dos Estados, el Estado receptor estará obligado, entre otras cosas a "*...respetar y proteger, incluso en caso de conflicto armado, los locales consulares, los bienes de la oficina consular y sus archivos*".

De igual modo que en el caso de las representaciones diplomáticas, los archivos y documentos consulares son siempre inviolables dondequiera que se encuentran.

Por "archivos consulares" el Convenio de Viena sobre Relaciones Consulares en su entiende "*...todos los papeles, documentos, correspondencia, libros, películas, cintas magnetofónicas y registros de la oficina consular, así como las cifras y claves, los ficheros y los muebles destinados a protegerlos y conservarlos*", (Artículo 1.1 k).

Por lo que se refiere a la libertad de comunicación, es similar a la de las representaciones diplomáticas." *El estado receptor permitirá y protegerá la libertad de comunicación de la oficina consular para todos los fines oficiales. La oficina consular podrá utilizar todos los medios de comunicación apropiados, entre ellos los correos diplomáticos o consulares, la valija diplomática o consular y los mensajes en clave o cifra, para comunicarse con el gobierno, con las misiones diplomáticas y con los demás consulados del Estado que envía, dondequiera que se encuentren. Sin embargo, solamente con el consentimiento del Estado receptor, podrá la oficina consular instalar y utilizar una emisora de radio.*

c) Nuevas formas de diplomacia.

Junto a las formas de diplomacia clásicas, encontramos otras surgidas como consecuencia de la mayor intervención directa de los representantes de los partidos o de los miembros de las Cámaras legislativas en la política exterior, del predominio que los aspectos puramente técnicos van tomando en las relaciones internacionales y de la creciente internacionalización del mundo en general.

Todo ello ha influido y sigue influyendo en la creación y desarrollo de nuevas formas de diplomacia denominadas Diplomacia ad-hoc y Diplomacia Parlamentaria.

A la primera pertenecen las oficinas temporales o permanentes que los Estados crean para fines específicos, el envío de funcionarios técnicos para discusión de asuntos concretos y las llamadas Misiones especiales.

La Diplomacia Parlamentaria es la que se lleva a cabo a través de Conferencias internacionales y también en el marco de las Organizaciones internacionales.

De la diplomacia llevada a cabo a través de Misiones especiales se ocupa la Convención aprobada por la Asamblea General de las Naciones Unidas el 8 de diciembre de 1.969 y abierta a la firma y ratificación o adhesión el 16 de diciembre del mismo mes y año.[46]

Según el Breve Diccionario Diplomático de Martínez Lage, *"Misión especial"* es la que envía un Estado a otro, con carácter temporal y para tratar asuntos determinados de cualquier clase e importancia (negociación de un acuerdo, asistencia a una toma de posesión presidencial...).

Pueden enviarse o recibirse Misiones Especiales aún sin existir relaciones diplomáticas o consulares entre los Estados en cuestión, pero debe contarse en todo caso con el consentimiento del Estado receptor. La Misión Especial puede estar compuesta por una o numerosas personas, y a su frente puede figurar desde un simple funcionario hasta el Jefe del Estado.

Existe un Convenio sobre Misiones Especiales, negociado bajo los auspicios de las Naciones Unidas, abierto a la firma el 16 de diciembre de 1.969, y aún no entrado en vigor, que regula ampliamente el envío, recibo, funciones y estatuto de las Misiones Especiales. España no es hasta el momento parte de este Convenio. Las misiones especiales se conocen comúnmente en el lenguaje no técnico con el nombre genérico de Delegaciones".[47]

El artículo 28 de esta Convención transcribe literalmente el contenido del artículo 27 de la Convención sobre Relaciones Diplomáticas y, en similares términos se pronuncia el artículo 27 del Convenio de Viena sobre la representación de los Estados en sus relaciones con las organizaciones internacionales [48] de carácter universal.

Organización internacional es la Asociación de varios Estados en virtud de un Tratado multilateral (Tratado constitutivo), dotada de ciertos órganos llamados a formular una voluntad colectiva en determinadas materias correspondientes a sus fines.

Las Organizaciones internacionales se denominan a veces Organizaciones intergubernamentales para distinguirlas de aquellas otras Organizaciones que teniendo carácter internacional no están constituidas por Estados. A estas segundas se las conoce bajo la denominación de Organizaciones no gubernamentales.

Existen muy diversos tipos de Organizaciones internacionales: de carácter universal como la O.N.U. o especializadas como la O.M.S., etc .

4.2.1.4.- Ámbitos de confidencialidad en la Administración General del Estado.

Como consecuencia del contenido del artículo 105 b) de la Constitución referido a que la Ley regulará el acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas, puede surgir algún tipo de confusión entre secreto de Estado o secreto oficial y secreto administrativo.

La doctrina cuando se refiere al secreto administrativo lo hace pensando en relación con los expedientes resultantes de los procedimientos administrativos de carácter general, que se inician, tramitan y resuelven en las oficinas públicas,[49] todo ello, sin perjuicio de que el secreto de Estado sea una clase específica de secreto administrativo.

En todo caso, la Ley 30/1.992, de 26 de noviembre de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común", en su artículo 37.5 al regular el derecho de acceso a los archivos y registros, lo impide en determinados casos, perfilando así entornos que requieren algún tipo de protección, con lo que la Ley estaría configurando ámbitos de confidencialidad.

Siguiendo el precepto indicado nos encontramos con los siguientes ámbitos de confidencialidad diferenciados:

a) Informaciones sobre las actuaciones del gobierno del Estado ó de las comunidades Autónomas, en el ejercicio de sus competencias constitucionales no sujetas a Derecho Administrativo.

b) La información sobre la Defensa Nacional ó la Seguridad del Estado.

c) La información sobre la investigación de los delitos cuando pudiera ponerse en peligro la protección del os derechos y libertades de terceros, o las necesidades de las investigaciones que se estén realizando.

d) Las relativas a materias protegidas por el secreto comercial o industrial.

e) Las informaciones relativas a las actuaciones administrativas derivadas de la política monetaria.

f) También contribuye a la definición de los perfiles de los ámbitos de confidencialidad, el apartado 6 del citado artículo 37, cuando dice que se regirán por disposiciones específicas el acceso a determinados archivos tales como:

f.1.- Archivos de materias clasificadas,

f.2.- Los datos sanitarios de los pacientes.

f.3.- Los datos electorales.

f.4.- Los datos relativos a la intimidad.

De todo lo indicado se podría derivar que en las Administraciones Públicas existen los siguientes ámbitos de confidencialidad: *Defensa*

Nacional, Seguridad del Estado, Materias Clasificadas, Averiguación del delito, Derechos y Libertades, Actuaciones Políticas del Gobierno del Estado, Actuaciones Políticas de los Gobiernos de las Comunidades Autónomas, Política Monetaria, Intimidad, Secreto Comercial, Secreto Industrial, Datos Sanitarios de Pacientes, y Datos Electorales.

4.2.2.- DELIMITACIÓN DE ÁMBITOS PRIVADOS DE CONFIDENCIALIDAD

Los derechos de la personalidad se manifiestan dentro de la legislación internacional y nacional como uno de los núcleos del reconocimiento y garantía de los derechos.

El artículo 10 de la C.E. al reconocer que *"la dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social"*, se manifiesta en favor de un reconocimiento iusnaturalista de la dignidad, entendida no sólo como garantía negativa de que la persona no va a ser objeto de ofensas o humillaciones, sino también de forma positiva, como desarrollo de la personalidad de cada individuo.

Como afirma Pérez Luño, [50], "el pleno desarrollo de la personalidad supone, a su vez, de un lado, el reconocimiento de la total autodisponibilidad, sin interferencias o impedimentos externos, de las posibilidades

de actuación propias de cada hombre; de otro, la autodeterminación que surge de la libre proyección histórica de la razón humana antes que de una predeterminación dada por la naturaleza". Pese a todo no puede entenderse como un ámbito exento de limitaciones.

Los derechos de la personalidad están encuadrados por dos tipos de límites. Uno externo y otro interno. El primero alcanza hasta donde lo hace el derecho ajeno, la moral vigente, el orden público y el bien común. Desde la perspectiva interna, y como con posterioridad veremos de forma concreta, en cada uno de los derechos de la personalidad son inalienables, imprescriptibles, inembargables, irrenunciables e intransmisibles.

De esta forma, y siguiendo con Pérez Luño,[51] "la dignidad humana supone el valor básico, fundamentador de los derechos humanos que tienden a explicitar y satisfacer las necesidades de la persona en la esfera moral".

4.2.2.1.- HONOR, INTIMIDAD Y PROPIA IMAGEN.

El honor es la buena fama o reputación que una persona merece al conjunto social.

También hemos de diferenciar con De Castro [52], el honor de la fama. "El honor está referido directamente al trato dado o recibido por los demás, y la fama, es el rumor, voz pública, renombre, que está relacionado con el eco que la persona produce en la opinión pública". De esta forma el honor se aproxima a lo que la persona piensa o considera de sí misma. Por

contra, la fama es la opinión externa a la persona, lo que los demás piensan de ella.

Al igual que otros derechos, el honor tiene su raíz en la idea de patrimonialidad o pertenencia a la persona. Se configura y desarrolla en planteamientos históricos liberales.

Al igual que en otros muchos derechos, el honor ha sufrido un proceso de democratización, de generalización social, de tal forma, que hoy toda persona tiene derecho al honor por el mero hecho de serlo.

Constitucionalmente, si bien existe el reconocimiento de manifestaciones del derecho a la intimidad (inviolabilidad de la persona, domicilio, correspondencia, etc.), hasta la vigente Constitución, no puede hablarse de un reconocimiento concreto y específico del derecho al honor.

No parece seguir el constituyente español de 1978, las prescripciones que el derecho en el ámbito internacional ya había realizado al respecto del honor. La Declaración Universal de Derechos del Hombre y del Ciudadano aprobada por la 183 Asamblea General de las Naciones Unidas, de fecha 10 de diciembre de 1948, reconoce el derecho al honor individual, estableciendo en su art. 12, lo siguiente: "... nadie puede ser objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio, o su correspondencia, ni de ataques a su honor y a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

En el mismo sentido, no cabe entender el contenido del art. 18 C.E., sin hacer referencia previa al art. 10.1 del mismo texto. Si el fundamento del orden político y la paz social es el respeto a la dignidad de la persona, los derechos inviolables que le son inherentes y el libre desarrollo de la personalidad, el derecho al honor es una consecuencia necesaria de ello. Así lo reconoce el Tribunal Constitucional en la Sentencia 214/1992 de 11 de noviembre, en el fundamento jurídico 1°, donde manifiesta que "el derecho al honor y otros de los derechos reconocidos en el art. 18 de la C.E. aparecen como derechos fundamentales vinculados a la propia personalidad del individuo, derivados sin duda de la dignidad de la persona que reconoce el art. 10 C.E.".

El art. 18.1 de la C.E. ha sido desarrollado mediante Ley Orgánica, [53] la cual resume la protección en dos ámbitos concretos; la obligación de respeto, por parte de terceros, de la intimidad y el honor de los demás, obligación que es genérica e indeterminada; y en el deber de abstención que tiene que cumplir cada individuo frente a los demás.

Pese al campo jurídico que abre la Ley Orgánica referida, no entraremos en su estudio, en base a que la perspectiva del presente trabajo son los derechos al honor, la intimidad y la propia imagen desde la perspectiva de su interacción con la protección de datos personales, contenido propio de otra Ley Orgánica [54], en este caso en desarrollo del art. 18.4 de la C.E..

Además de ello, y como la propia Ley Orgánica de 1.982 establece, algunos de estos derechos gozan además de una protección penal, la cual disfruta de una aplicación preferente, por ser sin duda, de más fuerte efectividad. Por ello entendemos como propio del presente trabajo entrar en el conocimiento de la ley de protección de datos personales, más que en la Ley Orgánica de 1982, dado que ésta es genérica, mientras que aquélla previene y garantiza una violación concreta.

La intimidad como derecho es la manifestación y reconocimiento jurídico de una necesidad social. El derecho reconoce un ámbito reservado e inaccesible a terceros de toda persona. Este aspecto, que es el más significativo desde nuestra perspectiva.

Nos queda por último una manifestación de la intimidad, como es la idea de intimidad. A este respecto, no todas las sociedades tienen conciencia de intimidad, lo cual no implica su ausencia de uso. Como afirma Ruiz Miguel [55] "la forma de conciencia sobre la intimidad, no se encuentra en todas las sociedades, y aún en las sociedades en que se encuentra, el grado de teorización puede variar".

En lo referido al origen de la intimidad, no parece existir acuerdo, dándose diversas teorías. Los denominados racionalistas, entienden que la idea de intimidad aparece con la disgregación feudal, afirmando que el nacimiento de la intimidad coincide con la afirmación revolucionaria de los derechos del hombre, y en concreto está ligada al nacimiento de una clase

social, la burguesía. Frente a esta opinión existe la teoría, denominada histórica, que liga su origen al término propiedad.

En un principio, el derecho protege ciertas manifestaciones de la intimidad. No existe en Grecia un reconocimiento jurídico de la intimidad, debido al concepto globalizante y socializador de la *Polis*. Roma, por el contrario, realizará la distinción entre derecho público y privado. Dentro de éste último, se reconocen manifestaciones del derecho a la intimidad como la protección de la correspondencia y del domicilio.

En la Edad Media, estará presente el cristianismo respecto del derecho a la intimidad, fundamentalmente a través de la obra de San Agustín y del redescubrimiento del Derecho Romano. Junto a ello, la aportación de lo propio, de la libertad del individuo frente a lo público, influirá de forma definitiva en reconocimientos puntuales del derecho a la intimidad. Ello arrancará de la idea de dignidad del hombre. Esto se traducirá en la manifestación concreta en la inviolabilidad del domicilio, que en Castilla será entendida como la paz de la casa. También las Cortes de León de 1.188 recogen el derecho a la inviolabilidad del domicilio. Este derecho, como manifestación del derecho a la intimidad también será recogido en el Fuero Viejo de Castilla de 1.250, Leyes de Estilo de 1300, entre otras.

En la Edad Moderna aparece la protección de la libertad de conciencia, o la libertad religiosa, y se reconoce el derecho a gran número de manifestaciones de intimidad. Hemos de tener en cuenta, que en esta

época surgirán las primeras constituciones modernas (Estados Unidos 1787), y las primeras declaraciones de derechos (Francesa de 1789). En España, previo al constitucionalismo se reconoce la inviolabilidad del domicilio, el secreto de las comunicaciones, así como la intimidad corporal.

Pese a todo lo manifestado, no puede hablarse de una configuración propia del derecho a la intimidad hasta 1.890 . Con anterioridad, existe el reconocimiento de aspectos de la intimidad, pero no hay una concepción global del derecho, ni una conciencia de su necesidad, así como tampoco una delimitación conceptual ni jurídica.

Como afirma Ruiz Miguel [56] "este aspecto ya se encontraba jurídicamente protegido en el continente europeo merced a las antiguas normas que protegían contra la difamación y el libelo, para preservar el honor y buena fama de las personas". Pese a todo, la construcción que surge en 1.890 en Estados Unidos, configura un nuevo derecho que pasará en primer lugar a formar parte del ordenamiento norteamericano a través de la jurisprudencia. Con posterioridad dará el salto a las declaraciones internaciones de derechos, para poco después pasar a los textos constituciones (fundamentalmente a los europeos). De esta forma, no hay en el constitucionalismo histórico español ningún precedente del reconocimiento del derecho a la intimidad en su integridad o de forma individual. Existía, el acogimiento constitucional de ciertos aspecto de la intimidad (prohibición de entrada en

el domicilio, de violación de la correspondencia, etc.), pero no un reconocimiento expreso y determinado del derecho a la intimidad.

La Constitución de 1978, en su artículo 18 agrupa en un mismo precepto, el reconocimiento de tres nuevos derechos, como consecuencia de su vigencia internacional.

No faltan autores, para los que el derecho a la propia imagen carece de sentido peculiar, puesto que no es más que una categoría subsidiaria del derecho al honor. Como afirma Herrero-Tejedor [57] el derecho a la propia imagen aparece unido al derecho al honor o la intimidad, como una mera manifestación de los mismos, por lo cual, "tarda más en adquirir un reconocimiento independiente".

Pese a todo lo manifestado, entendemos que si bien el derecho a la propia imagen puede presentar concomitancias tanto con el derecho al honor y con el derecho a la intimidad, no cabe duda de que se trata de un derecho autónomo y virtual en nuestro ordenamiento jurídico. La autenticación de esta afirmación radica en la posibilidad de lesionar o realizar una intromisión en el derecho a la propia imagen sin que exista violación del honor o intromisión en la intimidad. De esta forma se manifiesta también el contenido de la Ley Orgánica 1/82, que si bien en un principio relaciona la propia imagen con el derecho a la intimidad, y en concreto, en alguno de los supuestos del art. 7.5, también establece la posibilidad de intromisión ilegítima en su ámbito exclusivo en el art. 7.6.

Partiendo ya de la base de la configuración del derecho a la propia imagen como un derecho autónomo, fundamental y constitucionalmente reconocido, nos cabe ahondar en su definición. Son pocos los juristas que han esbozado una definición de tal derecho. entre los que lo hacen, destaca de forma significativa Gitrama [58], quien entiende que el derecho a la propia imagen "es un derecho innato de la persona, que se concreta en la reproducción o representación de la figura de ésta, en forma visible y recognoscible. Es un derecho subjetivo de carácter privado y absoluto. Es un derecho personalísimo, pero dotado de un contenido potencialmente patrimonial. Es un derecho inalienable e irrenunciable y en general inexpropiable...en fin, es un derecho imprescriptible".

Nuestro constitucionalismo, no conoce hasta 1.978 derecho alguno identificable con el actual derecho a la propia imagen, si bien existen algunos aspectos jurisprudenciales curiosos .

4.2.2.1.- EL SECRETO DE "LO PRIVADO".

De igual modo que la transparencia de lo público es consustancial a los regímenes democráticos, en estos se da un desarrollo creciente de la sensibilidad social sobre el secreto de lo privado y muy especialmente de las consecuencias que para ello tienen las nuevas tecnologías de la información y las comunicaciones y su incidencia para las estructuras y valores generalmente admitidos y, esencialmente, para la privacidad del individuo.

4.2.2.1.1.- EL SECRETO DE LAS COMUNICACIONES.

El secreto de las comunicaciones 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 reaccional o de defensa frente al Estado para exigir su no injerencia en el objeto del derecho, salvo los supuestos de su limitación constitucionalmente previstos y, aun en este supuesto, para exigir que tales injerencias o limitaciones se produzcan con respeto a las garantías debidas.[59]

El artículo 18 de la Constitución Español, dedicado a regular en general la intimidad de las personas como derecho fundamental, en su apartado 3, garantiza el secreto de las comunicaciones [60] al decir:

"Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial".

La seguridad de los datos es el auténtico talón de Aquiles de la sociedad de las telecomunicaciones. Un sistema de información es tanto más seguro cuanto menos accesible sea, pero también es menos útil y eficaz.

La consideración de la seguridad de la información, en si misma, como un bien jurídico protegible se empieza a abrir camino entre la doctrina. [61]

El secreto de las comunicaciones constituye, se configura como un derecho que garantiza a los particulares una esfera de libertad que ha de ser respetada.

Los titulares de este derecho son tanto las personas físicas como las personas jurídicas. Y aunque el derecho a la intimidad sólo es atribuible a las personas físicas (T.C. Auto de 17 de abril de 1.985), el derecho al secreto de las comunicaciones, al igual que otros derechos de la personalidad, puede ser atribuido a las personas morales.

El objeto del derecho fundamental recogido en el artículo 18.3 de la Constitución, viene constituido por el secreto de las comunicaciones y está referido sólo a las comunicaciones privadas. Las comunicaciones públicas están tuteladas por el artículo 20 de la Constitución, referido a la libertad de expresión e información.

El derecho al secreto de las comunicaciones privadas, no parece que sea una concreción del derecho a la intimidad recogido en el artículo 18.1 de la Carta Magna. Porque éste, el derecho a la intimidad, posee un contenido material, aunque relativo y fluctuante, mientras que el derecho del secreto de las comunicaciones privadas posee un contenido formal.

El secreto no depende del contenido de las comunicaciones. Ni de que lo comunicado esté o no dentro del ámbito de la intimidad. "El concepto de "secreto" en el artículo 18.3, tiene un carácter "formal", en el sentido de que se predica de lo comunicado, sea cual sea su contenido, y pertenezca o no el objeto de la comunicación misma al ámbito de la persona, lo íntimo y lo reservado" (STC 114/1.984, de 29 de noviembre). La misma

sentencia afirma que este "derecho fundamental consagra la libertad de las comunicaciones, implícitamente y, de modo expreso, su secreto".

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. Aunque el precepto constitucional subraya especialmente *"las postales, telegráficas y telefónicas"*, la cobertura no se otorga sólo y exclusivamente a este tipo de comunicaciones.

Este derecho puede conculcarse tanto por la interceptación que suponga la aprehensión del soporte del mensaje -con conocimiento o no del mismo- como por el conocimiento antijurídico de lo comunicado.

Según la sentencia comentada, sería ilícita la utilización de aparatos técnicos que, aun sin captar el contenido de lo comunicado, registren los números marcados en un concreto teléfono, así como la hora y duración de la llamada, o la captación de comunicaciones cifradas (criptogramas), eventualmente destinadas al criptoanálisis.

El artículo 18.3 de la C.E., al reconocer el derecho fundamental del secreto de las comunicaciones, determina su carácter relativo, ya que permite su limitación por una resolución judicial que autorice la injerencia en su objeto.

En este mismo sentido se pronuncian los textos internacionales.

Según la Declaración Universal de Derechos Humanos, artículo 29.2 , *"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".

Tanto el artículo 10.2 del Convenio de Roma, como el 19.3 del Pacto de Nueva York, disponen que las restricciones "deberán estar expresamente fijadas por la ley". Es decir, únicamente se reconoce potestad restrictiva de las libertades en ellos protegidas al legislador, que es quien debe valorar el criterio de necesidad de la limitación y, su juicio, adopta la forma de ley.

Para el Convenio Europeo para la Protección de Derechos Humanos y Libertades Fundamentales, artículo 10.2, *"el ejercicio de estas libertades, por cuanto implica deberes y responsabilidades, 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".*

Para el artículo 19.2 del Pacto Internacional de Derechos Civiles y Políticos, el ejercicio de estos derechos 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".*

La "Declaración de los Derechos y Libertades fundamentales", aprobado por Resolución del Parlamento Europeo de 1.989, en su artículo 26 establece que los derechos y libertades a que se refiere, *"sólo podrán ser restringidos, dentro de los límites razonables y necesarios en una sociedad democrática, por una ley que respete en cualquier caso su contenido esencial".*

Cualquier limitación de estas libertades sólo es válida en cuanto hecha por ley, no ya porque así lo exijan los diversos pactos internacionales ratificados por España, sino sobre todo, porque así lo impone la propia Constitución que, extremando aún más las garantías, exige para esas leyes limitativas una forma especial e impone al propio legislador una barrera infranqueable (arts. 53 y 81 de la C.E.).

El legislador ordinario,-en nuestro caso orgánico por imperativos constitucionales-. sólo es el legitimado en una sociedad democrática para establecer hasta donde puede llegar la difusión de opiniones, juicios de valor e informaciones de todo tipo. Todo límite no consagrado expresamente en un texto legal debe tenerse por inexistente.

La resolución judicial, para que sea efectiva en su limitación del secreto de las comunicaciones, exige que estas, en el caso de estar protegidas criptológicamente, lo estén en base a un sistema que, siendo impenetrable por exigencia de la propia naturaleza de la protección, tenga organizada la gestión de claves de forma que permita a la autoridad judicial hacer realidad la limitación constitucionalmente prevista.

Todo ello sin olvidar que la libertad es un valor superior del ordenamiento jurídico -recogido en el artículo 1.1. de la C.E., que "obliga a considerar que el ejercicio del *'ius puniendi'* del Estado no debe perseguir a cualquier precio la eficacia, teniendo que ceder este interés público, en determinados casos, ante el interés individual en mantener el "status libertatis" libre de injerencias".

El derecho a una comunicación secreta está recogido en el artículo 18.3 de la Constitución requisito imprescindible para la libertad de comunicaciones.

El fenómeno de interceptación de las comunicaciones tiene tipificación penal en los artículos 197, 198 y 536 del Código Penal, aprobado por Ley Orgánica 10/1.995, de 23 de noviembre.

Por cuanto se refiere a la intimidad, la L.O. 1/1.982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, en su artículo 7, establece que tendrán la consideración de intromisiones ilegítimas en el ámbito de protección de esta

Ley, entre otras, *"el emplazamiento en cualquier lugar de aparatos de escucha, de filmación, de dispositivos ópticos o de cualquier otro medio apto para grabar o reproducir la vida íntima de las personas"* y también *"la utilización de aparatos de escucha, dispositivos ópticos, o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o cartas privadas no destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción"*.

La Ley 62/1.978, de 26 de diciembre, de protección jurisdiccional de los derechos fundamentales de la persona, en sus artículos 1 a 5 establece la garantía jurisdiccional penal para los delitos contra el derecho fundamental del secreto y la libertad de las comunicaciones telefónicas, y, en los artículos 11 a 15, la misma ley establece la garantía jurisdiccional civil del derecho fundamental referido. (El Real Decreto Legislativo 342/1.979, de 20 de febrero, incorpora al ámbito de protección de la Ley 62/1.978, entre otros, el derecho al secreto de las comunicaciones telefónicas).

La Ley 31/1.987, de 18 de diciembre, de Ordenación de las Telecomunicaciones vino a responder a la necesidad de establecer un marco jurídico básico en el que se contengan las líneas maestras a las que debía ajustarse la prestación de las diversas modalidades de telecomunicación, a la vez que se definieran las funciones y responsabilidades de la Administración Pública y de los sectores público y privado.

Como principio general, la Ley configura a las telecomunicaciones como servicios esenciales de titularidad estatal reservados al sector público.

Por lo que se refiere al secreto de las comunicaciones contemplado en el artículo 18.3 de la Constitución, tiene proyección en esta ley y, el Título Primero referido a Disposiciones Generales, en el artículo 2.2 dice que *"Los servicios de telecomunicación se organizarán de manera que pueda garantizarse eficazmente el secreto de las comunicaciones de conformidad con lo previsto en el artículo 18.3 de la Constitución".*

En el Título II, relativo a los Servicios Civiles de Telecomunicación, en el Capítulo II, Servicios finales y portadores, el artículo 16.1. f), reitera el respeto al secreto de comunicaciones constitucionalmente establecido al establecer que *"La prestación de los servicios portadores y de los servicios finales de telecomunicación deberá ajustarse, con carácter general, a los siguientes principios: ... f) Garantía del secreto de las comunicaciones, de conformidad con lo previsto en el artículo 18.3 de la Constitución".*

Y el artículo 24.7 de la Ley vuelve a referirse al secreto de las comunicaciones al decir:*"Las entidades explotadoras de servicios de valor añadido vendrán obligadas a garantizar el secreto de las comunicaciones y el principio de no discriminación de ningún potencial usuario del servicio siempre que se encuentre dentro de la zona de cobertura del mismo y se*

disponga de instalaciones suficientes para ello, todo esto sin perjuicio de lo que establece la Ley General para la Defensa de los Consumidores y Usuarios".

Textos internacionales, como el Convenio de Roma de 4 de noviembre de 1.950, establece que [62] *" Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.*

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", (artículo 8°).

Tanto la Declaración Universal de los Derechos Humanos, -especialmente su artículo 12-, como la Constitución, obligan al desarrollo legislativo que salve la laguna legal existente, porque 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.

La mera enumeración de derechos fundamentales en el texto constitucional es insuficiente para que estos puedan desplegar todo su significado.Esta se presenta como una enumeración que hace relativamente

incompleta la efectiva protección de los derechos. Se hace así necesaria una efectiva actuación de los poderes públicos que, en primer término, reviste un caracter normativo,[63] aunque la toma de conciencia de la necesidad de incluir ciertas necesidades y pretensiones en textos jurídicos no significa la conclusión del camino hacia la verdadera satisfacción de estos[64] que, en el caso del secreto de las comunicaciones exige la aplicación de medidas de seguridad -especialmente de naturaleza criptológica- que con carácter preventivo impidan que la violación se produzca.

4.2.2.1.2.- LOS DATOS DE CARÁCTER PERSONAL.

Ante la necesidad de un tratamiento masivo de información, con las máximas garantías de fidelidad y rapidez, surge la Informática, que se ocupa del proceso y almacenamiento de informaciones mediante soportes automatizados.

La exigencia de transmitir a distancia esas informaciones mediante redes interconectadas, ha determinado la aparición de la Telemática, tecnología de la comunicación para el intercambio de información entre equipos informáticos.[65]

El derecho que se trata de proteger tiene una mayor profundidad que la intimidad.

Al surgir la informática, y su simbiosis con las comunicaciones, es cuando aparece una nueva relación entre datos y personas, que necesita ser protegida más allá de las normas relativas a la intimidad.[66]

a) L.O.R.T.A.D.

Según la Exposición de Motivos de la Ley Orgánica número 5/1.992, de 29 de octubre, de Regulación del tratamiento automatizado de los datos de carácter personal *"...el progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la privacidad, en efecto, a una amenaza potencial antes desconocida..."* .

Esta ley, comunmente conocida como LORTAD, viene a dar respuesta al mandato del artículo 18.4 de la Constitución, dirigido a la limitación del uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el legítimo ejercicio de sus derechos.

La Ley, limitadora del uso de la informática, en lo concerniente al ámbito de los "ficheros de datos" de carácter personal, considera que su existencia y utilización supone un riesgo para los derechos de la personalidad.

Trata de prevenir violaciones de la privacidad, derivadas del tratamiento de datos considerados como una globalidad de procesos informáticos, que incluyen aspectos estáticos referidos al almacenamiento, y los dinámicos derivados de su cruce y relación, cuyo resultado puede proporcionar el retrato de la personalidad de un individuo, que tiene el derecho de preservar.

El ámbito de aplicación de la ley viene definido por exclusión de aquellos otros ámbitos, necesitados de publicidad, de uso estrictamente personal, entornos singulares con regulaciones específicas, como el caso de los ficheros sometidos a la normativa sobre protección de materias clasificadas; o por datos que no han de estar sometidos a régimen cautelar, en virtud de un interés público prevalente.

Como principios generales, la ley establece unas pautas genéricas para la recogida de datos encaminadas a garantizar, tanto la veracidad, como la utilización de los mismos, en evitación de una difusión incontrolada.

Las garantías de la persona se configuran jurídicamente como derechos subjetivos, contemplando la autodeterminación, el amparo, la rectificación y la cancelación.

El principio de autodeterminación otorga la posibilidad personal de determinar el nivel de protección de los datos, en base a un consentimiento para la licitud de la recogida de los mismos.

La Ley distingue entre ficheros públicos y privados, estableciendo regímenes diferenciados y, mediante una transposición del artículo 12 del Convenio 108 del Consejo de Europa, aborda el flujo transnacional de datos. Exige para poder llevarse a cabo, que el país de destino cuente con un ordenamiento con sistemas de protección equivalentes al español, o cuente, al menos, con garantías suficientes.

Para garantizar su eficacia, configura un órgano especializado e independiente.

A la hora de regular aspectos relacionados con la evolución tecnológica, acude a mecanismos jurídicos susceptibles de una elaboración o modificación más rápida. Intentando evitar el desfase de la norma respecto a las rápidas transformaciones que se producen en este campo, para lo que se remite a normas de autorregulación elaboradas por iniciativas de las asociaciones y organizaciones pertinentes.

La adopción de las medidas de seguridad necesarias, dentro del marco reglamentario respecto a las condiciones de integridad y de seguridad, corresponden al responsable del fichero.

La Criptología tiene su aplicación en hacer efectivo el mandato legal, dentro de las medidas de seguridad y en unión de otros procedimientos.

La Ley recoge una serie de principios de protección de datos, pero no recoge suficientemente los mecanismos para una protección efectiva. No contempla la seguridad en la transmisión de datos, con los problemas que implican las comunicaciones y su vulnerabilidad.

La LORTAD no es una ley de seguridad de la información, ni tampoco una norma destinada a limitar el uso y abuso de la informática de forma general, sino que está referida específicamente a la regulación del tratamiento de datos personales.[67]

Existen precedentes de aportaciones importantes, sobre los efectos de las nuevas tecnologías.

El Tribunal Europeo de Derechos Humanos, en la sentencia sobre el caso Klass, recaida en recurso interpuesto contra la Ley de 13 de agosto de 1.968, limitadora del secreto de la correspondencia y de las comunicaciones telefónicas y telegráficas de la entonces República Federal de Alemania, reconocía como dos de los aspectos más característicos de la situación política europea, la proliferación del terrorismo y el desarrollo de la tecnología de control y vigilancia de los gobiernos.

En Francia, el informe publicado en 1.978 titulado "L'informatisation de la société", se parte de la de que la sociedad informatizada es la consecuencia necesaria del desarrollo tecnológico. Que su orientación futura depende del equilibrio entre los poderes estatales, y del fortalecimiento de la sociedad civil, siendo la informática, uno de los principales ingredientes de esa dosificación.

El acopio de datos en bancos públicos y privados, ha creado una psicosis colectiva de temor a una paulatina "polución de las libertades" a partir de la utilización abusiva e incontrolada de la informática.

La Sentencia del Tribunal constitucional Federal de la República Federal de Alemania de 15 de diciembre de 1.983, en la que se declara inconstitucional la Ley del Censo de Población de 4 de marzo de 1.982, vino

a reavivar el debate sobre las amenazas que entraña el progreso tecnológico para el sistema de libertades en los países democráticos occidentales.

El texto internacional más importante es el Convenio 108 para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal, adoptado por el Comité de Ministros del Consejo de Europa de 22 de septiembre de 1.980, abierto a la adhesión de los Estados miembros a partir del 28 de enero de 1.981, y ratificado por España, el 27 de enero de 1.984 (B.O.E. de 15 de noviembre de 1.985).

El Título VI de la LORTAD, ha configurado la Agencia de Protección de Datos como el ente independiente que debe garantizar el cumplimiento de las previsiones y mandatos en ella establecidos.

Entre las funciones de la Agencia de Protección de Datos, está la cooperación en la elaboración y aplicación de las normas y, a tal efecto, el artículo 5, d), del Real Decreto 428/1.993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, establece que dictará recomendaciones de aplicación de las disposiciones legales y reglamentarias en materia de seguridad de los datos y control de acceso a los ficheros.

La Agencia ejercerá el control de la observancia de lo dispuesto en la ley 12/1.989, de 9 de mayo, de la función Estadística Pública y, por lo que se refiere a los ficheros estadísticos, el artículo 6, d) de su estatuto dice

que: *"Dictaminará sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos".*

En base a la función inspectora, la Agencia, a través de la Inspección de Datos, podrá :

"a) Examinar los soportes de información que contengan los datos personales.

b) Examinar los equipos físicos.

c) Requerir el pase de programas y examinar la documentación pertinente al objeto de determinar, en caso necesario, los algoritmos de los procesos de que los datos sean objeto.

d) Examinar los sistemas de transmisión y acceso a los datos.

e) Realizar auditorías de los sistemas informáticos con miras a determinar su conformidad con las disposiciones de la Ley Orgánica 5/1.992. ..." (Art. 28 del Estatuto).

b) Libertad informática.

La libertad informática tiene sus orígenes en el "derecho de autodeterminación informativa" surgido de la Sentencia de 13 de abril de 1.983, del Tribunal Constitucional Alemán, sobre la Ley del Censo de Población, que constituyó el punto de partida del reconocimiento de la libertad informática, a lo que ha contribuido la doctrina y la jurisprudencia de la República Federal de Alemania, cuya evolución ha configurado el concepto de "libertad informática", como hoy lo entendemos. [68]

- Como libertad de controlar el uso de los propios datos personales insertos en un programa informático.

- Como control para que los datos se usen adecuadamente y no se atente contra los derechos y libertades.

- Como derecho de acceso a los bancos de datos, derecho de control de su exactitud, puesta al día y rectificación, derecho de autorización para su difusión y, derecho de secreto para los datos "sensibles".

El carácter *"sensible"* de los datos, no depende sólo de su conexión directa e inmediata con los aspectos centrales de la información. Existe toda una serie de datos colaterales, aparentemente inócuos, que, adecuadamente procesados, pueden aportar un conocimiento substancial. La preservación del núcleo esencial de la información, requiere, además de la protección de los datos referidos a él directamente, la protección de toda una serie de datos situados en la periferia del mismo, ya que como ha reconocido el Tribunal Constitucional alemán, hoy no existe ningún dato "sin interés".

Para F. Herrero Tejedor, la "privacy" hoy se concibe como una libertad positiva de ejercer un derecho de control sobre los datos referidos a la propia persona, que han salido ya de la esfera de la intimidad para convertirse en elemento de un archivo electrónico privado o público. Es lo que Frosini ha denominado la "libertad informática", que consiste en el derecho de autotutela de la propia identidad informática. [69]

En esta sentencia, el Tribunal constitucional alemán indica que la proliferación de centros de datos ha permitido, gracias a los avances tecnológicos, producir una imagen total y pormenorizada de la persona respectiva, incluso en el ámbito de su intimidad, convirtiéndose así el ciudadano en *"hombre de cristal"*.

El interés de esta sentencia reside en haber configurado el derecho a la intimidad como expresión de un derecho a la autodeterminación informativa. De la dignidad y de la libertad entendida como libre autodeterminación, deriva la facultad de la persona de "decidir básicamente por sí misma, cuando y dentro de qué límites, procede revelar situaciones referentes a la propia vida".

A juicio del Tribunal Constitucional, el derecho a la autodeterminación informativa no carece de límites. Porque el ciudadano de un Estado Social de Derecho no tiene un derecho sobre sus datos, en el sentido de una soberanía absoluta e ilimitada, sino que es una persona que se desenvuelve en una comunidad social en la que la comunicación y la información resultan imprescindibles. Por ello, la información, aún aquella que se refiere a los datos personales, ofrece una imagen de la realidad social que no puede ser patrimonio exclusivo del interesado. "El individuo tiene que aceptar determinadas limitaciones de su derecho a la autodeterminación informativa en aras del interés preponderante de la colectividad".

Los límites que la política de información y documentación del Estado Social de Derecho imponen al ejercicio de los derechos fundamentales y, en particular, al derecho a la autodeterminación informativa, deben respetar las siguientes garantías: a) Claridad normativa. b) Proporcionalidad de la restricción, que exige circunscribirla a lo que es indispensable para defender el interés general. c) Adecuación de los medios a la finalidad

perseguida por los procesos de documentación e información, y d) Garantías organizativas que eviten la ulterior interrelación indebida de los bancos de datos, porque , como el propio Tribunal reconoce, los nuevos avances tecnológicos en el tratamiento automatizado de información y la elaboración estadística de datos, hace que hoy no exista ningún dato sin interés.

Para el juzgador alemán, la sensibilidad de las informaciones no depende tanto de su conexión inmediata con aspectos que afecten a la intimidad como de la posibilidad de que puedan utilizarse en procesos que afecten al ejercicio de los derechos fundamentales y, en concreto, al libre desarrollo de la personalidad.

Cuestiones que reavivan la tensión derechos fundamentales y libertades públicas frente a deberes de los individuos con respecto al Estado, realidad siempre abierta y sobre la que los tribunales tienen mucho que decir.[70]

El artículo 6 de la "Declaración de los Derechos y libertades fundamentales", aprobado por Resolución del Parlamento Europeo de 1.989 (DOCE C 120/51, de 16 de mayo; doc. A 2-3/89), establece que *"1.- Toda persona tiene derecho al respeto y a la protección de su identidad.*

2.- Se garantizará el respeto de la esfera privada y de la vida familiar, del honor, del domicilio y de las comunicaciones privadas".

De igual modo se contemplan los derechos de acceso y rectificación.

En el sistema constitucional español, la libertad informática encuentra un reconocimiento inmediato en el artículo 18.4 de la Constitución al decir que "*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*".

Y que se regulará *"...b) El acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas"*. (105. b).

La libertad informática tiene, asimismo, soporte en la propia definición de nuestra forma política como "Estado social y democrático de Derecho, que propugna como valores superiores del ordenamiento jurídico la libertad, la justicia, la igualdad y el pluralismo político", en equilibrada relación con otros principios constitucionales y, fundamentalmente, con las libertades de expresión y derecho a la información, o el secreto de las comunicaciones, de los artículo 20 y 18.3 de nuestra Carta Magna, respectivamente.

El derecho de "secreto de los datos sensibles", para que sea real y efectivo, exige la aplicación de medidas de seguridad que lo protejan, lo cual comporta infraestructura de comunicaciones seguras, terminales seguros, procesadores y bases de datos seguros y, una utilización segura de todo ello.

El derecho al secreto de las comunicaciones tiene un carácter omnicomprensivo y es aplicable a cualquier medio o servicio que sirva para la transmisión de las mismas. Aunque el precepto constitucional subraya especialmente "las postales, telegráficas y telefónicas", la cobertura no se otorga sólo y exclusivamente a este tipo de comunicaciones.

Se podría decir que el secreto de las comunicaciones aplicado a la información almacenada, tratada o transmitida electrónicamente, viene a complementar y reforzar la "libertad informática" en su faceta de derecho de secreto para los datos "sensibles".

Ante los avances tecnológicos que permiten el acceso a las bases de datos y la interceptación de las transmisiones efectuadas por cualquier medio, y la creciente importancia de cualquier dato para conocer el perfil de la personalidad -así como la necesidad de protección sistemática de las comunicaciones privadas, derivada del artículo 18.3 de la C.E.-, la protección criptológica, como forma de preservar el secreto de los datos , es una aplicación concreta, imprescindible, para que la "libertad informática" sea real y efectiva.

La Sentencia del Tribunal Constitucional Alemán, de 13 de abril de 1.983, sobre la Ley del Censo de Población -en la que está el origen del concepto de "libertad informática"-, señalaba como limitaciones admisibles las derivadas del marco de un interés superior con fundamento en la constitución, cuyas normas, además de tomar las precauciones necesarias para

neutralizar el peligro derivado de la vulneración del derecho, apliquen el principio de proporcionalidad, y preserven los intereses generales.

Por lo que se refiere a la intimidad de las personas jurídicas, la STC 64/1.988, de 12 de abril viene a indicar que la titularidad de los derechos fundamentales "no corresponde sólo a los individuos aisladamente considerados, sino también en cuanto se encuentran insertos en grupos y organizaciones cuya finalidad sea específicamente la de defender determinados ámbitos de libertad o realizar los intereses y los valores que forman el substrato último del derecho fundamental"

Los derechos fundamentales y las libertades públicas son derechos individuales que tienen un sujeto activo, individual o colectivo, y al Estado como sujeto pasivo.

Por lo que se refiere a la relación entre libertad informática y criptología, una comunicación presentada en el II Congreso Internacional de Informática y Derecho, celebrado durante el mes de mayo de 1.995, [71] establecía entre otras conclusiones, las siguientes:

1.- El derecho de secreto para los datos "sensibles" es una manifestación concreta de la "libertad informática".

2.- Las limitaciones a la "libertad informática" sólo son admisibles en el marco de un interés general, superior, con fundamento en los principios básicos de una organización democrática del Estado, reconocidos internacionalmente.

3.- El secreto de las comunicaciones, aplicado a la información almacenada, tratada o transmitida electrónicamente, viene a complementar y reforzar la "libertad informática", añadiendo un plus de confidencialidad en su faceta de derecho de secreto para los datos.

4.- La protección criptológica, como medio para que la "libertad informática" sea real y efectiva, se ha convertido en una exigencia ineludible de cualquier sistema informático.

c) Medidas de seguridad.

En cuanto a las medidas de seguridad, el artículo 9.1 de la LORTAD, establece que *"el responsable del fichero deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural"*.

La recogida y tratamiento automatizado para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas, están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al

efecto, que deberán clasificarse por categorías, en función de su grado de fiabilidad.

Por lo que se refiere a los ficheros de titularidad privada, la Ley indica que por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener (Art. 24.2).

Entre las medidas que garantizan la seguridad de los datos, tanto las adoptadas por el responsable del fichero como las determinadas por vía reglamentaria, ocupan un lugar destacado las aplicaciones criptológicas.

Entre las infracciones graves, el artículo 43.3 d) señala la de tratar los datos de carácter personal *"... con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave"*, y, el artículo 43.3., h) señala, *"mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria, se determinen"*.

Tanto el Convenio 108 del Consejo de Europa, como la Ley Orgánica 5/1.992, y la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1.995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, se refieren a las medidas de seguridad que deben cumplir los ficheros automatizados que contengan datos de carácter personal.

Las referencias a las medidas de seguridad en los textos indicados ha ido experimentando una evolución. En el Convenio 108 la obligación es de tomar medidas de seguridad apropiadas, sin distinción alguna en cuanto a ellas; la LORTAD impone la adopción de medidas técnicas y organizativas necesarias que garanticen la seguridad de los datos a un nivel de seguridad adecuado, reforzando las medidas cuando se trate de datos especialmente protegidos y se remite a un posterior desarrollo reglamentario, lo que se llevó a efecto por Real Decreto 1332/1.994, de 20 de junio, pero este reglamento dejó sin desarrollar lo referido a las medidas de seguridad, con todas las consecuencias que ello comporta.

La Directiva 95/46 del Parlamento Europeo va más lejos y no basa el reforzamiento de las medidas de seguridad solamente en la naturaleza especialmente protegida de los datos personales sino que, también tiene en cuenta su transmisión dentro de una red.

La Directiva establece que los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales. *"Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y el coste*

de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse".

El responsable del tratamiento deberá elegir un encargado del tratamiento que reúna garantías suficientes en relación con las medidas de seguridad técnica y de organización que deban efectuarse.

Por lo que se refiere al tratamiento de los datos personas y a la protección de la intimidad en el sector de las telecomunicaciones, la Directiva 97/66/Ce del Parlamento Europeo y del Consejo de 15 de diciembre de 1.997, a la que nos referimos en el apartado f) de este epígrafe, aborda las medidas de seguridad.

d) Régimen de protección de las personas jurídicas en el Convenio 108 del Consejo de Europa de 28 de enero de 1.981.

El Convenio 108 del Consejo de Europa para la protección de las personas, con respecto al tratamiento automatizado de los datos de carácter personal, en su artículo 3 b) deja abierta la posibilidad de que los Estados miembros puedan extender el régimen de protección a las personas jurídicas.

Para F. Herrero Tejedor, de la doctrina del Tribunal Constitucional se pueden extraer dos conclusiones:

1ª Las personas jurídicas poseen legitimación para actuar en juicio, incluso en el recurso de amparo, para instar la tutela de sus intereses legítimos.

2ª Desde el punto de vista de la titularidad de los derechos fundamentales, no puede darse una norma taxativa, sino que habrá que estar a la naturaleza propia de cada derecho, si bien las personas jurídicas deben ser admitidas como posibles titulares de tales derechos siempre que vengan a colocarse en el lugar del sujeto privado comprendido dentro del área de la tutela constitucional y no sean incompatibles con la naturaleza y especialidades del ente colectivo.

En relación con los derechos del artículo 18.1, no parecen existir obstáculos insalvables para configurar a las personas jurídicas como titulares del derecho al honor, al nombre y a ciertas parcelas de la intimidad personal, mientras que su naturaleza resulta incompatible con el derecho a la propia imagen y a la intimidad familiar. [72]

La protección de datos también guarda relación con la "libertad de empresa" reconocida en el artículo 38 de la Constitución en el marco de la economía de mercado.

El derecho de libre empresa no supone sólo la libertad de acceder al mercado o emprender actividades económicas; implica también la libre gestión empresarial, sometida a las leyes de un mercado libre.

La libertad de empresa representa, también, la libertad para gestionarlas libremente, en el marco de la economía de mercado.

La protección de los datos, -tanto en fase de proceso o archivo, como durante la transmisión- requiere la aplicación de medidas de

seguridad, para evitar accesos no autorizados y garantizar el secreto de las comunicaciones, entre las que destacan las de naturaleza criptológica.

Esta libertad del titular de la empresa -la propiedad privada está reconocida por el artículo 33- se manifiesta tanto frente a los poderes públicos como frente a los consumidores y frente a los trabajadores de la propia empresa".[73]

e) R.D. 263/1.996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado.

En nuestro ordenamiento, la Ley 30/1.992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, opta de forma clara por la tecnificación de la actuación administrativa frente a las tendencias burocráticas formalistas.

Entre las previsiones de la citada Ley destaca el artículo 45, verdadera piedra angular del proceso de incorporación de dichas técnicas en la producción jurídica de la Administración Pública, así como en sus relaciones con los ciudadanos, que ha sido desarrollado por R.D. 263/1.996, de 16 de febrero.

Como criterio inspirador de la elaboración del Real Decreto, se ha prestado especial atención a recoger las garantías y derechos de los ciudadanos frente a la Administración cuando ésta utiliza las tecnologías de la información.

La utilización de estas técnicas, según el artículo 2 del R.D. 263/1.996, de 16 de febrero, "*tendrán las limitaciones establecidas por la Constitución, la Ley 30/1.992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y el resto del ordenamiento jurídico, respetando el pleno ejercicio de los ciudadanos de los derechos que tienen reconocidos. En especial, se garantizará el honor y la intimidad personal y familiar de los ciudadanos ajustándose, a tal efecto, a lo dispuesto en la ley Orgánica 5/1.992, de Regulación del Tratamiento Automatizado de los datos de carácter personal, y en las demás Leyes específicas que regulan el tratamiento de la información así como en sus correspondientes normas de desarrollo...*".

El artículo 4 del citado Real Decreto, referido a las garantías generales de la utilización de soportes, medios y aplicaciones electrónicas, informáticas y telemáticas, establece que *"Cuando se utilicen los soportes, medios y aplicaciones referidos en el apartado anterior, se adoptarán las medidas técnicas y de organización necesarias que aseguren la autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información. Dichas medidas de seguridad deberán tener en cuenta el estado de la tecnología y ser proporcionadas a la naturaleza de los datos y de los tratamientos y a los riesgos a los que estén expuestos.*

Las medidas de seguridad aplicadas a los soportes, medios y aplicaciones utilizados por los órganos de la Administración General del

Estado y sus entidades de derecho público vinculadas o dependientes deberán garantizar:

a) La restricción de su utilización y del acceso a los datos e informaciones en ellos contenidos a las personas autorizadas.

b) La prevención de alteraciones o pérdidas de los datos e informaciones.

c) La protección de los procesos informáticos frente a manipulaciones no autorizadas.

4.- Las especificaciones técnicas de los soportes, medios y aplicaciones utilizados en el ámbito de la Administración General del Estado en sus relaciones externas y cuando afecten a derechos e intereses de los ciudadanos deberán ser conformes, en su caso, a las normas nacionales e internacionales que sean exigibles".

Las comunicaciones en soportes o a través de medios o aplicaciones informáticos, electrónicos o telemáticos, se regulan en el Capítulo II, artículo 7, según el cual *"1.- La transmisión o recepción de comunicaciones entre órganos o entidades del ámbito de la Administración General del Estado o entre estos y cualquier persona física o jurídica podrá realizarse a través de soportes, medios y aplicaciones informáticos, electrónicos y telemáticos, siempre que cumplan los siguientes requisitos:*

a) La garantía de su disponibilidad y acceso en las condiciones que en cada caso se establezcan.

b) La existencia de compatibilidad entre los utilizados por el emisor y el destinatario que permita técnicamente las comunicaciones entre ambos, incluyendo la utilización de códigos y formatos o diseños de registro establecidos por la Administración General del Estado.

c) La existencia de medidas de seguridad tendentes a evitar la interceptación y alteración de las comunicaciones, así como los accesos no autorizados...."

En los programas y aplicaciones que efectúen tratamientos de información cuyo resultado sea utilizado para el ejercicio de los órganos y entidades del ámbito de la Administración General del Estado de las potestades que tienen atribuidas deberán ser objeto de aprobación y difusión públicas y, cuando estas aplicaciones vayan a ser utilizadas en el ejercicio de competencias compartidas por varios Departamento o entidades de derecho público de la Administración General del Estado vinculadas o dependientes de Departamentos diferentes deberán ser aprobadas mediante Orden del Ministerio de la Presidencia, a propuesta de los titulares de los Departamentos afectados, debiéndose solicitar previamente la emisión de los informes técnicos que se estimen convenientes (artículo 9.2), estos informes se pronunciarán sobre los siguientes aspectos:

"b) Seguridad de aplicación: preservación de la disponibilidad, confidencialidad e integridad de los datos tratados por la aplicación".

En la Disposición Adicional Primera, por lo que se refiere a las atribuciones del Consejo Superior de Informática, se añade un nuevo apartado 2 al artículo 3 del Real Decreto 2291/1.983, de 18 de julio, con la siguiente redacción:

"Corresponde al Consejo Superior de Informática la aprobación y difusión de los criterios generales de seguridad, normalización y conservación de las aplicaciones a que se refiere el artículo 5 del Real Decreto 263/1.996, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado".

Las disposiciones de este Real Decreto relativas a la obtención o difusión de informaciones sobre la identificación de los soportes, medios y aplicaciones utilizados o sobre sus características no serán de aplicación a aquellos que efectúen tratamientos de información que afecte a la Defensa Nacional o a la Seguridad del Estado.(Disposición Adicional Segunda).

f) Tratamiento de datos personales y protección de la intimidad en el sector de las telecomunicaciones.

Recientemente se ha publicado la Directiva 97/66/CE (DOCE L 24 de 30/01/98) relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, para establecer la armonización de las disposiciones de los Estados miembros necesarias para garantizar un nivel equivalente de protección de las libertades y de los derechos fundamentales y, en particular, del derecho a la intimidad, en lo

que respecta al tratamiento de los datos personales en el sector de las telecomunicaciones, así como la circulación de tales datos y de los equipos y servicios de telecomunicación en la Comunidad.

Las disposiciones de esta Directiva especificarán y completarán la directiva 95/46/CE,y protegerán los intereses legítimos de los abonados que sean personas jurídicas. Se aplicará al tratamiento de datos personales en relación con la prestación de servicios públicos de telecomunicación en las redes públicas de telecomunicación en la Comunidad y, especialmente, a través de la red digital de servicios integrados (RDSI) y las redes móviles digitales públicas.

Esta Directiva no se aplicarán a las actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea y, en cualquier caso, a las actividades que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dichas actividades estén relacionadas con la seguridad del Estado) y a las actividades del Estado en materia penal.

En lo referido a la confidencialidad de las comunicaciones, el artículo 5 de la Directiva establece que los Estados miembros garantizarán, mediante normas nacionales, la confidencialidad de las comunicaciones realizadas a través de las redes públicas de telecomunicación y de los servicios de telecomunicación accesibles al público. En particular, prohibirán la

escucha, la grabación, el almacenamiento u otros tipos de interceptación o vigilancia de las comunicaciones por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando esté autorizada legalmente.

Todo ello no será de aplicación a las grabaciones legalmente autorizadas de comunicaciones en el marco de una práctica comercial lícita destinada aportar pruebas de una transacción comercial o de cualquier otra comunicación comercial.

En todo caso, los Estados miembros *"...podrán adoptar medidas legales para limitar el alcance de las obligaciones y derechos, cuando dichas limitaciones constituyan una medida necesaria para proteger la seguridad nacional, la defensa, la seguridad pública, la prevención, la investigación, la detección y la persecución de delitos o la utilización no autorizada del sistema de telecomunicación..."* (Artículo 14.1).

Por cuanto se refiere a la seguridad, el artículo 4 establece que:

"1.- El proveedor de un servicio público de telecomunicación deberá adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios, de ser necesario en colaboración con el proveedor de la red pública de telecomunicación por lo que respecta a la seguridad de la red. Considerando las técnicas más avanzadas y el coste de su aplicación, dichas medidas garantizarán un nivel de seguridad adecuado para el riesgo existente.

2.- En caso de que exista un riesgo concreto de violación de la seguridad de la red, el proveedor de un servicio público de telecomunicación deberá informar a los abonados sobre dicho riesgo y sobre las posibles soluciones, incluidos los costes necesarios".

Además, la Directiva establece plazos a los Estados miembros para poner en vigor las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a su contenido, fijando, como fecha límite el 24 de octubre de 1.998, excepto para lo que se refiere a la confidencialidad de las comunicaciones, (artículo 5 en relación con el 14.1), para cuyo cumplimiento fija como fecha límite el 24 de octubre del año 2.000.

El artículo 50 de la Ley 11/1.998, de 24 de abril, General de Telecomunicaciones, referido a la "Protección de los datos de carácter personal establece la obligación de los operadores de proteger los datos de carácter personal conforme a la LORTAD y normas de carácter técnico que exija la normativa comunitaria en materia de protección de datos personales.

4.3.- PROTECCIÓN REAL Y EFECTIVA DE LOS ÁMBITOS DE CONFIDENCIALIDAD: EL CIFRADO.

Las características de la información, del conocimiento y de las nuevas tecnologías, hace que su vulneración produzca daños irreversibles, sin que la sanción jurídica sea suficiente, por lo que una protección real y efectiva requiere de mecanismos que lo eviten.

La plenitud del ordenamiento jurídico exige que, además de la protección *"a posteriori"* sancionando conductas contrarias al mismo, disponga de mecanismos que garanticen de forma eficaz, *"a priori"*, en determinadas circunstancias, las consecuencias irreparables de eventuales violaciones, lo que se lleva a cabo a través de lo que se conoce como medidas de prevención, entre las que destaca la Criptología.

4.3.1.- NATURALEZA JURÍDICA DE LA CRIPTOLOGÍA.

La Criptología como medida de prevención requiere, además de una eficacia operativa, una fundamentación y un soporte jurídico legitimador de su aplicación que, lejos de desequilibrar la balanza de la tensión libertad-seguridad, -en este caso concreto, libertad de información-secreto de las comunicaciones- con detrimento para la libertad, sea, por el contrario, un presupuesto básico de la misma, para lo que la naturaleza y condiciones de los ámbitos a los que se aplique y las garantías en su uso y control, son condiciones indispensables para su legitimidad.

"La protección de los derechos no se contrae a la reparación de los perjuicios originados, sino que han de extenderse a las medidas de prevención que razonablemente impidan ulteriores lesiones", (STS de 10 de diciembre de 1.980).

La Ley Orgánica 1/1.982, de 5 de mayo, de Protección Civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, en su artículo 7.1, dice que tendrán la consideración de intromisiones ilegítimas

en el ámbito de protección civil de la intimidad y la propia imagen, el emplazamiento de aparatos de escucha, filmación, dispositivos ópticos o de cualquier otro medio apto para grabar o reproducir la vida íntima de las personas.

La utilización de aparatos de escucha, dispositivos ópticos, o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones, así como su grabación registro o reproducción.

La tutela judicial frente a estas intromisiones ilegítimas *"...comprenderá la adopción de todas las medidas necesarias para poner fin a la intromisión ilegítima de que se trate y restablecer al perjudicado en el pleno disfrute de sus derechos, así como para prevenir o impedir intromisiones ulteriores. ..." (art. 9.2).*

Para prevenir e impedir, de forma eficaz estas intromisiones, en muchos de estos supuestos las medidas de prevención no sólo han de ser de carácter jurídico, sino que la exigencia de eficacia requiere medidas extrajurídicas entre las que están las constituidas por lo que se conoce como seguridad de la información y de las comunicaciones, que requiere, entre otras, la utilización de técnicas criptológicas.

La Ley y Reglamento de Secretos Oficiales, las contempla en los términos indicados. En relación con los asuntos clasificados por aplicación de la ley, lo están, como secreto, "las claves y material criptográfico".[74]

La evolución de la importancia de la protección de la información y las comunicaciones en la sociedad de la información, ha ido incrementandose.

La conveniencia inicial de proteger se ha transformando en necesidad, que deviene en obligación cuando se refiere a la protección de derechos.

La seguridad de la información como instrumento efectivo, coadyuva con el derecho y el poder como instrumentos de ordenación social y, juridificada se sitúa en el pórtico de su reconocimiento como deber.

Los medios técnicos -entre los que destaca la criptología- como componente estelar de la seguridad de la información y las comunicaciones, participan de esta consideración y se podría afirmar que el cifrado de información, además de ser un medio de protección efectiva de derechos, en determinados casos puede ser un deber jurídicamente exigible.

Este salto cualitativo se puede observar en la Ley 11/1.998, de 24 de abril, General de Telecomunicaciones, al orientar las disposiciones relativas al secreto de las comunicaciones, a la protección de datos personales y al cifrado, como garantes de derechos fundamentales y considerarlo como deber de los operadores de telecomunicaciones y proveedores de servicios, (artículos 49 y 50).

No obstante la ley en su artículo 52.1, parece incurrir en una contradicción al utilizar la expresión *"podrá"* para referirse al cifrado de

cualquier tipo de información que circule por redes de telecomunicaciones, en lugar de *"deberá"*, que consideraríamos más adecuada.

En similar contradicción incurre cuando se refiere al establecimiento de las condiciones para los procedimientos de cifrado en las normas de desarrollo cuando utiliza de nuevo el verbo *"poder"* del que se deriva una facultad potestativa de hacer o no hacer, cuando en realidad la complejidad del cifrado exige para que produzca los efectos perseguidos, que el soporte criptográfico no sea cualquiera, sino que sea el del nivel adecuado.

Entendemos por ello que el establecimiento de condiciones para los procedimientos de cifrado ha de fijarse no como una mera facultad, sino como un requisito imprescindible, del que va a depender la efectividad del fin perseguido.

La Ley General de Telecomunicaciones, en su artículo 52.2. define el cifrado como instrumento de seguridad de la información e introduce toda una regulación que afecta de forma decidida al uso del cifrado, que consideramos de extraordinario interés y supone un importante avance en la regulación de la Criptología en España, al decir:

"2.- El cifrado es un instrumento de seguridad de la información. Entre sus condiciones de uso, cuando se utilice para proteger la confidencialidad de la información, se podrá imponer la obligación de notificar bien a un órgano de la Administración General del Estado o a un organismo público, los algoritmos o cualquier procedimiento de cifrado

utilizado, a efectos de su control de acuerdo con la normativa vigente. Esta obligación afectará a los fabricantes que incorporen el cifrado en sus equipos o aparatos, a los operadores que lo incluyan en las redes o dentro de los servicios que ofrezcan y, en su caso, a los usuarios que lo empleen".

Este precepto encierra un alto contenido y viene a configurar, en gran medida, la forma de concebir el uso de la Criptología en nuestro país, lo que hace prever un detallado desarrollo reglamentario.

Además, como quiera que los derechos subyacentes en el cifrado de cualquier información son de naturaleza e intensidad distinta, se necesita articular la protección técnica por niveles que den respuesta a la seguridad adecuada de los distintos ámbitos de confidencialidad.

En las colisiones que se producen entre los bienes jurídicos protegidos de los derechos subyacentes -algunos de los cuales tienen carácter de prevalentes- la criptología es solo un instrumento de eficacia de esos derechos, pero dada la impregnación de seguridad que cada vez está más presente en los procesos de información y comunicaciones, tal vez requiera avanzar a configurar la "seguridad de la información", en sí misma, como un bien jurídico digno de protección y, en determinados casos, la adopción de medidas como las criptológicas pueden llegar a adquirir el carácter de deber jurídicamente exigible.

De otra parte, el extraordinario avance experimentado por la tecnología y sus aplicaciones bélicas, ha determinado que el concepto

clásico de arma haya quedado desfasado y que, por el contrario, adquieran importancia trascendental los elementos, partes integrantes de los mismos y tecnologías que, aún no teniendo en sí mismos una finalidad destructora, aumentan las capacidades ofensiva o defensiva de un Estado y que, a la vez, tienen aplicaciones civiles.

Estos elementos o tecnologías son los que la legislación y la práctica internacional denominan *"materiales de doble uso"*, y configura a la Criptología como tecnología de doble uso.

Estados Unidos clasifica los productos de cifrado como municiones, y considera que es prudente tener en cuenta estos productos fuera del país. En esta idea basan las restricciones a la exportación.

Además, no todos los productos criptográficos son iguales, y restringe la exportación de los más robustos basado en la idea que "No todo el mundo necesita conducir por todas partes un tanque".[75]

Se podría afirmar que la Criptología jurídicamente es una medida de prevención con múltiples aplicaciones basada en una tecnología que tiene la consideración legal de "tecnología de doble uso".

4.3.2.- Regulación de la protección criptológica de la información.

Las motivaciones de la regulación legal de la Criptología tienen su origen, fundamentalmente, en las dificultades que su empleo provoca en la investigación, persecución y prevención de actos delictivos en general y

especialmente la delincuencia organizada, la lucha contra el narcotráfico y el terrorismo, siendo previsible que este efecto se incremente en el futuro, por lo que urge articular leyes y medios técnicos que salven esta dificultad.

Para ello existen diversas posibilidades:

a) Prohibir el uso de los sistemas criptográficos resistentes y abordar mediante el criptoanálisis el descifrado de los sistemas débiles, lo que supone exponer la seguridad del sistema a todo el que disponga de capacidad de criptoanálisis.

Las leyes restrictivas del uso de la criptografía tienen siempre limitaciones derivadas de la disponibilidad pública de algoritmos criptográficos y la existencia de investigadores independientes.

b) Otras iniciativas se orientan hacia el uso de sistemas criptográficos robustos, pero diseñados de forma que no sea posible ocultar el contenido del mensaje en el transcurso de una investigación judicial, bien mediante la habilitación legal a la justicia para pedir la entrega de la clave usada en una comunicación cifrada o por otro procedimiento, lo que puede vulnerar derechos reconocidos en los países democráticos. Incluso este procedimiento puede ser ineficaz ante modernos desarrollos criptológicos en los que el conocimiento de lo que conocemos como clave es insuficiente para obtener el descifrado.

Es previsible que la alta delincuencia sea indiferente a leyes que no van a cumplir, y que los servicios de inteligencia no modifiquen

sustancialmente su tradicional juego de procurar la mejor criptografía propia a la vez que intentan contrarrestar la del adversario.

Generalmente la criptografía ha sido tratada por los distintos ordenamientos con actitudes más o menos restrictivas, permisivas o de mera tolerancia, en definitiva posiciones que se podrían calificar de pasivas o negativas respecto a su uso. Hoy, el uso de la criptografía se orienta hacia la protección de derechos, que en muchos casos tienen la consideración de fundamentales, por lo que el cifrado de las comunicaciones se torna en una obligación de los poderes públicos para su protección.

Esta garantía en unos casos es una obligación de no interferencia de los poderes del Estado, pero en otros, es positiva e implica promoción y actuaciones concretas, en definitiva, es una obligación de actuar de los poderes del Estado como sería el caso de la protección de la información y las comunicaciones.

La ordenación de los criterios para el estudio de la situación legal de la Criptología son variados, agrupándose fundamentalmente en torno a dos polos: uno regido por el grado de actualidad de la norma en el que se distinguen las leyes vigentes de los proyectos e iniciativas legislativas y, otro, basado en el tipo de restricción legal, en el que se engloban las restricciones de uso, las restricciones a la exportación y las patentes.

Las normas restrictivas están presentes en muchos países y responden a la consideración de la Criptología como tecnología de doble uso.

Mucho más limitadas son las normas restrictivas basadas en las patentes de algoritmos criptográficos, circunscritos a países con capacidad tecnológica para su desarrollo, siendo este un fenómeno particularmente importante en Estados Unidos.

En base a los argumentos expuestos de obligatoriedad de actuación del Estado en determinados casos, entre los criterios de clasificación de la situación legal de la Criptología comunmente utilizados hasta ahora, consideramos conveniente incorporar un criterio basado en la obligatoriedad legal del uso de la Criptología.

CRITERIOS DE CLASIFICACIÓN DE LA SITUACIÓN LEGAL DE LA CRIPTOLOGÍA.

- *POR LOS TIPOS DE RESTRICCIONES LEGALES:*
  - *. Restricciones de uso.*
  - *. Restricciones a la exportación.*
  - *. Patentes.*
- *POR LA OBLIGATORIEDAD LEGAL DE SU USO.*
- *POR LA ACTUALIDAD DE LA NORMA.*
  - *. Leyes vigentes.*
  - *. Proyectos e iniciativas legislativas*
- *POR EL ÁMBITO GEOGRÁFICO.*
  - *. EE.UU.*
  - *. Europa.*
  - *. Resto del mundo.*
  - *. España.*

La legislación sobre Criptología es un caso particular en Estados Unidos, entre otros motivos, porque la Criptología está rígidamente regulada desde hace mucho tiempo, sus leyes tienen múltiples consecuencias fuera de EE.UU. y es un país en el que existen varias patentes sobre software de algoritmos de cifrado que no existen en otros países.

Esther Dyson en su obra *"Release 2.0"* [76] recoge que el gobierno de Estados Unidos está preocupado por la seguridad de la información pero, en su opinión, está tomando el camino equivocado. Su postura se centra ahora en relentizar el desarrollo y el uso del cifrado, pese a que informes de diversas organizaciones científicas y de asesoramiento recomiendan lo contrario. Ha impuesto tales restricciones a la exportación de tecnología de cifrado que los productores han optado por no desarrollarla, al ser muy complicado crear versiones de cada producto para consumo interior y otra para el extranjero. E igualmente quiere convertir la gestión de claves duplicadas en una actividad regulada.

Los gobiernos ruso y francés también están preocupados por el uso generalizado del cifrado de datos y tratan de controlarlo mediante restricciones que no solo ponen controles a la exportaciones, sino que afectan directamente el uso. La Unión Europea está elaborando una política.

La mayor parte de los gobiernos de los demás países ni siquiera han tratado el asunto todavía.

El principal argumento gubernamental contra el cifrado es que esta técnica dificultad enormente la labor de las fuerzas de seguridad a la hora de detectar y perseguir a los delincuentes.

Para Dyson, el uso generalizado de la tecnología de cifrado ayudaría a prevenir los actos delictivos, siempre y cuando se dotase a los individuos, a las empresas y a los gobiernos de los medios necesarios para protegerse a sí mismos.

Prohibir o dificultar el cifrado hará que sólo los que operan al margen de la ley lo utilicen.

Los gobiernos deberían permitir e incluso fomentar el desarrollo y el uso de una potente tecnología de cifrado de datos.

El cifrado es una de las pocas herramientas de la tecnología moderna que es enteramente defensiva: protege la información y la intimidad y proporciona el refuerzo necesario para el comercio electrónico seguro, la confidencialidad, la integridad de las comunicaciones y la intimidad de los individuos, además de las comunicaciones estatales.[77]

4.3.2.1.- Normas Internacionales sobre protección de la información diplomática y cifra.

Los Convenios de Viena sobre relaciones diplomáticas y consulares ratificados por España el 21 de noviembre de 1.967 y 3 de febrero de 1.970 respectivamente, la Convención aprobada por la Asamblea General

de Naciones Unidas sobre diplomacia a través de Misiones especiales a la que se adhirió España el 3 de febrero de 1.970, y el Convenio de Viena sobre la representación de los Estados en sus relaciones con las organizaciones internacionales de carácter universal, recogen de forma expresa la protección efectiva de las comunicaciones para fines oficiales permitiendo la utilización de los "mensajes en clave o en cifra" y la valija diplomática, en sus artículos, 27, 35, 28 y 27 respectivamente.

Todos ellos en términos similares al artículo 27 del Convenio de Viena sobre Relaciones Diplomáticas como ya se ha indicado en este Capítulo.

Lo que viene a suponer el reconocimiento internacional de un ámbito de confidencialidad de la información diplomática así como del uso de mecanismos para su protección efectiva.

4.3.2.1.1.- INICIATIVA NORTEAMERICANA. "CLIPPER CHIP".

La complejidad de la aplicación de la criptología en una moderna sociedad democrática, ha llevado a la Administración de EE.UU. al anuncio de una iniciativa para mejorar la seguridad de las comunicaciones telefónicas en garantía de la privacidad del individuo y de los secretos comerciales e industriales que, a la vez, satisfaga las exigencias del Derecho.

El 16 de abril de 1.993, la Secretaría de Prensa de la Casa Blanca efectúa un comunicado dando a conocer la iniciativa.

Producto de la cooperación entre el sector privado y el mundo del derecho y tras la consulta a industrias afectas, el Congreso y los grupos que propugnan los derechos de la privacidad como alternativa política; la Administración norteamericana obtuvo un microcircuito denominado "Clipper chip" que incorpora una tecnología de cifrado con un algoritmo más potente que el utilizado, en muchos casos, para usos comerciales y, a la vez, esta tecnología permite la intervención de conversaciones con garantías legales.

Cada equipo contiene un chip con dos únicas claves que, al fabricarse, son depositadas, por separado, (Key Escrow System - KES) en dos bases de datos controladas por la Fiscalía General.

Estas dos claves son necesarias para que las agencias gubernamentales autorizadas puedan descifrar el mensaje.

La iniciativa norteamericana ofrece, a través de un procedimiento elaborado, la configuración del perfil de un sistema de cifra básico, apto para su implantación masiva para usos individuales y comerciales, pero no exento de críticas y, obviamente, totalmente al margen de las exigencias de una cifra estratégica para usos gubernamentales.

En febrero de 1.994, el gobierno de los Estados Unidos anunció la adopción de la tecnología que constituye el Escrowed Encryption Standard (EES), como estándar voluntario para las comunicaciones telefónicas sensibles pero no clasificadas, incluyendo voz, fax y datos.

La iniciativa norteamericana del "Clipper chip", en estos momentos, parece ser que está abandonada, lo cual no quiere decir que el gobierno de los EE.UU. haya renunciado a otras futuras iniciativas de tipo key-scrow.

Estas iniciativas, las europeas y las de países fuera de estas zonas, indican que la legislación sobre criptografía seguirá sometida a cambios.

4.3.2.1.2.- INICIATIVAS EUROPEAS.

En Europa, tras diversas iniciativas, como la Recomendación del Consejo en relación con las directrices que regulan la Protección de la Privacidad y el Flujo Transfronterizo de Datos Personales de 23 de septiembre de 1.980, Recomendación del Consejo 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 Acuerdo de Wassenaar sobre Controles de Exportación para Armamento Convencional y Productos y Tecnologías de doble Uso acordado el 13 de julio de 1.996, la Decisión y la Regulación del Consejo de la Unión Europea de julio de 1.995 sobre la exportación de productos de doble uso, la situación sigue siendo de confusión.

En el "Green Book on the Security of Information Systems", se planteaba la necesidad de establecer servicios de confidencialidad, sin embargo en algunos casos se declara la preocupación por el crecimiento de la actividad académica y comercial de la Criptología, por cuanto puede suponer para la limitación de las capacidades gubernamentales en la vigilancia y cumplimiento de la Ley.[78]

Los europeos aceptan el control gubernamental del secreto de las comunicaciones dentro del Estado de Derecho, pero con garantías y controles de eficacia probada.

La posición de los distintos países miembros de la Unión Europea no es unánime respecto al uso civil de la Criptología.

En Europa, por lo que se refiere al derecho de extender la protección criptológica de las comunicaciones a los ciudadanos, se está planteando la posibilidad de establecer un sistema público de licencias o certificaciones sobre el que construir circuitos de comunicaciones seguros, siempre que:

- *Tenga carácter universal.*
- *Sea voluntario.*
- *Exista garantía del secreto de las comunicaciones.*
- *Sea de alta calidad.*
- *Contemple la posibilidad de acceso legal cuando lo establezca la ley o lo determine libremente el ciudadano.*

En los casos de utilización de criptosistemas de claves depositadas, se opta porque sean varias las agencias depositarias y que para la recuperación de las claves se necesite la cooperación de un subconjunto del total de las agencias depositarias.

En todo caso, el futuro de los sistemas de protección criptológica de información privada y comercial parece que se orienta hacia los sistemas de claves depositadas o de recuperación de claves.

Proponer como estándar un único método de protección criptológica, además de conculcar la libertad de elección por parte del ciudadano, limitaría considerablemente la confianza en el uso de la criptología para fines privados y comerciales.

Tanto en los sistemas de claves depositadas como de recuperación de claves, y teniendo en cuenta que la aplicación comercial requiere una implantación internacional; no se ha de concentrar el control en un sólo gobierno y se ha de ir a una pluralidad de Estados depositarios que, a través de subconjuntos del total, formados por sus respectivas agencias, tendrían el control del depósito o la recuperación.

La Directiva 97/66/CE del Parlamento Europeo y el Consejo de la Unión Europea de 15 de diciembre de 1.997, da un paso más y aborda el tratamiento de los datos personales y la protección de la intimidad en el sector de las telecomunicaciones, establece una armonización de las disposi-

ciones de los Estados miembros, fijando los plazos para la puesta en vigor de las disposiciones legales correspondientes.

4.3.2.1.3.- RECOMENDACIONES DE LA O.C.D.E.

La Organización para la Cooperación y el Desarrollo Económico preocupada por la importancia que tiene para el desarrollo económico y comercial mundial las modernas redes de información y comunicaciones, así como los efectos derivados de una globalización de las comunicaciones, y la necesidad de que estas sean seguras y generen confianza, viene teniendo una serie de iniciativas sobre la protección criptológica, considerando que su aplicación, es la forma segura de generar seguridad y confianza.

a) Recomendación del Consejo de la O.C.D.E. de 26 de noviembre de 1.992.

El 26 de noviembre de 1.992, el Consejo de la Organización para la Cooperación y el Desarrollo Económico, elaboró una recomendaciones sobre las líneas directrices para la seguridad de los sistemas de información, dirigidas a los sectores públicos y privados y aplicables a todos los sistemas de información.

Las recomendaciones tienen por finalidad, sensibilizar sobre los riesgos que amenazan a los sistemas de información; crear un marco general de ayuda a los responsables de implantar para garantizar la seguridad de los sistemas de información; promover la cooperación entre sectores público y privado; suscitar confianza en la utilización de los sistemas de información;

facilitar la utilización de sistemas de información en el plano nacional e internacional y, promover la cooperación internacional, todo ello con el objeto de proteger los intereses de los que utilizan sistemas de información frente a la falta de disponibilidad, confidencialidad e integridad.

A tal efecto, las recomendaciones contienen nueve principios: Responsabilidad, sensibilización, ética, pluridisciplinariedad, proporcionalidad, integración, oportunidad, reevaluación y democracia. Y, basado en estos principios, instan al establecimiento de medidas prácticas, procedimientos, instituciones de naturaleza jurídica, administrativa o de autorregulación, para garantizar la seguridad de los sistemas de información.

b) Foro gobierno-sector privado sobre una política mundial de cifrado.

En marzo de 1.996, la O.C.D.E. organizó en París el "Foro gobierno-sector privado sobre una política mundial de cifrado" como grupo de expertos sobre la seguridad, la vida privada y la protección de la propiedad intelectual en la infraestructura mundial de la información.

a) El sector privado fijó sus posiciones en los siguientes aspectos:

1.- Las empresas necesitan de la Criptología.

2.- Las empresas reconocen las legítimas necesidades de los Estados para, en su caso, poder descifrar la información civil y comercial protegida criptológicamente.

3.- Las empresas necesitan disponer de libertad de elección de algoritmos, de sistemas de gestión de claves, arbitrajes técnicos y económicos.

4.- Las empresas consideran de especial importancia la consideración de los aspectos jurídicos de documentos y firmas digitales, así como la determinación de su valor probatorio.

5.- Las empresas consideran que, de forma conjunta con los gobiernos, se debe elaborar una política mundial de cifrado, en el marco de un plan internacional.

6.- Las empresas basan sus posiciones sobre la Criptología en la confianza, la responsabilidad y la facilidad de gestión.

7.- En el aspecto jurídico, las empresas desean que se fijen a los gobiernos, los límites para el acceso a la información protegida criptológicamente, en general, los aspectos jurídicos de la información electrónica y las cuestiones de responsabilidad.

b) El sector público resumió sus puntos de vista de la siguiente forma:

1.- Existen diferencias de posiciones y puntos de vista, pero también, aspectos comunes, entre los distintos gobiernos nacionales y entre estos y el sector privado.

2.- En los debates sobre política de cifrado existe preocupación por la terminología, el respeto a las leyes, la responsabilidad y la remisión de claves separadas.

3.- Existe una prioridad absoluta de un consenso mundial -con múltiples soluciones- y la confianza.

4.- Subrayan el carácter emocional del debate sobre la política criptológica en la que interviene aspectos de la intimidad, la intervención de comunicaciones, almacenamiento de datos e información, y la soberanía nacional.

5.- Consideran cuestiones esenciales: estructuras internacionales, cuestiones económicas, longitud de claves, políticas de exportación, confianza, control de la utilización de la Criptología, y planes nacionales de criptología.

6.- Los estados participantes tienen un sentimiento de urgencia sobre las incertidumbres de una política de cifrado, que debe desarrollar un conjunto de reglas lo más rápidamente posible.

7.- Consideran que se ha alcanzado una etapa crítica en la tecnología, en la voluntad política y en las necesidades de las empresas, que crean unas condiciones que permiten impulsar la búsqueda de soluciones.

8.- Que una política criptológica, para ser útil, debe ser internacional o planetaria, e inspirada en los principios democráticos, libre funcionamiento de los mercados. Que ha de encontrarse un equilibrio entre la

protección de la privacidad, la integridad de las personas, la protección de los derechos y libertades, los imperativos comerciales, el respeto a la ley y a la seguridad nacional.

c) Recomendaciones del Consejo de la O.C.D.E. de 27 de marzo de 1.997, sobre las directrices de política criptográfica.

El Comité para la Política de la Información, Comunicaciones e Informática de la O.C.D.E. considera que las infraestructuras nacionales y mundial de la información se están desarrollando rápidamente para proporcionar una red inconsútil de comunicaciones mundial y de acceso a la información, que es muy probable que tenga gran repercusión sobre el desarrollo económico y comercial mundial.

Los usuarios de las tecnologías de la información necesitan confiar en la seguridad de las infraestructuras de información y comunicaciones, redes y sistemas, tanto en la confidencialidad, integridad y disponibilidad de los datos que sobre ellas circulan como en poder probar su origen y destino.

De igual modo reconoce que la criptografía es una herramienta eficaz para la utilización segura de la tecnología de la información en todas sus aplicaciones, pero que la utilización de métodos criptográficos puede afectar negativamente, ya que la protección puede estar realizada de forma inadecuada, lo que generaría desconfianza. Y que la calidad de la protección

criptográfica conseguida no depende solamente de los medios técnicos, sino también de buenos procedimientos operativos, de organización y gestión.

El ICCP reconoce que los gobiernos tienen responsabilidades en relación con la criptografía entre las que se incluye la protección de la privacidad, la promoción del comercio, el mantenimiento de la seguridad pública, aplicación de las leyes y la protección de la seguridad nacional. Pero, también, evitar que la criptografía tenga resultados cuando se aplique para actividades ilegales, por lo que ha de desarrollar una política equilibrada.

Asimismo, por el carácter global de las redes de comunicación e información, las políticas nacionales precisan una coordinación internacional, sin perjuicio de los derechos soberanos de los gobiernos nacionales.

4.3.2.2.- NORMAS NACIONALES.

El punto de partida de la normativa nacional radica en los artículos 18 y 20 de la C.E. que recogen el tratamiento jurídico constitucional de la información privada y pública respectivamente, y 55.2 del mismo cuerpo legal, referido a la suspensión de derechos y libertades.

Estos bloques de información pública y privada responden a principios distintos, mientras que en las comunicaciones privadas, la regla general es el secreto y la excepción la transparencia; en las comunicaciones públicas, la regla general es la transparencia y la excepción el secreto, lo que nos llevaría a deducir unas necesidades de protección criptológica

sistemáticas de las comunicaciones privadas y, solo de forma excepcional de las públicas, aunque con niveles distintos, de forma que permita el normal funcionamiento de la sociedad y del Estado, y no impida el ejercicio de derechos prevalentes.

El secreto de las comunicaciones con independencia que tenga su origen en la excepción aplicada a las comunicaciones públicas o sea consecuencia del principio general aplicable a las comunicaciones privadas, afecta, de modo directo, a las libertades y a los derechos fundamentales y, consecuentemente, vincula a todos los poderes públicos.

Por imperativo del artículo 9.2 de la Constitución, *"corresponde a los poderes públicos promover las condiciones para que la libertad y la igualdad del individuo y de los grupos en que se integra sean reales y efectivas; remover los obstáculos que impidan o dificulten su plenitud..."*.

Resulta difícil imaginar cómo se podría fundar un recurso de inconstitucionalidad por infracción de esta norma, o como podría obligarse a las Cortes o a la Administración a hacer algo concreto utilizándolo como título jurídico. En su defensa parlamentaria se dijo que suponía la implantación de la democracia real. [79]

1.- La Ley 9/1.968, de 5 de abril, sobre Secretos Oficiales, modificada por la Ley 48/1.978 de 7 de octubre, establece que las personas facultadas para tener acceso a una materia clasificada quedarán obligadas a

cumplir con las medidas y prevenciones de protección que reglamentariamente se determinen (art. 11).

Los órganos con facultades de calificación atenderán *"mantenimiento y mejora de los sistemas de protección y velarán por su efectivo cumplimiento..."* (art. 12).

En su Disposición Final se determina que: *"En Reglamento único, de aplicación general a toda la Administración del Estado y a las Fuerzas Armadas, se regularán los procedimientos y medidas necesarios para la aplicación de la presente Ley y protección de las "materias clasificadas".*

2.- El Decreto 242/1.969, de 20 de febrero, del Reglamento de Secretos Oficiales, por el que se desarrolla la Ley, establece:

"Por lo menos, los documentos, información y material clasificado de secreto, estará guardado en una caja fuerte o armario-archivador a prueba de incendios y dotados de cerraduras de combinación de disco, cuyas dimensiones, peso, construcción e instalación hagan mínimas las posibilidades de robo, violación e indiscreciones.

De ser ello necesario, por el volumen total del material clasificado, podrán habilitarse salas o sótanos aprobados al efecto por la persona responsable del Servicio de Protección de Materias Clasificadas que impliquen unas condiciones, cuando menos, similares a los sistemas indicados en el apartado anterior.

Si no fuese posible disponer de las instalaciones especificadas en los párrafos anteriores, las materias clasificadas de secreto deberán estar protegidas por una guardia armada". (Artículo 13).

"Como mínimo, los documentos, información y material clasificados de reservado deberán ser almacenados en la forma especificada para los clasificados de secreto o en armarios-archivadores metálicos y equipados con barras de cierre en acero, con candado cambiable, tipo combinación, o en otras instalaciones que garanticen unas condiciones de seguridad semejantes". (Artículo 14).

"La transmisión del material secreto se llevará a cabo, preferiblemente, por medio de contacto directo de los funcionarios a quienes tal función corresponda, o por personal específicamente designado, valija diplomática, por un sistema de correos creado expresamente para este fin o por medios de transmisión en forma cifrada". (Artículo 20).

"La transmisión de material reservado se llevará a cabo de la misma manera que la expuesta para el secreto en el artículo anterior o por medio de los comandantes de aeronaves o navíos con categoría de oficial o correo certificado si no fuere practicable ninguno de los procedimientos anteriores, cifrándose los textos siempre que sea posible". (Artículo 21).

"Si la transmisión de material clasificado se llevase a cabo dentro del órgano de origen, se regirá por las normas que elabore el Servicio de Protección de Materias Clasificadas correspondiente, las cuales deberán garantizar un grado de seguridad equivalente al indicado para transmisión fuera del mismo". (Artículo 22).

Según el Reglamento, está prohibida la transmisión de información por teléfono , salvo que cuenten con la protección adecuada y, expresamente establece:

"La información clasificada no podrá ser transmitida o revelada por medio del teléfono, excepto en los casos en que así se disponga, expresamente, por medio de determinados circuitos tanto civiles como militares". (Articulo 24).

Estos circuitos se han de entender como adecuadamente protegidos, que actualmente implicarían protección con sistemas para el cifrado de la voz.

Sin perjuicio de lo dispuesto en el Reglamento de Secretos Oficiales y teniendo en cuenta las características de las Fuerzas Armadas, éstas podrán elaborar normas específicas de régimen interior.

De igual modo, y en atención a las peculiaridades del servicio diplomático y a las circunstancias en que éste desarrolla sus funciones fuera del territorio nacional, el Ministerio de Asuntos Exteriores podrá elaborar normas específicas de régimen interior para sus oficinas en el extranjero, sin perjuicio de las normas de carácter general contenidas en el Reglamento. (Disposición Adicional).

En el Reglamento se hace una referencia muy genérica a la protección criptológica, sin descender a detalles que deja para las normas específica de régimen interior y a desarrollos posteriores realizados por los Departamentos interesados, en forma de circulares, órdenes comunicadas, instrucciones, etc.

La mayor parte del Reglamento se ocupa de las medidas físicas para proteger los secretos oficiales, esta es una de las razones por la que esté tan en desuso, si se tiene en cuenta el cambio radical producido en el procesamiento, almacenamiento y transmisión de información por aplicación de las Nuevas Tecnologías de la Información y de las Comunicaciones.

El Reglamento de Secretos Oficiales, que data de 1.969, no ha sido actualizado. Estamos en presencia de una norma obsoleta en gran parte de su contenido.

Hoy, cuando los soportes informáticos permiten que cantidades ingentes de material quepan en pequeños espacios, parece poco útil el comentario sobre un texto tan arcaico como el Reglamento de Secretos

Oficiales y no se puede olvidar la legislación sobre informática.

La preocupación ha de centrarse en medidas de seguridad acorde con los avances tecnológicos actuales y previsibles, contemplando la realidad de las telecomunicaciones y la informática, tanto en el proceso y almacenamiento de datos como en su transmisión, donde adquiere una singular importancia las medidas de protección de naturaleza criptológica.

Pero la eficacia de la criptología en la protección de información, la necesidad de su uso, los distintos niveles de exigencia y variedad; así como los efectos que puede producir, tanto su aplicación como su no aplicación o, incluso, su aplicación inadecuada; los distintos derechos que protege y las consecuencias jurídicas y prácticas de todo ello, pone de relieve una importante laguna en el ordenamiento en materia de medidas de protección, adecuadas a las exigencias físicas, lógicas, tecnológicas, jurídicas y políticas de la sociedad actual, que aconsejan una revisión normativa.

El texto conocido del Proyecto de Ley de Secretos Oficiales en la Disposición final Primera, establece que, el Gobierno, en el plazo de un año a partir de la promulgación de la presente Ley, dictará el Reglamento General para el desarrollo y aplicación de la misma.

Dicho Reglamento regulará las siguientes cuestiones:

"a) El miembro del gobierno que sea designado como Autoridad Nacional de Seguridad y sus relaciones con los diferentes servicios del Estado con atribuciones y competencias en materia de secretos oficiales.

b) Las normas generales sobre protección, control, anotación e identificación de los documentos y medios materiales clasificados.

c) Los procedimientos de comunicación en materia de secretos oficiales.

d) Las normas relativas al archivo, registro, traslado, revisión y destrucción de los documentos y medios materiales clasificados".

3.- El Real Decreto 1.883/1.996, de 2 de agosto por el que se regula la estructura del Ministerio de Defensa, en su artículo 5 señala que al Centro Superior de Información de la Defensa le corresponde *"coordinar la acción de los distintos organismos que utilicen medios o procedimientos de cifra, garantizar la seguridad criptográfica, promover la adquisición coordinada de material y formar al personal especialista"*

4.- Ley 31/1.987, de 18 de diciembre de Ordenación de las Telecomunicaciones,(hoy derogada excepto en sus artículos 25, 26, 36 apartado 2, y su disposición adicional sexta),[80] recogía el secreto de las comunicaciones en sus artículos 2.2, 16.1,f), y 24.7, pero lo regula por remisión al artículo 18.3 de la Constitución y no llega más lejos de configurarlo como ámbito de confidencialidad que se debe proteger, sin especificar como hacerlo.

5.- Ley 11/1.998, de 24 de abril, General de Telecomunicaciones, publicado en el Boletín Oficial del Estado núm. 99, de 25 de abril de 1.998,[81] supone un salto cualitativo por lo que se refiere a la seguridad de las comunicaciones. En su Exposición de Motivos indica que se introducen *"...disposiciones relativas al secreto de las comunicaciones, la protección de los datos personales y el cifrado, dirigidas, todas ellas, a garantizar*

técnicamente los derechos fundamentales constitucionalmente reconocidos".

En el artículo 3 de la Ley, en su apartado f) señala entre los objetivos de la Ley *"Defender los intereses de los usuario, asegurar su derecho al acceso a los servicios de telecomunicaciones en adecuadas condiciones de calidad, salvaguardar, en la prestación de estos, la vigencia de los imperativos constitucionales, en particular el de los derechos al honor, a la intimidad y al secreto en las comunicaciones y el de la protección a la juventud y a la infancia. A estos efectos, podrán imponerse obligaciones a los prestadores de los servicios para garantía de estos derechos."*

En el artículo 40 de la Ley referido a servicios obligatorios de telecomunicaciones, señala que el Gobierno, previo informe de la Comisión del Mercado de las Telecomunicaciones y mediante norma reglamentaria,, podrá declarar incluidos determinados servicios como servicios obligatorios, entre ellos, en el apartado 2. a) se refiere a *"los servicios de télex, los telegráficos, y aquellos otros de características similares que comporten acreditación de la fehaciencia del contenido del mensaje remitido o de su remisión o recepción, ..."*

De especial interés para esta es el Capítulo III referido al secreto de las comunicaciones y protección de los datos personales y derechos y obligaciones de carácter público vinculado con las redes y servicios de telecomunicaciones.

En su artículo 49 se establece que los operadores de telecomunicaciones y los proveedores de servicios, en la prestación de servicios o en la explotación de redes de telecomunicaciones, deberán garantizar el secreto de las comunicaciones, de conformidad con el artículo 18.3 de la Constitución, y el cumplimiento, en su caso, de lo establecido en el artículo 55.2 de la misma y en el artículo 579 de la Ley de Enjuiciamiento Criminal. Para ello, deberán adoptar las medidas técnicas que se exijan por la normativa vigente en cada momento, en función de las características de la infraestructura utilizada.

Asímismo deberán garantizar, en la prestación de servicios de telecomunicaciones, la protección de los datos personales, conforme a lo dispuesto en la Ley Orgánica 5/1.992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter personal, en las normas dictadas en su desarrollo y en las normas reglamentarias de carácter técnico cuya aprobación exija la normativa comunitaria en materia de protección de los datos personales. (Artículo 50).

El Proyecto de Ley aborda de forma expresa, por primera vez, el cifrado de información en las redes y servicios de telecomunicaciones al decir en su artículo 52 que *"1.- Cualquier tipo de información que se transmita por redes de telecomunicaciones podrá ser protegida mediante procedimientos de cifrado. Podrán establecerse condiciones para los procedimientos de cifrado en las normas de desarrollo de esta Ley.*

2.- El cifrado es un instrumento de seguridad de la información. Entre sus condiciones de uso, cuando se utilice para proteger la confidencialidad de la información, se podrá imponer la obligación de notificar bien a un órgano de la Administración General del Estado o a un organismo público, los algoritmos o cualquier procedimiento de cifrado utilizado a efectos de su control de acuerdo con la normativa vigente. Esta obligación afectará a los fabricantes que incorporen el cifrado a sus equipos o aparatos, a los operadores que lo incluyan en las redes o dentro de los servicios que ofrezcan y, en su caso, a los usuarios que lo emplean.

3.- Los operadores de redes o servicios de telecomunicaciones que utilicen cualquier procedimiento de cifrado deberán facilitar a la Administración General del Estado, sin coste alguno para ésta y a efectos de la oportuna inspección, los aparatos descodificadores que empleen, en los términos que se establezcan reglamentariamente".

El incumplimiento grave o reiterado de estas obligaciones se considerarán infracciones muy graves.

No obstante lo dispuesto en esta Ley, una adecuada regulación de la protección criptológica de la información y las comunicaciones dependerá de la forma en que se elabore su desarrollo reglamentario.

6.- Ley Orgánica 5/1.992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de carácter personal.

Por lo que se refiere a la regulación del tratamiento automatizado de los datos de carácter personal, la regulación de su protección ha ido experimentado una evolución orientada en una línea de mayor concreción.

Tanto el Convenio 108 del Consejo de Europa, de 28 de enero de 1.981, de Protección de las personas en relación con el tratamiento automatizado de datos de carácter personal, como la Ley Orgánica 5/1.992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de carácter personal, y la Directiva 95/46/CE del Parlamento Europeo y del Consejo , de 24 de octubre de 1.995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, se refieren a las medidas de seguridad que deben cumplir los ficheros automatizados que contengan datos de carácter personal.

Las referencias a las medidas de seguridad en los textos indicados ha ido experimentando una evolución. En el Convenio 108 la obligación es tomar medidas de seguridad apropiadas, sin distinción alguna en cuanto a las medidas. La LORTAD impone la adopción de medidas técnicas y organizativas necesarias que garanticen la seguridad de los datos de carácter personal a un nivel de seguridad adecuado, reforzando las medidas de seguridad cuando se trate de datos especialmente protegidos y se remite a un posterior desarrollo reglamentario.

La Ley Orgánica número 5/1.992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de carácter personal, comúnmente conocida como LORTAD, viene a dar respuesta al mandato constitucional del artículo 18.4 de la Constitución, dirigido a la limitación del uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el legítimo ejercicio de sus derechos.

La Ley, limitadora del uso de la informática, en lo concerniente al ámbito de los "ficheros de datos" de carácter personal, considera que su existencia y utilización supone un riesgo para los derechos de la personalidad.

Trata de prevenir violaciones de la privacidad, derivadas del tratamiento de datos considerados como una globalidad de procesos informáticos.

La adopción de las medidas de seguridad necesarias, dentro del marco reglamentario respecto a las condiciones de integridad y de seguridad corresponden al responsable del fichero.

La Criptología tiene su aplicación en hacer efectivo el mandato legal, dentro de las medidas de seguridad y en unión de otros procedimientos.

La Ley recoge una serie de principios de protección de datos, pero no recoge suficientemente los mecanismos para una protección efecti-

va. No contempla la seguridad en la transmisión de datos, con los problemas que implican las comunicaciones y su vulnerabilidad.

Según el artículo 9 de la LORTAD, referido a la seguridad de los datos *" El responsable del fichero deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural".*

El alcance de la medida llega a no permitir el registro de datos de carácter personal en ficheros automatizados que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas. Y se remite a un desarrollo reglamentario donde establecerán los requisitos y condiciones que deban reunir los ficheros automatizados y las personas que intervengan en el tratamiento automatizado de los datos a que se refiere el artículo 7 de la ley.

En un futuro Reglamento se deberá regular los distintos niveles de protección y las medidas específicas de seguridad, entre ellas, fundamentalmente, las de naturaleza criptológica.

El desarrollo reglamentario de la Ley Orgánica, llevado a efecto por Real Decreto 1332/1.994, de 20 de junio, deja sin regular lo referido a

las medidas de seguridad con las consecuencias que ello comporta, por lo que el desarrollo reglamentario de la Ley, en este sentido, está aún pendiente de realizar.

La Directiva 95/46 del Parlamento Europeo va más lejos y no basa el reforzamiento de las medidas de seguridad solamente en la naturaleza especialmente protegida de los datos personales, sino que también tiene en cuenta su transmisión dentro de una red. En su artículo 17, referido a la seguridad del tratamiento, dispone que *"1.- Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales.*

Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y el coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse.

Los Estados miembros establecerán que el responsable del tratamiento, en caso de tratamiento por cuenta del mismo, deberá elegir un encargado del tratamiento que reúna garantías suficientes en relación con

las medidas de seguridad técnica y de organización de los tratamientos que deban efectuarse, y se asegure de que se cumplen dichas medidas...".

Esta Directiva requiere su transposición al ordenamiento jurídico español, lo que es recogido, en parte, por el Proyecto de Ley General de Telecomunicaciones citado, cuando se refiere a los datos de carácter personal.

La Comunidad, se ha adoptado la Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1.997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones (DOCE L 24 de 30/01/98).

Por cuanto se refiere a la seguridad, el artículo 4 establece que:

"1.- El proveedor de un servicio público de telecomunicación deberá adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios, de ser necesario en colaboración con el proveedor de la red pública de telecomunicación por lo que respecta a la seguridad de la red. Considerando las técnicas más avanzadas y el coste de su aplicación, dichas medidas garantizarán un nivel de seguridad adecuado para el riesgo existente.

2.- En caso de que exista un riesgo concreto de violación de la seguridad de la red, el proveedor de un servicio público de telecomunicación deberá informar a los abonados sobre dicho riesgo y sobre las posibles soluciones, incluidos los costes necesarios".

En todo caso, los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones y derechos, cuando dichas limitaciones constituyan una medida necesaria para proteger la seguridad nacional, la defensa, la seguridad pública, la prevención, la investigación, la detección y la persecución de delitos o la utilización no autorizada del sistema de telecomunicación. La Directiva establece plazos para llevara cabo las medidas legales necesarias para su cumplimiento.

7.- Real Decreto 263/1.996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado, aborda el desarrollo del artículo 45 de la Ley 30/1.992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, piedra angular del proceso de incorporación de medios y técnicas automatizadas en la actuación administrativa.

Cuando se utilicen soportes, medios y aplicaciones electrónicas, informáticas y telemáticas en cualquier actuación administrativa, *"...se adoptarán las medidas técnicas y de organización necesarias que aseguren la autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información. Dichas medidas de seguridad deberán tener en cuenta el estado de la tecnología y ser proporcionadas a la naturaleza de los datos y de los tratamientos y a los riesgos a los que estén expuestos". (Art. 4.2).*

La transmisión o recepción de comunicaciones entre órganos o entidades del ámbito de la administración general del Estado o entre estos y cualquier persona física o jurídica, se podrán realizar a través de soportes, medios y aplicaciones informáticas, electrónicas y telemáticas, pero siempre que se cumplan, entre otros, los siguientes requisitos: *"c) La existencia de medidas de seguridad tendentes a evitar la interceptación y alteración de las comunicaciones, así como a los accesos no autorizados" (Art. 7).*

8.- La Ley 66/1.997, de 30 de diciembre de Medidas Fiscales, Administrativas y de Orden Social, en su artículo 70, referido a la "Prestación de Servicios de Seguridad por la Fábrica Nacional de Moneda y Timbre para las comunicaciones a través de técnicas y medios electrónicos, informáticos y telemáticos", en su apartado Uno dispone que *"...se faculta a la Fábrica Nacional de Moneda y Timbre (FNMT) para la prestación de los servicios técnicos y administrativos necesarios para garantizar la seguridad, validez y eficacia de la emisión y recepción de comunicaciones y documentos a través de técnicas y medios electrónicos, informáticos y telemáticos (EIT) en las relaciones que se produzcan entre:*

a) Los órganos de la administración General del Estado entre sí o con los organismos públicos vinculados o dependientes de aquélla, así como las de estos organismos entre sí.

b) Las personas físicas y jurídicas con la Administración General del Estado (AGE) y los Organismos Públicos vinculados o dependientes de ella."

En su apartado Dos se habilita en términos similares a la FNMT para prestar estos servicios a las Comunidades Autónomas, Entidades Locales y las Entidades de Derechos Público vinculadas o dependientes de ellas, siempre que se hayan formalizado los acuerdos o convenios procedentes.

Estos servicios se prestarán de conformidad con los requisitos técnicos que determine el Consejo Superior de Informática (apartado Cuatro).

9.- Circular 5/1.996, de 29 de marzo del Banco de España sobre criptografía y seguridad para transmisiones entre centros de proceso (Norma SNCE-002).

El Banco de España ha dispuesto que la criptografía y seguridad para la protección de la información en el Sistema Nacional de Compensación Electrónica se regirá por lo establecido en esta Circular, que estructurada en cuatro títulos proporciona una regulación suficientemente completa de las comunicaciones cifradas en el ámbito al que se refiere.

El Título II referido a los aspectos sustantivos de la Norma SNCE-002, comprende cuatro normas. La norma tercera referida a medios

técnicos, la cuarta regula los servicios de criptografía, la quinta las técnicas de criptografía y la sexta responsables personales.

10.- En España, la Ley Orgánica 3/1.992, de 30 de abril, de Contrabando-exportación, dice que se considerará material de doble uso, los productos y tecnologías de habitual utilización civil que puedan ser aplicados en algún uso militar como instrumento de fuerza, información o protección en conflictos armados, así como los destinados a la producción, ensayo o utilización de aquéllos y que se encuentren incluidos en la relación que, a estos efectos, apruebe el Gobierno por Real Decreto.

11.- Por Real Decreto nº 824/1.993, de 28 de mayo, se regula el Reglamento de comercio Exterior de Material de Defensa y de Material de Doble Uso.

En el Anexo II, Categoría 5, se recoge el material de doble uso referido a "Seguridad de la Información", e incluye equipos, conjuntos y componentes diseñados o modificados para utilizar criptografía, empleando técnicas digitales destinadas a garantizar la seguridad de la información o diseñados o modificados para realizar funciones criptoanalíticas.

También se refiere a estos equipos cuando utilizan técnicas analógicas, exceptuando los que utilicen técnicas de mezcla de bandas fijas para 8 bandas como máximo y en los que los cambios de transposición no se efectúen más de una vez cada segundo, o más de ocho bandas y en los que los cambios de transposición no se efectúen más de una vez cada diez

segundos y equipos de inversiones de frecuencia fija en los que los cambios de transposición no se efectúen más de una vez cada segundo.

El Diario Oficial de las Comunidades Europeas L 278 de 30 de octubre de 1.996, publica la Decisión del consejo de 22 de octubre de 1.996 por la que se modifica la Decisión 94/942/PESC relativa a la acción común adoptada por el Consejo sobre la base del artículo J.3 del Tratado de la Unión Europea referente al control de las exportaciones de productos de doble uso.

En la Categoría 5, Telecomunicaciones y "seguridad de la información", considera tecnología de doble uso los sistemas, equipos, conjuntos electrónicos, módulos o circuitos integrados destinados a la "seguridad de la información", así como otros componentes diseñados o modificados para utilizar la criptografía empleando técnicas digitales destinadas a garantizar la seguridad de la información, para realizar funciones criptoanalíticas, o diseñados o modificados para utilizar criptografía empleando técnicas analógicas destinadas a garantizar la seguridad de la información.

4.4.- INTERCEPTACIÓN Y CRIPTOANÁLISIS.

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 al secreto, lo que supone obligación de garantizar de forma eficaz la seguridad de las comunicaciones

y, consiguientemente su secreto, y, a la vez, estar en condiciones de poder, -también de forma eficaz- llevar a término el cumplimiento del mandato judicial, cuando a través de la oportuna resolución motivada, ordene la intervención de las comunicaciones, lo que exigiría no solo aprehender el soporte del mensaje que, en el caso que estuviese cifrado, de poco serviría, sino de poner a disposición de la justicia el contenido de esa comunicación, lo que, en el supuesto que comentamos, exigiría su descifrado o descriptación, según los casos.

De forma que el alcance del concepto de intervención de las comunicaciones, cuando estas son cifradas, rebasa la mera intervención e incorpora al proceso exigencias de naturaleza criptológica que hagan posible el descifrado o la descriptación de las mismas, en su caso. Lo que añade una complejidad aún mayor tanto organizativa como técnica, y obviamente, normativa.

El derecho al secreto de las comunicaciones, como todo derecho, no es absoluto, aquí la protección constitucional se construye sobre un delicado equilibrio entre el interés del individuo y el interés estatal en perseguir determinados objetivos que puedan hacer necesaria la intromisión en la esfera privada del individuo y hacer que decaiga el derecho al secreto de las comunicaciones.

Los conflictos que pueden surgir son mayores si se tienen en cuenta los riesgos para los derechos individuales que comporta una

intervención de comunicaciones que afecta no sólo a quién es objeto directo del control, sino también a las personas que entren en contacto con él a través del medio observado.

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

Pero la complejidad tecnológica del momento actual y del futuro previsible, demanda, para que ese control judicial sea eficaz, un auxilio de elevado componente tecnológico, organizativo y criptológico.

La interceptación de comunicaciones electrónicas es un tema de actualidad mundial.

1.- Estados Unidos.

El FBI -la mítica policía norteamericana- pidió en 1.992 al Gobierno de los EE.UU. "una ley que permita nuevas formas de intervención en las comunicaciones".

Los cambios tecnológicos "hacen cada vez más difícil la intervención de los gobiernos a través de sus respectivas policías para interceptar legalmente las comunicaciones por razones de seguridad nacional o para luchar contra el delito".

Las pretensiones del FBI eran introducir una enmienda a la Ley de Comunicaciones de 1.934, que permite la intervención de comunicaciones por orden judicial de forma que "se obligue a las empresas fabricantes y proveedores de determinados servicios de comunicaciones a colaborar con

las fuerzas de seguridad, "porque éstas no consiguen penetrar en los mensajes cifrados ni en las nuevas redes digitales que permiten la transmisión codificada.[82]

El 16 de abril de 1.993, la Oficina de la Secretaria de Prensa de la Casa Blanca hace una declaración sobre la iniciativa presidencial, conocida como "clipper chip", para mejorar la seguridad y la privacidad de las comunicaciones telefónicas dejando a salvo las exigencias del Derecho , cuya materialización práctica no ha tenido el éxito esperado y ha suscitado opiniones diversas.

Mientras Al Gore, Vicepresidente de los EE.UU. señalaba que este tema es muy importante para la ley y el orden y evitar que los terroristas y los delincuentes puedan utilizar en su provecho esta tecnología, John Gage, director de la oficina científica de la empresa Sun Microsystems, Inc de California decía un rotundo "Nos negamos", "quieren que exportemos millones de ordenadores con un chip en el que sea lea 'J. Edgar Hoover en el interior' ".

Y, a la vez los Cypherpunks que quieren proporcionar a todo el mundo técnicas potentes y gratuitas de cifrado han estado discutiendo la forma de engañar a la Administración para que parezca que conoce las claves del Clipper. O el caso de John Perry, fundador de un grupo de defensa de los consumidores de informática que afirma "es el último

esfuerzo de las superpotencias para establecer control imperial sobre el ciberespacio".[83]

2.- Bélgica.

El Gobierno belga aprobó el 24 de noviembre de 1.995 una proposición de ley que autoriza la realización de escuchas telefónicas sin permiso judicial previo. En un principio, el Gobierno tenía intención de autorizar las escuchas tanto al Servicio General de Información (militar) como a la Seguridad del Estado (civil), e incluso dar cierta libertad de acción a los servicios de inteligencia de las comisarías de policía.

Finalmente se ha limitado la autorización al espionaje militar con la cautela añadida de que sólo puede escuchar las conversaciones procedentes del extranjero. Los expertos se preguntan cómo van a evitar ahora escuchar conversaciones emitidas desde el propio país cuando el sistema utilizado capta todas las radiocomunicaciones.

La actual normativa de escuchas obliga a que éstas se ciñan a un proceso judicial abierto. La policía debe recibir el permiso del juez instructor y éste haberlo obtenido antes de un tribunal. Todas las personas escuchadas deben ser informadas posteriormente de que se les ha espiado y todas las conversaciones grabadas deben ser transcritas en la lengua original de la conversación y en la del proceso judicial".[84]

3.- Alemania.

En diciembre de 1.995, en Alemania surge la polémica sobre las escuchas y la ministra de Justicia, presenta su dimisión en desacuerdo con la decisión de los militantes del FDP, partido al que pertenece, de apoyar una polémica ley para permitir las escuchas en domicilios privados sin permiso judicial en caso de sospechar que se está cometiendo un delito.[85]

En junio de 1.996, el Gobierno alemán aprobó un paquete de medidas que por primera vez permitirá a la policía intervenir los teléfonos de particulares. La vigilancia electrónica en hogares privados deberá ser sancionada por un juzgado especial conforme a los términos de la legislación que el gobierno tiene previsto presentar al Parlamento. La ley está pensada para investigar especialmente los delitos de narcotráfico, toma de rehenes, secuestros y otras actividades de delincuencia organizada (tráfico ilegal de personas, prostitución, extorsión...). Con este acuerdo concluyen años de disputas entre los democristianos y el Partido Liberal, que se resistían a lo que consideraban un atentado contra la libertad.

La ley para su implantación requiere un cambio en la Constitución.[86]

4.- Austria.

De otra parte, el gobierno austriaco prepara un proyecto de ley que permitirá las escuchas telefónicas y un control policial exhaustivo de

sospechosos en casos de blanqueo de dinero, narcotráfico, contrabando de coches y tráfico de inmigrantes ilegales.[87]

Dentro de la Constitución Española, en el artículo 55 dedicado a la suspensión de los derechos y libertades, se refiere expresamente al derecho fundamental del artículo 18.3, distinguiendo dos posibilidades de suspensión de su ejercicio. Las del apartado 1 del artículo 55, referida a la suspensión del secreto de las comunicaciones telefónicas en los casos de declaración del estado de excepción o de sitio., en desarrollo de lo cual se promulga la L.O. 4/1.981, de 1 de junio, de los estados de alarma, excepción y sitio, que, en su artículo 18 autoriza a la autoridad gubernativa, siempre que lo autorice el Congreso, para intervenir las comunicaciones, cuando sea necesario para el esclarecimiento de los hechos delictivos o el mantenimiento del orden público.

El artículo 18 de la L.O. 4/ 1.981, de 1 de junio dice:

"1. Cuando la autorización del Congreso comprenda la suspensión del art. 18.3 de la Constitución, la autoridad gubernativa podrá intervenir toda clase de comunicaciones, incluidas las postales, telegráficas y telefónicas. Dicha intervención sólo podrá ser realizada si ello resulta necesario para el esclarecimiento de los hechos presuntamente delictivos o el mantenimiento del orden público.

2. La intervención decretada será comunicada inmediatamente por escrito motivado al Juez competente".

El apartado 2 del mismo artículo 55 de la Constitución, permite la suspensión del derecho al secreto de las comunicaciones para personas determinadas en relación con las investigaciones correspondientes a la actuación de bandas armadas o elementos terroristas. En base a esta

previsión constitucional nos encontramos hoy con la L.O. 4/ 1.988, de 25 de mayo, de reforma de la Ley de Enjuiciamiento Criminal, que regula la intervención de las comunicaciones telefónicas privadas a efectos del proceso penal por delitos comunes y, en su artículo 579 establece que *"Podrá el Juez acordar la detención de la correspondencia privada, postal y telegráfica que el procesado remitiere o recibiere y su apertura y examen, si hubiera indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa.*

El juez es vigilante constitucional tanto del derecho de secreto de las comunicaciones como de su excepción.[88]

Asimismo, el Juez *" ...podrá acordar, en resolución motivada, la intervención de las comunicaciones telefónicas del procesado, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa; ... por un plazo de hasta tres meses, prorrogable por iguales períodos, la observación de las comunicaciones postales, telegráficas o telefónicas de las personas sobre las que existan indicios de responsabilidad criminal, así como de las comunicaciones de las que se sirvan para la realización de sus fines delictivos.*

En caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas o rebeldes, la medida prevista *"...podrá ordenarla el*

Ministerio del Interior o, en su defecto, el Director de la Seguridad del Estado, comunicándolo inmediatamente por escrito motivado al Juez competente, quién, también de forma motivada, revocará o confirmará tal resolución en un plazo máximo de setenta y dos horas desde que fue ordenada la observación".

Dentro del ámbito procesal penal existen especialidades normativas como son los artículo 506 a 511 y 527 de la Ley de Enjuiciamiento Criminal, relativos a la incomunicación de detenidos o presos, o en el artículo 524 de la LECr. referido a los medios de correspondencia y comunicación de presos o detenidos no incomunicados. al respecto han de tenerse en cuenta los artículo 89, 91.1 y 99 y 100 del Reglamento Penitenciario, aprobado por real Decreto 1201/1.981, de 8 de mayo, parcialmente reformado por Real Decreto 787/1.984, de 28 de marzo, en relación con la L.O. 1/1.979, de 26 de septiembre, General Penitenciaria.

Además el Código Procesal Militar (L.O. 2/1.989, de 13 de abril), en su artículo 188 dispone que los Jueces Togados militares podrán acordar, *"la intervención y, en su caso, grabación de las comunicaciones telefónicas o radiofónicas de cualquier persona, y la fotografía o filmación de sus actividades cuando hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia objeto del proceso".*

A nivel internacional, la Declaración Universal de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos de aplicación en nuestro país hacen referencia al secreto de las comunicaciones.

Especial referencia merece la Convención Europea para la salvaguardia de los Derechos Humanos y de las Libertades Fundamentales, por cuanto se refiere a la posibilidad de utilización de las medidas técnicas de intervención de comunicaciones con finalidades preventivas en base a su artículo 8 que dice:

"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".

Los criterios y requisitos procesales válidos para todos los supuestos de aplicación siguen sin una regulación completa en nuestro ordenamiento jurídico con el peligro que supone en este derecho el excesivo arbitrio judicial.

Se sabe que la intervención telefónica es legítima si la autoriza el juez pero se desconoce como puede estructurarse, eficazmente, esta excepcional medida.

La Constitución exige que para interceptar las comunicaciones sea imprescindible una resolución judicial, la Jurisprudencia añade que esta

ha de ser motivada. A partir de ahí, corresponde a la legislación ordinaria precisar los supuestos en los que es procedente conceder esta autorización.

La intervención de comunicaciones está prevista, como se ha indicado, en la Ley que regula los estados de alarma, excepción y sitio; en la Ley de Enjuiciamiento Criminal en los supuestos de causas penales, de presos o detenidos no incomunicados, y de bandas armadas o elementos terroristas; el Código Procesal Militar también referido a hechos o circunstancias objeto de proceso, pero nada se dice de la seguridad nacional, la defensa, la seguridad pública, o la prevención, por citar ejemplos muy significativos.

Con todo lo cual se viene a subrayar la "profundidad" de la laguna legal existente en materia de información y comunicaciones, que quedaría zanjada en gran medida, con la entrada en vigor de las disposiciones legales, reglamentarias y administrativas previstas en la Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1.997.

Cubriendo esta laguna y desarrollando plenamente el artículo 18.3 de la Constitución, -con todo lo que significa en cuanto a la eficacia, tanto de la garantía del secreto de las comunicaciones como de la excepcionalidad de su intervención, soportada en resolución judicial-, la investigación judicial y policial y, eventualmente, las labores de inteligencia [89] y contrainteligencia,[90] podrían ser más complejas pero sin duda se ganará en

respeto a la persona y a los derechos fundamentales y se fortalecerán las instituciones.

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

La ley 11/1.998, de 24 de abril, General de Telecomunicaciones, prevé la interceptación de las telecomunicaciones por los servicios técnicos a efectos de tareas de control para la eficaz utilización del dominio público radioeléctrico establecida en los Convenios internacionales, y siempre con pleno respeto al derecho.

La doctrina se ha planteado algunas consideraciones acerca de las autorizaciones judiciales para la intervención de comunicaciones a traves de redes informáticas. .

Maza Martín, [91] aborda la interrogante de en qué régimen y de acuerdo con qué requisitos se podría practicar en nuestro ordenamiento una intervención de las comunicaciones que circulan por Internet, en la investigación de unos hechos presuntamente constitutivos de infracción criminal.

Parte de la base de que en este caso nos encontramos ante el supuesto de una comunicación.

Ante la falta de previsiones legales expresas y partiendo de la obviedad indiscutible de que, en averiguación de posibles hechos delictivos, la autoridad judicial está plenamente facultada para autorizar o decretar la

intervención de las comunicaciones al amparo de lo dispuesto en el art. 579.3 *in fine* in fine de la Ley de Enjuiciamiento Criminal, *"... así como de las comunicaciones para la realización de sus fines delictivos"*, *in genere* y conforme se han admitido las de las comunicaciones por radio, según sentencia de la Audiencia Nacional de 15 de septiembre de 1.995.

Nos encontramos ante comunicaciones de carácter privado y bajo la protección del secreto de las comunicaciones, en general. La asimilación de esta clase de comunicaciones a cualquiera de las reguladas expresamente por la Ley (postal, telegráfica o telefónica) a fin de poder poner en práctica los mecanismos de la analogía se producen con las comunicaciones telefónicas y ello aunque los textos pudieran ser escritos.

En favor de esta asimilación Maza Martín esgrime razones de orden técnico, en especial el soporte o la vía por la que discurren los contenidos: la propia línea telefónica. Asimismo invoca previsiones legales, y sobre todo el desarrollo jurisprudencial, de las "intervenciones telefónicas" cuyo proceder y garantía de forma bastante aproximada a las analizadas.

Concluyendo que su asimilación a las intervenciones telefónicas a efectos procesales, los requisitos para su eficacia probatoria, en la medida de lo posible, habrán de ser los mismos que los aplicables a esta. Y según numerosa jurisprudencia (como ejemplo Sentencia del Tribunal Supremo de 24 de junio de 1.995), será:

a) La autorización de su realización por autoridad judicial en resolución motivada.

b) El carácter excepcional y por tiempo determinado.

c) El que se dirijan a la obtención de pruebas sobre un hecho delictivo concreto de que consten los indicios de su comisión.

d) Practicadas sólo sobre teléfonos de personas sospechosas de participar en los delitos investigados y llegados a cabo bajo riguroso control del Juez autorizante, y

e) Con la obligación de entrega a la autoridad judicial de los soportes originales en que se haya recogido el contenido de las intervenciones.

Sobre todo ello conviene señalar el problema de determinación de la autoría en el caso que nos ocupa, pues en la mayor parte de las ocasiones se llegará a establecer con certeza las terminales entre las que esa comunicación se ha producido, sobre lo que habrá que añadir elementos probatorios adicionales para determinar el autor.

Por nuestra parte añadimos que además de los problemas de autoría, e incluso, antes de llegar a ellos, estaría los graves problemas de conocer el contenido de la comunicación interceptada si esta se ha producido de forma cifrada, lo que llevaría a la necesidad de pruebas periciales criptológicas que, mediante el criptoanálisis puedan determinar la información que contiene la comunicación intervenida.

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, delincuencia organizada e, incluso, delincuentes comunes.

Ante estas situaciones el Estado debe reaccionar en defensa de la Sociedad y ha de procurarse medios tecnológicos suficientes que le permitan, 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 lícita o 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.[92]

La finalidad de la interceptación de las comunicaciones es conocer su contenido, si este se encuentra cifrado se requerirán operaciones adicionales para lograrlo, operaciones que consideramos quedarían cubiertas legalmente por la correspondiente resolución judicial motivada.

Las operaciones de criptoanálisis quedarían amparadas legalmente, lo que no supone habilitación pericial o legal para que cualquiera pueda hacerlo, habida cuenta no sólo de la gran complejidad que pueden alcanzar

estas operaciones y la fiabilidad de sus resultados, sino del poder que otorga la posesión de estos conocimientos, equipos y sistemas.

El artículo 11.1, último párrafo, del R.D. 2632/85 de 27 de diciembre que asigna al Centro Superior de Información de la Defensa, a través de la Jefatura de Apoyo Operativo, la función de criptoanalizar, descriptar y realizar las investigaciones tecnológico-criptográficas.

Sin perjuicio de la garantía del secreto de las comunicaciones y de la exigencia de autorización judicial para la interceptación de contenidos, la Ley General de Telecomunicaciones contempla, en su artículo 51, la posibilidad de realizar intervención de las telecomunicaciones por los servicios técnicos, al decir:

"Con pleno respeto al derecho al secreto de las comunicaciones y a la exigencia, conforme a lo establecido en la Ley de Enjuiciamiento Criminal, de autorización judicial para la interceptación de contenidos, cuando para la realización de las tareas de control para la eficaz utilización del dominio público radioeléctrico establecidas en el Convenio internacional de telecomunicaciones, sea necesaria la utilización de equipos, infraestructuras e instalaciones técnicas de interceptación de señales no dirigidas al público en general, será de aplicación lo siguiente:

a) La Administración de las telecomunicaciones deberá diseñar y establecer sus sistemas técnicos de interceptación de señales en forma tal que se reduzca al mínimo el riesgo de afectara los contenidos de las comunicaciones.

b) Cuando, como consecuencia de las interceptaciones técnicas efectuadas, quede constancia de los contenidos, los soportes en los que éstos aparezcan no podrán ser ni almacenados ni divulgados y serán inmediatamente destruidos.

Las mismas reglas se aplicarán para la vigilancia del adecuado empleo de las redes y la correcta prestación de los servicios de telecomunicaciones..."

4.5.- RELACIONES ENTRE LOS DISTINTOS ÁMBITOS DE CONFIDENCIALIDAD, CONFLICTO DE DERECHOS Y CONCILIACIÓN DE INTERESES.

Henry L. Stimson, Secretario de Estado del Presidente Edgar Hoover, cuando disolvió el Gabinete Negro del Departamento de Estado en 1.929, lo justificó en su biografía diciendo que *"Gentlemen do not read each other's mail"*.

La criptología no concierne sólo a las autoridades diplomáticas y militares de los diferentes estados. No podemos olvidar el permanente conflicto de intereses entre el ciudadano o el individuo y el Estado representante de una sociedad libre, afectado por la criptología.

De una parte hay un indiscutible derecho del ciudadano o de una corporación para proteger su esfera privada o sus intereses comerciales con un criptosistema eficaz y, de otra parte existe el deber constitucional del estado a proteger su seguridad interior y exterior, que puede requerir la penetración de mensajes cifrados por necesidades de inteligencia.[93]

La posición de Estados Unidos, expresada por Charles A. Hawkins, Acting Assistant Secretary of Defense, el 3 de mayo de 1.993 es la siguiente:*"The law enforcement and national security communications argue that if the public's right to privacy prevails and free use of cryptography is allowed, criminals and spies will avoid wire taps and other intercepts"*.

Europa, con su tal vez diferente historia, no va hasta ahora por este camino.

Whitfield Diffie, elaboró una corta formula: *"...an individual's privacy as opposed to Gobernment secrecy"*.

Hasta ahora existe la necesidad de encontrar una formula imaginativa en el marco de cada constitución política como medio para regular el criptoanálisis, un límite debe ser definido. Esto es necesario también para la existencia de un marco legal. Extrañamente, los grandes países tienen en esto más dificultades en alcanzar resultados que los pequeños.[94]

De igual modo, es necesaria, también, una solución para el comercio mundial.

En el último siglo, la cultura jurídica occidental ha elaborado un nuevo derecho subjetivo, característico de la sociedad industrial de masas referido al sujeto humano, designado como "the right to privacy" y que se entiende como reserva de la vida privada y tutela de la intimidad personal; es un derecho de libertad atribuido al hombre como persona.[95]

El mercado exige, también, que las empresas dispongan de ámbitos propios de forma que se pueda preservar su información en aras a la competitividad.

De otra parte, el secreto de las comunicaciones privadas posee un contenido formal y se configura como un derecho que garantiza a los particulares una esfera de libertad.

Por lo que se refiere a la Seguridad y Defensa del Estado, de la referencia constitucional se deriva su consideración como persona jurídica unitaria que actúa como tal en la esfera internacional. Lo que no impide referirla igualmente, y en no menor medida, a la organización política que la misma prefigura.

El artículo 2 de la Ley Orgánica 6/1.980, del 1 de julio, por la que se aprueban los criterios básicos de la defensa nacional y de la organización militar, se define la defensa nacional del siguiente modo:

"La defensa nacional es la disposición, integración y acción coordinada de todas las energías y fuerzas morales y materiales de la Nación, ante cualquier forma de agresión, debiendo todos los españoles participar en el logro de tal fin".

Disponiendo a su vez el artículo 3 del citado cuerpo legal que la defensa nacional ha de ser regulada de tal forma que proporcione una efectiva seguridad nacional.

Afirmación que exigirá entender la defensa nacional como una función de garantía, de preservación de la seguridad nacional; renunciandose así, por expresa voluntad de la nación española, según debe colegirse de la lectura del preámbulo del texto constitucional , y en consonancia con lo dispuesto en el artículo 1.2 de la Carta Fundacional de las Naciones Unidas, a toda acción que suponga agresión ilegítima contra otro Estado; en tanto que la expresión seguridad hace alusión a un hallarse fuera de todo peligro

inmediato o encontrarse libre y exento de todo peligro, daño o riesgo según el Diccionario de la Real Academia Española de la Lengua.

Misión defensiva, cuyo cumplimiento precisará de un conjunto de medios humanos y materiales que garanticen, tanto en el fuero interno como en el externo, el cumplimiento de una serie de condiciones mínimas, pero indispensables, de cara a la efectividad de la convivencia pacífica. Tarea en la cual jugarán destacado papel las Fuerzas Armadas, parte integrante del complejo administrativo y que tienen encomendadas, art. 8 de la CE, una serie de funciones básicamente reconducibles a las categorías de defensa interior y exterior del Estado.

Actuación cuya ejecución precisará del complemento de un conjunto amplio de potestades, preservación de la seguridad del Estado que involucra a toda la sociedad y que representará en ocasiones un límite al ejercicio de los derechos fundamentales.

Seguridad exterior del Estado que tiende a centrar toda nuestra atención, por cuanto es precisamente en la escena internacional donde el complejo jurídico-político estatal se presenta dotado de una personalidad unitaria, como un centro de imputación de relaciones jurídicas.

La salvaguarda del Estado y de sus instituciones democráticas exigirá, asimismo, una intervención preventiva, de acopio de información sensible a fin de evitar todo intento ilegítimo de quiebra del juego constitucional.

Pero no toda información de la que disponen los distintos órganos administrativos se puede considerar incluida dentro de dicha categoría, ni siquiera toda la información que afecta a la seguridad del Estado deberá ser considerada por ello automáticamente como excluida del conocimiento público.

Antes, "deberá procederse a la realización de un juicio previo de probabilidad, mediante el cual se determine la idoneidad de los datos para provocar lo que la jurisprudencia estadounidense ha denominado un peligro cierto e inminente (clear and present danger), de tal forma que tan sólo serán susceptibles de quedar encuadrados en dicha categoría aquellas informaciones que, referidas a hechos ciertos, su revelación indiscriminada pudiera poner en peligro de un modo evidente la protección de los intereses que se trata de asegurar, manteniendo las mismas extramuros de la publicidad".[96]

Este planteamiento viene a situar el problema en la determinación de la idoneidad de la información para afectar de modo cierto e inminente a la protección de la seguridad estatal, con lo que se traslada el centro de gravedad al juicio previo de probabilidad lo que exige la utilización de técnicas no estrictamente jurídicas, sino sociológicas, jurídicas y de prospectiva.

En cuanto a la averiguación y prevención del delito, el artículo 11 de la Ley Orgánica 2/1.986, de 13 de marzo de Fuerzas y Cuerpos de Seguridad, estas tienen como misión proteger el libre ejercicio de los

derechos y libertades y garantizar la seguridad ciudadana mediante el desempeño de las siguientes fines:

"... f) Prevenir la comisión de actos delictivos.

g) Investigar los delitos para descubrir y detener a los presuntos culpables, asegurar los instrumentos, efectos y pruebas del delito, poniéndolos a disposición del Juez o Tribunal competente y elaborar los informes técnicos y periciales procedentes.

h) Captar, recibir y analizar cuantos datos tengan interés para el orden y la seguridad pública, y estudiar, planificar y ejecutar los métodos y técnicas de prevención de la delincuencia...".

El objeto de la prevención es la limitación, incluso, la supresión de la infracción, y constituye una de las funciones principales de la policía. [97]

Por último, el secreto y consiguientemente la protección de la información pública es muy restringida y excepcional, destinada solo a preservar materias que afecten a los altos intereses del Estado y de la sociedad; es una protección selectiva, muy intensa pero poco extensa. A diferencia del secreto y consiguiente protección de las comunicaciones privadas, que es genérica, dirigida a un espectro muy amplio de comunicaciones, extensa, pero que requiere una menor intensidad en la protección.

La intensidad y nivel criptológico de las comunicaciones públicas necesitadas de protección requiere, además, estar en condiciones de garantizar la seguridad de las comunicaciones a los niveles criptológicos internacionales más avanzados, en un mundo de comunicaciones globales, para poder neutralizar las eventuales amenazas procedentes de los modernos y sofisticados desarrollos electrónicos.

La protección criptológica de las comunicaciones se sitúa en el contexto de las nuevas tecnologías de la información en el entorno social, jurídico y político de una sociedad democrática donde encuentra su legitimación, pero también, sus límites.

Al no ser un valor absoluto, la protección criptológica de la información encuentra su justificación en función de los intereses que protege, los cuales tienen elementos comunes, pero, a su vez, pueden responder a principios diferentes, operar bajo coordenadas distintas y, en determinados casos, incluso pueden llegar a ser contrapuestos; por lo que es necesario armonizar las necesidades de seguridad de las comunicaciones de estos distintos ámbitos entre sí y con los demás intereses que entran en juego en la vida del Estado y de la sociedad en su conjunto, y dar una respuesta general a las necesidades de seguridad de las comunicaciones, al nivel criptológico adecuado, como garantía de eficacia en la protección de derechos y libertades.

Parece evidente que la excepción a la garantía general de secreto de las comunicaciones solo puede ser autorizada por el Juez, pero las condiciones para que esta excepción sea real y efectiva, así como para que no afecte a otros intereses constitucionalmente tutelados, le corresponde a los poderes públicos.

¿Pero quién autoriza la excepción al secreto de las comunicaciones públicas?, ¿En base a qué normas?.

Parece evidente que las comunicaciones públicas -las que a lo largo de este trabajo hemos denominado, a veces, como comunicaciones gubernamentales- pueden plantear situaciones que requieran excepcionar el secreto en base a razones de seguridad nacional, las cuales tienen pleno soporte constitucional pero carecen del desarrollo normativo que regule las intervenciones de comunicaciones por este motivo, de forma análoga a las intervenciones realizadas dentro en el seno de un proceso penal.

Para el cumplimiento real y efectivo de una resolución judicial de intervención de comunicaciones, no es indiferente el nivel de seguridad - y en concreto, el nivel criptológico- con que esté o deba estar protegida la información o las comunicaciones a que se refiera.

Y surge una interrogante, ¿debe haber límite al nivel de protección criptológica?, en caso afirmativo ¿cual debe ser?.

El hecho de que no exista límite puede suponer que, en determinados casos, no se pueda cumplir la resolución judicial por insuficiencia técnica de los medios que la Administración dispone para conseguirlo.

Todo ello con independencia de que el mecanismo ordinario sea a través de la gestión de claves, lo que permitiría estar protegido a los máximos niveles criptológicos y utilizar las posibilidades de la gestión y administración de claves para permitir los accesos en los casos que legalmente corresponda.

Ello nos puede llevar a pensar en la necesidad de limitar el nivel de protección o bien a incrementar el nivel técnico y criptológico de la Administración -o ambas cosas- para hacer cumplir las resoluciones judiciales en casos extraordinarios o de incumplimientos, o bien establecer los adecuados sistemas de gestión de claves.

En todo caso, en Criptología, se exige estar a la altura de los niveles tecnológicos más avanzados y mantenerse en ellos.

Por lo que el nivel de protección del secreto de las comunicaciones privadas, ha de guardar relación con la capacidad técnica del Estado para hacer cumplir la resoluciones judiciales que lo excepcionen, en su caso.

A la vez, el nivel de protección del secreto oficial, y muy especialmente los que afectan a la seguridad, integridad e independencia del Estado -excepción a la transparencia de las comunicaciones públicas- ha de estar por encima de la capacidad técnica de cualquier otro estado u organización internacional

De todo lo indicado no se oculta la necesidad de armonizar y conciliar todos los intereses en juego para obtener un resultado que posibilite el cumplimiento razonable de todos los derechos en presencia.

La intimidad, la seguridad del Estado, el secreto de las comunicaciones y la averiguación y prevención del delito, responden a principios distintos y las relaciones entre las normas que los sustentan pueden ser complejas.

Uno de los principales problemas relacionados con la propia existencia de un ordenamiento jurídico es el derivado de las relaciones entre las diversas normas que lo integran.

Conocer si estas normas constituyen una unidad y en qué forma lo consiguen llevará al problema de la jerarquía normativa. También se trata de saber si el ordenamiento jurídico constituye un sistema más que una unidad, lo que nos llevará a discutir el problema de las antinomias jurídicas.

Todo ordenamiento jurídico, unitario y sistemático tiene vocación también de ser completo, lo que nos llevará al estudio de las lagunas del derecho.

Pero entre los hombres no existe un solo ordenamiento, sino múltiples y de los más variados y diversos tipos, lo que nos llevará al estudio de los problemas derivados del reenvío de un ordenamiento a otro.

La necesidad de regular conductas de la más variada índole deriva en ordenamientos jurídicos complejos y, mediante diversos mecanismos, lograr la unidad sistemática necesaria.

La intimidad, la seguridad del Estado, el secreto de las comunicaciones, la averiguación y prevención del delito -ámbitos todos ellos a los que se aplica la criptología- ¿se puede decir que son incompatibles? ¿que suscitan antinomias jurídicas?.[98]

La tendencia de todo ordenamiento a constituirse en sistema y ser coherente, hace que el intérprete tienda a eliminar la presencia de antinomias que no son otra cosa que el choque de dos proposiciones incompatibles.

La coherencia no es condición de validez, pero es condición de justicia del ordenamiento.

Si dos normas contradictorias son ambas válidas, el juez podría aplicar indistintamente una u otra, según su criterio, atentando contra las exigencias de certeza y de justicia.

Los criterios generalmente aceptados para resolver la antinomia: el cronológico, el jerárquico y el de especialidad, brindan suficientes posibilidades para resolver cualquier conflicto que pudiera surgir entre estos conceptos jurídicos.

La integridad del ordenamiento jurídico ha de entenderse en el sentido que éste contiene las reglas con las cuales el buen intérprete puede resolver todos los problemas jurídicos que se le presentan o puedan presentársele. Lo cual no supone, en modo alguno, desconocer el carácter dinámico de la sociedad y los nuevos problemas a los que tiene que ir dando respuesta el ordenamiento; lo que obliga a una producción normativa adecuada a las nuevas exigencias y a un esfuerzo interpretativo.

El Tribunal Constitucional viene declarando que a los Jueces ordinarios le corresponde la ponderación de los derechos que entran en conflicto. Un primer paso fundamental en esa función es la correcta

identificación y delimitación de cuáles son, en el supuesto concreto enjuiciado, los derechos fundamentales en conflicto, habida cuenta de la distinta significación y función de cada uno de ellos.

La STC 219/1.992, en su F. 2°, declara que "...tal ponderación no constituye una labor hermenéutica substancialmente distinta de la de determinar el contenido de cada uno de los derechos en presencia y los límites externos que se derivan de su interacción recíproca".

Según Ignacio De Otto y Pardo, "la llamada ponderación de bienes es el método propio de esta construcción teórica para determinar, en abstracto o en concreto, cómo, cuándo y en qué medida debe ceder el derecho fundamental que entra en colisión con otro o con un bien".[99]

Respecto a la ponderación como técnica resolutoria de conflicto entre derechos fundamentales partiendo del carácter no absoluto tanto de estos derechos como de sus limitaciones y, concretamente, en lo referente al conflicto entre las libertades de expresión e información y otros derechos fundamentales y bienes jurídicos en general, la STC 159/1.986, de 12 de diciembre, en su F. 6° dice:

"Es cierto, como señalan las sentencias impugnadas, que los derechos y libertades fundamentales no son absolutos, pero no lo es menos que tampoco puede atribuirse dicho carácter a los límites a que han de someterse el ejercicio de tales derechos y libertades. Tanto las normas de libertad como las llamadas normas limitadoras se integran en un único

ordenamiento inspirado por los mismos principios en el que, en último término, resulta ficticia la contraposición entre el interés particular subyacente a las primeras y el interés público que, en ciertos supuestos, aconseja su restricción. Antes al contrario, tanto los derechos individuales como sus limitaciones, en cuanto éstas derivan del respeto a la ley y a los derechos de los demás, son igualmente considerados por el artículo 10.1 de la Constitución como "fundamento del orden político y de la paz social". Así, este Tribunal pudo declarar en su Sentencia 25/1.981, de 14 de julio, que los derechos fundamentales resultan ser "elementos esenciales de un ordenamiento objetivo de la comunidad nacional", reiterando posteriormente el destacado interés público que se halla en la base de la tutela de los derechos fundamentales.

Se produce, en definitiva, un régimen de concurrencia normativa, no de exclusión, de tal modo que tanto las normas que regulan la libertad como las que establecen límites a su ejercicio vienen a ser igualmente vinculantes y actúan recíprocamente. Como resultado de esta interacción, la fuerza expansiva de todo derecho fundamental restringe, por su parte, el alcance de las normas limitadoras que actúan sobre el mismo; de ahí la exigencia de que los límites de los derechos fundamentales hayan de ser interpretados con criterios restrictivos y en el sentido más favorable a la eficacia y a la esencia de tales derechos."

Esta técnica de ponderación de bienes, consecuencia del carácter no absoluto de los derechos fundamentales y de las libertades públicas, viene a justificar un amplio margen de discrecionalidad al juzgador, propios de un sistema judicial basado en la libre creación judicial como el Common Law, pero no en los sistemas judiciales continentales en los que el papel tradicional del juez es el de ser *"la voz de la ley"* y la discrecionalidad ha de reducirse mediante la adecuada producción normativa.[100]

Ejemplos para conciliar intereses en los ámbitos de la seguridad de las comunicaciones, la intimidad, la seguridad del Estado y la averiguación y prevención del delito, por lo que se refiere al uso de la criptología, nos los muestran las iniciativas norteamericana y europeas en el ámbito de la seguridad de la información.

La regulación del conflicto entre la protección de la esfera privada del ciudadano respetuoso con la ley, garantía de confidencialidad de sus mensajes y, de otra parte, el cumplimiento de las funciones del Estado, ha sido abordado en varios esquemas, recogidos por F.L. Bauer en su obra "Descrypted secrets":

1.- Una limitación del uso de los criptosistemas en el ámbito civil por una exigencia de solicitar aprobación oficial, en casos individuales o modelos de utilización, impuesto sobre vendedores.

2.a.- Una restricción de la seguridad de cifrado por regular la disponibilidad del criptosistema conveniente en el ámbito civil. La agencia

que hace el criptosistema asequible puede algunas veces dar al ciudadano una garantía criptoanalítica y de este modo puede aumentar el incentivo para una conformidad voluntaria.

2.b.- Semejante al 2a, pero en conjunción con una restricción de uso de otros criptosistemas en el ámbito civil.

3.- Un "escrow system", necesita tener el depósito completo de datos por cada criptosistema usado en el ámbito civil, la "escrow agemcy" es independiente y requiere mantener confidencialidad.

Pueden surgir otras propuestas, así como mezclas entre las indicadas anteriormente. Se puede esperar que diferentes estados democrático aportarán diferentes soluciones dentro de los límites de su soberanía.

En Francia, por ejemplo, estaría dentro del esquema 1, con una solución a lo largo de vías de qué puede ser considerado antidemocrático está ya establecida, y los Países Bajos coquetean desde hace tiempo con esta regulación.

En Alemania, hay una tendencia por una solución semejante a la 2a, con la reciente creación del *Bundesamt für Sicherheit in der Informationstechnik* (BSI).

Todavía no es evidente cual es la solución que adoptará el Reino Unido con su "Official Secrets Act".

En Estados Unidos, en 1.993, una solución similar a la del esquema 3, "key escrow sistem", causó fuerte protesta y provocó una

modificación en la dirección del esquema 2a, con una especie de sumisión voluntaria, estaba en discusión en 1.996.

Para la Unión Europea, en tanto se legisla sobre esta cuestión, ni la solución 1 ni la 3 son opciones viables.[101]

La gran importancia de la Criptología se pone de relieve, también, por el tratamiento que se le da a su estudio y análisis en el país más importante del mundo: Estados Unidos.

4.6.- CONTROLES.

Los grandes y graves efectos que puede producir un inadecuado uso de las capacidades tecnológicas actuales en los aspectos descritos donde están en juego importantes intereses, derechos y libertades fundamentales, aconsejan que todo el proceso de seguridad de la información y las comunicaciones disponga de controles eficaces, orientados a dar credibilidad y garantía -jurídica, política y técnica- a todo el proceso.

El Defensor del Pueblo como alto comisionado de las Cortes Generales, designado por éstas para la defensa de los derechos comprendidos en el Título I de la Constitución, ("De los derechos y deberes fundamentales"), puede supervisar la actividad de la Administración respecto a la garantía efectiva en la protección de los derechos y libertades relacionados con la protección de las comunicaciones, dando cuenta a las Cortes Generales, (Artículo 54 de la C.E.).

De otra parte, el artículo 55 de la Constitución dice que una ley orgánica podrá determinar la forma y los casos en los que, de forma individual y con la necesaria intervención judicial y el adecuado control parlamentario, el secreto de las comunicaciones privadas puede ser suspendido para personas determinadas, en relación con las investigaciones correspondientes a la actuación de bandas armadas o elementos terroristas.

Hay que distinguir que una cosa es "suspender el derecho" en los casos de estado de excepción o de sitio o para personas determinadas en relación con las investigaciones a la actuación de bandas armadas o elementos terroristas y otra, la "excepción a la garantía" del secreto de las comunicaciones que introduce la resolución judicial.

La excepción a esa garantía general sólo puede ser autorizada por el Juez, pero la creación de las condiciones para que esta excepción sea real y efectiva y no afecte a otros intereses constitucionalmente tutelados, le corresponde a los poderes públicos.

Para el logro real y efectivo del cumplimiento de una eventual resolución judicial dirigida a excepcionar el secreto de las comunicaciones, no es indiferente el nivel de seguridad con que éstas comunicaciones estén protegidas y, por consiguiente, el nivel criptológico empleado.

Si salimos del ámbito nacional para adentrarnos en el internacional de la sociedad global de la información, la situación adquiere dimensiones que han de ser tratadas internacionalmente. Lo que nos llevaría a una

política mundial de seguridad de la información que fije el marco de referencia básico en el que enmarcar las normas internas de los Estados en la materia y donde se dé cabida a todos los intereses en juego.

En las comunicaciones públicas, la naturaleza de la información clasificada, su gran incidencia en los intereses generales, así como la apetencia de ser conocida por individuos, grupos organizados u otras potencias, exige que las condiciones de seguridad para que el secreto sea real y efectivo esté a la altura de las eventuales amenazas. Es tarea que también compete a los poderes públicos y exige la utilización de las medidas de seguridad necesarias.

Pero el nivel de estas medidas para que realmente sean efectivas, exige que sean del más alto grado. Y aunque tenga el Estado a su alcance incidir en otros factores que no sean precisamente el del nivel de protección de su información y sus comunicaciones, (tales como adoptar medidas de naturaleza política, previsibilidad de sus acciones, pactos, alianzas, etc.) que atenúen la necesidad y apetencia de terceros en conocer lo protegido, la exigencia de estar protegidos al más alto nivel no desaparece.

Por todo ello, la capacidad técnica para rebasarlo depende de factores ajenos al mismo Estado, entre ellos el estado de la tecnología a nivel mundial; no quedando otro camino que estar protegido a los máximos niveles internacionalmente conocidos, en función de la vulnerabilidad que se

ofrezca, lo cual dependerá, entre otros factores, de su peso económico, político y militar, así como de líneas de política exterior y de seguridad.

La protección de información puede incidir en la garantías de la soberanía e independencia, integridad territorial y ordenamiento constitucional (art. 8 de la C.E.), por lo que la elección del nivel de seguridad y, en consecuencia, del nivel criptológico, es una decisión política.

¿Pero quién controla todo este proceso?.

El Gobierno dirige la política interior y exterior, la Administración civil y militar y la defensa del Estado. Ejerce la función ejecutiva y la potestad reglamentaria de acuerdo con la Constitución y las leyes (art. 97 de la C.E.).

Teniendo en cuenta, sobre todo, que estamos ante algo tan sutil como el nivel de seguridad técnica de la información, que es una realidad cambiante, que tiene fuertes implicaciones de intereses estratégicos, políticos, económicos, militares y diplomáticos, y para los derechos y libertades individuales, con alto componente tecnológico; en el que el gran riesgo está en "no hacer", permitir o tolerar, a través de lo que se podría llegar, eventualmente, hasta el delito de traición (art. 584 del Código Penal) y que el Gobierno responde de su gestión política ante el Congreso de los Diputados (art. 108 de la C.E.), así como que las Cámaras y sus Comisiones podrán recabar la información y ayuda que precisen del Gobierno y de sus Departamentos y de cualesquiera autoridades del Estado y de las Comunidades

Autónomas (art. 109), así como el alto componente tecnológico de todo ello, además del autocontrol de las propias organizaciones y administraciones, además del papel del Defensor del Pueblo y el propio control judicial, se podría pensar en la posibilidad de constituir una Comisión específica en el Parlamento sobre seguridad de la información y las comunicaciones, que no sólo se refiera a materias clasificadas.

Por lo que se refiere a la protección de datos personales, la Directiva 95/46/CE de 24 de octubre de 1.995, confiere una gran importancia a la existencia de una autoridad encargada de vigilar la aplicación de las disposiciones adoptadas y en su artículo 28 recoge que los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas.

Esta autoridad de control entenderá de las solicitudes que cualquier persona, o cualquier asociación que la represente, le presente en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales.

El artículo 34 de la LORTAD y el artículo 2º del Estatuto de la Agencia de Protección de Datos, aprobado por R.D. 428/1.993, de 26 de marzo, indican que la Agencia goza de personalidad jurídica propia y plena capacidad pública y privada.

En base a todo ello, es fácil deducir que a la Agencia de Protección de Datos le corresponde crear las condiciones para que la protección de

los datos de carácter personal sea real y efectiva, así como controlar el cumplimiento de las disposiciones al respecto. Lo que supone una directa responsabilidad en la seguridad de los datos personales, y le corresponde, en el contexto del sistema criptológico nacional, tomar las iniciativas necesarias para la efectiva protección de los datos de carácter personal.

Pero las Administraciones -Consejo Asesor de Telecomunicaciones en su caso-, el Defensor del Pueblo, las Cortes Generales, el Poder Judicial, la Agencia de Protección de Datos,... ¿disponen de medios técnicos que les permitan realizar con eficacia su función en esta compleja y tecnologizada tarea?.

Todos los controles que se establezcan deben contar, de forma eficaz y fluida, con el apoyo técnico necesario para el ejercicio de sus funciones; sin ello, no será posible un control real y efectivo.

[1] Molina Mateos, J.M., op. cit., pág. 67 y 68.
[2] Segrelles de Arenaza, y., "Protección penal del secretado de Estado", Instituto de Criminología de Madrid, EDERSA, Madrid, 1.994, pág. 15.
[3] Segrelles de Arenaza, y., op. cit., pág. 15.
[4] Abril, G., op. cit. pág. 88.
[5] Ribagorda Garnacho, A., "Glosario de Términos de Seguridad de las T.I.", Ediciones CODA, Madrid, 1.997.
[6] Molina Mateos, J.M., "Jornadas interdisciplinares sobre Criptografía, Privacidad y Autodeterminación Informativa", Zaragoza, 26 y 27 de octubre de 1.995.
[7] Moreno Catena, "El secreto en la prueba de testigos del proceso penal", Editorial Montecorvo, Madrid, 1.980.
[8] Espinosa Carmona, "Protección de la información clasificada en los contratos de defensa", Segundas Jornadas de los Servicios Jurídicos de las Fuerzas Armadas, separata, Madrid, 1.985.
[9] Sainz Moreno, F., "Secreto e información en el Derecho Público", Estudios sobre la Constitución. tomo III, La Corona, Las Cortes Generales, Del Gobierno y de la Administración Pública, homenaje al profesor Eduardo García de Enterría, Edit. CIVITAS, Madrid, 1.991.
[10] Bauer, F.L., "Decrypted secrets", Methos and Maxims Cryptology, Springer Verlag, Berlín, 1.997.
[11] Ley 9/1.968 de 5 de abril sobre Secretos Oficiales, Exposición de Motivos.
[12] Cousido González, P., "Comentarios a la Ley de Secretos Oficiales y su Reglamento", Edit. BOSCH, Barcelona, 1.995.
[13] Cousido González, P., op. cit.
[14] Cousido González, P., op. cit.
[15] Bermejo Vera, J., "El secreto en las Administraciones Públicas. Principios básicos y regulaciones específicas del ordenamiento jurídico español". Revista Española de Derecho Administrativo, núm 57, enero-marzo, Madrid, 1.988.
[16] Cousido González, P., op. cit.
[17] Soriano, R., "Las libertades públicas", Edit. Tecnos, 1.990, pág. 106.
[18] Desantes Guanter, J.M., "Los límites de la información", Edit. Asolciación de la Prensa de Madrid, 1.991.
[19] De Esteban, J., "La amenaza totalitaria: los secretos de Estado", Diario El Mundo, 19 de septiembre de 1.996.
[20] El País, sábado 13 de diciembre de 1.997.
[21] Exposición de Motivos de la Ley 9/1.968, de 5 de abril, sobre Secretos Oficiales.
[22] Cousido González, P., op. cit.
[23] Cousido González, P., "Comentarios a la Ley de Secretos Oficiales y su Reglamento", Edit. BOSCH, Barcelona, 1.995, pág. 76.
[24] Cousido González, P., op. cit.
[25] Cousido González, P. op. cit.
[26] Espinosa Carmona y Blay Villasante, tomado de Segrelles de Arenaza, I., op. cit. pág. 25.

[27] Molina Mateos, J.M., op. cit. pág. 85.
[28] Artículo modificado por Ley 48/1.978, de 7 de octubre.
[29] Artículo modificado por Ley 48/1.978, de 7 de octubre.
[30] Artículo modificado por Ley 48/1.978, de 7 deoctubre.
[31] Boletín Oficial del Congreso de los Diputados, Serie D., número 153, del 23 de febrero de 1.988.
[32] Cousido González, P., op. cit. pág. 14.
[33] El Mundo, 3 de septiembre de 1.996. El texto integro del Anteproyecto de Ley de Secretos Oficiales aprobado por el Consejo de Ministros de 23 de agosto de 1.986.
[34] Espinosa Carmona, op. cit.
[35] OTAN, clasificaciones de seguridad de la OTAN son: *COSMIC Top secret, NATO Secreto, NATO Confidential y NATO Restricted.*
[36] Ley 9/1.968, de 5 de abril, sobre Secretos Oficiales, modificada por Ley 48/1.978, de 7 de octubre y el Reglamento, aprobado por Decreto 242/1.969, de 20 de febrero.
[37] Declaración Universal de Derechos Humanos de 10 de diciembre de 1.948.
[38] Pacto Internacional de Derecho Civiles y Políticos (Nueva York), 16 de diciembre de 1.966.
[39] Convención de salvaguardia de los Derechos del Hombre y de las Libertades Fundamentales (Roma), 4 de noviembre de 1.950.
[40] De Asis Roig, R., "La paradoja de los derechos fundamentales como límites al poder", Edit. Debate, 1.992.
[41] Martínez Lage, S., "Breve Diccionario Diplomático", O.I.D, Ministerio de Asuntos Exteriores, Madrid, 1.982.
[42] Martínez Lage, S., op. cit.
[43] Martínez Lage, S., op. cit.
[44] Martínez Lage, S., op. cit.
[45] Díez de Velasco, M., op. cit. pág. 398.
[46] Díez de Velasco, M., op. cit. pág. 392.
[47] Martínez Lage, S., op. cit.
[48] Martínez Lage, S., op. cit.
[49] Segrelles de Arenaza, y., op. cit. pág. 39.
[50] Pérez-Luño, A.e., "Derechos Humanos, Estado de Derecho y Constitución", Edit. Tecnos, Madrid, 1.986, pág. 327.
[51] Ibidem, pág. 318.
[52] De Castro, F, "Temas de Derecho Civil", Madrid, 1.970, pág. 18.
[53] España, Ley Orgánica 1/1.982 de 5 de mayo de protección civil del Derecho al Honor, intimidad personal y familiar y propia imagen.
[54] España, Ley Orgánica 5/1.992, de 29 de octubre de regulación del Tratamiento Automatizado de Datos de Carácter Personal.
[55] Ruiz Miguel, C., "El derecho a la protección de la vida privada en la Jurisprudencia del Tribunal Europeo de Derechos Humanos. Civitas. Madrid, 1.994, pág. 27.
[56] Ruiz Miguel, C., op. cit. pág. 57.
[57] Herrero-Tejedor, F., "Honor, intimidad y propia imagen", Colex,

Madrid, 1.990, pág. 92.
[58] Gitrama: "Voz "Imagen, derecho a". Nueva Enciclopedia Jurídica. tomo XI, Barcelona 1.962, pág. 326.
[59] Moreno Catena, "Garantía de los Derechos Fundamentales en la investigación penal", Revista del Poder Judicial, nº especial II, 1.987, pág. 132.
[60] "Declaración de los Derechos y Libertades Fundamentales", aprobados por Resolución del Parlamento Europeo de 1.989, artículo 6.
[61] Suñé Llinás, E., "Marco jurídico de las telecomunicaciones en la Unión Europea y en España", ponencia presentada en las Jornadas de la Abogacía y las Nuevas Tecnologías de la Información y la Comunicación. (octubre 1.996).
[62] Convenio de Salvaguardia de los Derechos del Hombre y de las Libertades Fundamentales, roma, 4 de noviembre de 1.950.
[63] De Asis Roig, r., "Las paradojas de los Derechos Fundamentales como límites al poder", Edit. Debate, 1.992, pág. 98.
[64] De Asis Roig, op. cit.
[65] Pérez Luño, A.E., "Nuevas tecnologías, sociedad y derecho", Fundesco, 1.987, pág. 25.
[66] Dávara Rodríguez, M.A., "Delas Autopistas de la Información a la Sociedad Virtual", Editorial Aranzadi, 1.996, pág. 126.
[67] Molina Mateos, J.M., op. cit.
[68] Herrero Tejedor, F., "Honor, intimidad y propia imagen", Colex, 1.990.
[69] Herrero Tejedor, F., op. cit. pág. 40.
[70] Velázque Bautista, R., "Protección jurídica de datos personales automatizados", Colex, 1.993, pág. 67.
[71] Molina Mateos, J.M., "Libertad informática y criptología", comunicación presentada en el II congreso Internacional de Informática y Derecho, celebrado en Mérida, mayo de 1.995. Publicada en la Revista "Informática y Derecho", de la UNED, Centro Regional de Extremadura (Acta del Congreso).
[72] Herrero Tejedor, F., op. cit. pág. 68.
[73] Velázquez Bautista, R., Edit. Colex, 1.993, pág. 71.
[74] Boletín Oficial del Congreso de los Diputados, Serie D., número 153, del 23 de febrero de 1.988.
[75] Bernstein, D.S., "Encryptions Internacional Labryrinth", en Building in Big Brother, Lance J., Hoffman, Springer-Verlag, Nueva York, 1.995.
[76] Dyson, E., "Release 2.0", Edit. Ediciones. Grupo Zeta, Barcelona, 1.998.
[77] Dyson, E., op. cit. pág. 324 y 325.
[78] Dávila,J., Morant, J.L., y Sancho, J., Facultad de Informática, UPM, "Control gubernamental en la protección de datos: Proyecto Clipper", X años de encuentros sobre Informática y Derecho 1.996-1.997, Universidad Pontificia Comillas, Madrid, Aranzadi.
[79] Garrido Falla, F., "Comentarios a la Constitución", Edit. Civitas, 1.980, pág. 9.
[80] Ley 11/98, de 24 de abril, General de Telecomunicaciones, Disposición derogatoria única.
[81] Boletín Oficial del Estado, núm. 99 del 25 de abril de 1.998.

[82] El País, martes 21 de abril de 1.992.
[83] El País, 2 de marzo de 1.994.
[84] Oppnheimer, W., El País, 25 de noviembre de 1.995.
[85] El País, 15 de diciembre de 1.995.
[86] El País, 20 de junio de 1.996.
[87] El País, 15 de febrero de 1.996.
[88] De Vega Ruiz, J.A., "Las libertades públicas y sus limitaciones en casos y circunstancias especiales", La Ley, 11 de marzo de 1.988.
[89] Rueda, F., "La Casa", Ediciones Temas de Hoy, Madrid, 1.993.
[90] Rueda, F., op. cit.
[91] Maza Martín, J.M., "Algunos apuntes a propósito de las autorizaciones judiciales para la intervención de comunicaciones a través de redes informáticas", Revista Jurídica LA LEY, Madrid, 18 de enero de 1.996.
[92] Centro Superior de Información de la Defensa, "Glosario de términos de Criptología", revisión marzo de 1.993.
[93] Bauer, F.L., op. cit. pág. 201.
[94] Bauer, F.L., op. cit.
[95] Herrero Tajedor, F., op. cit. pág. 34.
[96] Pomed Sánchez, L.A., "El derecho de acceso de los ciudadanos a los archivos y registros administrativos", Instituto Nacional de Administración Pública, Madrid, 1.989.
[97] Cubert, J., "La Policía y la prevención de la criminalidad", en "Policía y Sociedad Democrática", compilado por José María Rico, Alianza Editorial, 1.983.
[98] Bobbio, N. "Teoría General del Derecho", Editorial Debate, 1.993, pág. 200.
[99] Martín Retortillo, "La regulación del ejercicio de los Derechos y Libertades. La garantía de su contenido esencial en el artículo 53.1 de la Constitución", en la obra Derechos Fundamentales y Constitución, Madrid, 1.988, pág. 111.
[100] Martín de Pisón Cavero, J., "El derecho a la intimidad en la jurisprudencia constitucional", Madrid, 1.993.
[101] Bauer, F.L., op. cit. pág. 202.

CAPITULO V

CONCLUSIONES

5.1.- CONCLUSIONES GENERALES.

De todo lo expuesto en esta y a modo de síntesis, se extraen una serie de conclusiones, que alcanzan un mayor grado de concreción en unos principios que podrían inspirar una determinada política criptológica, los cuales, a su vez, permiten hacer una oferta de bases para la regulación normativa de la protección criptológica en España dentro de la pluralidad de opciones posibles:

PRIMERA.- La Política, considerada como estrategia, implica por su propia naturaleza el conocimiento, en su más alto grado, como capacidad de una organización para desenvolverse en un sentido concordante con el vigente en el ámbito de relaciones en el que opera, en cuya base se encuentra la información.

Resulta imprescindible el diseño y elaboración de un marco general para la estrategia del conocimiento; una política de la información que contemple las funciones de *adquisición, almacenaje y procesamiento, distribución y protección.*

Los grupos humanos, para la protección de determinados intereses, en el normal funcionamiento de su organización social y política, han requerido que determinadas informaciones solo fuesen conocidas por un número restringido de destinatarios; lo que históricamente se ha conseguido mediante la utilización de la Criptología como medio para ocultar o

disimular la información, especialmente en los ámbitos militar, diplomático y comercial. Y, recientemente, se está utilizando para la protección de derechos y libertades individuales, en cuya función adquiere una dimensión cívica.

El carácter instrumental de la Criptología la convierte en herramienta para el cumplimiento real y efectivo de una decisión previa que ha requerido la delimitación de ámbitos y niveles de confidencialidad, cuya configuración depende de la actitud que se tenga ante el *"secreto"*.

En las sociedades democráticas, paralelamente a la transparencia en los asuntos públicos, se está desarrollando una creciente sensibilidad acerca de los efectos de las tecnologías de la información y las comunicaciones sobre las estructuras y valores generalmente admitidos y, muy especialmente, sobre la privacidad del individuo.

Junto a las demandas de transparencia para asuntos de gobierno se admiten y justifican limitaciones a esa publicidad en determinados casos, relacionados con intereses generales o privacidad del individuo, provocando una tensión entre publicidad y secreto, cuyo resultado podría ser un punto crítico de equilibrio entre la transparencia como norma general y el secreto estrictamente necesario para asuntos y casos muy concretos. Lo que llevaría tal vez a replantear el secreto oficial tal y como se viene dando, para ir a una reducción substancial de su uso y, a la vez, lograr un fortalecimiento de su rigor.

Esta situación convive con el secreto de las comunicaciones privadas como norma general, solo excepcionable por resolución judicial.

SEGUNDA.- Tradicionalmente, el poder ha descansado en el control de la fuerza, la riqueza y el conocimiento. Actualmente ha cambiado la proporción en que tales factores contribuyen a la formación de ese poder, adquiriendo un notable protagonismo todo lo relacionado con el conocimiento, en cuya base está la información.

La creciente dependencia del conocimiento y consiguientemente, de la información puede constituir el eje central del enfrentamiento político de los estados y las organizaciones a nivel internacional y, en el plano interno, esta dependencia de la información es punto de conflicto entre el individuo y el Estado por la necesidad de una protección real y efectiva de derechos y libertades. A la vez, los efectos de las nuevas tecnologías traspasan las fronteras nacionales y comportan dificultades para la soberanía de los Estados y la territorialidad del Derecho.

Todo ello obliga a los gobiernos a prestar mayor atención a los asuntos relacionados con la información y el conocimiento y desarrollar políticas en las que se vean reflejados los aspectos involucrados entre los que destaca la seguridad y protección de la información, de donde se derivaría la necesidad de reglas claras y precisas, que sepan conjugar los distintos valores que entran en juego en la vida de la Sociedad y del Estado.

TERCERA.- Lo que se considera como necesidad no viene determinado por normas universales de razón o certidumbre, sino que será el entorno cultural y político y, en definitiva, el grado de desarrollo, el que lo defina.

Para ello, hemos de poseer un conocimiento previo de la razón por la que debemos conseguir algo, si queremos evitar daños graves, concretos y objetivos.

En nuestro entorno cultural, social, económico y político, con el actual grado de desarrollo de las nuevas tecnologías; será la propia naturaleza de la información y el conocimiento y, concretamente su valor, los que los sitúen en un nivel que demanda su posesión útil, controlada y necesitada de protección para evitar pérdidas no deseadas, producidas por cualquier motivo, ya sean causas naturales, tecnológicas, derivadas de la acción humana, o producto de egoísmos de terceros.

La comunicación de información valiosa en un clima de desconfianza es lo que suscitó la necesidad de protegerla e históricamente, dio lugar al nacimiento de la Criptología.

Múltiples acontecimientos han confirmado a lo largo de la historia y confirman permanentemente, "la necesidad" de proteger la información y, consiguientemente, la necesidad de utilizar la Criptología.

Esa necesidad, con el uso de las nuevas tecnologías se ha multiplicado exponencialmente.

CUARTA.- Todos los asuntos relacionados con la información a medida que se desarrollan y, especialmente, cuando se tratan de regular, arrojan toda clase de perfiles políticos, que, en algunos casos comportan la necesidad de establecer limitaciones al libre flujo de información; lo que configura actitudes hacia la libertad de expresión e información, influye en los derechos humanos, afecta al secreto de las comunicaciones o tiene directa incidencia en la seguridad del Estado.

Una política de la información en la que se contemplen los aspectos de la seguridad -especialmente la confidencialidad- y las medidas para su protección real y efectiva, constituye el soporte sobre el que se asienta el papel de la Criptología.

Las nuevas tecnologías de la información y las comunicaciones son cauce potencial para la intromisión en la intimidad personal del individuo y la confidencialidad de las organizaciones y todo ello, puede afectar al sistema de garantías del Estado de Derecho y repercutir en los intereses económicos, políticos o militares.

En el nuevo espacio comunicativo creado por las tecnologías de la información y las comunicaciones, la Criptología actúa como factor de equilibrio y elemento de socialidad, contribuyendo a preservar, en el ámbito comunicativo, los lugares del individuo y las organizaciones dentro del sistema, nacional o supranacional, en el marco de la globalidad.

La Criptología brinda a las tecnologías de la información, la posibilidad de reparar, por sus medios, el desequilibrio que su aplicación introduce en la socialidad.

A su vez, la Criptología, utilizada de forma abusiva o fraudulenta, puede contribuir a la creación de una cultura de opacidad incompatible con una sociedad democrática, y puede, incluso, ser un obstáculo para el normal desenvolvimiento de la sociedad y del Estado a través de la creación de reductos impenetrables. Su regulación resulta un imperativo de convivencia.

QUINTA.- *Todo acto comunicativo contribuye a la configuración de* una identidad, como forma particular de estar en relación y de establecer relaciones, señalando los límites del propio ámbito mediante el secreto, y conectándose con el entorno mediante el mensaje.

La intercomunicabilidad producida por la revolución de las comunicaciones, contribuye a la creación de problemas en las instituciones productoras de identidad social, lo que no excluye la posibilidad de crear nuevas formas de identidad merced a estas nuevas tecnologías comunicativas.

La sobrecarga de información obliga a la selección, y a la compartimentación; lo que genera problemas en cuanto a la convergencia en torno a valores comunes del sistema social.

Las nuevas tecnologías son un instrumento de comunicación, ponen en común pero de forma distinta, por lo que quita peso y valor a lo que se

tiene en común a nivel constitutivo en la sociedad. Si a ello se añade que en la sociedad actual las ligaduras son débiles y los flujos de información fragmentados, se pueden estar dando pasos hacia una disolución, al menos tal y como la entendemos en su concepción tradicional.

Tras apreciar la falta de sintonía entre estructura social y evolución tecnológica, resulta fundamental vislumbrar las reestructuraciones que estas nuevas tecnologías imponen a las demás partes del sistema social. Entre estas reestructuraciones está la necesidad de avanzar hacia la aplicación de la Criptología como garantía de confidencialidad y preservación de intromisiones indebidas, y garantía de identidades, personales o colectivas

SEXTA.- La histórica tensión entre individuo y Estado en la historia de los derechos fundamentales, ha sido matizada por el proceso de internacionalización que viene a suponer que la historia de los derechos fundamentales no es sólo un proceso de tensiones entre individuo y Estado, sino que en ella también tienen un papel relevante los poderes supranacionales y las colisiones y conflictos entre los individuos.

No siempre cabe entender a los derechos fundamentales como limitadores del poder estatal, sino también como limitadores de poderes privados, lo que suscita el papel del Estado en relación con estos derechos.

Existen ocasiones en las que los derechos fundamentales no son límites al poder político sino a la actuación de otros individuos.

Por lo que la actuación del Estado, en unos casos ha de ser negativa o de no interferencia, pero, en otros, positiva; lo que implica promoción y actuaciones para la garantía efectiva y exige *"un hacer"* del Estado.

En estas nuevas relaciones entre individuo y Estado nace una nueva, cuyos polos serían el Estado y la sociedad.

Los derechos de la libertad nacen contra el abuso del poder del Estado y para limitar ese poder, mientras que los derechos sociales, nacen para su protección efectiva y requieren un aumento de los poderes del Estado.

De forma que los derechos fundamentales dejan de ser meros límites al ejercicio del poder político para convertirse en un conjunto de acciones positivas de los poderes públicos entre las que han de incluirse las medidas necesarias para que su protección sea real y efectiva.

SÉPTIMA.- El secreto de las comunicaciones recogido en el artículo 18.3 de la Constitución, se configura como un derecho que garantiza a los particulares una esfera de libertad que ha de ser respetada y está referido, por tanto, a las comunicaciones privadas.

Este concepto de secreto tiene un carácter formal con independencia de su contenido. Es omnicomprensivo y aplicable a cualquier medio o servicio que sirva para la transmisión de comunicaciones.

Su conculcación puede venir tanto por la interceptación del soporte del mensaje, con conocimiento o no del mismo, como por el conocimiento

antijurídico de lo comunicado; por lo que para su garantía necesita que las comunicaciones estén protegidas criptológicamente.

Pero el artículo 18.3 reconoce al derecho fundamental del secreto de las comunicaciones un carácter relativo, ya que permite su limitación por resolución judicial que autorice la injerencia en su objeto; lo que obliga a los poderes públicos dotar al órgano judicial del apoyo organizativo, tecnológico y criptológico necesario para llevar a cabo el cumplimiento de sus resoluciones.

La Constitución exige que para interceptar las comunicaciones sea imprescindible una resolución judicial, la Jurisprudencia añade que esta ha de ser motivada. A partir de ahí, corresponde a la legislación ordinaria precisar los supuestos en los que es procedente conceder esta autorización.

La intervención de comunicaciones está prevista, en la Ley que regula los estados de alarma, excepción y sitio; en la Ley de Enjuiciamiento Criminal en los supuestos de causas penales, de presos o detenidos no incomunicados, y de bandas armadas o elementos terroristas; el Código Procesal Militar también referido a hechos o circunstancias objeto de proceso, pero nada se dice de la seguridad nacional, la defensa, la seguridad pública, o la prevención, por citar ejemplos muy significativos.

Los criterios y requisitos procesales válidos para todos los supuestos de intervención de comunicaciones, adolecen de una regulación completa en

nuestro ordenamiento jurídico; lo que viene a subrayar la laguna existente en materia de información y comunicaciones.

Cubrir esta laguna y desarrollar plenamente el artículo 18.3 de la Constitución, tanto en lo que se refiere a la eficacia de la garantía del secreto de las comunicaciones como a su excepcionalidad, la investigación judicial y policial y, eventualmente, las labores de inteligencia y contrainteligencia; podrían ser más complejas pero, sin duda, se ganará en respeto a la persona y a los derechos fundamentales y se fortalecerán las instituciones.

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

Este apoyo ya de ser mayor si se tiene en cuenta que el Juez es vigilante constitucional tanto del derecho de secreto de las comunicaciones como de su excepción.

El Estado, desde el punto de vista positivo tiene la obligación de procurar la efectividad del derecho; lo que exige, en primer término actuaciones normativas, pero, además, actuaciones para la protección real y efectiva de los derechos fundamentales; lo que, en el caso del secreto de las comunicaciones demanda medidas de seguridad de naturaleza criptológica que, con carácter preventivo impidan que la violación se produzca.

OCTAVA.- La competitividad como capacidad para luchar favorablemente en el mercado, se traduce en la obtención de ventajas respecto a los competidores.

De las diversas formas de obtener ventajas competitivas, las nuevas tecnologías de la información y las comunicaciones han venido aportando tradicionalmente ventajas basadas esencialmente en la automatización de operaciones.

Con su implantación y desarrollo generalizado, el uso de las nuevas tecnologías dejan de aportar singularidad, y se convierten en exigencias de las reglas de juego.

Los nuevos factores de competitividad ya no exigen solo capacidad para manejar de forma eficaz las operaciones internas, sino que, además, requieren la capacidad de conexión y adaptación al entorno.

En este nuevo escenario de competencia resulta imprescindible captar la necesidad del mercado y desarrollar de forma rápida un producto o servicio que dé respuesta; lo que exige captación de información, rapidez de flujos, innovación, facilitar la comunicación, aumento de la coordinación, etc.

Convierte el manejo de información en un tema crítico, al hacer posible la mejora de la capacidad de respuesta a las exigencias del mercado.

La importancia del conocimiento como factor de competitividad exige una defensa del activo del propio conocimiento frente a los

competidores; para lo que necesita incorporar la seguridad como parte de la dimensión estratégica de la información.

NOVENA.- La seguridad como calidad de estar libre y exento de todo peligro, daño o riesgo, resulta difícil cubrir en toda su plenitud conceptual y, en todo caso, viene determinada por los concretos peligros, riesgos y amenazas a que, en este caso, la información, puede verse sometida.

La variedad e intensidad de los riesgos y amenazas a la información son tan diversas que, a priori, resulta muy difícil establecer el grado de seguridad necesaria.

Si además se tiene en cuenta la diferencia de lógica del razonamiento del atacante que, en definitiva es el que va a configurar los riesgos y amenazas más significativos, para cuya neutralización se exigen los mayores niveles de seguridad; y la lógica de razonamiento del que elabora la defensa que, para ser efectiva, ha de elaborar una seguridad superior a los niveles de agresiones potenciales, resulta evidente la dificultad y complejidad del diseño de criterios de seguridad.

Quizás sea, desde el punto de vista de la teoría matemática de los juegos, bajo el que hay que estudiar y resolver los problemas de seguridad de la información.

A través de los diferentes modelos y sus múltiples combinaciones se puede llegar a determinar, matemáticamente, cuáles son los modos racionales de conducta en diversas circunstancias y prevenirlas.

La teoría de los juegos aplicada a la seguridad de la información, sería un juego de suma variable, donde lo que pierde el defensor puede ser menor o mayor que lo que gana el atacante, pudiendo incluso perder ambos.

La situación ideal del diseñador de seguridad sería la de anticiparse al atacante, incorporar los códigos y lógicas de razonamiento del atacante, en definitiva, tener un atacante en la cabeza.

DÉCIMA.- La historia de la Criptología ha sido paralela a la historia de las comunicaciones y el desarrollo de las técnicas de comunicación ha tenido y tiene una influencia decisiva sobre las "técnicas de guerra".

No en menor medida el desarrollo de las comunicaciones y la Criptología ha tenido influencia sobre la diplomacia como modo de comunicación pacífica e institucionalizada entre los actores del sistema internacional.

En la diplomacia actual, caracterizada por una acción exterior de operatividad inmediata, muy tecnificada y universal, afectada por presiones políticas, económicas y de opinión pública; la influencia de las comunicaciones y la Criptología redobla su importancia.

DECIMOPRIMERA.- La guerra moderna está dirigida por la información; en ella los hechos se aceleran de tal modo que se exigen decisiones rápidas con comunicaciones y respuestas instantáneas.

Para integrar la acción se necesita un alto nivel de coordinación entre fuerzas de tierra, mar y aire, apoyo espacial y sistemas centralizados.

La creciente diferenciación de misiones, instrumentos y unidades, aumenta la necesidad de información que ha de reunirse, procesarse e intercambiarse, y, consiguientemente, protegerse; por lo que el sistema de control y comunicaciones adquiere una importancia vital.

La nueva guerra será multidimensional, uniéndose a los tradicionales escenarios de tierra, mar y aire, nuevos campos de batalla como las redes informáticas y el espacio.

En la guerra informática se intentará destruir o confundir los sistemas de información enemigos y se tratará de evitar que esto ocurra con los propios, mediante su protección.

Por todo ello, y por los efectos que produce la protección criptológica, también, en aspectos no militares, -pero no por ello de menor interés para una solución favorable del conflicto-, la Criptología se convertirá en objetivo prioritario de cualquier ataque y, consiguientemente, su desarrollo y utilización, deviene una necesidad estratégica.

DECIMOSEGUNDA.- Tras la guerra fría han cambiado los parámetros estratégicos que han imperado en el mundo durante su vigencia. El concepto de seguridad nacional está experimentando fuertes transformaciones y ha ido evolucionando hacia concepciones no agresivas; dando entrada a otros actores entre los que está la información y el conocimiento con la revolución informática y de las comunicaciones y el incremento de las organizaciones supranacionales como base del sistema político internacional.

Cada país debe abordar su propia doctrina estratégica de acuerdo con sus circunstancias, lo que requiere una clara percepción, sentido y alcance de los cambios en los que estamos inmersos y la previsión que de ellos se deriva.

Para el desarrollo histórico de cada país es fundamental el conocimiento exacto de sus posibilidades y limitaciones y, en base a ello, poder diseñar las estrategias más conveniente en cada momento y, de este modo, estar en condiciones de prever escenarios futuros y alcanzar las metas que como sociedad se ha marcado.

Hoy la planificación estratégica exige cada vez más tener en cuenta factores no estrictamente militares tales como los económicos, los ecológicos, los tecnológicos, políticos, diplomáticos, históricos, culturales, sociales o los institucionales y, en todo caso, los factores relacionados con la información y el conocimiento aplicado a todo ello; sin que esto suponga que los factores estrictamente militares no sigan siendo imprescindibles. Y, fruto de todo ello conseguir la construcción de un modelo de seguridad nacional en base a la realidad de España en su dimensión nacional e internacional. Como potencia media, exenta de responsabilidades globales, pero con peso en una zona decisiva para el equilibrio global.

Como parte de un conjunto de estrategias que permitan asegurar nuestra posición internacional, prevenir acontecimiento y, en su caso, hacer frente a eventuales conflictos, es necesario un reforzamiento de la

Inteligencia, la información y las comunicaciones y los sistemas para su protección, especialmente los de carácter criptológico. Lo que exige una toma de conciencia de la importancia de la información y el conocimiento, su almacenamiento, transmisión y protección, en el nuevo escenario internacional.

Y, en definitiva, hacer los esfuerzos políticos, materiales, organizativos o de planeamiento necesarios para atender a uno de los vectores esenciales de cualquier estrategia nacional: la información.

DECIMOTERCERA.- La clasificación de la información que fluye por un sistema según el grado de sensibilidad determina la confidencialidad de la misma.

En base a ello, se define la que debe ser protegida y con qué niveles, para sólo permitir su conocimiento a quienes estén autorizados.

Todo ello es una forma de preservar la naturaleza del "secreto".

Pero el secreto encuentra su justificación como instrumento de paz y armonía, cuya singularidad está en subrayar el ámbito restringido y excluyente de los grupos que intercomunica; y su eficacia en el ámbito comunicativo se ve garantizada por la aplicación del lenguaje criptológico.

En un mundo de relaciones múltiples y frágiles, y soberanías compartidas, la intensidad del secreto se relativiza, para reducirse a aspectos concretos y vitales, directamente relacionados con esas "identidades"; que

para su juego conjunto, demandan distintos niveles que hagan posible el funcionamiento armónico de la unidad en la diversidad.

La clasificación de información es un acto de configuración de ámbitos de confidencialidad con toda la repercusión política, social y jurídica que comporta, por lo que es un tema esencial para una sociedad que ha de ser decidido en base a un consenso entre sociedad y Estado, en el que participen periodistas, juristas, politólogos junto con los representantes de las administraciones centrales y autonómicas.

La delimitación de ámbitos de confidencialidad es insuficiente, su protección real y efectiva en la era de la información añade exigencias que demandan ampliar el consenso con la incorporación de tecnólogos y expertos en criptología y, entre todos, sentar las bases para una solución integral en un clima de confianza de toda la sociedad.

DECIMOCUARTA.- Una de las limitaciones de las libertades de expresión e información está constituida por el secreto oficial como instrumento para garantizar la paz a través de la seguridad y la defensa.

El concepto de Defensa Nacional supera la dimensión militar para integrarse en la política general del Estado, teniendo en cuenta exigencias de otros tipos; por lo que la protección de los secretos de Estado comprende todos aquellos órdenes que pueden afectar a la seguridad de la nación, además de los militares, tales como los de índole política, diplomática, económica o industrial.

La Criptología como medida para la protección efectiva de la información, es garantía y protección de la propia comunidad y, como protección de las materias clasificadas, forma parte del derecho a la seguridad y a la defensa como instrumentos para el logro de la paz.

DECIMOQUINTA.- La seguridad de la información se ha convertido en un tema político esencial en el mundo contemporáneo; y es un objetivo de toda sociedad actual desarrollar estrategias generales que permitan a los usuarios de la información tratada, almacenada o transmitida electrónicamente, dotar a los sistemas de información de una protección adecuada frente a las amenazas accidentales o deliberadas.

La seguridad de la información tiene tres criterios o propiedades fundamentales, que son tres dimensiones distintas de la seguridad: la confidencialidad, la integridad y la accesibilidad.

Por virtud de la confidencialidad un sistema de información sólo permite el conocimiento de la misma a quienes estén autorizados y requiere la previa clasificación de la información que delimite los ámbitos a proteger.

La integridad es la garantía contra alteraciones y permite asegurar que no se ha falseado la información.

La accesibilidad es la propiedad que asegura que la información pueda ser utilizada por los usuarios autorizados.

La seguridad de la información ha de ser concebida de forma integral con gran peso de la seguridad física, la disponibilidad, la accesibilidad, la

confidencialidad y su protección, esencialmente criptológica, sin olvidar la organización y el factor humano.

DECIMOSEXTA.- La llegada de unas comunicaciones globales subraya la necesidad de contar con una "protección" adecuada y medidas de seguridad eficaces; las cuales son de los más variados y diversos tipos: políticas, legales, culturales, organizativas, físicas, lógicas, electromagnéticas o criptológicas.

DECIMOSÉPTIMA.- Por las características de la información y el conocimiento y la propia naturaleza, implantación y uso de las nuevas tecnologías de la información y las comunicaciones; las necesidades de protección rebasan el ámbito de cobertura que da la norma jurídica, toda vez que, ante la vulneración, incluso la sanción resulta insuficiente, al no hacer reversible el daño causado.

Las medidas legales son medidas de protección que actúan "a posteriori", y en un entorno tecnológico que comporta grandes dificultades de prueba.

El gran valor de la información y el conocimiento y las graves consecuencias producidas en casos de violación de su protección, de efectos irreparables en muchos casos, hacen necesario la utilización de medidas de prevención que, "a priori" eviten materialmente que la violación se produzca.

Las medidas criptológicas son las producidas por los modelos, equipos y sistemas, destinados a la ocultación o cifrado de la información.

La Criptología es la solución universalmente aceptada para evitar actos que puedan vulnerar la protección de la información y las comunicaciones y, en general, cualquier utilización no autorizada; y es la forma tradicional de preservar la confidencialidad de un sistema de información o una red de comunicaciones.

Los avances tecnológicos permiten el acceso a las bases de datos y la interceptación de las comunicaciones de todo tipo, efectuada por cualquier medio; lo que incrementa la necesidad del uso de aplicaciones criptológicas al nivel adecuado, hasta el extremo de resultar imprescindibles en un sistema de información.

La utilización clásica de la Criptología ha sido referida a los ámbitos militar, diplomático y comercial, extendiéndose actualmente a infinidad de campos en los que es necesaria la protección; hasta el punto de ser una necesidad de las redes públicas de comunicaciones, que constituiría una "cifra básica o general"; aunque los niveles de exigencias criptológicos son diferentes en función de la naturaleza y riesgos de la información en los distintos ámbitos; dándose la circunstancia que, en la actualidad, con el desarrollo e implantación de la informática, la criptografía estratégica ha desbordado el ámbito estrictamente militar, penetrando en los centros de cálculo, donde se custodian datos de gran valor.

DECIMOCTAVA.- Sobre la Criptología, como sobre otras ramas del saber, resulta difícil hacer un diagnóstico exacto de la situación presente. Si además se le une la reserva con la que, en algunos casos, se ha llevado todo lo relacionado con la Criptología, el diagnóstico resulta aún más difícil.

En la actualidad conviven sistemas de diversas épocas.

En plena sociedad de la información, hablar de presente es hablar de cifra electrónica y al hablar de futuro nos referimos a las posibilidades matemáticas y computacionales con la vista puesta en el "cifrado perfecto", según la terminología de Shannon.

Con el logro del cifrado perfecto, podría parecer que la criptografía ha agotado sus posibilidades de investigación y desarrollo; pero el problema del cifrado perfecto es que resulta difícil de utilizar, la clave es excesivamente larga y son muy costosos; por lo que la Criptología se orienta hacia sistemas de cifrado pseudoperfectos, que parecen ser suficientes para cubrir las necesidades criptológicas.

Hoy, los sistemas de cifra estratégica, elaborados por las más prestigiosas firmas mundiales especializadas en criptología para usos militares y diplomáticos, descartan el sistema de clave pública y se mantienen en el sistema de cifra de clave secreta y algoritmos propios, que alcanzan niveles de sofisticación muy próximos el "cifrado perfecto", que permiten que cada mensaje se cifre con claves distintas e irrepetibles, elegidas entre billones de combinaciones.

DECIMONOVENA.- La fortaleza alcanzada por los algoritmos de cifrado, orienta las preocupaciones de seguridad y facilidades de uso hacia el establecimiento y desarrollo de procedimientos adecuados de gestión de claves, como proceso que comprende la generación, distribución, almacenamiento, utilización, archivo y destrucción de claves empleadas en un criptosistema.

El adecuado establecimiento de un sistema de gestión de claves permitirá hacer efectivo una determinada política de seguridad de la información en todos sus aspectos.

VIGÉSIMA.- La lucha constante por desentrañar los contenidos de los mensajes cifrados es tan antigua como la propia Criptología que, con un carácter eminentemente defensivo, a lo largo de la historia viene soportando los embates ofensivos del criptoanálisis.

La tensión producida en la guerra silenciosa y constante, llevada a cabo por procedimientos científicos, entre la protección criptológica de la información y las comunicaciones y su quebranto, es lo que ha hecho evolucionar los distintos sistemas criptológicos.

Los diseñadores y fabricantes de sistemas criptológicos establecen un compromiso entre los costes de operaciones de cifrado y descifrado, que deben ser sencillas, y las operaciones de criptoanálisis, que deben ser muy complejas y de elevado coste.

El ideal de todo criptosistema es que la tarea del criptoanalista no pueda ser realizada con los recursos de cálculo disponibles, por el tiempo que necesita invertir, o por la memoria de ordenador precisa.

Los sistemas criptológicos tienen que tener propiedades matemáticas que los hagan invulnerables, no solo en el presente, sino , también, en el futuro previsible.

La potencia de los algoritmos, con la dificultad y elevado coste para su criptoanálisis, dará paso a una situación en la que se genere un mercado mundial de venta ilegal de información, con aumento de las acciones de inteligencia que poco o nada tienen que ver con la Criptología en su dimensión científica.

El resultado positivo del criptoanálisis de un equipo o sistema no suele ser conocido, al menos, mientras está siendo de utilidad para quien lo han conseguido. Su beneficiario tratará por todos los medios de mantener el secreto, para provecho propio o de terceros, el máximo tiempo posible.

El gran problema no es sólo que el criptoanálisis permita forzar, en un momento determinado, un algoritmo. Es mucho más importante para la organización que padece los efectos del criptoanálisis, poder conocer cuando se ha producido y, aún más importante, conocer cuando se producirá, para evitarlo. Y esto, tal vez, ya no sea tarea de la Criptología sino de los Servicios de Inteligencia.

VIGESIMOPRIMERA.- El poder de la información es un multiplicador de fuerza, incluido el "poder suave" como capacidad de conseguir los resultados deseados en asuntos internacionales mediante la atracción en lugar de la coerción.

En la defensa de la sociedad y del Estado se requiere la estrategia para tratar los casos de ausencia de armonía, que pueden degenerar en conflicto, para lo que el conocimiento del problema es la clave de la solución, hasta el extremo que la eficacia máxima del conocimiento y de la estrategia radica en conseguir que el conflicto sea totalmente innecesario, ganar sin luchar. Conseguir lo máximo haciendo lo mínimo.

La información previa, producto de la recogida, análisis y elaboración de la misma, sigue siendo un instrumento de primera magnitud y eficacia para prevenir las eventuales desestabilizaciones de la convivencia pacífica, siendo, en última instancia, una garantía de seguridad nacional.

Si con todo ello, el Estado consigue que otros canalicen o limiten sus actividades, puede que necesite emplear menos recursos económicos o militares.

La elaboración y desarrollo de planes para la obtención y análisis sistemáticos de información, su transmisión y explotación inteligente, está en el origen del nacimiento de los servicios de inteligencia, que utilizaban las tecnologías existentes en cada momento histórico.

La existencia de un nuevo sistema de creación de riqueza en el que cada vez interviene más la información y el conocimiento, las transferencias de tecnología, equipos y conocimientos de aplicación militar, la radicalización de conflictos nacionalistas, religiosos o étnicos, o la expansión internacional del crimen organizado, terrorismo y narcotráfico; en los Estados de Derecho exige el aumento de la tensión en la vigilancia para preservar su mantenimiento como regímenes de garantía y salvaguarda de derechos y libertades.

La complejidad de estos fenómenos y de los nuevos conflictos internacionales, exigen esfuerzos de especialización y madurez intelectual que permitan una completa comprensión de situaciones con implicaciones multidireccionales.

Todos estos cambios ponen de relieve la necesidad de redefinir el modelo de servicio de inteligencia vigente durante los años de la guerra fría.

A medida que un país asume mayores papeles en el campo diplomático, político y militar, en consonancia con su poder económico, necesita incrementar sus actividades de inteligencia; lo que, a su vez, provoca el incremento de actividades de inteligencia y contrainteligencia entre vecinos, socios comerciales, aliados y adversarios.

Lo que en el caso de España podría llevar a la necesidad de potenciar los servicios de inteligencia.

VIGESIMOSEGUNDA.- La forma en que se maneje la información y el conocimiento en general, y concretamente, la forma en que se delimite, proteja y administre el secreto, así como los servicios con él relacionados es un tema político esencial.

La información y el conocimiento y las nuevas tecnologías de la información y las comunicaciones -de las que dependen en la actualidad en gran medida-, son elementos constitutivos del poder nacional; por lo que son objeto de atención preferente de los servicios de inteligencia de todo el mundo, tanto en la obtención como en su protección, en la que juega un papel determinante la Criptología.

Esta situación obliga a los servicios y agencias de inteligencia a disponer de la información previa necesaria, a nivel internacional, sobre Criptología de forma que puedan conocer en qué momento los equipos y sistemas de protección criptológica utilizados por su país pueden ser rebasados por el criptoanálisis para, en su caso, y con carácter previo, aconsejar la utilización de mayores niveles criptológicos en la protección de las comunicaciones y, de esta forma, evitar el criptoanálisis por otras potencias u organizaciones.

Todo ello, en definitiva, para lograr estar protegidos a los niveles criptológicos internacionales más avanzados y neutralizar las amenazas procedentes de los modernos y sofisticados desarrollos electrónicos.

El nivel tecnológico y de conocimiento necesarios para cubrir esta dimensión de la protección, se ve incrementado por la necesidad de estar en condiciones de dar respuestas a eventuales requerimientos de los órganos judiciales para excepcionar el secreto de las comunicaciones.

Lo que viene a proporcionar unas capacidades que subrayan la necesidad de eficaces mecanismos de control sobre los servicios encargados de estas delicadas misiones, como garantía de derechos y libertades.

VIGESIMOTERCERA.- De una interpretación amplia del ordenamiento y con una perspectiva global, en el ámbito del Estado Español, correspondería al Centro Criptológico Nacional, único centro especializado en la administración española, actualmente adscrito el Centro Superior de Información de la Defensa, velar por la seguridad de la información en general, coordinar las acciones de las distintas administraciones públicas en cuanto a la utilización de medios o procedimientos de cifra, garantizar la seguridad criptográfica, promover la adquisición coordinada de material y formar especialistas.

No obstante sería conveniente que fuesen recogidas con mayor claridad en la norma, tanto las funciones descritas como el organismo competente para llevarlas a cabo, lo que podría encontrar respuesta en el desarrollo de las normas que eventualmente se efectúen tras la creación de una Autoridad Nacional de Seguridad, prevista en el Proyecto de Ley de Secretos Oficiales

VIGESIMOCUARTA.- Las libertades de expresión e información constituyen derechos fundamentales en el mundo contemporáneo y exponente de la salud democrática de cualquier organización política.

Estas libertades son al mismo tiempo libertades institucionales y libertades que están fuertemente limitadas en sus manifestaciones externas.

En nuestro ordenamiento constitucional están recogidas en el artículo 20 de la Constitución Española de 1.978.

En el plano sociopolítico existe una gran vinculación entre el principio de publicidad de las decisiones gubernamentales y los fundamentos de la democracia.

La ocultación de las decisiones gubernamentales y los motivos que las fundamentan, se suele considerar incompatible con los principios democráticos que deben inspirar toda actividad pública.

No obstante existen restricciones justificadas por la preservación de los intereses generales que vendrían a configurar los ámbitos de confidencialidad en cuya base está el secreto.

El artículo 20.4 de la Constitución establece los límites al derecho a la información y recoge la intimidad, el honor, la propia imagen y la protección de la juventud y de la infancia.

Los límites referidos a la seguridad del Estado no están expresamente recogidos en el artículo 20, pero se derivan implícitamente de la

consideración de la seguridad estatal como presupuesto del Estado de derecho y, consiguientemente de la efectividad de los derechos y libertades.

El secreto de las comunicaciones recogido en el artículo 18.3 de la Constitución, es un derecho fundamental que, a su vez, opera como límite de la libertad de expresión y del derecho a la información.

Pero a su vez, los límites pueden ser limitados, llegando a darse el caso que la misma figura jurídica es al mismo tiempo un derecho y un límite de otro derecho, e, incluso, darse conflictos de los límites entre sí.

VIGESIMOQUINTA.- La Ley 9/1.968, de 5 de abril, sobre Secretos Oficiales, modificada por Ley 48/1.978, de 7 de octubre, configura el ámbito de confidencialidad del secreto oficial y, en la Disposición Final dice que, en Reglamento único, de aplicación general a toda la Administración del Estado y a las Fuerzas Armadas, se regularán los procedimientos y medidas necesarias para la aplicación de la Ley y la protección de las materias clasificadas.

Se determinará con todo el detalle necesario y con especificación de las medidas técnicas precisas el régimen de custodia, traslado, registro, archivo, examen y destrucción de las materias clasificadas.

La Ley, en su artículo 12, dice que los órganos encargados de la clasificación atenderán al mantenimiento y mejora de los sistemas de protección y velarán por el efectivo cumplimiento de la ley.

En la regulación de las medidas preventivas para lograr una protección real y efectiva se pone de relieve la insuficiencia y falta de adecuación normativa.

Una nueva regulación ha de centrarse en medidas de seguridad acordes con los avances tecnológicos actuales y previsibles, contemplando la realidad de las telecomunicaciones y la informática, tanto en el proceso y almacenamiento de datos como en su transmisión, donde adquiere una singular importancia las medidas de protección de naturaleza criptológica.

La eficacia de la Criptología en la protección de la información y las comunicaciones, la necesidad de su uso, los distintos niveles de exigencia y variedad, así como los efectos que puede producir, tanto su aplicación como su no aplicación o, su aplicación inadecuada. Los distintos derechos que protege y las consecuencias jurídicas y prácticas de todo ello, pone de relieve una importante laguna en el ordenamiento en materia de medidas de protección adecuadas a las exigencias organizativas, lógicas, tecnológicas, jurídicas y políticas de la sociedad actual.

VIGESIMOSEXTA.- En base a lo dispuesto en el artículo 53 de la Constitución, los derechos y libertades vinculan a todos los poderes públicos y podrá regularse su ejercicio sólo por ley que, según el artículo 81 del texto constitucional, deberá ser orgánica.

Por lo que la regulación de la protección de la información y las comunicaciones, en tanto que afecta a derechos y libertades fundamentales,

sólo podrá llevarse a cabo por Ley Orgánica; excluyendo ordenaciones contenidas en leyes ordinarias, tanto estatales como autonómicas, de forma que la reserva de Ley Orgánica solo puede ser cumplimentada por el Estado.

Esta exigencia ha sido flexibilizada por el Tribunal Constitucional, al justificar ciertas ordenaciones introducidas por vía reglamentaria para regular el ejercicio de determinados derechos.

En todo caso, la falta de normas sobre el desarrollo de determinados derechos y libertades, según el Tribunal Constitucional han de cubrirse aplicando la ley válida en el anterior sistema de fuentes, si la hubiera, como es el caso de la vigente Ley y Reglamento de Secretos Oficiales que son preconstitucionales.

Cualquier limitación de la libertad de expresión e información sólo es válida, en cuanto hecha por ley; y no solo por la exigencia de la propia Constitución, sino por las exigencias derivadas de los pactos internacionales suscritos y ratificados por España.

VIGESIMOSÉPTIMA.- Las garantías internas que los estados conceden a los derechos fundamentales resultan insuficientes.

Frente a los nuevos problemas surgidos del desarrollo y aplicación de las nuevas tecnologías de la información y las comunicaciones, la colaboración internacional resulta imprescindible y, a través del carácter vinculante de una instancia supranacional, complementar las garantías

internas lo que requiere, previamente, poner el acento en la consideración del individuo como sujeto de Derecho Internacional.

VIGESIMOCTAVA.- El secreto de las comunicaciones, aplicado a la información almacenada, tratada o transmitida electrónicamente, viene a complementar y reforzar la "libertad informática", añadiendo un plus de confidencialidad en su faceta de derecho de secreto para los datos.

La exigencia que la libertad informática sea real y efectiva, así como la regla general de secreto en las comunicaciones privadas, ha convertido a la protección criptológica como una exigencia ineludible y sistemática de cualquier sistema informático.

VIGESIMONOVENA.- La plenitud del ordenamiento jurídico exige que, además de la protección "a posteriori" sancionando conductas contrarias al mismo, se disponga de mecanismos que garanticen, de forma eficaz, "a priori", en determinadas circunstancias, las consecuencias irreparables de eventuales violaciones de la información y las comunicaciones, lo que se lleva a cabo a través de las medidas de prevención.

Las medidas de prevención, además de requerir una eficacia operativa que les permita ser útiles en el cumplimiento de su finalidad, requieren una fundamentación y un soporte jurídico legitimador de su aplicación que lejos de producir desequilibrio entre libertad de información y secreto de las comunicaciones, en detrimento de la libertad, sea presupuesto básico de la misma.

Ya que la protección de los derechos no se circunscribe a la reparación de los perjuicios originados, sino que ha de extenderse a las medidas de prevención que, razonablemente, impidan ulteriores lesiones.

Lo que, en el orden de la información y las comunicaciones se consigue con aplicación de la Criptología.

Pero hablar solo de medidas de prevención, de forma genérica, es insuficiente; como insuficiente es hablar de cifrado o de protección criptológica, sin más, pues existe una gran variedad de grados y niveles de protección que, en determinados casos harían inoperante la protección y, en otros, dificultarían el normal funcionamiento de la sociedad y del Estado. Por lo que, la regulación ha de ir más lejos y llenar las lagunas que en nuestro ordenamiento se detectan, como consecuencia de los cambios tecnológicos operados en la sociedad y contemplar, normativamente, una compleja realidad que, sin duda, no existía en los momentos de promulgación de las normas vigentes; hoy obsoletas en gran parte de su contenido.

TRIGÉSIMA.- Las medidas de prevención para garantizar el secreto de la información y las comunicaciones y, concretamente la propia Criptología, se encuentran sometidas a una doble tensión; con tendencia ascendente hacia los máximos niveles de protección cuando se refiere a los intereses de la sociedad y del Estado, y orientada hacia niveles de menor exigencia en otros casos que, básicamente se corresponde con los dos

grandes bloques en que se encuentra agrupada la información: el destinado a garantizar el secreto de las comunicaciones privadas y el constituido por la protección de la información pública.

Estos bloques responden a principios distintos; mientras que en las comunicaciones privadas la regla general es el secreto y la excepción la transparencia; en las comunicaciones públicas, la regla general es la transparencia y la excepción el secreto; lo que nos llevaría a deducir unas necesidades de protección criptológica sistemáticas de las comunicaciones privadas y, solo de forma excepcional, de las públicas, aunque con niveles distintos, de forma que permita el normal funcionamiento de la sociedad y del Estado y no impida el ejercicio de derechos prevalentes.

El grado y niveles de protección criptológica de la información pública sería más intenso pero menos extenso, mientras que el grado de protección de la información privada sería más extenso pero menos intenso.

El secreto y, consiguientemente su protección criptológica, de la información pública es muy restringido y excepcional. Está destinado sólo a preservar materias que afecten a los altos intereses del Estado y de la sociedad; es una protección selectiva, muy intensa pero poco extensa.

La protección de estas comuniciones requiere que se garantice su seguridad a los niveles criptológicos internacionales más avanzados, origen y medio de sus posibles amenazas.

A diferencia del secreto y consiguiente protección de las comunicaciones privadas, que es genérica, dirigida a un espectro muy amplio de comunicaciones, extensa, pero que requiere una menor intensidad en la protección.

TRIGESIMOPRIMERA.- Crear las condiciones para que el secreto de las comunicaciones, tanto públicas como privadas, sea efectivo, corresponde a los poderes públicos por imperativo constitucional.

Cualquier diseño organizativo de la protección criptológica nacional en su conjunto y, por tanto, cualquier disposición que la regule, ha de tener presente que la protección criptológica encuentra su justificación en función de los intereses que protege.

Al estar referidos a distintos ámbitos de exigencias diversas, en algunos casos estos intereses tienen elementos comunes pero, pueden responder a principios diferentes, operar bajo coordenadas distintas e, incluso, pueden llegar a ser contrapuestos.

Por ello es necesario una armonización de las necesidades de seguridad de las comunicaciones de los distintos ámbitos entre sí y con los demás intereses que entran en juego en la vida del Estado y de la sociedad en su conjunto; y dar una respuesta general a las necesidades de protección de las comunicaciones, al nivel criptológico adecuado, como garantía de eficacia en la protección de derechos y libertades.

TRIGESIMOSEGUNDA.- La protección criptológica de la información y las comunicaciones por el elevado componente tecnológico con el que opera, inapreensible para la gran mayoría de los ciudadanos, e incluso para organizaciones y administraciones, en muchos casos; así como por los efectos que produce en intereses, derechos y libertades -tanto su uso, como su no utilización- y, por consiguiente, por su repercusión en el normal desenvolvimiento de la vida del Estado y de la Sociedad, demanda establecer los oportunos mecanismos de control, en consonancia con su alto grado de sofisticación, que garantice el adecuado uso de estas técnicas, en garantía del Estado, de la Sociedad y del Individuo.

TRIGÉSIMOTERCERA.- Todo ordenamiento jurídico, además de unitario y sistemático, tiene vocación de ser completo lo que lleva a la necesidad de estudiar las lagunas del derecho.

La tendencia a constituirse en un sistema coherente, hace que el intérprete tienda a eliminar la presencia de antinomias o choque de proposiciones incompatibles, y corresponde al Juez ordinario la ponderación de los derechos que entran en conflicto, lo que no es otra cosa que determinar el contenido de cada uno de los derechos en presencia y los límites externos que se derivan de su relación recíproca.

La técnica de la ponderación de bienes, consecuencia del carácter no absoluto de los derechos fundamentales y de las libertades públicas -y de sus límites- viene a conferir un amplio margen de discrecionalidad al juzgador,

propio de un sistema judicial basado en la libre creación judicial como el Common Law; pero no en los sistemas judiciales continentales, como el español, en los que el papel tradicional del juez es el de ser la voz de la ley.

La discrecionalidad ha de reducirse mediante la adecuada producción normativa.

En el caso que nos ocupa de la protección criptológica de la información y las comunicaciones, estamos en un régimen de insuficiencia normativa; por lo que se ha de caminar hacia la elaboración de un marco legal adecuado que dé respuestas a todas las necesidades de la protección de la información en una moderna sociedad democrática.

CONCLUSIÓN FINAL.- El ciudadano necesita proteger sus comunicaciones, el Estado y el comercio ha de proteger sus secretos..., la Sociedad tiene que protegerse.

El medio eficaz, históricamente contrastado, para la protección de las comunicaciones es la Criptología. Por consiguiente, el dilema no es "Criptología sí ó Criptología no", sino que, dentro de un posicionamiento favorable al uso de la Criptología, el dilema estaría en Criptología sí, pero... ¿ cómo ?.

Y no tanto porque determinadas organizaciones delictivas puedan utilizar la Criptología -que de hecho la utilizan si lo necesitan y con independencia de lo diga o deje de decir la ley-, sino porque la Sociedad, el Estado, los individuos, el comercio... necesitan el uso de la Criptología

precisamente para protegerse de actos ilícitos cometidos mediante la interceptación de sus comunicaciones, mediante la revelación de sus secretos.

La Criptología tiene su origen en la desconfianza, y como medida de protección surge para restablecerla.

Al ser un instrumento, no es en sí misma, ni buena ni mala, lícita ni ilícita. Cumpliría su función siendo efectiva. Lo que producirá consecuencias lícitas e ilícitas, legales e ilegales, buenas y malas, en función del uso que se haga de ella. La legitimación de su uso y su calificación procederá, por tanto, de la naturaleza de los intereses que proteja.

Dentro del ámbito de los intereses legítimos, y al igual que en otros aspectos de la vida; en las comunicaciones y, consiguientemente, en las comunicaciones telemáticas, las necesidades de protección son de distinta naturaleza e intensidad y, por ello, los medios para satisfacerlas son diferentes.

Un ciudadano particular tiene un riesgo distinto al de una organización bancaria, y ésta, tiene un riesgo de naturaleza e intensidad diferente al de un ejército o al de un Jefe de Estado. En función de estos riesgos, cada uno, necesita medidas de protección de niveles diferentes.

No siendo razonable permitir cualquier medida de protección a un ciudadano o una organización bancaria que podría conllevar, eventualmente, el uso de medios desproporcionados como, por ejemplo, armas de guerra. Ni

tampoco sería razonable prohibir, de modo absoluto, su defensa de modo que no pudiesen utilizar ningún tipo de protección, incluyendo armas cortas o blindajes.

De igual modo, tampoco sería razonable -e incluso sería una temeridad- que un Estado, un ejército, una gran organización financiera, no se protegiese, o se protegiese de forma insuficiente.

Y menos razonable aún, sería que una Sociedad, que un Estado, no regulase de forma adecuada todo esto.

Por consiguiente, sí a la protección del individuo, sí a la protección del Estado, sí a la protección del comercio, y sí a la protección de la Sociedad..., de donde se deriva, sí a la libre utilización de la Criptología, pero regulando su uso y recomendando su utilización.

Ante la situación descrita urge la elaboración de una política criptológica nacional y el desarrollo de las normas pertinentes, todo ello precedido de un amplio, sereno y profundo debate, en el que participen todos los sectores afectados.

5.1.1.- PRINCIPIOS BÁSICOS INSPIRADORES DE UNA POLÍTICA CRIPTOLÓGICA.

En base a las conclusiones anteriormente indicadas, y con objeto de contribuir a la solución de uno de los grandes temas que tiene planteado una moderna sociedad democrática, tratamos de extraer una serie de principios básicos que podrían inspirar una política criptológica nacional, dentro de una pluralidad de opciones.

En el contexto de la seguridad de los sistemas de información y de la realización de objetivos económicos, políticos y sociales; la política criptológica, como conjunto de directrices generales que deben inspirar y dirigir la protección criptológica de la información, para garantizar la confidencialidad, la disponibilidad y la integridad de la misma, constituye uno de los soportes esenciales de cualquier política de seguridad.

En todo caso se ha de tener en cuenta el carácter emocional del debate sobre una política criptológica en la que intervienen aspectos relacionados con la intimidad, secreto de las comunicaciones, almacenamiento de datos e informaciones, persecución y prevención del delito, y la soberanía nacional, en un contexto internacional de creciente globalización de las comunicaciones.

Una vez superado el nivel de la articulación de una política criptológica se habrán creado las bases sólidas para incrementar el grado de

competitividad de nuestro país a escala mundial, en todos los órdenes, en la era de la información.

La política criptológica ha de constituir el marco en el que se inscriba un Plan Criptológico Nacional, que permita dotar a la sociedad y al Estado español de los elementos necesarios para la adecuada protección de la información, en todos sus ámbitos, de acuerdo con la exigencias de una moderna sociedad democrática y una potencia media, -con responsabilidades de área- a la llegada del tercer milenio.

Dentro de los requisitos de funciones específicas de seguridad está la política de seguridad, que debe ser explícita y bien definida, con identificación de todos los sujetos y objetos en el sistema, y con un conjunto de reglas que permitan determinar qué sujetos pueden acceder a qué objetos.

Los sistemas por los que fluya información sensible deben poner en práctica políticas de acceso no-discrecional.

Entre los requisitos de adecuación, y por lo que se refiere a la seguridad, el sistema debe contener mecanismos que puedan ser evaluados independientemente.

Por lo que se refiere a la protección continua, los mecanismos que llevan a cabo estos requisitos básicos deben estar continuamente protegidos contra ataques o alteraciones no autorizadas. Ningún sistema se puede considerar seguro si sus mecanismos de seguridad son susceptibles de ser destruidos o modificados.

La política de seguridad, como conjunto de directrices generales que deben guiar la seguridad de la información, es uno de los componentes más importantes de la arquitectura de seguridad de un sistema. Su materialización requiere la previa transformación en un modelo de seguridad, que puede ser expresado en lenguaje matemático.

La política de seguridad se ha de centrar en resaltar el carácter de la información como activo de la organización y su necesidad de ser protegido.

Para ello es necesario implantar una cultura de seguridad que permita una toma de conciencia y mentalización de toda la organización, sobre la importancia de la información como activo de la misma y sobre la necesidad de tomar medidas al respecto.

De igual modo debe contemplar la organización y funciones, obligaciones y responsabilidades, de una administración de seguridad de la información, así como los canales de comunicación a utilizar.

Esta política ha de definir las normas de protección de la información y establecer la estructura de recursos materiales, humanos y organizativos, con definición de funciones, para hacer frente a dicha protección; así como definir los procedimientos para la determinación de cualquier tipo de medidas de seguridad a tomar y la tecnología a utilizar, con especial referencia a la protección criptológica.

Una organización puede tener, en sus diversos niveles, diferentes políticas de seguridad, que no serían contradictorias sino complementarias

entre sí. E incluso, en un mismo nivel se pueden establecer diferentes políticas.

Ademas de las políticas administrativas que se llevan a cabo a través de procedimientos de este tipo, los grupos fundamentales de políticas de seguridad de la información se centran en el control de accesos y el flujo de información.

Las políticas de control de accesos establecen en qué circunstancias un sujeto puede acceder a un objeto de información. Dentro de ellas y como polos opuestos está el conocido principio de *"Need-to-Know"* (necesidad de conocer), según el cual un usuario accede estrictamente a aquellos objetos de información que necesita conocer para la realización de su trabajo; frente al principio de máximo privilegio, escasamente aplicado, según el cual se tendría acceso a un amplio objeto de información.

Las políticas de control de flujo se ocupan de la utilización que se da a la información a la que se ha tenido acceso. Se ocupan de la difusión de la información obtenida, con indicación de los canales permitidos para la difusión de la misma.

Una política de control de flujos ha de establecer el orden de prioridad que ha de darse a cada una de las tres características de la seguridad: confidencialidad, integridad y disponibilidad. Indicando claramente si se debe potenciar el secreto, la evitación de modificaciones no autorizadas o la destrucción de información.

Los organismos vinculados a la seguridad y a la defensa se decantan por potenciar, sobre todo, la confidencialidad, seguida de la disponibilidad y la integridad. Mientras que los sectores gubernamentales no defensivos ni de seguridad se preocupan en primer lugar de la integridad seguida de la confidencialidad y la disponibilidad; y los sectores económicos ponen el acento en primer lugar en la integridad, seguido de la disponibilidad y sólo en tercer lugar consideran la confidencialidad.

Los principios básicos inspiradores de una política criptológica nacional, que abarque todas las necesidades, tanto públicas como privadas, y su complejo entramado de relaciones, podrían ser los siguientes:

1.- PRINCIPIOS DE CARÁCTER GENERAL.

I.- NECESIDAD DE PROTEGER.

El uso de la criptología se justifica cuando se necesitan proteger informaciones que por una u otra razón tienen un carácter selectivo y sólo deben ser conocidas por determinados destinatarios, por lo que para transmitirlas, los corresponsales precisan disponer de entornos que proporcionen protección eficaz y confianza. Pero sólo se legitima cuando los intereses que subyacen bajo las informaciones necesitadas de protección son lícitos.

La necesidad de proteger requiere, como paso previo, un acto de calificación del carácter selectivo de la información, lo que se conoce como "clasificación", con las categorías que cada organización determine. Las

clasificaciones vienen a configurar ámbitos de confidencialidad en cuya garantía y protección opera la criptología.

La necesidad de protección -y consiguientemente el uso de la criptología- en determinados ámbitos de confidencialidad puede llegar a configurar un deber de proteger al nivel adecuado, jurídicamente exigible.

II.- PROPORCIONALIDAD.

Los niveles, procedimientos, organización, medidas y costes deberán ser proporcionales a la gravedad, probabilidad y amplitud de los eventuales perjuicios, en función del sistema de información a que se refieran y el entorno en el que operen.

Con distinción entre los sectores gubernamentales, económicos e industriales y redes públicas; prestando una especial atención a las diferencias de requerimientos en los sectores gubernamentales relacionados con la seguridad y la defensa y las redes públicas de comunicación, que responden a principios radicalmente distintos: el de máximo nivel internacional de protección, el primero y el de protección sistemática, el segundo.

III.- INTERDISCIPLINARIEDAD.

Los procedimientos, medidas, normas, equipos y sistemas para la protección criptológica de la información deberán ser concebidos desde una perspectiva interdisciplinar; teniendo en cuenta todos los puntos de vista implicados, ya sean políticos, económicos, técnicos, jurídicos, culturales,

industriales o defensivos, que afecten a la organización, la explotación, la educación o el derecho.

IV.- CONCIENCIACIÓN.

Para una efectiva implantación y confianza en los sistemas de protección criptológica, la sociedad en general y especialmente los diseñadores, fabricantes y usuarios, deberán percibir los riesgos que amenazan los sistemas de información, así como sentir la necesidad de protegerse de ellos y conocer los medios disponibles para llevarlo a cabo de forma real y efectiva, en los distintos ámbitos.

Todo ello de un modo que sea compatible con la seguridad.

2.- PRINCIPIOS DE CARÁCTER SOCIOLÓGICO.

V.- SOCIALIDAD.

En el nuevo espacio comunicativo creado por las tecnologías de la información y las comunicaciones, la criptología actúa como factor de equilibrio y elemento de socialidad, contribuyendo a preservar, en el ámbito comunicativo, los lugares del individuo y las organizaciones dentro del sistema, nacional o supranacional, en el marco de la globalidad.

La criptología brinda a la tecnología, la posibilidad de reparar, por sus medios, el desequilibrio que su aplicación introduce en la socialidad y se convierte en instrumento imprescindible para la eficacia de la ordenación social.

VI.- EQUILIBRIO.

La protección criptológica de la información se justifica en función de los intereses que protege, los cuales tienen en algunos casos aspectos comunes, pero también, pueden responder a principios distintos, se desarrollan con criterios diferentes e, incluso, pueden llegar a ser contrapuestos; por lo que es necesario armonizar las necesidades de utilización de la criptología en los distintos ámbitos entre sí y con los demás intereses que entran en juego en la vida del Estado y de la sociedad en su conjunto, y dar una respuesta general a las necesidades criptológicas, al nivel adecuado, con garantías de eficacia en la protección de todos los intereses, derechos y libertades en presencia.

Cualquier política criptológica, para ser eficaz, debe saber conciliar los distintos intereses que entran en juego y lograr un equilibrio entre la protección de la vida privada, la integridad de las personas, la protección de los derechos y libertades fundamentales, el funcionamiento de la industria y el comercio, el respeto a la ley y la seguridad nacional.

3.- PRINCIPIOS DE CARÁCTER POLÍTICO.

VII.- INTERNACIONALIDAD.

Vivimos en un mundo de relaciones que se manifiestan como intercambios, conexiones o antagonismos. La internacionalidad implica contactos, relación y, por consiguiente, es una actividad comunicativa en sí misma.

En este contexto, la recíproca dependencia de los Estados en la vida internacional lleva a que cualquier solución nacional debe abordarse desde una perspectiva global; lo que es especialmente de aplicación a una política criptológica por cuanto supone para las relaciones comerciales, culturales o actos de cooperación, inscribibles en las relaciones de intercambio; para las acciones políticas y jurídicas, -especialmente las diplomáticas-, que constituyen relaciones de conexión; y los efectos de una política criptológica para todo el abanico de situaciones de crisis, incluida la guerra, que configuran las relaciones de antagonismo.

Todo ello, sin olvidar que una protección criptológica de las comunicaciones gubernamentales, eficaces frente a todos, señalan la línea divisoria entre dependencia exterior y soberanía, lo que no es óbice para la pertenencia a eventuales alianzas u organizaciones supranacionales concretas, que son realidades y ámbitos diferentes, con sus propias necesidades e intereses específicos -no necesariamente coincidentes en su totalidad con los de cada uno de los distintos Estados que las integran- y donde el aliado o socio puede ser un competidor político o económico.

VIII.- DEMOCRACIA.

La protección criptológica de la información debe ser, en todo caso, compatible con los principios inspiradores de una sociedad democrática, especialmente con las libertades de expresión e información y con la intimidad, expresados en textos y tratados internacionales y recogidos en la

Constitución Española de 1.978 y, además, debe ser instrumento para la garantía real y efectiva de derechos y libertades.

IX.- CONSENSO.

La solución omnicomprensiva en base al consenso de diversos sectores de la sociedad, propuesta por el Juez Warren de EE.UU., sigue siendo necesaria hoy. Pero solo la delimitación de ámbitos y niveles de confidencialidad es insuficiente.

Su protección real y efectiva en la era de la información añade exigencias que demandan ampliar el consenso, con la incorporación de tecnólogos y expertos en criptología y, entre todos, sentar las bases para una solución integral,[1] en un clima de confianza de toda la sociedad.

Por ello, tal vez sea conveniente la creación de un Grupo de Reflexión, análisis y seguimiento de una política criptológica nacional, integrado por parlamentarios, juristas, periodistas, politólogos, empresarios, tecnólogos, representantes de la Administración y de la universidad, y criptólogos.

4.- PRINCIPIOS DE CARÁCTER ORGANIZATIVO.

X.- UNIDAD EN LA DIVERSIDAD.

La política criptológica ha de ser concebida con un carácter plural y flexible, de forma que pueda cumplir las exigencias de las diversas organizaciones. Teniendo en cuenta que organizaciones diferentes pueden necesitar políticas distintas, que una organización puede tener, en sus

diversos niveles, diferentes políticas criptológicas. E incluso, que en un mismo nivel, se pueden establecer políticas diversas.

Todas ellas han de ser articuladas, de forma que sean complementarias entre sí, por lo que la política criptológica ha de ser abordada desde una visión global que permita tener una perspectiva de conjunto para, sin merma de la diversidad, no perder de referencia la unidad de acción que requiere un Plan Criptológico Nacional.

5.- PRINCIPIOS DE CARÁCTER JURÍDICO.

XI.- JURIDICIDAD.

La seguridad de la información y las comunicaciones y, por consiguiente, la criptología como medio para conseguirlo, han de ser consideradas, en sí mismas, como un bien jurídico digno de protección.

XII.- CARÁCTER REGLADO.

La criptología debe ser una actividad reglada. La política criptológica ha de materializarse en un marco regulador en el que se contemplen todos los aspectos esenciales de la misma. Debe ser explícita y bien definida, con identificación clara de todos los sujetos y objetos en el sistema de información y medios para protegerlo, así como un conjunto de reglas que permitan determinar qué sujetos pueden acceder a qué objetos y medidas para garantizarlo.

La insuficiencia normativa presente, debe dar paso a la elaboración de un corpus normativo, completo y global, que dé respuesta a las

necesidades legales derivadas del uso de la criptología, en un marco de libertad.

XIII.- RESPONSABILIDAD.

Deberán quedar claramente establecidas las responsabilidades de las organizaciones propietarias, profesionales que las apoyan, diseñadores, fabricantes y usuarios de sistemas de protección criptológica y demás afectados, al igual que han de ser garantizados los derechos de los usuarios de estos productos, sistemas, servicios y equipos.

XIV.- CONTROL.

Además de los límites derivados del carácter reglado que ha de tener el uso de la criptología y la legitimidad de su uso sólo cuando se necesitan proteger intereses lícitos; el alto riesgo para intereses, derechos y libertades que puede, eventualmente, comportar su no uso, uso inadecuado o abuso, en los entornos donde operan las nuevas tecnologías de la información y las comunicaciones, convierte a la criptología en "arma poderosa", que conviene controlar por los procedimientos habituales de una sociedad democrática, en garantía del individuo y del normal funcionamiento de la sociedad y del Estado.

Y, en este proceso, distinguir los ámbitos supra e interestatales, donde está en juego la propia subsistencia del Estado, su prestigio e intereses, donde se ha de operar con ausencia de controles exteriores, en base a los principios de soberanía e independencia, de aquellos otros

ámbitos de carácter infraestatal que tienen una directa relación con la sociedad, el individuo o agrupaciones de estos, y el funcionamiento y desarrollo armónico de una sociedad democrática.

La eficacia en el funcionamiento de ambos ámbitos demandas controles internos de naturaleza diferente.

6.- PRINCIPIOS DE CARÁCTER TÉCNICO.

XV.- INTEGRACIÓN.

Los procedimientos, medidas, equipos y sistemas criptológicos deberán ser coordinados entre sí, y con las demás medidas y procedimientos de protección de la organización a que se refiera, de modo que se cree un dispositivo coherente de seguridad.

Los métodos critológicos destinados a determinados ámbitos han de ser interoperables para permitir funcionar conjuntamente.

XVI.- OPORTUNIDAD.

El sector público y privado, tanto en el plano nacional como en el internacional, deberían actuar en el momento oportuno de manera coordinada con el fin de estar protegidos criptológicamente al nivel adecuado en cada momento, en función de los desarrollos tecnológicos y amenazas existentes.

Y, en términos generales, ser conscientes que se ha alcanzado una etapa crítica en la evolución de la tecnología y en las necesidades de protección en los distintos ámbitos afectados, que demandan soluciones, y

que, en estas circunstancias, solo se requiere una voluntad política que impulse la búsqueda de las más adecuadas.

XVII.- REEVALUACIÓN.

Las medidas de protección criptológicas deberán ser reevaluadas periódicamente, dado que su grado de eficacia no es estático, sino que varía a lo largo del tiempo en función del nivel de desarrollo del criptoanálisis y la tecnología.

XVIII.- NIVEL ADECUADO.

Del principio general de la transparencia que rige en las informaciones públicas deviene el carácter excepcional del secreto; pero de su naturaleza y entorno, así como de las graves consecuencias de la violación de determinadas informaciones públicas, se deriva que el grado e intensidad de la protección criptológica ha de ser del máximo nivel, sobre todo en lo relativo a la protección de secretos oficiales.

El principio general del secreto que rige en las comunicaciones privadas, cuya excepcionalidad sería la transparencia, -con la necesidad de resolución judicial motivada-, tiene como correlativo la necesidad de una protección criptológica sistemática de nivel suficiente.

XIX.- PROFESIONALIDAD.

El diseño, organización y gestión de redes o sistemas que incorporen el uso de procedimientos criptográficos, al igual que la formación, instrucción y auditorías en materia criptológica, deberán estar bajo la

dirección y responsabilidad de profesionales habilitados al efecto como garantía de eficacia.

7.- PRINCIPIOS DE CARÁCTER MORAL.

XX.- ÉTICA.

La utilización de medidas criptológicas ha de ser concebida como un instrumento de garantía efectiva de derechos, libertades e intereses; por lo que debe respetar, en todo caso, los legítimos intereses de terceros y las normas de sana convivencia, evitando contribuir a la implantación de una cultura del secretismo y la opacidad.

XXI.- LIBERTAD.

Los usuarios de Criptología deben tener libertad, respetando las leyes, para determinar el tipo y nivel de seguridad de sus datos y seleccionar y aplicar los métodos criptológicos apropiados, incluyendo un sistema de gestión de claves que se ajuste a sus necesidades.

Los controles públicos sobre la Criptología deberán ser los imprescindibles para el ejercicio de las responsabilidades destinadas a la preservación de los intereses generales.

XXII.- CORDURA.

La complejidad tecnológica y jurídica y los importantes efectos políticos y sociales que comportan las garantías de libertad y seguridad de las comunicaciones, en la moderna sociedad de la información, con la utilización de la criptología como instrumento para conseguirlo, ponen de

plena actualidad las palabras de Bertrand Russel, para quien "cada avance en la técnica exige, si lo que se quiere es producir un aumento y no una disminución de la felicidad humana, un aumento correlativo de cordura".

5.1.2.- BASES PARA UNA REGULACIÓN SISTEMÁTICA DE LA PROTECCIÓN CRIPTOLÓGICA.

Con fundamento en los principios inspiradores de una política criptológica, indicados anteriormente, y como paso previo a la articulación normativa, dentro de la pluralidad de opciones posibles; las bases para una regulación sistemática de la protección criptológica constituirían el punto de referencia para elaborar un corpus normativo que contemple, con la amplitud necesaria, una regulación completa y sistemática de la protección criptológica a nivel nacional.

I.- ANÁLISIS DE RIESGOS

BASE 1ª.- Análisis y gestión de riesgos.

La exigencia previa para la eficacia de la protección criptológica de un sistema de información, requiere la determinación de los riesgos a que está sometido y una apreciación completa y conjunta de las necesidades criptológicas, encuadradas dentro del marco general de necesidades de seguridad de la información.

Mediante el análisis de los riesgos se puede conocer la vulnerabilidad criptológica del sistema y prever los efectos potenciales que podrían derivarse, identificando y justificando las medidas criptológicas a adoptar.

El análisis y gestión de riesgos es un presupuesto básico para la implantación de una protección criptológica efectiva de cualquier organización, teniendo en cuenta que son múltiples las organizaciones afectadas por una política criptológica y que son variadas las exigencias.

Teniendo en cuenta una serie de conceptos básicos que afectan a cualquier organización, con independencia de su tipo y naturaleza.

1.- Necesidad de conocer las amenazas y estimar las pérdidas potenciales que se producirían en caso de materializarse.

2.- Conocer los activos de información que deben ser protegidos y, especialmente los que requieren medidas criptológicas, teniendo en cuenta los entornos en que se captan, procesan, almacenan, transmiten y distribuyen dichos activos.

3.- La evaluación de análisis de riesgos aplicando métodos cuantitativos y cualitativos, como base para la determinación de una adecuada gestión de los mismos.

4.- La evaluación de análisis de riesgos debe estar concebida como un conjunto de actividades encaminadas a determinar las soluciones criptológicas basadas en una adecuada relación del coste y la eficacia.

5.- Configurar el análisis y evaluación de riesgos de forma que, de su resultado, se pueda percibir las medidas criptológicas a utilizar, con asignación de medios, niveles y sistemas de gestión de claves.

6.- Distinguir en el análisis y gestión de riesgos, los efectuados en la fase de diseño y los que se realizan durante el funcionamiento de los sistemas de información.

7.- El análisis y gestión de riesgos asociados con la vulnerabilidad de los sistemas de información y afines.

II.- APRECIACIÓN COMPLETA DE NECESIDADES

BASE 2ª.- Necesidades de usuarios.

Elaborar una clasificación completa de necesidades de los distintos usuarios, ya sean públicos o privados, y sus relaciones con las medidas de seguridad de la información.

BASE 3ª.- Necesidades jurídicas.

A la vista de una valoración de las tendencias, en general, y la evaluación de la tecnología, es necesario determinar un catálogo de necesidades jurídicas, con indicación de medidas legislativas, reglamentarias, normas y procedimientos, atendiendo a todos los sectores afectados.

BASE 4ª.- Necesidades organizativas.

Las medidas organizativas no son indiferentes para el logro eficaz de una protección completa de la información, así como un adecuado sistema

de protección criptológica. De forma que un sistema altamente sofisticado puede perder su eficacia por unos inadecuados procedimientos operativos, organizativos y de gestión.

Por todo ello, resulta imprescindible establecer un Catálogo de necesidades organizativas que den respuesta a los distintos ámbitos de protección.

BASE 5ª.- Necesidades tecnológicas.

El catálogo de necesidades tecnológicas permitirá conocer las exigencias y niveles tecnológicos básicos sobre los que articular de una forma efectiva una política criptológica.

BASE 6ª.- Necesidades criptológicas.

En función de los ámbitos de confidencialidad, las posibilidades jurídicas, disponibilidades organizativas y exigencias tecnológicas, y realidades nacionales e internacionales, determinar un amplio catálogo de necesidades criptológicas.

BASE 7ª.- Necesidades terminológicas.

La terminología como medio para explicar la realidad es un elemento que posibilita la comunicación. La Criptología necesita contar con un sistema conceptual y una metodología que dé respuesta a las necesidades derivadas de su implantación y desarrollo.

Además de la necesidad internacional de unificar e incluso crear términos y expresiones comunmente aceptados que permitan describir con

precisión los diferentes aspectos de la Criptología, en el ámbito nacional sería necesario incorporar a la regulación normativa sobre el uso de la criptología un amplio y detallado glosario de términos criptológicos.

III.- CONFIDENCIALIDAD

BASE 8ª.- Delimitación de ámbitos de confidencialidad.

El diseño y elaboración de una política criptológica requiere que la información sea clasificada según el grado de sensibilidad e importancia que la misma tenga para la organización y, en base a ello, definir la que debe ser protegida y con qué niveles, por lo que se deberían incluir los criterios necesarios para tal clasificación.

Por ello, en primer lugar, se ha de distinguir la información que merece ser protegida de la que no lo requiere. Dentro de la que necesita protección, señalar la que es vital para el funcionamiento de la organización a que se refiera, y altamente sensible, por su grado de confidencialidad y susceptibilidad de revelación, riesgo de modificación, o destrucción.

La clasificación de la información se ha de realizar independientemente del soporte en que se encuentre y determinará el nivel de protección que requiere.

IV.- MODELOS DE SEGURIDAD

BASE 9ª.- Articulación de modelos de seguridad.

El modelo de seguridad, como formulación teórica de una política de seguridad, expresable matemáticamente debe contener elementos suficientes

para que los diseñadores del sistema conozcan lo necesario para determinar los controles de seguridad a construir, para que los usuario puede utilizar eficazmente el mismo, y para que los evaluadores dispongan de los elementos suficientes que les permitan determinar su consistencia y adecuación a las políticas que pretende poner en práctica, así como la correcta implementación de todo ello.

La articulación de los modelos de seguridad deben realizarse con amplitud y flexibilidad, de forma que permita incorporar modelos de seguridad discrecional, seguridad obligatoria, multinivel y flujo de información, u otros que pudieran establecerse.

BASE 10ª.- Modelos criptológicos.

En el marco de los modelos de seguridad de la información, se han de articular los modelos criptológicos, que es la formulación teórica de una política criptológica expresable matemáticamente.

Los modelos criptológicos se implantan en el sistema de información en forma de medidas y mecanismos criptológicos, constituidos, especialmente, por los equipos y sistemas de cifrado.

La definición de una política criptológica requiere articularse de forma que permita el juego de los distintos modelos de criptológicos y su relación entre ellos, así como la interoperabilidad , como capacitad técnica para funcionar conjuntamente, de los que pertenecen a determinados ámbitos.

Los modelos criptológicos deben contener elementos y características suficientes que les permitan cumplir los requerimientos en criptología del modelo de seguridad al que pertenecen e incorporar la versatilidad necesaria para la adecuada utilización de los mismos.

Los modelos criptológicos deben incorporar posibilidades para establecer una eficaz y flexible protección criptológica de la información, en la que sea posible establecer:

1.- Control de accesos.

2.- Distintos niveles de seguridad -agrupando los algoritmos por niveles criptológicos y estableciendo el sistema de gestión de claves.

3.- Fijar diferentes niveles de confidencialidad.

4.- Establecer diversos grados de autoridad.

5.- Compatibilizar las posibilidades anteriores con la delimitación de diversas áreas de actividad.

6.- Combinar todas las posibilidades, con identificación, en su caso, de los modelos que reúnen unos u otros de estos requerimientos.

BASE 11ª.- Factores externos.

El establecimiento e implantación de cualquier política criptológica y la determinación de los modelos de cifra ha de tener siempre en cuenta las estructuras internacionales, cuestiones económicas, cuestiones políticas y constitucionales, preocupaciones sociales y posibilidades tecnológicas y legales.

V.- PLAN CRIPTOLÓGICO NACIONAL

BASE 12ª.- Plan Criptológico Nacional.

Con los resultados del análisis de riesgo y apreciación completa de necesidades, se ha de elaborar un Plan Criptológico Nacional que contemple las amenazas a que está sometido todo el sistema de información, en su conjunto, las específicas de cada ámbito, y las diversas soluciones criptológicas para neutralizarlas, con indicación de los posibles modelos criptológicos a utilizar, en su caso, así como sus problemas de aplicación.

Y dado el carácter estratégico de la Criptología, considerar el Plan Criptológico Nacional, como parte del Plan General de la Defensa Nacional.

BASE 13ª.- Ficha de criptología.

Cualquier sistema de información debe incorporar la ficha criptológica, indicativa de necesidades, forma de cubrirlas y modelo o modelos criptológicos recomendados.

VI.- ASPECTOS GENERALES

BASE 14ª.- Marco general.

Creación de un marco general para contribuir a la implantación de la criptología, como necesidad, tanto en el sector público como en el privado y suscitar la confianza y ventajas de su uso.

BASE 15ª.- Preocupaciones sociales.

Cualquier Plan Criptológico debe dar respuesta y confianza a las preocupaciones sociales y empresariales, protección de la intimidad y secreto de las comunicaciones, a todos los niveles.

BASE 16ª.- Concienciación.

Sensibilizar y tomar conciencia sobre los riesgos que amenazan los sistemas de información, la necesidad de protegerlos y los medios disponibles para llevarlo a cabo de forma real y efectiva.

BASE 17ª.- Criptología.

La Criptología como ciencia ha de ser fomentada en los ámbitos de investigación y desarrollo, y divulgado su uso con objeto de promover su utilización en la protección de secretos oficiales, intereses empresariales, y redes de comunicaciones, tanto en el plano nacional como internacional, como garantía eficaz de protección de derechos, intereses y libertades.

BASE 18ª.- Confianza.

Toda regulación sobre protección criptológica debe conseguir inspirar confianza en que el resultado está orientado a la protección de derechos, intereses y libertades, así como debe exhibir los controles perceptibles que para su logro se establezcan.

VII.- FORMACIÓN Y EDUCACIÓN

BASE 19ª.- Formación.

Favorecer una sensibilización a los imperativos y objetivos de la protección criptológica, mediante,

1.- La Formación de:

.Diseñadores de sistemas criptológicos.
.Fabricantes.
.Usuarios.
.Especialistas.
.Auditores.
.Autoridades encargadas de la aplicación de la ley.
.Policía.
.Fiscales.
.Jueces.
.Abogados.

2.- Educación e información de la sociedad en general.

Con todo ello, se trataría de evitar que el desconocimiento pueda llevar a alguna organización usuaria a tomar decisiones contrarias a la lógica de las exigencias de la protección necesaria.

VIII.- DETERMINACIÓN DE EQUIPOS Y SISTEMAS

BASE 20ª.- Medidas criptológicas.

Una vez definidos los modelos de seguridad; las medidas que permiten garantizar la confidencialidad, la disponibilidad y la integridad de la información son las de naturaleza criptológica.

BASE 21ª.- Determinación de equipos y sistemas. El análisis y gestión de riesgos, la apreciación completa de necesidades, la delimitación

de ámbitos de confidencialidad, el modelo de seguridad y criptológico, son elementos que determinan los equipos y sistemas de cifra a utilizar.

BASE 22ª.- Fabricación de equipos y sistemas criptológicos.

En el ámbito de la fabricación de equipos y sistemas criptológicos merece una especial atención los algoritmos de cifrado.

El Algoritmo Nacional de Cifra, es el que su realización, propiedad y garantía de seguridad pertenece al Estado Español.

Los países más avanzados, generalmente, disponen de algoritmos de cifra propios, normalmente secretos, para protección de la información clasificada en los ámbitos oficiales; lo que exige estar a los niveles tecnológicos y criptológicos más avanzados para que estos algoritmos sean eficaces frente a las amenazas provocadas por los modernos desarrollos tecnológicos procedentes del entorno internacional.

Todo ello hace necesaria una gran concentración de esfuerzos en áreas de la tecnología avanzada para que los sistemas criptológicos propios sean idóneos para aportar la protección necesaria, única forma de poder hablar con rigor de algoritmo nacional, sin menoscabo de la seguridad requerida y evitar que se pueda crear una situación de vulnerabilidad. Lo que obliga a que este algoritmo y los elementos de seguridad complementarios estén a la altura de los más potentes desarrollos criptológicos de los países más avanzados.

Lo que requiere la promoción y apoyo de iniciativas empresariales nacionales, fuertes, que en el marco tecnológico europeo, sean capaces de agruparse y desarrollarse frente a sus competidores internacionales.

IX.- MEDIDAS DE CARÁCTER JURÍDICO

BASE 23ª.- Regulación legal.

Elaboración de las disposiciones legales y reglamentarias que constituyan el marco normativo que dé respuesta a las necesidades legales del uso de la criptología en todas sus dimensiones.

BASE 24ª.- Carácter reglado de la criptología.

En una sociedad basada en el conocimiento, la información y las comunicaciones adquieren dimensión estratégica y su protección es un imperativo de seguridad.

El alto valor añadido que aporta el uso de la criptología a las modernas sociedades, en todas sus dimensiones, incluida la seguridad y la defensa, convierten a las claves criptográficas en objetivos prioritarios de cualquier ataque; unido a la gran transcendencia que para los derechos y libertades individuales puede comportar el abuso, mal uso, e incluso, la no utilización, de criptología en determinados casos, aconseja que el uso de productos criptológicos tenga un carácter reglado.

Corresponderá a una Comisión Nacional de Criptología, la determinación de los modelos criptológicos, equipos y sistemas de cifra, en su más amplio espectro, así como sus características técnicas y criptológicas

y sistemas de gestión de claves, que podrán ser utilizados en cada nivel de confidencialidad.

BASE 25ª.- Responsabilidades.

Una de las exigencias para la eficacia de cualquier estructura normativa es la determinación precisa de los riesgos y la responsabilidad en casos de fallos en la protección.

BASE 26ª.- Sanciones.

Sanciones en caso de violaciones, negligencias o utilización abusiva de la criptología.

BASE 27ª.- Competencia jurisdiccional.

La alta sofisticación de las medidas criptológicas y sus inmensas posibilidades para influir en derechos y libertades y en la vida de relación comercial, aconsejan establecer una clara delimitación entre las competencias jurisdiccionales y las administrativas.

Es previsible el aumento del número de causas que dependen de la "evidencia criptológica", por lo que resultará determinante para una justa solución del proceso conocer cómo analizar y juzgar esas pruebas criptológicas en los casos de controversia y, eventualmente, pensar en juzgados especializados que entiendan de las causas relacionadas con las nuevas tecnologías, donde los conflictos relacionados con las evidencias criptológicas tendrán una presencia creciente.

BASE 28ª.- Pruebas.

Modalidades de obtención y valoración de pruebas cuando se utiliza la protección criptológica , con inclusión y regulación, en su caso, de la pericial criptológica que permita poner de relieve "la evidencia criptológica", en los casos que proceda.

Los aspectos jurídicos de la valoración de los documentos y firmas digitales, que pueden constituir prueba en un proceso judicial y transmitidos con protección criptológica, han de ser determinados; ya que se considera, en ámbitos criptológicos, que la firma digital tiene una capacidad superior a la manuscrita, al no incorporar sólo la autenticidad del documento firmado, sino su integridad.

BASE 29ª.- Colaboración.

Normas de consulta, coordinación y colaboración entre el sector público y el sector privado, administraciones entre sí, tanto en el ámbito nacional como internacional.

BASE 30ª.- Elección de algoritmos.

Marco en el que se ha de desarrollar el ejercicio de la libertad de elección de algoritmos, equipos y sistemas de cifra y de gestión de claves, teniendo en cuenta el carácter reglado de la Criptología.

BASE 31ª.- Garantías de uso de la criptología.

Establecer procedimientos adecuados para garantizar el respeto de los derechos y reparación de las violaciones derivadas de la utilización, no

utilización o mal uso de la Criptología. Teniendo en cuenta, en todo caso, que la Criptología no puede amparar el abuso del derecho o el ejercicio antisocial del mismo.

BASE 32ª.- Extraterritorialidad.

El carácter internacional de las comunicaciones requiere un esfuerzo para la determinación de la ley aplicable en el caso de comunicaciones con protección criptológica.

Con independencia de la conveniencia de avanzar hacia un marco jurídico internacional, en principio, se podría establecer el sometimiento a la ley de origen de la comunicación.

BASE 33ª.- Instituciones.

Establecer procedimientos y crear o estimular la creación, en su caso, de instituciones jurídicas, administrativas, públicas o privadas, nacionales o internacionales, de cualquier naturaleza, para promover y mantener la implantación, seguimiento, aplicación y uso de la criptología y, general la protección de los sistemas de información y comunicaciones.

Dentro de las instituciones y en el caso de que se opte para la cifra comercial por la modalidad de "claves depositadas", establecer con claridad los criterios para acceder a la condición de "autoridad de certificación".

X.- MEDIDAS DE CARÁCTER ADMINISTRATIVO

BASE 34ª.- Cooperación entre Administraciones.

La complejidad de la Criptología exige esfuerzos de cooperación y asistencia mutua entre Administraciones.

BASE 35ª.- Apoyo técnico.

El elevado componente técnico y la complejidad de la Criptología, requiere disponer de un apoyo técnico criptológico a las organizaciones usuarias públicas o privadas que lo requieran, y a los órganos jurisdiccionales, como forma de hacer posible la efectiva aplicación de una política criptológica.

BASE 36ª.- Organización.

Para abordar una implantación efectiva de un Plan Nacional de Criptología resulta necesario prestar especial atención a los aspectos organizativos, de infraestructuras administrativas. y profesionales.

BASE 37ª.- Infraestructuras.

Dotación de infraestructuras adecuadas, de carácter físico, lógico, tecnológico, criptológico y especialmente en comunicaciones, con inclusión de medios materiales y humanos.

BASE 38ª.- Medidas de seguridad en los distintos sectores.

Medidas de seguridad en los distintos sectores y su efectiva aplicación, en función de las necesidades de las diferentes áreas de aplicación.

BASE 39ª.- Organismo específico.

El Centro Criptológico Nacional ha de ser el embrión sobre el que se articule una Agencia Nacional para la Seguridad de la Información como organismo especializado dependiente de la Presidencia del Gobierno; o, eventualmente, de un Departamento Ministerial específico para la Información y la Seguridad, que con la participación de los sectores afectados aborde el estudio de la regulación de todo el sector de la seguridad de la información y las comunicaciones, con especial atención a la criptología, aplicando rigurosos criterios técnicos, jurídicos y políticos.

Sea órgano de coordinación interministerial y fije niveles y medidas de seguridad y determine modelos, distinguiendo ámbitos públicos y privados necesitados de protección.

De igual modo sería órgano de homologación de equipos y sistemas y autoridad nacional de certificación -con funciones de coordinación de las distintas autoridades de certificación-, de asesoramiento, estudio e investigación, así como delimitaría los ámbitos generales y específicos a los que se aplicarían medidas de seguridad de la información, con indicación de los niveles apropiados.

Tanto el Centro Criptológico Nacional existente, o la Autoridad Nacional de Seguridad prevista en el Proyecto de Ley de Secretos Oficiales, una Agencia Nacional para la Seguridad de la Información, u otros organismos que pudieran surgir, tal vez se deberían orientar en la dirección

de dar respuesta a todos los problemas derivados de las necesidades de seguridad de la información.

BASE 40ª.- Procedimientos.

Las normas, procedimientos y principios generales, deben ser reunidos en un manual que, sin perjuicio de la necesaria seguridad, dé a conocer todo lo necesario para una eficaz utilización del Plan Criptológico Nacional en su conjunto y del sistema específico al que pertenezca el usuario.

BASE 41ª.- Niveles criptológicos.

Los niveles de protección criptológica de un criptosistema, expresados a través de la consistencia de los algoritmos matemáticos como factor esencial, han de ser proporcionales a las amenazas a que está sometido.

La variedad de amenazas conlleva la conveniencia de una clasificación y agrupamiento de la información en función de la intensidad y alcance de las amenazas para poder neutralizarlas con los medios apropiados. De donde se deriva la necesidad correlativa de una clasificación de la protección criptológica, asignándole el nivel adecuado, proporcional que evite una exposición del sistema de información a que se refiera a riesgos innecesarios por utilización de bajos niveles y, por otro lado, evite un exceso de protección, asignando potentes y sofisticados sistemas, de alto coste, para protegerse de amenazas de escasa entidad.

Mediante el establecimiento de modelos de seguridad, determinar los distintos grados de amenazas y a los que, previo agrupamiento por niveles, se les asignaría su correlativo de protección criptológica.

En este proceso, distinguir entre grupos abiertos y grupos cerrados de usuarios, prestando especial atención a la elaboración de procedimientos, normas y productos, para garantizar la seguridad de la información en las redes públicas de comunicaciones, las que protejan intereses comerciales y empresariales, y en los sectores relacionados con la seguridad y la defensa.

BASE 42ª.- Gestión de claves.

Dentro del Plan Criptológico Nacional se debe prestar una especial atención a los sistemas de gestión de claves, como uno de los puntos centrales de la seguridad de los modernos sistemas de cifra y vía de acceso legal en los casos de los sistemas criptológicos que lo contemplen.

BASE 43ª.- Cooperación.

Promover la cooperación entre el sector público y sector privado, universidad, empresa y sociedad, tanto a nivel nacional como internacional.

BASE 44ª.- Exportación e importación de productos criptológicos.

Con independencia de la libertad de comercio en los productos criptológicos, el carácter reglado de la Criptología aconseja establecer normas detalladas para la importación y exportación de equipos y sistemas de cifra en base a las potencias de sus algoritmos, en el marco de la normativa comunitaria.

BASE 45ª.- Adquisiciones.

La adquisición de equipos y sistemas de Criptología suma a las exigencias de los productos de alto componente tecnológico un elemento añadido de seguridad que se constituye en factor determinante.

La tecnología sin el soporte de una adecuada organización puede llegar a producir resultados contrarios a los deseados o, en el mejor de los casos, obtener resultados poco significativos en relación a sus potencialidades, que no justificarían su incorporación; este aspecto en el campo de la Criptología se hace especialmente patente.

La Criptología, actualmente, está muy tecnologizada y los más sofisticados sistemas pueden resultar inútiles si no disponen de una organización que los explote adecuadamente.

Pero la adquisición de Criptología, superado los requerimientos tecnológicos, exige sobre todo confianza, por lo que no es indiferente una clasificación dinámica de proveedores de estos sistemas que, además de la homologación tecnológica y criptológica de sus productos, incorporen el factor confianza, dentro del cual el *"Who is who"* (quién es quién) de suministradores y usuarios resulta esencial.

Hoy, y con este tipo de tecnologías, no sólo es necesario conocer a quién se compra, sino, a quién se vende.

Cuando así se considere en la correspondiente norma, la adquisición de equipos y sistemas criptológicos, de determinados niveles, podría estar regulada.

XI.- EVALUACIÓN, AUDITORIA Y CONTROL

BASE 46ª.- Criterios de evaluación.

En toda organización se ha de establecer un sistema de auditoría permanente de valoración y eficacia de la política de seguridad y política criptológica, sus procedimientos y gestión, con indicación de los criterios a utilizar para determinar la adecuación de los modelos, equipos y sistemas criptológicos, normas y procedimientos, a la satisfacción de las necesidades en materia de seguridad y grado de fiabilidad de los mismos.

BASE 47ª.- Control.

Partiendo de la base que corresponde a los poderes públicos promover las condiciones para que la libertad y la igualdad del individuo y de los grupos en que se integra sean reales y efectivas; así como que le corresponde remover los obstáculos que impidan o dificulten su plenitud; serán los poderes públicos los que deben crear las condiciones para la protección criptológica de la información, como una manifestación concreta de esa libertad.

La alta potencialidad de las nuevas tecnologías, las comunicaciones y un inadecuado uso de su protección, para la vulneración de derechos y

libertades, así como la exigencia de fiabilidad que todas ellas demandan para su plena implantación, requiere el establecimiento de los controles necesarios.

¿ Pero, quien debe controlar la seguridad de la información?.

La enorme complejidad y alta sensibilidad de los intereses en juego, así como la gran concentración de poder que comporta, exige que una política criptológica incorpore pluralidad de controles, entre los que podrían estar:

1.- Un ***control político*** a través de una Comisión parlamentaria específica sobre seguridad de la información.

2.- El ***Defensor del Pueblo*** como alto comisionado de las Cortes Generales, designado por estas para la defensa de los derechos y libertades puede supervisar la actividad de las Administraciones respecto a la garantías del secreto de las comunicaciones, dando cuenta a las Cortes Generales.

3.- El Juez es el único que puede excepcionar la garantía del secreto de las comunicaciones y, por consiguiente le corresponde que en condiciones de normalidad este derecho se respete. A través del Juez ordinario o de un órgano jurisdiccional específico, se ha de establecer un ***control judicial*** sobre la seguridad de las comunicaciones.

4.- La ***Agencia de Protección de Datos***, en lo que se refiere al ámbito específico de los datos de carácter personal.

5.- Las Administraciones públicas, en el ámbito de sus respectivas responsabilidades han de establecer los necesarios ***controles administrativos*** sobre la seguridad de la información.

6.- Dada la alta tecnologización de la seguridad de la información y la complejidad de la Criptología, así como de las redes de comunicaciones; todos los controles anteriormente indicados, para ser efectivos requieren contar con un apoyo de alto nivel tecnológico, lo que permitiría controlar de forma real la aplicación de una política criptológica, que constituiría el ***control técnico***.

BASE 48ª.- Utilización de criptología.

Con objeto de conocer las posibilidades y recomendar su utilización, un Plan Criptológico Nacional debería incorporar los distintos ámbitos de actividad que deben incorporar protecciones criptológicas y niveles aconsejables.

XII.- MEDIDAS DE CARÁCTER TÉCNICO

BASE 49ª.- Arquitecturas de seguridad.

Orientaciones claras para arquitecturas de seguridad físicas, lógicas y criptológicas.

Determinación del modelo criptológico.

Tipos de cifrado.

Elección de algoritmos.

Elección de equipos y sistemas de cifrado.

Diseño de la red. (en su caso).

Protección adicionales (TEMPEST etc.).

BASE 50ª.- Acceso a las claves.

La regulación de la gestión de claves ha de estar claramente establecida y en ella se ha de precisar y posibilitar técnicamente, quien, para qué y en qué circunstancias se tiene acceso a las claves, lo que debe estar establecido por ley.

BASE 51ª.- Armonización normativa.

La regulación de la Criptología recomienda una armonización con las normas técnicas y métodos internacionales que permita a la protección criptológica nacional operar en un contexto armonizado con el exterior.

BASE 52ª.- Competencias técnicas.

Igualmente se requiere el desarrollo y determinación de las competencias técnicas y reglas de actuación claras y precisas.

BASE 53ª.- Claves y algoritmos de cifra.

El carácter reglado de la Criptología y la diversidad de niveles existentes, así como la influencia en la potencia de sus algoritmos de la longitud de claves, aconseja hacer referencia a estos parámetros.

BASE 54ª.- Homologación.

Desde el punto de vista técnico se hace aconsejable, antes de asignar su utilización a determinado modelo, proceder a una homologación de los modelos, equipos y sistemas de cifrado.

BASE 55ª.- Investigación y desarrollo.

Estudio e investigación sistemática como requisito esencial para elaborar medidas apropiadas y eficaces, y mantenimiento y mejora del nivel tecnológico y criptológico.

XIII.- HABILITACIÓN PROFESIONAL

BASE 56ª.- Profesionalidad.

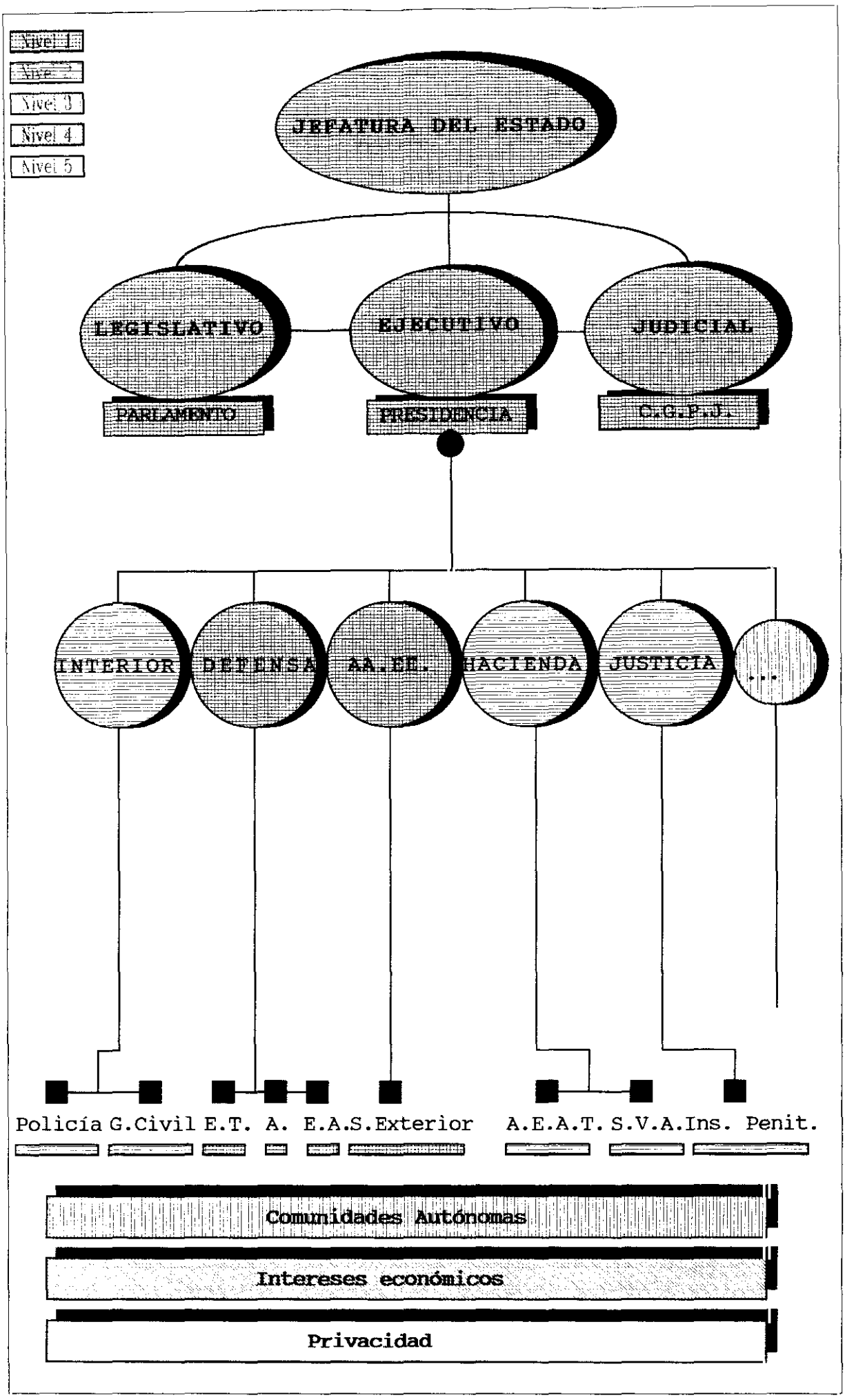
Solo los profesionales pueden evaluar la resistencia de un sistema de cifra. Por consiguiente se han de establecer de forma clara y precisa los profesionales habilitados para intervenir en los distintos aspectos que comporta una protección criptológica, tanto en el diseño y dirección de redes y organizaciones que incorporen criptología, como adquisición de equipos y sistemas, criptoanálisis y autoridades de certificación, estableciendo, en su caso, la titulación correspondiente.

XIV.- EMERGENCIA

BASE 57ª.- Planes de emergencia.

Las situaciones de crisis y catástrofes, requieren el establecimiento de sistemas alternativos que permitan garantizar la protección criptológica en cualquier situación.

En todo caso, es aconsejable establecer normas que permitan prevenir que el desastre ocurra, y recuperarse, mediante el establecimiento de un plan específico, o la elaboración criptológica de mecanismos de emergencia.


Nivel 1
Nivel 2
Nivel 3
Nivel 4
Nivel 5
JEFATURA DEL ESTADO
LEGISLATIVO
EJECUTIVO
JUDICIAL
PARLAMENTO
PRESIDENCIA
C.G.P.J.
INTERIOR
DEFENSA
AA.EE.
HACIENDA
JUSTICIA
...
Policía
G.Civil
E.T.
A.
E.A.S.Exterior
A.E.A.T.
S.V.A.
Ins. Penit.
Comunidades Autónomas
Intereses económicos
Privacidad

EPILOGO

El creciente carácter mundial de la tecnología, hace que la política de un país respecto a la información sea motivo de preocupación para otros. La información se está haciendo mundial y cada vez es más difícil retenerla dentro de las fronteras nacionales.[2]

Las incidencias del desarrollo tecnológico -con el apoyo de las telecomunicaciones- mueven a plantear, también, la duda de la soberanía de los Estados, que no son soberanos en el estricto sentido del término, sino dentro de unas limitaciones que estarían fundadas en la necesidad de las relaciones con otros Estados mediante los tratados internacionales o las normas de apoyo, reciprocidad y subsidiaridad.

La organización de diferentes centros de actividad, con efectos para las sociedades y los individuos, con la unión de actuaciones distintas que se salen de un orden jurídico y social establecido, viene a cuestionar la validez y eficacia del Estado moderno en el que sus pilares están empezando a fallar.

El Estado, como orden social y forma de convivencia solidaria no es único, ya que es factible que se abra el camino a nuevas normas de convivencia donde pueda existir esa solidaridad, situación en la que el derecho tendría un ámbito distinto, y en ese derecho se plantearía también la delimitación geográfica del ámbito. Podría tratarse de una delimitación flexible, cambiante por diferentes intereses y movida en una regulación teórica de necesidades que pudieran no coincidir, en diferentes aspectos, con las estrictamente sociales.

Se podría llegar a plantear una reducción en las normas tradicionales, dejándolas centradas en las mínimas necesarias; al tiempo que se desarrollarían códigos universales de conducta, bajo principios éticos en las diferentes áreas de actuación, basadas, tal vez, en lo que hoy llamamos principios generales del derecho; de forma que esas normas universales de convivencia, coexistan a su vez con otras normas de gobierno, tan extensas y precisas como fuese necesario, separando claramente el derecho que puede ser regulador de una situación social en un territorio determinado y bajo una soberanía estatal y el derecho que puede ser estructurado en una relación regional internacional, con aquellas normas mínimas que permitan la flexibilidad de adaptación a las circunstancias que lo condicionan, lo que se traduciría en una convivencia

de ordenamientos supranacional, estatal, regional y local, donde la ética jugaría un papel destacado en la fijación de unos principios básicos.

La globalización como expresión de la internacionalización de las redes y los sistemas es un hecho, pero también es una ideología que esconde la complejidad del nuevo orden mundial.

Para Brezinski, las "tecnotrónicas" habrían transformado el mundo en un "nudo de relaciones interdependientes, nerviosas, agitadas y tensas y habría aumentado la amenaza de anomia además del riesgo de aislamiento, y de soledad, para los individuos".

La "diplomacia de los cañones" pertenece al pasado y, según él, la del futuro será la "diplomacia de las redes".

Diplomacia de las redes en la que la preservación y defensa de los intereses nacionales pasa por el desarrollo e implantación de una basta red de comunicaciones, concebida con sentido estratégico, y dotada de potentes sistemas criptológicos capaces de proporcionar la seguridad necesaria, de forma que estén garantizados, el almacenaje, procesamiento, distribución, transmisión y protección de información en las condiciones que exige la acción exterior del Estado al entrar el siglo XXI.

El Pentágono estima que el mundo ha entrado en un "periodo de pausa estratégica", que podría durar hasta el año 2.010, en el que no parece probable que ningún país esté en condiciones de desafiar el papel de EE.UU. como única superpotencia. Sin embargo, sus analistas estiman que "el mundo sigue siendo un lugar peligroso y altamente inseguro", donde se prevén nacionalismos desatados que desemboquen en conflictos regionales, ataques terroristas con armas químicas o biológicas y delitos y sabotajes en las redes informáticas,[3] lo que demanda la necesidad de dispositivos flexibles y capaces, en condiciones de hacer frente a estas amenazas.

La libertad de expresión de los ciudadanos está en competencia directa con la libertad de expresión comercial, que genera una tensión entre la soberanía absoluta del consumidor y la voluntad de los ciudadanos.

A su vez, la libertad de expresión comercial es indisociable del principio de libre flujo de información, acuñado a principio de la guerra fría, que atribuye poca importancia a la desigualdad de los intercambios en materia de comunicaciones.[4]

De igual modo existen amenazas tecnológicas que se ciernen sobre las libertades públicas y el mundo económico libre con programas mundiales como Echelon.

En este contexto, la Criptología es un elemento de ordenación social de las relaciones llevadas a cabo por medio de las tecnologías de la información y las comunicaciones cuyos efectos se dejan sentir no solo en los Estados, sino en organizaciones supra e infraestatales y en el individuo.

Con independencia de la protección real y efectiva, a cualquier nivel, que ha de brindar la Criptología; en el mundo de relación internacional como factor de mutua confianza, fiabilidad y predecibilidad, en aras a una

convivencia pacífica, entre aliados cabría la posibilidad de estar en lo que podríamos denominar régimen de transparencia selectiva convenida, (o secretos compartidos); según el cual, un aliado estaría en condiciones de conocer la información que circula por determinadas redes de otro, actuando, potencialmente, como un corresponsal más.

Esta posibilidad derivada de las relaciones internacionales, no puede ser consecuencia de una situación tolerada, o admitida de hecho procedente de fragilidad organizativa, debilidad tecnológica, o vulnerabilidad criptológica; que supondría un grave atentado a la soberanía, y entraría en el ámbito del derecho penal,[5] sino que, por el contrario, en caso de darse; ha de ser una manifestación clara y expresa, precisamente de esa soberanía, que ha de implicar, necesariamente, la reciprocidad y la reversibilidad, esto es, la posibilidad, en un momento dado, de anularla, y, además, haber sido convenida por los procedimientos de las relaciones entre Estados, con todas las garantías jurídicas y operativas del caso. Para lo cual, es necesario que la transparencia selectiva convenida, se derive de una aplicación concreta de las posibilidades que, en estos y otros aspectos, brindan la Criptología y las nuevas tecnologías.

Jefferson, con madura reflexión, declaró que "no postulamos cambios frecuentes e improvisados en leyes y constituciones... Pero sabemos también que las leyes e instituciones deben ir emparejadas con el progreso de la mente humana... A medida que se realizan nuevos descubrimientos, se revelan nuevas verdades y cambian costumbres y opiniones con la mudanza de las circunstancias, las instituciones han de progresar también y mantenerse al ritmo de los tiempos".

Mucho más próximo a nuestros días, para Ralf Dahrendorf, "uno de los grandes logros de los cambios recientes ha sido la medida en que la esfera privada de los individuos ha sido puesta a reparo de los ojos y oídos de la ley. Y, por cierto, una de las grandes pérdidas de los recientes desarrollos técnicos ha sido la medida en que los ojos y los oídos de los organismos gubernamentales se han inmiscuido en esta esfera privada.

Hay aquí un nuevo espacio para la ley, que debe ser rellenado en interés de la libertad individual. Pero allí donde dicha contracción no ha tenido lugar -y no debería tener lugar, porque los fundamentos del contrato social están en juego- la ley pierde su credibilidad si no es aplicada. Entrar en esta "área prohibida" es un requisito de legitimidad".[6]

Dahrendorf, apuesta por que la clave para la reconstrucción de las modernas sociedades democráticas se hallaría en una construcción consciente de instituciones dotadas de sentido e inspiradas en principios racionales; y ello porque la experiencia histórica muestra como no es posible la libertad fuera de las instituciones.

La sociedad de la información es un concepto global, que exige medios de regulación también globales y, en este sentido, la criptología y el derecho como instrumentos de ordenación, adquieren especiales

dimensiones. La cuestión tal vez sea cómo "reequilibrar nuestro superdesarrollo tecnológico y nuestro subdesarrollo social".[7]

Todo ello demanda, eventualmente, una política criptológica internacional elaborada en base a principios comúnmente aceptados, que supere los criterios en los que se ha basado durante la "guerra fría", y aborde, eventualmente, la creación de una nueva organización internacional especializada, en el seno de Naciones Unidas, precedida de una convención internacional sobre tecnología, información, comunicaciones y seguridad, que sirva de foro para el establecimiento de una nueva ordenación internacional en las relaciones derivadas de la sociedad de la información, con elaboración de un marco, que de respuesta a las exigencias del mundo de postguerra fría y sea válido para la articulación normativa del orden político del siglo XXI. Mundo en el que una protección criptológica eficaz de las comunicaciones gubernamentales marcarán las línea divisoria entre dependencia exterior y soberanía e independencia nacional.

Semejante desarrollo, mediante sofisticadas tecnologías y complejas relaciones, abre a la humanidad posibilidades de una magnitud insospechada, que conviven con zonas de sombra, con ataques a la privacidad del individuo, en un mundo de relaciones donde se hacen especialmente necesarios y retoman fuerza los valores tradicionales del hombre.

Pensar en una estrategia para España requiere hacer una amplia y profunda prospección sobre los cambios culturales, la globalización de los procesos de producción y las nuevas tecnologías de la información y las comunicaciones; todo ello enmarcado en un proceso de complejización creciente de las relaciones políticas y sociales, donde la defensa de la sociedad y de las instituciones ha de compaginarse con el respeto de los derechos individuales, el crecimiento económico y la defensa del medio ambiente.

En lo político se combinan tendencias hacia formas de integración más extensas que respeten la personalidad de las unidades integradas, lo que viene a brindar un amplio juego de relaciones entre los distintos niveles.

A este proceso se vienen a sumar las nuevas tecnologías de la información como medios que contribuyen a reconfigurar los sistemas de poder y redes de relaciones, con efectos en las demás partes del sistema social. De tal forma, que las identidades en el futuro no serán campos territorialmente bloqueados, sino una forma particular de estar en relación. Los nuevos avances crean formas de espacios nuevos.

A la vez, las nuevas tecnologías permiten que la economía local sea competitiva y, en paralelo, la economía avanzada transfiere otras formas de producción al plano mundial. Esta doble tendencia tiene su reflejo en las

presiones políticas descentralizadoras que conviven con una irresistible tendencia a la supranacionalidad.

A la hora de pensar sobre España, o sobre cualquier otra organización política, ya sea nacional o supranacional, en el próximo milenio , hemos de pensar con conceptos políticos diferentes a los actuales y visualizar una realidad resultado de flujos de relaciones cambiantes, articulados en un orden que, sin perjuicio de disponer de una base territorial, será un espacio fluctuante de poder militar, económico, político, tecnológico y cultural que, conjuntamente con otros actores de naturaleza similar, podrán articular de forma compartida un ordenado sistema mundial.

Si queremos no perder el tren de la historia, y que España haga oir su voz en el proceso de producción de las nuevas normas universales, debemos asumir estas realidades y dotarnos de los medios de todo tipo que permitan abordar con solidez la nueva situación, convencidos que esa es la mejor forma de defender los intereses nacionales, en un mundo, donde se corre el riesgo de dilución, y donde muchas son la posibilidades, pero no menores las incertidumbres.

En todo caso, y sin llegar a considerar que el universo sea un gigantesco criptograma puesto en marcha por el Todopoderoso, como pretendió probar Newton, la grandeza de la situación que se abre ante la humanidad, por las inmensas posibilidades que brindan las nuevas tecnologías de la información y las comunicaciones, a pesar de sus riesgos, produce el íntimo convencimiento de que podemos albergar un futuro esperanzador confiando en el hombre y en la existencia de un Ser Superior.

[1] Molina Mateos, J.M., "Jornadas Interdisciplinares sobre Criptografía, Privacidad y Autodeterminación Informativa", Zaragoza, 1.995.
[2] Toffler, A., "El cambio del poder", Edit. Plaza & Janes, Barcelona, 1.990.
[3] The Washington Post, Borrador que esboza las líneas básicas de la defensa estratégica de EE.UU.,tomado de El País, 3 de abril de 1.997.
[4] Mattelart, A., "Los nuevos escenarios de la comunicación mundial", Le Monde diplomatique, octubre 1.996.
[5] España, Ley Orgániza, 10/1.995, de 23 denoviembre, del Código Penal, Título XXIII, "De los delitos de traición y contra la paz o la independencia del Estado, y relativos a la defensa nacional".
[6] Dahrendorf, r., "Ley y Orden", Edit. Cívitas, 1.994, traducción al castellano de Luis María Diez-Picazo, pág. 170.
[7] Castella, M., "La sociedad de la información", El País, 25 de febrero de 1.995.

APÉNDICE BIBLIOGRÁFICO

[1] ALAMILLO, F.,"EL SECRETO MÉDICO PROFESIONAL" ADPCP, MADRID,1.950.

[2] ALBACAR LÓPEZ, J.L., "LA PROTECCIÓN DE LOS DERECHOS FUNDAMENTALES EN LA NUEVA CONSTITUCIÓN ESPAÑOLA, MINISTERIO DEL INTERIOR, MADRID,1.979.

[3] ALBERDI ALONSO, C, "EL PODER JUDICIAL COMO GARANTE Y SUJETO DEL DERECHO A LA INFORMACIÓN", PODER JUDICIAL, NÚMERO ESPECIAL X, MADRID, 1.989.

[4] ALCOVER GARAU, G. "ASPECTOS JURÍDICOS DEL EDI: LA FIRMA ELECTRÓNICA", JORNADAS INTERDISCIPLINARES SOBRE CRIPTOGRAFÍA, PRIVACIDAD Y AUTODETERMINACIÓN INFORMATIVA, ZARAGOZA, 1.995.

[5] ALONSO ZALDÍVAR, C. Y CASTELL, M., "ESPAÑA FIN DE SIGLO", ALIANZA EDITORIAL, MADRID, 1.992.

[6] ALZAGA VILLAAMIL, O., "COMENTARIO SISTEMÁTICO A LA CONSTITUCIÓN ESPAÑOLA DE 1.978", MADRID, 1.978.

[7] AMAT, N., "DE LA INFORMACIÓN AL SABER", FUNDESCO, MADRID, 1.990.

[8] AMEDEO AULETTA, T., "RISERVATEZZA E TUTELA DELLA PERSONALITÀ", GIUFFRÈ, MILANO,1.978.

[9] ANGARITA BARON, C., "COLOMBIA: DERECHO A LA INTIMIDAD Y BANCOS DE DATOS PERSONALES. NOTAS PARA UNA PROPUESTA". UNIVERSIDAD DE LOS ANDES, BOGOTÁ, 1.987.

[10] ANTÓN Y ABAJO, A., "EL DELITO DE DESCUBRIMIENTO DE SECRETOS INDUSTRIALES". DOCTORAL LEIDA EN LA U.N.E.D., MADRID, 1.991.

[11] ARANGUREN, J.L., "ETICA Y POLÍTICA," GUADARRAMA, MADRID, 1.963 .

[12] AREITIO, J., "IDENTIFICACIÓN DE PARÁMETROS DE SEGURIDAD EN REDES DE ÁREA LOCAL", III REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA, BARCELONA, 1.994.

[13] ASOCIACION ESPAÑOLA DE CRIPTOLOGIA, REVISTA "CRIPTOSISTEMAS", MADRID, 1.996.

[14] ASSOCIATION DES ARCHIVISTES FRANÇAIS, "DROIT A L'INFORMATION, DROIT AU SECRET", LA COMMUNICATION DES ARCHIVES CONTEMPORAINES, PARIS, 1.985.

[15] BAJO FERNÁNDEZ, M., "PROTECCIÓN DEL HONOR Y DE LA INTIMIDAD", EN "COMENTARIOS A LA LEGISLACIÓN PENAL, DERECHO PENAL Y CONSTITUCIONAL", DIR. M. COBO DEL ROSAL, EDERSA, MADRID, 1.982.

[16] BAKER, K., "DATA SURVEILLANCE BILL", HMSO, LONDON,1.969.

[17] BALDASSARRE, A., "PRIVACY E COSTITUZIONE. L'ESPERIENZA STATUNITENSE", BULZONI, ROMA, 1.974.

[18] BAPTISTA PORTA, IO, "DE OCCULTIS LITERARUM NOTIS", EDICIÓN DE 1.593. EDICIÓN FACSÍMIL, UNIVERSIDAD DE ZARAGOZA, 1.995.

[19] BARBÉ, E., "RELACIONES INTERNACIONALES", TECNOS, MADRID, 1.995.

[20] BARREIRO, A.J., "EL DELITO DE REVELACIÓN DE SECRETOS (PROFESIONALES Y LABORALES)", LA LEY, AÑO XVII, Nº 4038, MADRID,1996.

[21] BARRERO ASENJO, P. "EL DERECHO A LA INFORMACIÓN, PRIMER DERECHO HUMANO", INFORMACION Y DERECHOS HUMANOS (DANIEL INNERARITY Y ARIES VAZ, EDITORES), PAMPLONA, 1.987.

[22] BARROSO ASENJO, P, "LÍMITES CONSTITUCIONALES DEL DERECHO A LA INFORMACIÓN", MITRE, BARCELONA, 1.984.

[23] BAUER, F.L., "DESCRYPTED SECRETS", METHODS AND MAXIMS OF CRYPTOLOGY, SPRINGER-VERLAG, BERLIN HEIDELBERG, 1.997.

[24] BECERRA PAEZ, J., "SEGURIDAD DE LAS COMUNICACIONES EN LA ALIANZA ATLÁNTICA", JORNADA SOBRE ACTUALIDAD EN CRIPTOGRAFÍA, CIRCULO DE ELECTRÓNICA MILITAR, MADRID, 1.991.

[25] BEKER, H., "CIPHER SYSTEMS", NORTHWOOD BOOKS, F. PIPER, LONDON, 1.982.

[26] BEKER, H., AND PIPER, F., "SECURE SPEECH COMMUNICATIONS", ACADEMIC PRESS, LONDON, 1.985.

[27] BENSOUSSAN, A., "DROIT DE L'INFORMATIQUE ET DE LA TÉLÉMATIQUE: THÈORIE ET PRATIQUE", BERGER-LEVRAULT, PARÍS, 1.985.

[28] BERMEJO VERA, J., "EL SECRETO DE LAS ADMINISTRACIONES PÚBLICAS. PRINCIPIOS BÁSICOS Y REGULACIONES ESPECÍFICAS DEL ORDENAMIENTO JURÍDICO ESPAÑOL", REVISTA ESPAÑOLA DE DERECHO ADMINISTRATIVO, Nº 57, MADRID, 1.988.

[29] BETH, T., KNOBLOCK, J.J., AND OTTEN, M., "VERIFIABLE SECRETO SHARING FOR MONOTONE ACCESS STRUCTURES," PROC. 1ST ACM CONF, ON COMMUNICATION AND COMPUTER SECURITY, NOV. 1.993.

[30] BETH, T., KNOBLOCK, J.J., OTTEN, M., SIMMONS, G.J., AND WICHMANN, P., "CLIPPER REPAIS KIT-TOWARDS ACCEPTABLE KEY ESCROW SYSTEMS", E.I.S.S. KARLSUHE UNIV., E.I.S.S., KARLSRUHE, GERMANY, 1.994.

[31] BETH, T., FRIXCH, M. AND SIMMONS, G., (EDS.), PUBLIC KEY CRYPTOGRAPHY: STATE OF THE ART AND FUTURE DIRECTIONS, LECTURE NOTES IN COMPUTER SCIENCE, NO. 578, SPRINGER-VERLAG, NUEVA YORK, 1.993.

[32] BIHAM, E. AND SHAMIR, A.,"DIFFERENTIAL CRYPTANALYSIS OF THE DATA ENCRYPTION STANDARD", SPRINGER-VERLAG, BERLÍN, 1.992.

[33] BLANCO RUIZ, F., "LA SEGURIDAD DE LAS COMUNICACIONES. NECESIDADES Y SITUACIÓN ACTUAL", JORNADA SOBRE ACTUALIDAD EN CRIPTOGRAFÍA, CIRCULO DE ELECTRÓNICA MILITAR, MADRID, 1.991.

[34] BLAZE, M., "PROTOCOL FAILURE IN THE ESCROWED ENCRYPTION STANDARD", AT&T BELL LABORATORIES, PRELIMINARY DRAFT, 1.994.

[35] BOBBIO, N., "TEORÍA GENERAL DEL DERECHO", DEBATE, MADRID,1.993.

[36] BRASSARD, G., "MODERN CRYPTOLOGY". VOLUME 325 OF LECTURE NOTES IN COMPUTER SCIENCE, SPRINGER-VERLAG, NEW YORK, 1.989.

[37] BRUNNER, E.R.,"EFFICIENT SPEECH SCRAMBLING :ANECONOMIC SOLUTION TO THE SECURE VOICE COMMUNICATION PROBLEMS", PROCEDINGS OF THE INTERNATIONAL CONFERENCE ON COMMUNICATION EQUIPMENT AND SYSTEMS, BRIGHTON, U.K. 1.976.

[38] C.S.I.C. - UNIVERSIDAD DE LAS ISLAS BALEARES, "SEGURIDAD EN REDES INFORMÁTICAS . PUNTO DE VISTA DEL USUARIO", I REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA, PALMA DE MALLORCA, 1.991.

[39] CABALLERO, R. Y ROJO, J., "AN EFFICIENT IMPLEMENTATION OF THE RSA CRYPTOGRAPHIC TECHNIQUE", IV REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA, VALLADOLID, 1.996.

[40] CAMACHO LOSA, L., "EL DELITO INFORMÁTICO COMO NUEVA FIGURA JURÍDICA", MADRID. 1.987.

[41] CARMONA SALGADO, C., "LA LIBERTAD DE EXPRESIÓN Y SUS LÍMITES", EDERSA, MADRID, 1.991.

[42] CARRASCOSA, V., REVISTA INFORMÁTICA Y DERECHO, U.N.E.D., MÉRIDA, 1.995

[43] CARRILLO, M., "LA TUTELA DE LOS DERECHOS FUNDAMENTALES POR LOS TRIBUNALES ORDINARIOS". B.O.E. Y CENTRO DE ESTUDIOS CONSTITUCIONALES, MADRID,1.997.

[44] CASTELL, M., "LA CIUDAD INFORMACIONAL. TECNOLOGÍAS DE LA INFORMACIÓN, REESTRUCTURACIÓN ECONÓMICA Y PROCESO URBANO-REGIONAL". ALIANZA EDITORIAL, MADRID, 1.995.

[45] CATALA, P., "LES TRANSFORMATIONS DU DROIT PAR L'INFORMATIQUE" EN EMERGENCE DU DROIT DE L'INFORMATIQUE. ED. DES PARQUES, PARIS,1.983.

[46] CENTRO SUPERIOR DE INFORMACION DE LA DEFENSA, "GLOSARIO DE TÉRMINOS DE CRIPTOLOGÍA", MADRID, 1.993.

[47] CITEMA, COLOQUIO SOBRE IMPLICACIONES SOCIO-JURÍDICAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN, MADRID, 1.985.

[48] COMUNIDADES EUROPEAS, "CONFIDENTIALITY OF MEDICAL RECORDS", HMSO, LONDON, 1.985.

[49] CONSEJO DE EUROPA, ACTES DE LA CONFERENCE DES INSTITUCIONS RESPONSABLES DE L'INFORMATISATION: BILAN. SOUS LA DIR. D'ISABELLE DE LAMBAERTERIE ET JEROME JUET. PARIS, LIBRAIRE GENERALE DE DROIT ET DE JURISPRUDENCE, 1.987.

[50] CORNELLA, A., "LOS RECURSOS DE INFORMACIÓN", SERIE MCGRAW-HILL DE MANAGEMENT, ESADE, MADRID, 1.994.

[51] CORNWELL, R., AND STAUNTON, M., "DATA PROTECTION: PUTTING THE RECORD STRAINGHT", STATE MUTUAL BK, NEW YORK, 1.985.

[52] COURT, J.M., "PERSONAL DATA PROTECTION. THE 1.984 ACT AND ITS IMPLICATIONS", NATIONAL COMPUTING CENTER, OXFORD ROAD,1.984.

[53] CÓDIGO DE LEGISLACIÓN INFORMÁTICA, B.O.E., MADRID, 1.988.

[54] CUBERT, J., "LA POLICÍA Y LA PREVENCIÓN DE LA CRIMINALIDAD", EN "POLICÍA Y SOCIEDAD DEMOCRÁTICA", COMPLILADO POR JOSÉ MARIA RICO, ALIANZA EDITORIAL, MADRID, 1.983.

[55] CUEVAS CALABIA, J.L., "LA LORTAD Y LA SEGURIDAD DE LOS SISTEMAS AUTOMATIZADOS DE DATOS", ACTUALIDAD INFORMÁTICA ARANZADI, Nº 13. PAMPLONA,

[56] D.E. DENNING, D.E., "CRYPTOGRAPHY AND DATA SECURITY", ADDISON-WESLEY, 1.983.

[57] DAHRENDORF, FURET Y GEREMECK, "LA DEMOCRACIA EN EUROPA", MADRID, ALIANZA, 1.993.

[58] DAHRENDORF,R.,"LEY Y ORDEN", CIVITAS, MADRID, 1.994.

[59] DAMIEN, A., "LE SECRET NÉCESSAIRE", DESCLÉE DE BROUWER, PARÍS,1.986.

[60] DAVARA RODRIGUEZ, M.A., "X AÑOS DE ENCUENTROS SOBRE INFORMÁTICA Y DERECHO", UNIVERSIDAD PONTIFICIA COMILLAS. FACULTAD DE DERECHO E INSTITUTO DE INFORMÁTICA JURÍDICA, MADRID, 1.997.

[61] DAWSON, E., GOLDBURG, B., AND SRIDHARAN, S.,"THE AUTOMATED CRYPTANALYSIS OF ANALOG SPEECH SCRAMBLERS", PROCEEDINGS OF EUROCRYPT'91, UNIVERSITY OF SUSSEX, BRIGHTON, U.K., 1.991.

[62] DÁVARA RODRÍGUEZ, M.A., "DERECHO INFORMÁTICO", EDITORIAL ARANZADI, PAMPLONA, 1.993.

[63] DÁVARA RODRÍGUEZ, M.A., "DE LAS AUTOPISTAS DE LA INFORMACIÓN A LA SOCIEDAD VIRTUAL", ARANZADI, PAMPLONA, 1.996.

[64] DE MIGUEL CASTAÑO, A., "DERECHO A LA INFORMACIÓN FRENTE AL DERECHO A LA INTIMIDAD. SU INCIDENCIA EN EL SERVICIO DE INFORMACIÓN ESTADÍSTICA". MADRID, 1.983.

[65] DE ASIS ROIG, R., "LAS PARADOJAS DE LOS DERECHOS FUNDAMENTALES COMO LÍMITES AL PODER", EDITORIAL DEBATE, MADRID,1.992.

[66] DE LA GUIA, D., Y FUSTER, A., "ARQUITECTURAS CRIPTOGRÁFICAS A PARTIR DE PRODUCTOS MODULARES", III REUNIÓN ESPAÑOLA DE CRIPTOLOGÍA, BARCELONA 1.994.

[67] DEAVOURS, C.A., KAHN, P., AND KRUH, L., "CRYPTOLOGY, YESTERDAY, TODAY AND TOMORROW", ARTECH HOUSE, 1.987.

[68] DEL PESO NAVARRO Y MIGUEL, E., Y RAMOS GONZÁLEZ, L.A., "CONFIDENCIALIDAD Y SEGURIDAD DE LA INFORMACIÓN: LA LORTAD Y SUS IMPLICACIONES SOCIOECONÓMICAS", EDICICIONES DIAZ DE SANTOS, MADRID,1.994.

[69] DELAHAIE H., ET PAOLETTI, F., "INFORMATIQUE ET LIBERTÉS", PARÍS, DÉCOUVERTE, 1.986.

[70] DELANNOI G., Y TAGUIEFF, P.A., "TEORÍAS DEL NACIONALISMO", EDICIONES PAIDÓS, BARCELONA, 1.993.

[71] DEMANDT, A., "LOS GRANDES PROCESOS. DERECHO Y PODER EN LA HISTORIA", CRÍTICA, BARCELONA, 1.993.

[72] DENNING, D.E., "THE U.S. KEY ESCROW ENCRYPTION TECHNOLOGY", COMPUTER COMMUNICATIONS, VOL. 17, NO. 7, BUTTERWORTH-HEINEMANN LTD. LINACRE HOUSE, JORDAN HILL, OXFORD, 1.994.

[73] DENNING, D.E. AND SMID, M., "KEY ESCROWING TODAY", IEEE COMMUNICATIONS, SEPT. 1.994.

[74] DENNING, DOROTHY, AND MILES SMID, "KEY ESCROWING TODAY", (TO APPEAR IN IEEE COMMUNICATIONS), 1.994.

[75] DESANTES GUANTER, J.M., "LOS LÍMITES DE LA INFORMACIÓN", ASOCIACIÓN DE LA PRENSA, MADRID, 1.991.

[76] DIEZ DE VELASCO, M., "INSTITUCIONES DE DERECHOS INTERNACIONAL PÚBLICO", EDITORIAL TECNOS, MADRID,1.976.

[77] DIFFIE, W., AND HELLMAN, M.E., "PRIVACY AND AUTHENTICATION: AN INTRODUCTION TO CRYPTOGRAPHEY", PROCEEDINGS OF THE IEEE, VOL, 67, NO. 3, MARCH 1.979.

[78] DIFFIE, W., AND HELLMAN, M.E., "NEW DIRECTIONS IN CRYPTOGRAPHY", IEEE TRANSACTIONS ON INFORMATION THEORY, VOL IT-22, PP. 74-84, JUNE, ...1.976.

[79] DIRECCIÓN GENERAL DE LA GUARDIA CIVIL-U.N.E.D.,"SEGURIDAD NACIONAL- SEGURIDAD INTERNACIONAL", VIII SEMINARIO "DUQUE DE AHUMADA". DIRECCIÓN GENERAL DE LA GUARDIA CIVIL-UNIVERSIDAD NACIONAL DE EDUCACIÓN A DISTANCIA, MADRID, 1.996.

[80] DORSEN, N Y GILLERS, S., (EDS), "NONE OF YOUR BUSINESS. GOVERNMENT SECRECY IN AMERICA, NUEVA YORK, THE VIKING PRESS, 1.974.

[81] DOYALE, L., E GOUGH, I., "TEORÍA DE LAS NECESIDADES HUMANAS", EDIT. FUHEM Y COMUNIDAD DE MADRID, MADRID, 1.994.

[82] DROSNIN, M., "EL CÓDIGO SECRETO DE LA BIBLIA", EDIT. PLANETA, BARCELONA, 1.997.

[83] DUVERGER, M., "SOCIOLOGÍA POLÍTICA", TRADUCCIÓN DE JORGE DE ESTEBAN, 3ª EDICIÓN, EDICIONES ARIEL, BARCELONA, 1.972.

[84] DYSON, E, "RELEASE 2.0", EDICIONES GRUPO ZETA, BARCELONA, 1.998.

[85] ECHEVERRÍA, J., "MODELOS LÓGICOS APLICADOS A LA CRIPTOGRAFÍA", II REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA, MADRID, 1.992.

[86] EDGAR, H. Y SCHMID, B, "THE ESPIONAGE STATUTES AND THE PUBLICATION OF DEFENSE INFORMATION", COLUMBIA LAW REVIEW, 1.973.

[87] EDGAR, H. Y SCHMIDT, B, "CURTIS-WRIGHT COMES HOME: EXECUTIVE POWER AND NATIONAL SECURITY SECRECY", HARVARD CIVIL RIGHT-CIVIL LIBERTATIES LAW REVIEW, 1.986.

[88] ELZABURO MÁRQUEZ, F. Y MARTITEGUI SUSUNAGA, J., "LA CRISIS MUNDIAL", ESPASA CALPE, MADRID, 1.988.

[89] ESPAÑA, BOLETÍN OFICIAL CONGRESO DE LOS DIPUTADOS, CONGRESO, SERIE A, Nº 59, DE 24 DE JULIO DE 1.991.

[90] ESPAÑA, PRESIDENCIA DEL GOBIERNO, CONFERENCIA SOBRE LOS PROBLEMAS DE LA LEGISLACION EN MATERIA DE PROTECCIÓN DE DATOS, MADRID, 1.984.

[91] ESPAÑA, PRESIDENCIA DEL GOBIERNO, PROBLEMAS LEGISLATIVOS DE LA PROTECCIÓN DE DATOS: ACTAS Y DOCUMENTOS DE LA CONFERENCIA INTERNACIONAL... ORGANIZADA POR EL CONSEJO DE EUROPA, MADRID , 1.986.

[92] ESPAÑA, PRESIDENCIA DEL GOBIERNO, INFORMÁTICA: LEYES DE PROTECCIÓN DE DATOS, MADRID, 1.983.

[93] ESPAÑA, MINISTERIO DE JUSTICIA, COLECCIÓN DE "INTRODUCCIÓN A LOS DERECHOS FUNDAMENTALES", MADRID,1.988.

[94] ESPAÑA, MINISTERIO DE ADMINISTRACIONES PUBLICAS, INFORMÁTICA: LEYES DE PROTECCIÓN DE DATOS. MADRID, 1.988.

[95] ESPASA CALPE, ENCICLOPEDIA UNIVERSAL ILUSTRADA, MADRID,

[96] ESPASA CALPE, DICCIONARIO BÁSICO ESPASA, SÉPTIMA EDICIÓN, MADRID, 1.989.

[97] ESTADOS UNIDOS, NATIONAL INSTITUTE FOR STANDARS AND TECHNOLOGY, FEDERAL INNFORMATION PROCESSING STANDARDS PUBLICATION 185, DEPT. OF COMMERCE, WASHINGTON, 1.994.

[98] ESTADOS UNIDOS, NATIONAL INSTITUTE FOR STANDARDS AND TECHNOLOGY. TECNICAL FACT SHEET ON BLAZE REPORT AND KEY ESCROW ENCRYPTION. 1.994.

[99] ESTADOS UNIDOS, THE WHITE HOUSE, DIRECTIVE ON PUBLIC ENCRYPTION MANAGEMENT, WASHINGTON, 1.993.

[100] FARIÑAS MATONI, L.M., "EL DERECHO A LA INTIMIDAD", TRIVIUM, MADRID, 1.983.

[101] FELCMAN, L.I., "BUROCRACIA PÚBLICA TECNOLOGÍA INFORMÁTICA, TRANSFORMACIÓN CULTURAL Y CONDICIONANTES POLÍTICOS. INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA, MADRID, 1.988.

[102] FERNANDEZ, J., GOMEZ, A., SÁNCHEZ, J. Y RODRIGUEZ, A., "PROYECTO ESIDE: UNA EXPERIENCIA DE IMPLANTACIÓN DE SERVICIOS DE SEGURIDAD EN EDI", III REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA, BARCELONA, 1.994.

[103] FERNÁNDEZ-MIRANDA Y CAMPOAMOR, A., "LIBERTAD DE EXPRESIÓN Y DERECHO A LA INFORMACIÓN" EN "COMENTARIO A LAS LEYES POLÍTICAS. CONSTITUCIÓN ESPAÑOLA DE 1.978".EDERSA, MADRID, 1.985.

[104] FERRER, J.L. Y HUGUET, LL, "UNA NUEVA VÍA DE ATAQUE AL DES", IV REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA, VALLADOLID, 1.996.

[105] FERRER, J.LL., ROTGER, A. Y HUGUET LL., "FIRMA ELECTRÓNICA DE CONTRATOS", III REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA, BARCELONA, 1.994.

[106] FERRY, J.M., (ED.) "EL NUEVO ESPACIO PÚBLICO", GEDISA, BARCELONA, 1.992.

[107] FLAHERTY, D.H., "PRIVACY AND ACCESS TO GOBERNMENT DATA FOR RESEARCH: AN INTERNATIONAL BIBLIOGRAPHY, MANSELL, LONDON, 1.979.

[108] FLAHERTY, D.H., "PRIVACY AND DATA PROTECTION", MANSELL, LONDON, 1.984.

[109] FLAHERTY, D.H., "PRIVACY AND GOVERNMENT DATA BANK: AN INTERNATIONAL PERSPECTIVE, MARSELL, LONDON, 1.979.

[110] FLAHERTY, D.H., "PROTECTING PRIVACY IN TWO-WAY ELECTRONIC SERVICES", MANSELL, LONDON, 1.985.

[111] FORNE, J., MELUS, J.L. Y REBOLLO, D., "GESTIÓN EFICIENTE DE CLAVES EN GRANDES REDES", IV REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA, VALLADOLID, 1.996.

[112] FORNE, J. Y RECACHA, F., "GESTIÓN DE CLAVES EN UN TERMINAL MULTIMEDIA PARA RDSI-BA", III REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA, BARCELONA, 1.994.

[113] FORTRESS U & T LTD., "KEEP THE INVADERS (OF PRIVACY) SOCIALLY SANE-KISS" OVERHEADS OF PRESENTATION, ISRAEL, 1.994.

[114] FREEH, L., 1.994, "WRITTEN STATEMENT BEFORE THE SUBCOMMITTEE ON TECHONOLOGY AND THE LAW OF THE COMMITTEE OF THE JUDICIARY, UNITED STATES SENATE AND TEHE SUBCOMMITTEE ON CIVIL AND CONSTITUTIONAL RIGHT OF TEHE COMMITTEE ON THE JUDICIARY, HOUSE OF REPRESENTATIVES, MARCH 18, WASHINGTON, DC. 1.994.

[115] FRIGINAL FERNANDEZ-VILLAVERDE, L., "LA PROTECCIÓN DE LOS DERECHOS FUNDAMENTALES EN EL ORDENAMIENTO ESPAÑOL", MONTECORVO, MADRID,1.981.

[116] FROSINI, V., "CIBERNÉTICA, DERECHO Y SOCIEDAD.", TECNOS, MADRID, 1.982.

[117] FROSINI, V., "INFORMÁTICA Y DERECHO", TR. DE J. GUERRERO Y M. AYERRA. TEMIS, BOGOTÁ, 1.988.

[118] FUNDACIÓN CIENCIA, DEMOCRACIA Y SOCIEDAD, SERIE DEMOCRACIA, PUBLICACIONES, MADRID, 1.990.

[119] GALAN PASCUAL, C., "LA CRIPTOGRAFÍA EN LAS FUERZAS Y CUERPOS DE SEGURIDAD DEL ESTADO. UN PROYECTO DE MODERNIZACIÓN", JORNADA SOBRE ACTUALIDAD EN CRIPTOGRAFÍA, CIRCULO DE ELECTRÓNICA MILITAR, MADRID, 1.991.

120 GALENDE DÍAZ, J.C., "CRIPTOGRAFÍA: HISTORIA DE LA ESCRITURA CIFRADA", EDIT. JUAN CARLOS GALENDE DIAZ, 1ª DE. 1.995.

121 GALENDE DÍAZ, J.C., "INTRODUCCIÓN A LA CRIPTOGRAFÍA HISTÓRICA", EDIT. JUAN CARLOS GALENDE DIAZ, 1.993.

122 GALENDE DÍAZ, J.C., "CRIPTOGRAFÍA MODERNA", EDIT. JUAN CARLOS GALENDE DÍAZ, 1.990.

123 GALINDO AYUDA, F., "AUTODETERMINACIÓN INFORMATIVA: MEDIDAS DE SEGURIDAD Y CÓDIGOS TIPO", JORNADAS INTERDISCIPLINARES SOBRE CRIPTOGRAFÍA, PRIVACIDAD Y AUTODETERMINACIÓN INFORMATIVA, ZARAGOZA, 1.995.

124 GARCÉS, J.E., "SOBERANOS E INTERVENIDOS", SIGLO XXI DE ESPAÑA, EDITORES, MADRID ,1.996.

125 GARCIA VITORIA, A.,"EL DERECHO A LA INTIMIDAD EN EL DERECHO PENAL Y EN LA CONSTITUCIÓN DE 1.978", ARANZADI, PAMPLONA, 1.983.

126 GARCIA MADARIAGA, J. M., "CÓDIGO DE LEGISLACIÓN INFORMÁTICA", BOLETÍN OFICIAL DEL ESTADO, MADRID,1.988.

127 GARCÍA DE ENTERRÍA, E., "DEMOCRACIA, JUECES Y CONTROL DE LA ADMINISTRACIÓN", CIVITAS, MADRID,

128 GAREY, M.,"COMPUTERS AND INTRACTABILITY", FREEMAN, NEW YORK, 1.979.

129 GARRIDO FALLA, F., "COMENTARIOS A LA CONSTITUTICIÓN", CIVITAS, MADRID, 1.980.

130 GIDDENS, "THE CONSEQUENCES OF MODERNITY", OXFORD, 1.990.

131 GINER, S.,"EL DESTINO DE LA LIBERTAD", ESPASA CALPE, MADRID, 1.987.

132 GOMEZ, A., "USO DE CERTIFICADOS PARA LA PROVISIÓN DE SERVICIOS DE SEGURIDAD", II REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA, MADRID, 1.992.

133 GONZÁLEZ BALLESTEROS, T., "LAS LIBERTADES DE EXPRESIÓN E INFORMACIÓN EN LA RESOLUCIONES DE LOS TRIBUNALES DE JUSTICIA", JORNADAS DE ESTUDIO JUSTICIA Y MEDIOS DE COMUNICACIÓN, REVISTA "ACTUALIDAD ADMINISTRATIVA", Nº 19, FEBRERO 1.987.

134 GONZÁLEZ BALLESTEROS, T., Y OTROS, "LEGISLACIÓN INFORMATIVA", EDIT. COLEX, MADRID, 1.991.

135 GÓMEZ SEGADE, J.A., "EL SECRETO INDUSTRIAL (KNOW-HOW). CONCEPTO Y PROTECCIÓN". TECNOS, MADRID, 1.978.

136 GÓMEZ PAVÓN, P., "LA INTIMIDAD COMO OBJETO DE PROTECCIÓN PENAL", AKAL, MADRID,1.989.

137 GÓMEZ-REINO Y CARNOTA, E., "EL PRINCIPIO DE PUBLICIDAD DE LA ACCIÓN DEL ESTADO Y LA TÉCNICA DE LOS SECRETOS OFICIALES", REVISTA ESPAÑOLA DE DERECHO ADMINISTRATIVO Nº 8, MADRID,1.976.

138 GUIJARRO, F., "IMPLICACIONES SOCIO-JURÍSICAS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN", III COLOQUIO. MADRID, CITEMA, 1.985 Y 1.987.

139 HALPERIN, M. Y HOFFMAN, D, "TOP SECRET NATIONAL SECURITY AND THE RIGHT TO KNOW", NEW REPUBLIC BOOKS, WASHINGTON, 1.977.

140 HARTMANN, H.P.,"ANALOG SCRAMBLING VS DIGITAL SCRAMBLING IN POLICE COMMUNICATION NETWORKS", CARNAHAN CONFERENCE, UNIVERSITY OF KENTUCKY, U.S.A, 1.978.

141 HARVEY, D., "THE CONDITIONS OF POSTMODERNITY: AN ENQUIRY INTO THE ORIGINS OF CULTURAL CHANGE", OXFORD, 1.989.

142 HEREDERO, M., "LA INFORMÁTICA Y EL USO DE LA INFORMACIÓN PERSONAL E INTRODUCCIÓN A LA INFORMÁTICA JURÍDICA". ED. A CARGO DE A.M. RIVERO Y A. SANTODOMINGO, FUNDESCO, MADRID,1.986.

143 HERNANDO COLLAZO, I., "MODELO EUROPEO DE ACUERDO EDI. DISPOSICIONES LEGALES", JORNADAS INTERDISCIPLINARES SOBRE CRIPTOGRAFÍA, PRIVACIDAD Y AUTODETERMINACIÓN INFORMATIVA, ZARAGOZA, 1.995.

144 HERRERO TEJEDOR, F., "HONOR, INTIMIDAD Y PROPIA IMAGEN", COLEX, MADRID, 1.990.

145 HEWITT, P., "COMPUTERS, RECORDS AND THE RIGHT TO PRIVACY", ED. BROOK-FIELD, VT, GOWER PUBLISHING CO., 1.979.

146 HINSLEY, FRANCIS H., AND STRIPP, ALAN (EDS.), "CODEBREAKERS". THE INSIDE STORY OF BLETCHLEY PARK, OXFORD UNIVERSITY PRESS, 1.993.

147 HOFFMAN, L.J.,"COMPUTERS AND PRIVACY IN THE NEST DECADE", C.A. ACADEMIC PRESS, SAN DIEGO, 1.980.

148 HOFFMAN, L.J., "BUILDING IN BIG BROTHER", THE CRYPTOGRAPHIC POLICY DEBATE, SPRINGER VERLAG, NEW YORK, 1.995.

149 HOYO AGUILERA, F.J., "LA CRIPTOGRAFÍA EN LAS FAS. ORGANIZACIÓN Y NORMATIVA VIGENTE", JORNADA SOBRE ACTUALIDAD EN CRIPTOGRAFÍA, CIRCULO DE ELECTRÓNICA MILITAR, MADRID, 1.991.

150 HTTP://BBS.SEKER.ES/~ALVY/CRIPTO/CRIPTORECURSOS.HTML

151 HTTP://WWW.ARRAKIS.ES/~QUIJADA/ENLACE.HTM

152 HTTP://WWW.CTV.ES/USERS/MPQ/- SIZE 9K . 21 -OCT-97 - SPANISH

153 HTTPP://WWW.SUPER.UNAM.MX/SEGURIDAD/FMS.HTML

154 HUET, J., "DROIT DE L'INFORMATIQUE ET DES TÉLÉCOMMUNICATIONS: ETAT DES QUESTIONS, TEXTES ET JURISPRUDENCE, ÉTUDES ET COMMENTAIRES", LITEC, PARIS, 1.989.
COSTA, J., "IMAGEN PÚBLICA. UNA INGENIERÍA SOCIAL", FUNDESCO, MADRID, 1.992.

155 HUGUET Y ROTGER, LL. Y FERRER GOMILA, J.L., "INFORMÁTICA Y MEDIDAS DE SEGURIDAD EN EL TRÁFICO COMERCIAL A TRAVÉS DEL EDI", JORNADAS INTERDISCIPLINARES SOBRE CRIPTOGRAFÍA, PRIVACIDAD Y AUTODETERMINACIÓN INFORMATIVA, ZARAGOZA, 1.995.

156 HUNTINGTON, S.P., "EL CHOQUE DE CIVILIZACIONES Y LA RECONFIGURACIÓN DEL ORDEN MUNDIAL", EDIT. PAIDOS, BARCELONA, 1.997

157 I REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA, ACTAS, PALMA DE MALLORCA, 1.991.

158 II REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA, ACTAS, MADRID, 1.992.

159 III REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA, ACTAS, BARCELONA, 1.994.

160 ITALIA, CAMERA DEI DIPUTATI, CONSEJO DE EUROPA, LEGISLACIÓN ET PROTECTION DES DONNÉES, ACTES DE LA CONFERENCE DE ROME (DÉCEMBRE 1.982) SUR LES PROBLÈMES D'ÉLABORATION ET D'APPLICATION DE LA LÉGISLATION EN MATIÉRE DE PROTECTION DES DONNÉES. ROMA, 1.983.

161 IV REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA, ACTAS, VALLADOLID, 1.996.

162 JORNADA SOBRE: ACTUALIDAD EN CRIPTOGRAFÍA, CIRCULO DE ELECTRÓNICA MILITAR, MADRID, 1.991.

163 JORNADAS INTERDISCIPLINARES SOBRE CRIPTOGRAFÍA, PRIVACIDAD Y AUTODETERMINACIÓN INFORMATIVA, ACTAS, ZARAGOZA, 1.995.

164 JORNADAS DE LA ABOGACIA Y LAS NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN, 1.996.

165 KAHN, D., "THE CODEBREAKERS", THE MCMILLAN CO, NUEVA YORK, 1.996.

166 KENDOURIE, E., "NACIONALISMO", CENTRO DE ESTUDIOS CONSTITUCIONALES, MADRID, 1.988.

167 KENNEDY, P., "PREPARIN FOR THE TWENTY-FIRST CENTURY", HARPER COLINS, LONDRES, 1.993.

168 KISSINGER, H., "DIPLOMACIA", EDICIONES B, BARCELONA, 1.996.

169 KOBLITZ, N.,"A COURSE IN NUMBER THEORY AND CRYPTOGRAPHY", SPRINGER, NUEVA YORK, 1.987.

170 KOBLITZ, N., "A COURSE IN NUMBER THEORY AND CRYPTOGRAPHY", 2ª EDICCIÓN 1.994.

171 KONHEIM, A.G., "CRYPTOGRAPHY: A PRIMER", JOHN SILEY, 1.981.

172 KRESS, K., "LEGAL INDETERMINANCY", CALIFORNIA LAW REVIEW, 1.989.

[173] LAI, X., MASSEY, J.L., AND MURPHY, S., "MARKOV CIPHERS AND DIFFERENTIAL CRYPTANALYSIS", ADVANCES IN CRYPTOLOGY-EUROCRYPT'91, D.W. DAVIES, ED., SPRINGER-VERLAG, BERLIN, 1.992.

[174] LAVER, M., "LOS ORDENADORES Y EL CAMBIO SOCIAL",TECNOS, MADRID,1.983.

[175] LEE, L., "A SPEECH SECURITY SSYSTEM NOT REQUIRING SYSCHRONIZATION", IEEE COMMUNICATIONS MAGAZINE, JULY 1.985.

[176] LOPEZ CRESPO, F., "NOTAS SOBRE SOLUCIONES DE LA UNIÓN EUROPEA Y DE LA ADMINISTRACIÓN ESPAÑOLA", JORNADA INTERDISCIPLINARES SOBRE CRIPTOGRAFÍA, PRIVACIDAD Y AUTODETERMINACIÓN INFORMATIVA, ZARAGOZA, 1.995.

[177] LOSANO, M.G., PÉREZ LUÑO, A.E., Y GUERRERO MATEUS, M.F., "LIBERTAD INFORMÁTICA Y LEYES DE PROTECCIÓN DE DATOS PERSONALES", CENTRO DE ESTUDIOS CONSTITUCIONALES, MADRID, 1.989.

[178] LOZANO BARTOLOZZI, P., "ESTRUCTURA DINÁMICA DE LAS RELACIONES INTERNACIONALES", MITRE, BARCELONA ,1.987.

[179] LÓPEZ-FRAGOSO ALVAREZ, T., "LAS INTERVENCIONES TELEFÓNICAS EN EL PROCESO PENAL", COLEX, MADRID,1.991.

[180] LÓPEZ, J. Y MARAVAL, C., "SISTEMA DE CIFRADO DE CORREO ELECTRÓNICO EN RED DE ÁREA LOCAL", III REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA, BARCELONA, 1.994.

[181] LYOTARD, J.F., "LA CONDICIÓN POSTMODERNA", CÁTEDRA, MADRID,1.980.

[182] MADRID CONESA, F., "DERECHO A LA INTIMIDAD INFORMÁTICA Y ESTADO DE DERECHO", UNIVERSIDAD,VALENCIA, 1.984.

[183] MARCO, C., Y MORILLO, P., "UN ALGORITMO CRIPTOGRÁFICO VERSATIL Y EFICIENTE ADECUADO PARA TARJETAS INTELIGENTES", IV REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA, VALLADOLID, 1.996.

[184] MARIÑO, D., "LA PROBLEMÁTICA DE LA CALIDAD EN LA SEGURIDAD CRIPTOLÓGICA", JORNADA SOBRE ACTUALIDAD EN CRIPTOLOGÍA, CIRCULO DE ELECTRÓNICA MILITAR, MADRID, 1.991.

[185] MARTIN-CASALLO LÓPEZ, J.J., "MEDIDAS DE SEGURIDAD. LA AGENCIA DE PROTECCIÓN DE DATOS, ACTUACIONES CONCRETAS Y POSIBLES", JORNADAS INTERDISCIPLINARES SOBRE CRIPTOGRAFÍA, PRIVACIDAD Y AUTODETERMINACIÓN INFORMATIVA, ZARAGOZA, 1.995.

[186] MARTINEZ SOLER, J.A., ROS, F., E SANTILLANA, I., "LAS AUTOPISTAS DE LA INFORMACIÓN", DEBATE, MADRID,...

[187] MARTÍNEZ LAGE, S.,"BREVE DICCIONARIO DIPLOMÁTICO", O.I.D., MINISTERIO DE ASUNTOS EXTERIORES, MADRID, 1.982.

[188] MAURER, U.M., "PROVABLE SECURITY IN CRYPTOGRAPHEY", PHD THESIS ETH NO. 9260, ZURICH, 1.990.

[189] MAURER, U.M., "NON-INTERACTIVE PUBLIC-KEY CRYPTOGRAPHY", PROCEEDINGS OF EUROCRYPT'91, BRIGHTON, U.K., 1.991.

[190] MAURER, U.M., "NEW APPROACHES TO THE DESING OF SELF-SYNCHONIZING STREAM CIPHERS", PROCEEDINGS OF EUROCRYPT'91, BRIGHTON, U.K., 1.991.

[191] MEIER, W., "FAST CORRELATION ATTACKS ON STREAM CIPHERS", JOURNAL OF CRYPTOLOGY, VOL. 1, NO. 3, PP. 159-176, 1.988.

[192] MEIER, W., AND STAFFELBACH, O., "NONLINEARITY CRITERIA FOR CRYPTOGRAPHIC FUNCTIONS", PROCEEDINGS OF EUROCRYPT'89, LECTURE NOTES IN COMPUTER SCIENCE, SPRINGER VERLAG, NEW YORK,1.990.

[193] MELLEN G., AND WINKEL, B., "PROCEEDINGS OF EUROCRYPT,1.982-1.992", SPRINGER-VERLAG, BERLÍN, 1.993.

[194] MELLEN, G.E., "CRYPTOLOGY, COMPUTERS AND COMMON SENSE", PROCEEDINGS NATIONAL COMPUTER CONFERENCE, AFIPTS, 1.973.

[195] MENEZES, A.J. Y OTROS, "HANDBOOK OF APPLIED CRYPTOGRAPHY", CRC PRESS, NUEVA YORK, 1.997.

[196] MERLE, M., "SOCIOLOGÍA DE LAS RELACIONES INTERNACIONALES", ALIANZA UNIVERSIDAD, MADRID, 1.984.

[197] MEYER, C., "CRYPTOGRAPHY: A NEW DIMENSION IN COMPUTER DATA SECURITY", JOHN WISLEY, 1.982.

[198] MICALI, S.,"FAIR CRYPTOSYSTEMS", MIT LABORATOY FOR COMPUTER SCIENCE, NOVERBER 1.993.

[199] MOLINA MATEOS, J.M., "SEGURIDAD, INFORMACIÓN Y PODER", INCIPIT, MADRID, 1.994.

[200] MOLINA MATEOS, J.M., "CRIPTOLOGÍA, USUARIOS Y CONSUMIDORES", IV REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA, VALLADOLID, 1.996.

[201] MOLINA MATEOS, J.M., "LAS COMUNICACIONES PRIVADAS EN LA CONSTITUCIÓN ESPAÑOLA DE 1.978", III REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA, BARCELONA 1.994.

[202] MOLINA MATEOS, J.M., "CRIPTOLOGÍA Y POLÍTICA", JORNADAS INTERDISCIPLINARES SOBRE CRIPTOGRAFÍA, PRIVACIDAD Y AUTODETERMINACIÓN INFORMATIVA, ZARAGOZA, 1.995.

[203] MOLINA MATEOS, J.M., "CRIPTOLOGÍA Y ASOCIACIONISMO", III REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA, MADRID, 1.992.

[204] MORALES PRATS, F., "LA TUTELA PENAL DE LA INTIMIDAD: PRIVACY E INFORMÁTICA", DESTINO, BARCELONA, 1.984.

[205] MORANT RAMÓN, J.L., RIBAGORDA GARNACHO, A., Y SANCHO RODRÍGUEZ, J., "SEGURIDAD Y PROTECCIÓN DE LA INFORMACIÓN", EDITORIAL CENTRO DE ESTUDIOS RAMÓN ARECES, MADRID, 1.994.

[206] MOREYRA, C. A., "LOS CRIPTOGRAMAS DE STA. TERESA", DEAN FUNES, CÓRDOBA, ARGENTINA, 1.964.

[207] MUÑOZ ALONSO, A., "POLÍTICA Y NUEVAS TECNOLOGÍAS", FUNDESCO, MADRID,1.989.

[208] MUÑOZ MACHADO, S., "DERECHO PÚBLICO DE LAS COMUNIDADES AUTÓNOMAS", CIVITAS, MADRID, 1.984.

[209] MUÑOZ, J. L., "LA CRIPTOGRAFIA EN ANÉCDOTAS", EDICIONES EJÉRCITO, MADRID, 1.955.

[210] NIBLETT, B., "DATA PROTECTION ACT 1.984", LONGMAN, LONDON,1.984.

[211] OLIVEROS LAPUERTA, M.V., "ESTUDIO SOBRE LA LEY DE PROTECCIÓN CIVIL DEL DERECHO AL HONOR, A LA INTIMIDAD PERSONAL Y FAMILIAR Y A LA PROPIA IMAGEN". MADRID, PRESIDENCIA DEL GOBIERNO, 1.980.

[212] ORTEGA GARCIA, R., "CONTROL INTERNO, AUDITORIA Y SEGURIDAD INFORMÁTICA", EXPANSIÓN, MADRID, 1.996.

[213] OTAZU, F., "SEGURIDAD INTEGRADA EN LAS COMUNICACIONES", JORNADA SOBRE ACTUALIDAD EN CRIPTOGRAFÍA, CIRCULO DE ELECTRÓNICA MILITAR, MADRID, 1.991.

[214] PASTOR FRANCO, J., "CRIPTOGRAFÍA MODERNA, INFORMÁTICA Y SOCIEDAD", UNIVERSIDAD DE ZARAGOZA, 1.989..

[215] PASTOR FRANCO, J. "COMUNICACIONES DIGITALES Y PRIVACIDAD. LAS POSIBILIDADES DE LA CRIPTOGRAFÍA Y LOS CONFLICTOS QUE SE PLANTEAN", JORNADAS INTERDISCIPLINARES SOBRE CRIPTOGRAFÍA, PRIVACIDAD Y AUTODETERMINACIÓN INFORMATIVA, ZARAGOZA, 1.995.

[216] PASTOR FRANCO, J., "CRIPTOPOST: UNA APLICACIÓN INUSITADA DE LA CLAVE PÚBLICA", I REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA, PALMA DE MALLORCA, 1.991.

[217] PASTOR FRANCO, J., "LA TIENDA DE SECRETOS", III REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA, BARCELONA, 1.994.

[218] PASTOR PETIT, I. "DICCIONARIO ENCICLOPÉDICO DEL ESPIONAJE", EDITORIAL COMPLUTENSE, MADRID,1.996

[219] PATTERSON, W., "MATHEMATICAL CRYPTOLOGY", ROWMAN & LITTLEFIELD, 1.987.

[220] PECES-BARBA, G., "DERECHOS POSITIVO DE LOS DERECHOS HUMANOS", DEBATE, MADRID, 1.987.

221 PECES-BARBA, G., "TEXTOS BÁSICOS SOBRE DERECHOS HUMANOS", UNIVERSIDAD COMPLUTENSE, MADRID, 1.973.

222 PENZIAS, A., "IDEAS E INFORMACIÓN", FUNDESCO, MADRID,1.990.

223 PÉREZ LUÑO, A.E., "NUEVAS TECNOLOGÍAS, SOCIEDAD Y DERECHO. EL IMPACTO SOCIO-JURÍDICO DE LAS N.T. DE LA INFORMACIÓN", FUNDESCO, MADRID,1.987.

224 PÉREZ LUÑO, E., "LOS DERECHOS FUNDAMENTALES", EDIT. TECNOS, MADRID, 1.986.

225 PICAZO, J.L., "CRIPTOLOGÍA OTAN VERSUS CRIPTOLOGÍA NACIONAL: PROPUESTA DE TRANSICIÓN", JORNADA SOBRE ACTUALIDAD EN CRIPTOGRAFÍA, CIRCULO DE ELECTRÓNICA MILITAR, MADRID, 1.991.

226 POMED SÁNCHEZ, L.A., "EL DERECHO DE ACCESO DE LOS CIUDADANOS A LOS ARCHIVOS Y REGISTROS ADMINISTRATIVOS". INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA, MADRID, 1.989.

227 PRATT, F., "HISTOIRE DE LA CRYPTOGRAPHIE: LES ÉCRITURES SECRÈTES DEPUIS L'ANTIGUITÉ JUSQU'Á NOS JOURS. FLETCHER PRATT, 1.940.

228 QUINTANILLA, M.A., "TECNOLOGÍA: UN ENFOQUE FILOSÓFICO", FUNDESCO, MADRID, 1.987.

229 REAL ACADEMIA ESPAÑOLA, DICCIONARIO DE LA LENGUA ESPAÑOLA , MADRID, 1.984.

230 REESE, J., "EL IMPACTO SOCIAL DE LAS MODERNAS TECNOLOGÍAS DE INFORMACIÓN", FUNDESCO, MADRID, 1.982.

231 REID, B.C., "CONFIDENTIALITY AND THE LAW", WATERLOW, LONDON, 1.986.

232 REMIRO BROTONS, A., "CIVILIZADOS, BARBAROS Y SALVAJES", MCGRAW-HILL, MADRID, 1.996.

233 REVEL, J. F., "EL CONOCIMIENTO INÚTIL", PLANETA, BARCELONA,1.989.

234 REVENGA SÁNCHEZ, M., "EL IMPERIO DE LA POLÍTICA", ARIEL, BARCELONA, 1.995.

235 REVISTA DEL INSTITUTO BARTOLOMÉ DE LAS CASAS. DERECHOS Y LIBERTADES, Nº 1, UNIVERSIDAD CARLOS III, MADRID, 1.993.

236 RICO, J.M., "POLICÍA Y SOCIEDAD DEMOCRÁTICA", ALIANZA EDITORIAL, MADRID, 1.983.

237 RICO, F.J. Y SANVICENTE, E., "FIRMA DIGITAL PARA SISTEMAS DE RADIODIFUSIÓN", III REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA, BARCELONA 1.994.

238 RICHARD FISCHER, L., "THE LAW OF FINANCIAL PRIVACY: A COMPLIANCE GUIDE", WARREN GORHAM AND LAMONT, NEW YORK, 1.983.

239 RIFÁ Y COMA, J. Y HUGUET Y ROTGER, LL., "COMUNICACIÓN DIGITAL, TEORÍA MATEMÁTICA DE LA INFORMACIÓN. CODIFICACIÓN ALGEBRAICA. CRIPTOLOGÍA.", MASSON, S.A., EDICIONES MEDICINA CIENCIAS, BARCELONA, 1.991.

240 RIGO VALLBONA, J., "EL SECRETO PROFESIONAL DE ABOGADOS Y PROCURADORES EN ESPAÑA", BOSCH, BARCELONA, 1.988.

241 RIVES, R., SHAMIR, A., ADDELMAN, L., "A METHOD FOR OBTAINING DIGITAL SIGNATURES AND PUBLIC KEY CRYPTOPTENS", COMM. OF ACM 21, N.Y. 1.978.

242 RIVEST, R.L., CRYTOGRAPHY. IN J. VAN LEEUWEN, EDITOR, HANDBOOC OF TEORETICAL COMPUTER SCIENCE, MIT PRES/ELSEVIER, AMSTERDAM, 1.990.

243 RODRIGUEZ PRIETO, A. "PROTECCIÓN DE LA INFORMACIÓN", PARANINFO, MADRID, 1.986.

244 ROMERO CASABONA, C.M., "PODER INFORMÁTICO Y SEGURIDAD JURÍDICA", FUNDESCO, MADRID, 1.987.

245 ROMM, J., "DEFINING THE NATIONAL SECURITY. THE NONMILITARY ASPECTS", COUNCIL OF FOREIGN RELATIONS PRESS, NUEVA YORK, 1.993.

246 RUBIN, B, "SECRETS OF THE STATE. THE STATE DEPARTMENT AND THE STRUGGLE OVER U.S. FOREIGN PLICY", OXFORD UNIVERSITY PRESS, NUEVA YORK, 1.985.

247 RUEDA, FERNANDO,"LA CASA", TEMAS DE HOY, MADRID, 1.993.

248 RUSSELL, B., "SOCIEDAD HUMANA: ÉTICA Y POLÍTICA", CÁTEDRA, MADRID, 1.987.

249 SADOFSKY, D., "KNOWLEDGE AS POWER, POLITICAL AND LEGAL CONTROL OF INFORMATION", PRAEGER BOOKS, NUEVA YORK, 1.990.

250 SAINZ MORENO, F., "SECRETO E INFORMACIÓN EN DERECHO PÚBLICO", CÍVITAS, MADRID, 1.991.

251 SARASA LÓPEZ, M., "SOLUCIONES AL CONFLICTO SOCIAL PLANTEADO ENTRE EL ESTADO Y EL INDIVIDUO", JORNADAS INTERDISCIPLINARES SOBRE CRIPTOGRAFÍA, PRIVACIDAD Y AUTODETERMINACIÓN INFORMATIVA, ZARAGOZA, 1.995.

252 SARASA, M.A. Y PASTOR, J., "PROTOCOLO PARA LA TRANSFERENCIA AUTORIZADA DE INFORMACIÓN PERSONAL ENTRE ORGANIZACIONES CONSERVANDO LA PRIVACIDAD DE LOS DATOS", IV REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA, VALLADOLID, 1.996.

253 SARAZA JIMENA, R., "LIBERTAD DE EXPRESIÓN E INFORMACIÓN FRENTE A HONOR, INTIMIDAD Y PROPIA IMAGEN", ARANZADI, PAMPLONA,1.995.

254 SARPE, EDIT. "HISTORIA DEL PENSAMIENTO, FILOSOFÍA CONTEMPORÁNEA", MADRID, 1.988.

255 SÁNCHEZ DE DIEGO Y FERNÁNDEZ DE LA RIVA, M., Y OTROS, "EL CAMBIODE LAS ORGANIZACIONES EN LA NUEVA SOCIEDAD DE LA INFORMACIÓN", CADERNOS DO NOROESTE, VOL. 10 (1), 1.997, CENTRO DE CIENCIAS HISTÓRICAS Y SOCIALES, UNIVERSIDAD DE MINHO, PORTUGAL.

256 SÁNCHEZ DE DIEGO Y FERNÁNDEZ DE LA RIVA, M., "LOS MEDIOS DE COMUNICACIÓN SOCIAL EN LA CONSTRUCCIÓN DE LA DEMOCRACIA", VI CONGRESO INTERNACIONAL SOBRE PARTICIPACIÓN Y AUTOGESTIÓN, GUANAJUATO, MEXICO, 1.993.

257 SÁNCHEZ DE DIEGO Y FERNÁNDEZ DE LA RIVA, M., "LA LIBERTAD DE EXPRESIÓN DEL MILITAR PROFESIONAL", DOCTORAL, UNIVERSIDAD COMPLUTENSE, MADRID, 1.991.

258 SÁNCHEZ DE DIEGO Y FERNANDEZ DE LA RIVA, M., "LA TRANSPARENCIA DE LAS BASES DE DATOS COMO MECANISMOS DE PROTECCIÓN DE LA INTIMIDAD DE LAS PERSONAS" EN INFORMÁTICA Y DERECHO, Nº 4, MÉRIDA, 1.989.

259 SÁNCHEZ FERRIZ, R., "ESTUDIO SOBRE LAS LIBERTADES", TIRANT LO BLANCH ALTERNATIVA, VALENCIA, 1.995.

260 SÁNCHEZ GONZÁLEZ, S., "LA LIBERTAD DE EXPRESIÓN", EDIT. MARCIAL PONS, MADRID, 1.992.

261 SCHEIER, B.,"APPLIED CRYPTOGRAPHY", WILEY, NEW YORK, 1.995.

262 SCHMID, P.E., "REVIEW OF CIPHERING METHODS TO ACHIEVE COMMUNICATION SECURITY IN DIGITAL DATA TRANSMISSION NETWORKS", INTERNATIONAL ZURICHSEMINAR ON DIGITAL COMMUNICATIONS, SWISS FEDERAL INSTITUTE OF TECHONOLOGY (ETH), ZURICH,1.976.

263 SCHMID, P.E., "THE EVOLUTION OF VOICE COMMUNICATION SECURITY", SINGLE MARKET COMMUNICATIONS REVIEW APRIL , 1.992.

264 SCHNEIER, B., "APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITMS AND SOURCE", BRUCE SCHNEIER, 2ª DE. 1.996.

265 SCHNORR, C.P., "EFFICIENT IDENTIFICATION AND SIGNATYURES FOR SMART CARDS. IN ADVANCES IN CRYPTOLOGY", SPRINGER-VERLAG, NEW YORK, 1.990.

266 SCHOROEDER, M.R., "NUMBER THERY IN SCIENCE AND COMMUNICATIONS", SPRINGER, BERLÍN,1.984.

267 SEGRELLES DE ARENAZA, Y., "PROTECCIÓN PENAL DEL SECRETO DE ESTADO", INSTITUTO DE CRIMINOLOGÍ, MADRID, 1.994.

268 SGARRO, A., "CÓDIGOS SECRETOS", PIRÁMIDE, MADRID, 1.990.

269 SIMMONS, G., "CONTEMPORANS CRYPTOGRAPHY THE SCIENCE OF INFORMATION INTEGRITY", IEEE, PRESS, 1.992.

270 SINKOV, A.,"ELEMENTARY CRYPTANALYSIS", MATEMATIAL ASSOCIATION OF AMERICA, WASHINGTON, 1.966.

271 SONKOW, A., "ELEMENTARY CRYPTANALYSIS:A MATHEMATICAL APPROACH". NEW MATHEMATICAL LIBRARY, 1.966.

272 SORIANO, R.,"LIBERTADES PÚBLICAS", TECNOS, MADRID, 1.990.

273 STINSON, D., "CRYPTOGRAPHY: THEORI AND PRACTICE", 1.995.

274 SUIZA, OMNISEC, A.G. , FONDO DOCUMENTAL, REGENSDORF (ZURICH), 1.993.

275 THUROW, L., "LA GUERRA DEL SIGLO XXI", JAVIER VERGARA, BUENOS AIRES, 1.993.

276 TIEMPO, "MANUAL DE INTELIGENCIA", JULIO DE 1.995.

277 TIERNO GALVÁN, E., "LEYES POLÍTICAS ESPAÑOLAS FUNDAMENTALES (1.808-1.978), TECNOS, MADRID, 1.984.

278 TILBORG, H.C.A., "THE MANY FACES OF CRYPTOGRAPHY", IV REUNIÓN ESPAÑOLA SOBRE CRIPTOLOGÍA, VALLDOLID, 1.996.

279 TOFFLER, A., "EL CAMBIO DEL PODER", PLAZA Y JANÉ, BARCELONA, 1.990.

280 TOFFLER, A. Y H.,"LA CREACIÓN DE UNA NUEVA CIVILIZACIÓN, LA POLÍTICA DE LA TERCERA OLA", PLAZA & JANÉS, BARCELONA, 1.996.

281 TOFFLER, A Y J., "LAS GUERRAS DEL FUTURO", PLAZA & JANÉ, BARCELONA, 1.994.

282 TRUSTED INFORMATION SYSTEMS, "SOFTWARE KEY ESCROW", OVERHEADS OF PRESENTATION, GLENWOOD, MD, 1.994.

283 TSE, S. "THE ART OF THE WAR", THE CLARENTON PRESS, OXFORD, 1.963.

284 TUSELL, J., LAMO DE ESPINOSA, E., Y PARDO, R., "ENTRE DOS SIGLOS: REFLEXIONES SOBRE LA DEMOCRACIA ESPAÑOLA", ALIANZA EDITORIAL, MADRID, 1.996.

285 URQUÍA, A., DICCIONARIO TÉCNICO MILITAR, INGLÉS-ESPAÑOL, ESPAÑOL-INGLÉS, EDICIONES AGULLÓ, MADRID, 1.980.

286 VELÁZQUEZ BAUTISTA, R., "PROTECCIÓN JURÍDICA DE DATOS PERSONALES AUTOMATIZADOS", COLEX, MADRID, 1.993.

287 VICENTE Y GUERRERO, G., "OBTENCIÓN CLANDESTINA DE DATOS VERSUS PRIVACIDAD. NUEVAS PERSPECTIVAS EN LA PERMANENTE DIALÉCTIVA JUSTICIA SEGURIDAD JURÍDICA", JORNADAS INTERDISCIPLINARES SOBRE CRIPTOGRAFÍA, PRIVACIDAD Y AUTODETERMINACIÓN INFORMATIVA, ZARAGOZA, 1.995.

288 VITALIS, A., "INFORMATIQUE, POVOIR ET LIBERTÉS", ECONÓMICA, PARÍS, 1.981.

289 WELSH, D., " "CODES AND CRPTOGRAPHY", REIMPRESIÓN EN 1.988.

290 WITKER, J., "CÓMO ELABORAR UNA EN DERECHO", CÍVITAS, MADRID, 1.986.

291 ZUBIRI, X., "CINCO LECCIONES DE FILOSOFÍA", MONEDA Y CRÉDITO, MADRID,1.970.

APENDICE NORMATIVO

- Acuerdo sobre Seguridad de Información Militar Clasificada entre España y los Estados Unidos de América, y sus anejos, de 12 de marzo de 1.984.
- Bill of Right (EE.UU.) enmiendas a la constitución de 1.791.
- Constitución Española de 27 de diciembre de 1.978.
- Convención americana de Derechos Humanos de 22 de noviembre de 1.969. Pacto de San José de Costa Rica.
- Convención americana sobre Derechos Humanos, abril de 1.970.
- Convenio de 28 de enero de 1.981 para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal.
- Convenio de Viena sobre relaciones diplomáticas de 18 de abril de 1.961.
- Convenio para la protección de los Derechos y Libertades fundamentales de 4 de noviembre de 1.950.
- Convenio para la protección de los Derechos Humanos y de las libertades fundamentales, de 4 de noviembre de 1.950.
- Decisión del Consejo de Europa de 31 de marzo de 1.992, relativa a la seguridad de los sistemas de información.
- Declaración de los Derechos del Hombre y del Ciudadano de 24 de junio de 1.793.
- Declaración de los Derechos del Hombre y del Ciudadano, 26 de agosto de 1.789.
- Declaración de los Derechos y Libertades fundamentales. Resolución del Parlamento Europeo de 1.989.
- Declaración americana de los Derechos y Deberes del Hombre de 2 de mayo de 1.948.
- Declaración de Derechos del buen Pueblo de Virginia, 12 de junio de 1.776.
- Declaración Universal de los Derechos Humanos, 1.948.
- Declaración de independencia de los EE.UU. de América, 4 de julio de 1.776.
- Decreto 242/1.969, de 20 de febrero, Reglamento de Secretos Oficiales.
- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1.995, relativa a la protección de las personas físicas en lo que respecta al tratamientode datos personales y a la libre circulación de estos datos.
- Directiva 97/66/CE del Parlamento Europeo y del Consejo, de15 de diciembre de 1.997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

- LEY 62/1.978, DE 26 DE DICIEMBRE DE PROTECCIÓN JURISDICCIONAL DE LOS DERECHOS FUNDAMENTALES DE LA PERSONA.
-LEY 9/1.968, DE 5 DE ABRIL, SOBRE SECRETOS OFICIALES, MODIFICADA POR LA LEY 48/1.978 DE 7 DE OCTUBRE.
- LEY ORGÁNICA 1/1.982, DE 5 DE MAYO, DE PROTECCIÓN DEL DERECHO AL HONOR, A LA INTIMIDAD PERSONAL Y A LA PROPIA IMAGEN.
- LEY 11/1.998, DE 24 DE ABRIL, GENERAL DE TELECOMUNICACIONES.
- LEY ORGÁNICA NÚMERO 5/1.992, DE 29 DE OCTUBRE, DE REGULACIÓN DEL TRATAMIENTO AUTOMATIZADO DE LOS DATOS DE CARÁCTER PERSONAL.
- LEY 26/1.984, DE 19 DE JULIO, GENERAL PARA LA DEFENSA DE LOS CONSUMIDORES Y USUARIOS.
- LEY ORGÁNICA 10/1.995 DE 23 DE NOVIEMBRE DEL CÓDIGO PENAL.
- PACTO INTERNACIONAL DE DERECHOS ECONÓMICOS, SOCIALES Y CULTURALES DE 16 DE DICIEMBRE DE 1.966.
- PACTO INTERNACIONAL DE DERECHOS CIVILES Y POLÍTICOS DE 1.966.
- REAL DECRETO DE 24 DE JULIO DE 1.889 POR EL QUE ORDENA LA PUBLICACIÓN EN LA GACETA DE MADRID DE DE LA EDICIÓN REFORMADA DEL CÓDIGO CIVIL
- REAL DECRETO 632/1.987, DE 8 DE MAYO SOBRE ORGANIZACIÓN DE LA ADMINISTRACIÓN DEL ESTADO EN EL EXTERIOR.
- REAL DECRETO 1.883/1.996, DE 1 DE ENERO, SOBRE ESTRUCTURA BÁSICA DEL MINISTERIO DE DEFENSA.
- REAL DECRETO Nº 2.632, DE 27 DE DICIEMBRE DE 1.985, (PRESIDENCIA).
- REAL DECRETO 428/1.993, DE 26 DE MARZO, POR EL QUE SE APRUEBA EL ESTATUTO DE LA AGENCIA DE PROTECCIÓN DE DATOS.
- REAL DECRETO NÚMERO 287/1.991, DE 8 DE MARZO, CATÁLOGO DE PRODUCTOS, BIENES Y SERVICIOS A DETERMINADOS EFECTOS DE LA LEY GENERAL PARA LA DEFENSA DE LOS CONSUMIDORES Y USUARIOS.
- REAL DECRETO 263/1.996, DE 16 DE FEBRERO, POR EL QUE SE REGULA LA UTILIZACIÓN DE TÉCNICAS ELECTRÓNICAS, INFORMÁTICAS Y TELEMÁTICAS POR LA ADMINISTRACIÓN GENERAL DEL ESTADO.
- RECOMENDACIÓN DEL CONSEJO DE LA O.C.D.E.DE 26 DE NOVIEMBRE DE 1.992.
- FORO GOBIERNO-SECTOR PRIVADO SOBRE UNA POLÍTICA MUNDIAL DE CIFRADO. O.C.D.E. MARZO DE 1.996.
- RECOMENDACIONES DEL CONSEJO DE LA O.C.D.E., DE 27 DE MARZO DE 1.997, SOBRE DIRECTRICES DE POLÍTICA CRIPTOGRÁFICA.
- TRATADO CONSTITUTIVO DE LA C.E.E.
- PROYECTO DE LEY DE SECRETOS OFICIALES.(1.996).