





# **LIBERTAD Y SEGURIDAD EN EL ÁMBITO TECNOLÓGICO**

José María Molina  
Doctor en Derecho  
Criptólogo  
Director de CRIPTOSISTEMAS,S.A.  
[www.criptosistemas.com](http://www.criptosistemas.com)

## **SUMARIO:**

Introducción. Libertad. Medidas de prevención. Concepción sistémica: 1. La seguridad de la información como sistema. 2. Articulación de los elementos de “un sistema de seguridad de la información”. Conflicto de derechos y conciliación de intereses. Hacia una política global de seguridad de la información y las comunicaciones.

## **INTRODUCCIÓN**

La necesidad de un tratamiento masivo de información, con las máximas garantías de fidelidad y rapidez, demandó un procesamiento y almacenaje de información mediante soportes automatizados, que dio lugar a la Informática.

Cuando la exigencia se extiende a la transmisión a distancia de esa información mediante redes interconectadas, aparece la Telemática, como tecnología de la comunicación para el intercambio de información entre equipos informáticos.

La confluencia de estas formas de procesamiento, almacenaje y transmisión de información de forma automatizada, hace desaparecer las barreras de la distancia y el tiempo a la vez que permite la concentración de activos de conocimiento, haciéndolo más vulnerable, de donde surge una nueva relación entre datos y sus titulares, que necesita de una especial protección.

Existen importantes y numerosos precedentes sobre los efectos de las nuevas tecnologías que tal vez tengan su origen en la conocida sentencia del Tribunal Europeo de Derechos Humanos sobre el caso Klass, recaída 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.

## **LIBERTAD**

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, cuya evolución ha configurado el concepto de “libertad informática”, como hoy lo entendemos: 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”.

Este concepto de libertad informática, que nace vinculado al tratamiento del dato personal, va consolidando el perfil de una nueva libertad pública vinculada al entorno tecnológico y que es un producto de aluvión, formado por el precipitado de las diversas libertades concernidas en el proceso de uso y aplicación de las nuevas tecnologías de la información y las comunicaciones y su incidencia en el individuo.

En este sentido, en la Declaración de los Derechos y Libertades Fundamentales, aprobado por Resolución de 1.989, del Parlamento Europeo (DOCE C 120/51, de 16 de mayo; doc. A 2-3/89), en su artículo 6.2 establece que *“se garantizará el respeto de la esfera privada y de la vida familiar, del honor, del domicilio y de las comunicaciones privadas”*.

Esta garantía de respeto, esta libertad de comunicaciones, dada la naturaleza del entorno tecnológico en el que se produce, requiere control tanto de accesos como de archivos, garantía de integridad de los datos y garantía de confidencialidad de los mismos. En definitiva control de acceso, integridad y confidencialidad que, son los componentes esenciales de la seguridad de las comunicaciones. Lo que nos permite establecer un punto de confluencia e incluso, interdependencia, entre libertad y seguridad, tomando una nueva dimensión el clásico enfrentamiento entre libertad y seguridad, cuando se produce en un entorno tecnológico de comunicación.

### **MEDIDAS DE PREVENCIÓN**

Una característica esencial de la información, el conocimiento y el almacenamiento y comunicación de todo ello mediante la utilización de las nuevas tecnologías, es el carácter irreversible del daño causado. No sólo por la propagación de sus efectos que hace imposible determinar y cuantificar su alcance, sino por la ineficacia de los mecanismos judiciales para la persecución y sanción en el caso de comportamientos delictivos o contrarios a Derecho y, muy especialmente, las dificultades probatorias.

Esta irreversibilidad de los daños causados en casos de vulneración de los mecanismos tecnológicos hace que la sanción jurídica sea insuficiente por lo que la tutela real y efectiva de los derechos subyacentes requiere algo más que la actuación “a posteriori” del ordenamiento jurídico.

El propio ordenamiento jurídico exige para su plenitud, además de esta protección clásica “a posteriori”, sancionando conductas contrarias al mismo después de haberse producido, disponer de mecanismos que eviten de forma eficaz, “a priori”, en determinadas circunstancias, las consecuencias irreparables de eventuales violaciones, lo que se lleva a cabo a través de las medidas de seguridad.

Estas medidas de seguridad requieren, además de una eficacia operativa, una fundamentación y un soporte jurídico legitimador de su aplicación y lejos de desequilibrar la balanza libertad/seguridad en detrimento de la libertad, son, por el contrario, un presupuesto básico de la misma.

En España, la Sentencia del Tribunal Supremo de 10 de diciembre de 1.980 determina que *“La protección de los derechos no se contrae a la reparación de los perjuicios originados, sino que ha de extenderse a las medidas de prevención que razonablemente impidan ulteriores lesiones”*.

Para prevenir e impedir, de forma eficaz las intromisiones ilegítimas y neutralizar la vulnerabilidad tecnológica del almacenamiento y transmisión de información, estas medidas de prevención están constituidas, generalmente, por lo que se conoce como **“seguridad de la información”**, que incorpora, entre otros factores, la utilización de técnicas criptológicas.

Unas comunicaciones globales eficaces vienen a subrayar la necesidad de contar con una protección adecuada y unas medidas de seguridad eficientes, en cuanto disponibilidad del servicio, integridad de los mensajes, controles de acceso y confidencialidad, concordantes con la previsible gravedad de la amenaza.

En el uso de las tecnologías de la información y las comunicaciones no es concebible libertad sin seguridad.

### **CONCEPCIÓN SISTÉMICA**

En la sociedad actual los sistemas de información emergen inmersos en una compleja trama de relaciones cambiantes mediante las cuales se crean, se modifican, se agrupan, de combaten, o se extinguen, en superposición o competencia con otros sistemas, a los que tratan de reemplazar.

Esta parcela de la realidad dotada de elementos diferenciales se integra, junto con otras realidades de distinta naturaleza, dando lugar al *sistema de información*, que a su vez, integra otros de ámbito menor.

La acción y el sentido de actuación de todo sistema, implica una relación de colaboración con otros, en un proceso de complejización de relaciones y, a la vez, conlleva un esfuerzo por conservar su individualidad frente a los demás, todo ello en armónica relación.

Todo sistema de información contempla, al menos, las siguientes fases: *adquisición, procesamiento, distribución y protección de la información.*

La realidad del sistema de información se manifiesta como una trama de relaciones con distintos niveles, unos tienen sentido en sí mismos y otros, por el contrario, son incompletos y solo tienen sentido fuera de ellos.

Cada una de estas fases podría constituir *un sistema en sí mismo*, pero integrados en uno de nivel superior, el sistema de información.

### **1.- LA SEGURIDAD DE LA INFORMACIÓN COMO SISTEMA.**

El planteamiento básico que hemos de hacernos ante la seguridad informática para contemplarla como sistema, es la propia definición del *sistema, el modelo y la solución*, lo que nos permitirá ir del *problema a la solución*.

Los elementos esenciales de un sistema de seguridad de la información, siguiendo los criterios RRH, serían:

#### **1.1.- El objetivo.**

Para analizar la seguridad de la información como sistema hemos de determinar, en primer lugar su objetivo, que no es otro que *lograr la protección de la información*. Y este objetivo es *posible* utilizando diversos medios.

#### **1.2.- Las alternativas técnicas.**

El objetivo de proteger la información puede ser alcanzado a través de diversas alternativas técnicas o instrumentales, que no son otra cosa que diferentes “*sistemas*” que dan solución al problema,

El objetivo es tan amplio que para su logro los medios pueden ser de naturaleza normativa, política, física, organizativa, *criptológica*, electromagnéticas, etc.

Cuando hablamos de *sistema de seguridad informático* estamos refiriéndonos a una *combinación de todo lo anterior*.

#### **1.3.- Costes.**

Los recursos requeridos para la utilización de cada alternativa o, como es el caso del sistema de seguridad de la información, para el conjunto de alternativas necesarias, implica unos *costes* y *proporciona un beneficio o ventaja, medible en cuanto a la consecución del objetivo buscado*.

Siendo necesario asumir tanto los costes como las ventajas en un sentido muy amplio y no solo contemplarlos en su traducción monetaria. Aspecto particularmente significativo en lo que se refiere al sistema de seguridad de la información por cuanto de intangible, y dificultad de comprensión tiene, en algunos casos, la ventaja resultante.

#### **1.4.- El modelo matemático.**

La seguridad de la información viene determinada por los peligros, riesgos y amenazas a que puede verse sometida la información.

La variedad e intensidad de los riesgos y amenazas son tan diversas 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, que para ser efectiva la seguridad ha de ser superior a los niveles de agresiones potenciales. Por todo ello, 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* bajo el que hay que estudiar el problema de la seguridad.

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 cual 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.

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.

Con la teoría de los juegos se pueden construir matrices y esquemas utilizables para la solución de problemas reales o eventuales.

En el caso concreto de la teoría de los juegos aplicada a la seguridad de la información, estaríamos en presencia de *juegos 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 podría ser la de anticiparse al atacante, incorporar los códigos y lógica del atacante, “tener un atacante en la cabeza”.

### **1.5.- Criterios.**

Los criterios que relacionan y tratante medir objetivos y costes o recursos empleados para poder escoger la alternativa óptima.

El criterio comunmente aceptado es el de coste/beneficio o de *coste/eficacia*.

En los sistemas de información se pueden diseñar con criterios de eficacia, eficiencia, criterios económicos, etc, porque para dichos criterios se conocen parámetros que, maximizando unos y minimizando otros, se puede tender hacia *diseños óptimos*.

Cuando se trata del criterio de seguridad el problema se torna *más complejo* y difícilmente resoluble. Los criterios y puntos de vista que utiliza el diseñador para obtener seguridad no son los mismo bajo los cuales se moverá el atacante, sería, como hemos indicado, la puesta en práctica de la teoría matemática de los juegos.

## **2.- ARTICULACIÓN DE LOS ELEMENTOS DE UN “SISTEMA DE SEGURIDAD DE LA INFORMACIÓN”.**

El propio proceso del análisis de un sistema de seguridad de la información, es un sistema en sí mismo en el que las salidas de cada fase hace reconsiderar la siguiente y, por interacciones sucesivas, nos aproximamos gradualmente al resultado buscado, iniciándose el proceso con el *problema* y finalizando con la *solución*.

El orden secuencial de las fases de articulación de los elementos de un sistema de seguridad de la información sería el siguiente:

### **2.1.- Formulación.-**

#### *2.1.1.- Planteamiento del problema.*

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 y, concretamente, su valor, la sitúan en un nivel que demanda su posesión útil y controlada, lo que requiere su adquisición, procesamiento y distribución y, necesita protección para evitar pérdida no deseadas, producidas por cualquier motivo, ya sean causas naturales, tecnológicas, derivadas de la acción humana, o producto de egoismos de terceros.

#### 2.1.2.- *Concreción de objetivos a conseguir.*

Conseguir la protección de la información, con medios posibles en una relación proporcionada de coste/beneficio.

### 2.2.- **Exploración.-**

#### 2.2.1.- *Delimitación de entorno.*

En nuestro entorno cultural, social, económico y político, y con un grado elevado de desarrollo tecnológico, con sistemas de comunicaciones que pueden ser globales, y en un clima de desconfianza, la comunicación de información valiosa, tiene la **necesidad de protegerla**. Las reiteradas vulneraciones de los sistemas empleados por la evolución de los medios y el conocimiento, provocan necesidades de seguridad en **permanente cambio**.

#### 2.2.2.- *Determinar sus límites.*

Los límites a los objetivos a conseguir vienen derivados de una parte de la exigencia de proporcionalidad en la utilización de medios y recursos, el nivel tecnológico y las exigencias legales.

#### 2.2.3.- *Definición e identificación de componentes esenciales.*

- Variedad e intensidad de los **riesgos y amenazas** a que está sometido un sistema de información, lo que provoca una gran dificultad para el establecimiento de "seguridad necesaria".

- Estos riesgos pueden ser de orden tecnológico, organizativo, físico, lógico, normativos, electromagnéticos, humanos, etc.

- Aplicación de la teoría de los juegos para determinación del **modelo matemático**.

- Acceso al sistema.

- Manipulaciones,

- Pérdidas,

- Modificaciones.

- Conocimiento por personal no autorizado.

- Medios a utilizar: Políticos, normativos, organizativos, lógicos dentro de los cuales destacan los criptológicos, electromagnéticos, administrativos, físicos, humanos.

### 2.3.- **Comprensión.-**

#### 2.3.1.- *Recogida de información para comprender funcionamiento del sistema.*

- **Estudio de conjunto** en profundidad y desde una perspectiva global, considerando todas las implicaciones de un sistema de seguridad de la información, tales como las variables políticas, jurídicas, tecnológicas, sociales, culturales, y como no, económicas.

### 2.4.- **Concepción.-**

2.4.1.- *Busqueda de soluciones alternativas que permitan conseguir los objetivos asignados.*

- **Políticas de seguridad** de la información:

. Control de accesos: Estas políticas establecen en qué circunstancias un sujeto puede acceder a un objeto de información. Estas políticas pueden ir desde el "Need-to-Know", según el cual un usuario accede estrictamente a aquellos objetos de información que necesita conocer para la realización de su trabajo,

hasta el principio de *máximo privilegio*, según el cual se tendría acceso a un amplio objeto de información.

. Flujo 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.

- Diseño específico del *modelo de seguridad* para el ámbito a que se refiera.

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 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.

. Modelo de seguridad discrecional, en los que 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.

. Modelo de seguridad obligatoria, se ocupa 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 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 reacción 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 autoridad (los sujetos), estableciéndose una relación de orden entre confidencialidad y autoridad.

- Medios a utilizar, naturaleza y niveles.

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.

## **2.5.- Evaluación.-**

### *2.5.1.- Valoración de alternativas.*

Evaluación de las políticas de seguridad, los modelos y los distintos medios y niveles que consigan la protección efectiva de la información, determinará las distintas alternativas posibles.

## **2.6.- Interpretación.-**

### *2.6.1.- Análisis e interpretación de las distintas valoraciones.*

El análisis pormenorizado de las alternativas con las políticas, modelos, medios y sus respectivos niveles de forma que se llegue a la concreción de los medios idóneos, en los marcos indicados, y los niveles de seguridad (y en su caso criptológico) necesarios para solucionar el problema de protección de información específico.

## **2.7.- Selección.-**

### *2.7.1.- Determinación de los resultados elegidos para la toma de decisiones.*

La toma de decisiones se ha de basar en la selección de:

*-Política de seguridad.*

*-Modelo de seguridad.*

*-Medios y mecanismos de seguridad:*

*.Físicos.*

*.Organizativos.*

*.Normativos*

*.Criptológicos.*

*.Electromagnéticos.*

Dentro de estos medios y mecanismos de seguridad existen varios *niveles* por lo que habrá que pronunciarse sobre ello en la preparación de la decisión.

De todo ello se conseguirá la decisión concreta para la *solución* específica del problema de seguridad de la información, con lo que se cierra el sistema.

## **CONFLICTO DE DERECHOS Y CONCILIACIÓN DE INTERESES**

Existe un permanente conflicto de intereses entre el ciudadano -de forma individual o integrado en corporaciones privadas- y las necesidades de seguridad del Estado.

Este conflicto se da entre el indiscutible derecho del ciudadano de proteger su esfera privada, que ha dado en llamarse "*the right to privacy*", y el deber constitucional de todo Estado de proteger su seguridad.

En los extremos del conflicto podrían estar las posiciones representadas por Henry L. Stimson, Charles A. Haswkins y Whitfield Diffie que tal vez encarnen el pensamiento norteamericano y europeo en este tema.

En Norteamérica se pasó del "*Gentlemen do not read each other's mail*" de Henry L. Stimson, Secretario de Estado del Presidente Edgar Hoover, 1929, a Charles A. Hawkins, Acting Assistant Secretary of Defense, 3 de mayo de 1993: "*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*".

Para Whitfield Diffie: "*...an individual's privacy as opposed to Government secrecy*".

Además de este clásico conflicto existen otros que se dan dentro del ámbito privado y se produce entre sus distintos actores como el que surge en el mercado, en el que las empresas han de preservar su información en aras a la competitividad, y los ciudadanos -a veces convertidos en consumidores- necesitan preservar su vida privada.

El Estado como persona jurídica unitaria que actúa como tal en la esfera internacional y la organización política que encarna, necesita asimismo, del acopio de información para su normal funcionamiento que, generalmente, suele ser pública. Para

evitar todo intento ilegítimo de quiebra del juego constitucional, la salvaguarda del Estado y de sus instituciones democráticas, a veces, se exige el acopio de información sensible.

En términos generales 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 protección de las comunicaciones privadas, que es genérica, dirigida a un espectro muy amplio de comunicaciones, es extensa, y requiere tal vez una menor intensidad en la protección.

Cuando hay conflicto, tanto libertad como seguridad tienen sus límites fundamentados en la eficacia de protección de derechos y libertades. La seguridad es, un instrumento para la libertad, y el mejor uso que se puede hacer de la libertad nunca es el “suicidio”.

### ***HACIA UNA POLÍTICA GLOBAL DE LIBERTAD Y SEGURIDAD EN LAS COMUNICACIONES***

Lo que conocemos como sociedad de la información es un concepto global, que para alcanzar su plenitud ha de generar la confianza necesaria. Los medios generadores de confianza, con la seguridad de las comunicaciones como elemento central, han de ser también globales.

En la nueva sociedad, la criptología, y el derecho como instrumentos de ordenación, adquieren especiales dimensiones.

La amplificación de los efectos de la información debido al 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.

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

Los elementos del problema están constituidos por la colisión que se produce, 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.

La situación es global y, demanda, eventualmente, una política global de seguridad de las comunicaciones, elaborada en el seno de Naciones Unidas, que armonizando libertad y seguridad de respuesta a los retos individuales y colectivos que tiene planteados y sean válidos para la construcción de un nuevo orden político en el comienzo del tercer milenio.

Madrid, julio 2.002

## **TEXTOS INTERNACIONALES MÁS SIGNIFICATIVOS QUE RECOGEN LA LIBERTAD DE EXPRESIÓN.**

### **C) Declaraciones de principios:**

#### **- Declaración de Derechos del Buen Pueblo de Virginia (12 de junio de 1.776).**

XII.-"Que la libertad de prensa es uno de los grandes baluartes de la libertad y no puede ser restringida jamás, a no ser por gobiernos despóticos".

#### **- Declaración de independencia de los EE.UU. de América (4 de julio de 1.776).**

"...que todos los hombres son creados iguales; que son dotados por su creador de ciertos derechos inalienables; entre los cuales están la vida; la libertad y la búsqueda de la felicidad..."

#### **- Declaración de los Derechos del Hombre y del Ciudadano (26 de agosto de 1.789).**

Artículo 10.- "Nadie debe ser inquietado por sus opiniones, incluso religiosas, en tanto que su manifestación no altere el orden público establecido por la ley".

Artículo 11.- "La libre comunicación de los pensamientos y las opiniones es uno de los derechos más preciados del hombre; todo ciudadano puede, por tanto, hablar, escribir e imprimir libremente, salvo la responsabilidad que el abuso de esta libertad produzca en los casos determinados por la Ley".

#### **- Declaración de los Derechos del Hombre y del Ciudadano (24 de junio de 1.793).**

Artículo 7.- "No pueden ser prohibidos el derecho a manifestar el pensamiento y las opiniones, sea por medio de la prensa, sea de cualquier otra forma, el derecho de reunirse pacíficamente, el libre ejercicio del culto. La necesidad de enunciar estos derechos supone o la presencia o el recuerdo reciente del despotismo".

### **D) Textos internacionales:**

#### **- Declaración Universal de los Derechos Humanos, 1.948.**

Artículo 19.- "Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir información y opiniones y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión".

Artículo 18.- "Toda persona tiene derecho a la libertad de pensamiento, de conciencia y de religión; este derecho incluye la libertad de cambiar de religión o de creencia, así como la libertad de manifestar su religión o su creencia, individual y colectivamente, tanto en público como en privado, por la enseñanza, la práctica, el culto y la observancia".

#### **- Declaración americana de los Derechos y Deberes del Hombre (2 de mayo de 1.948).**

Artículo 4.- "Toda persona tiene derecho a la libertad de investigación de opiniones, de expresión y de difusión del pensamiento por cualquier medio".

#### **- Convenio para la protección de los Derechos y Libertades Fundamentales (4 de noviembre de 1.950).**

Artículo 10.- " 1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber ingerencias 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, que entrañan deberes y responsabilidades, podrá ser sometido a ciertas formalidades, condiciones, restricciones o sanciones, previstas por la ley, que constituyan medidas necesarias, en una sociedad democrática, para la defensa del orden y la prevención del delito, la protección de la salud o de la moral, la protección de la reputación o de los derechos ajenos, para impedir la divulgación de informaciones confidenciales o para garantizar la autoridad y la imparcialidad del poder judicial".

#### **- Convenio para la protección de los Derechos Humanos y de las libertades fundamentales (4 de noviembre de 1.950 -Convenio Europeo-).**

Artículo 9.- "1. Toda persona tiene derecho a la libertad de pensamiento, de conciencia y de religión; este derecho implica la libertad de cambiar de religión o de convicciones, así como la libertad de manifestar su religión o sus convicciones individual o colectivamente, en público o en privado, por medio del culto, la enseñanza, las prácticas y la observancia de los ritos.

2. La libertad de manifestar su religión o sus convicciones no puede ser objeto de más restricciones que las que, previstas por la ley, constituyan medidas necesarias, en una sociedad democrática, para la seguridad pública, la protección del orden, de la salud o de la moral públicas, o la protección de los derechos o las libertades de los demás".

#### **- Convenio Internacional sobre la eliminación de todas las formas de discriminación racial, 1.965.**

Artículo 5.- "En conformidad con las obligaciones fundamentales estipuladas en el artículo 2 de la presente Convención, los Estados parte se comprometen a prohibir y eliminar la discriminación racial en todas sus formas y garantizar el derecho de toda persona a la igualdad ante la ley, sin distinción de raza, color y origen nacional o étnico, particularmente en el goce de los derechos siguientes: ...d) VII.- El

derecho a la libertad de pensamiento, de conciencia y de religión. VIII.- El derecho a la libertad de opinión y de expresión".

**- Pacto Internacional de Derechos Económicos, Sociales y Culturales (16 de diciembre de 1.966).**

Artículo 15.3.- "Los Estados partes en el presente Pacto se comprometen a respetar la indispensable libertad para la investigación científica y para la actividad creadora".

**- Pacto Internacional de Derechos Civiles y Políticos (1.966).**

Artículo 19.- "1. Nadie podrá ser molestado a causa de sus opiniones.

2. 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.

3. El ejercicio del derecho previsto en el párrafo 2º 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".

Artículo 18.- "1. Toda persona tiene derecho a la libertad de pensamiento, de conciencia y de religión; este derecho incluye la libertad de tener o de adoptar la religión o sus creencias, individual o colectivamente, tanto en público como en privado, mediante el culto, la celebración de los ritos, las prácticas y la enseñanza.

2. Nadie será objeto de medidas coercitivas que puedan menoscabar su libertad de tener o de adoptar la religión o las creencias de su elección.

3. La libertad de manifestar la propia religión o las propias creencias estará sujeta únicamente a las limitaciones prescritas por la ley que sean necesarias para proteger, la seguridad, el orden, la salud o la moral pública o los derechos y libertades fundamentales de los demás.

4. Los Estados parte en el presente Pacto se comprometen a respetar la libertad de los padres y, en su caso, de los tutores legales para garantizar que los hijos reciban la educación religiosa y moral que esté de acuerdo con sus propias convicciones".

**- Convención americana de Derechos Humanos (22 de noviembre de 1.969). Pacto de San José de Costa Rica.**

Artículo 13.- "1. Toda persona tiene derecho a la libertad de pensamiento y 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.

2. El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar:

a) El respeto a los derechos o a la reputación de los demás, ó

b) La protección de la seguridad nacional, el orden público o la salud o la moral públicas.

3. No se puede restringir el derecho de expresión por vías o medios indirectos, tales como el abuso de controles oficiales o particulares de papel para periódicos, de frecuencias radioeléctricas o de enseres y aparatos usados en la difusión de información o por cualquier otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones.

4. Los espectáculos públicos pueden ser sometidos por la ley a censura previa, con el exclusivo objeto de regular el acceso a ellos para la protección moral de la infancia y la adolescencia, sin perjuicio de lo establecido en el inciso 2.

5. Estará prohibida por la ley toda propaganda en favor de la guerra y toda apología del odio nacional, racial o religioso que constituyan incitaciones a la violencia o cualquier otra acción similar contra cualquier persona o grupo de personas, por ningún motivo, inclusive los de raza, color, religión, idioma u origen nacional".

Artículo 14.- "2. En ningún caso la rectificación o la respuesta eximirán de las otras responsabilidades legales en que se hubiere incurrido".

3. Para la efectiva protección de la honra, y de la reputación, toda publicación o empresa periodística, cinematográfica, de radio o televisión tendrá una persona responsable que no esté protegida por inmunidades ni disponga de fuero especial".

**- Convención americana sobre Derechos Humanos (Abril de 1.970).**

Artículo 13.- "1. Toda persona tiene derecho a la libertad de pensamiento y 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.

2. El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura, sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la Ley y ser necesarias para asegurar:

- a) El respeto a los derechos o a la reputación de los demás.
- b) La protección de la seguridad nacional, el orden público o la salud o la moral públicas".

**- Declaración de los Derechos y Libertades Fundamentales. Resolución del Parlamento Europeo de 1.989.<sup>1</sup>**

Artículo 5.- Libertad de opinión y de información.

"1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o comunicar informaciones o ideas, en particular filosóficas, políticas y religiosas.

2. El arte, la ciencia y la investigación son libres. Se respetará la libertad académica.

Artículo 6.- Vida privada.

"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."

Artículo 18.- Derecho de acceso a la información.

"Toda persona tiene derecho de acceso y de rectificación en lo que se refiere a los documentos administrativos y los datos que les afecten".

Artículo 26.- Límites.

"Los derechos y libertades enumerados en la presente Declaración 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".

Artículo 27.- Nivel de protección.

"Ninguna de las disposiciones de la presente Declaración se podrá interpretar en el sentido de limitar la protección ofrecida por el Derecho comunitario, el Derecho de los Estados miembros, el Derecho Internacional y los Tratados y Acuerdos Internacionales relativos a los derechos y libertades fundamentales, ni de oponerse a su desarrollo".

Artículo 28.- Abuso de derechos.

"Ninguna disposición de la presente Declaración podrá interpretarse en forma tal que confiera derecho alguno para emprender una actividad o desarrollar actos tendentes a la limitación o supresión de cualquiera de los derechos y libertades proclamados en la presente Declaración".

**E) Textos de la Iglesia.**

**- Pacem in Terris (11 de abril de 1.963).**

"Derechos referentes a los valores morales y culturales: ...Todo ser humano tiene derecho..., a la libertad para buscar la verdad y, dentro de los límites del orden moral y del bien común, para manifestar y defender sus ideas, para cultivar cualquier arte y finalmente para tener una objetiva información de los sucesos públicos".

## **RESUMEN**

La aparición de las nuevas tecnologías aplicadas a la información y las comunicaciones ha potenciado, de forma que no ha tenido precedentes en la historia, el masivo tratamiento y comunicación de información, con una directa incidencia en el progreso y desarrollo del hombre. En un proceso paralelo se han incrementado las vulnerabilidades y riesgos, lo que suscita nuevos requerimientos tecnológicos, jurídicos y políticos para hacer posible la denominada Sociedad de la Información.

En la nueva sociedad comienza a emerger el perfil de una nueva libertad pública vinculada al entorno tecnológico con exigencias de naturaleza técnica como control de acceso, integridad, o confidencialidad, y de naturaleza jurídica vinculada a las medidas de prevención..

La seguridad de las comunicaciones adquiere una dimensión que trasciende su funcionalidad directa y se convierte en un instrumento que posibilita la libertad, con lo que viene a añadir nuevos enfoques al tradicional dilema libertad/seguridad.

La magnitud del proceso es global y por ello consideramos de esencial importancia hacer un enfoque sistémico de la seguridad de las comunicaciones.

La seguridad técnica como instrumento de seguridad jurídica y de libertad no deja de suscitar conflictos de derechos que demandan conciliación de intereses. El secreto de las comunicaciones, la privacidad del individuo, la intimidad, los secretos comerciales e industriales, la prevención y persecución del delito, las necesidades de seguridad y defensa del Estado requieren para su armonización un balanceo ponderado de los intereses en juego. Si todo ello se proyecta a escala global, como es el caso, estamos en presencia de la necesidad de formular una política mundial de seguridad de las comunicaciones, elaborada en el seno de Naciones Unidas, que armonizando libertad y seguridad sepa dar respuesta a los retos individuales y colectivos que tiene planteado la humanidad con la implantación de las nuevas tecnologías.

## **SUMMARY**

The appearance of the new technologies applied to the information and the communications it has promoted, so that it has not had precedents in the history, the massive treatment and communication of information, with a direct effect in the progress and development of the man.

In a parallel process there have been increased the vulnerabilities and risks, which provokes new technological, juridical and political requirements to do possibly the Society called of the Information. In the new society it begins to emerge the profile of a new public freedom linked to the technological environment with requirements of technical nature as control of access, integrity, or confidentiality, and of juridical nature linked to the measurements of prevention..

The safety of the communications acquires a dimension that trasciende its direct functionality and is converted into an instrument that makes possible the freedom, with what it comes to add new approaches to the traditional dilemma freedom/security. The magnitude of the process is global and for it we considered of essential importance to do an approach sistemic of the safety of the communications.

The technical safety as instrument of juridical safety and of freedom does not stop provoking conflicts of rights that sue conciliation of interests. The secret of the communications, the privacy of the individual, the intimacy, the commercial and industrial secrets, the prevention and pursuit of the crime, the safeties needs and defense of the State need for its harmonization a balancing considered of the interests in game.

If all this is projected to global scale, since it is the case, we are in presence of the need to formulate a world security communications politics, elaborated in the bosom of United Nations, which harmonizing freedom and security can give response to the individual and collective challenges that there has the humanity raised with the introduction of the new technologies.