FACULTAD DE DERECHO Y CIENCIAS SOCIALES

DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN EL INTERNET DE LAS COSAS

Trabajo de Titulación presentado en conformidad a los requisitos establecidos para optar por el Título de Abogada de los Tribunales y Juzgados de la República

Profesor Guía

Ms. Lorena Naranjo Godoy

Autora

Stephanie Monserrat Medina Cevallos

Año

2017

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.”

_____

Lorena Naranjo Godoy

Máster en Derecho de las Nuevas Tecnologías

C.C.: 170829378-0

DECLARACIÓN DEL PROFESOR CORRECTOR

“Declaro haber revisado este trabajo, dando cumplimiento a todas las disposiciones vigentes que regulan los trabajos de titulación.”

Elsa Jacqueline Guerrero Carrera

Máster en Derecho con mención en Derecho Económico

C.C.: 200002747-0

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

Stephanie Monserrat Medina Cevallos

C.C.: 172130083-6

AGRADECIMIENTO

A Dios por darme valentía para vencer todos los obstáculos.

A mis padres por su apoyo y su sacrificio constante.

A mi familia cercana y amigos que estuvieron en los momentos más importantes cuidando de mí y alentándome a seguir adelante.

A mi docente guía quien, con mucho cariño y gran sabiduría, dirigió mi trabajo de titulación, además me enseñó grandes lecciones de vida como a dar lo mejor de mí siempre.

Stephanie

DEDICATORIA

A mis padres por haberme dado la vida, darme amor e inculcarme valores como la humildad, la bondad y el sacrificio.

Stephanie

RESUMEN

La tecnología, dentro de los últimos años, ha avanzado a pasos agigantados; de modo que, el internet se ha convertido en un elemento indispensable en la vida de las personas. Cada día, son más el número de dispositivos electrónicos que hacen uso de internet. A esta infraestructura tecnológica de dispositivos interconectados a internet en cualquier tiempo y lugar, se ha denominado como internet de las cosas, también llamado *internet of things*, por su nombre en inglés.

El origen de este tipo de tecnología trae consigo una serie de beneficios para los usuarios, así también, puede desatar una serie de riesgos, lo que crea la necesidad de tomar medidas que protejan a los datos personales que son recolectados en los dispositivos que hacen uso de internet de las cosas, tanto desde el diseño del producto, así como la norma que regula el territorio donde se han utilizado los dispositivos.

El internet de las cosas, es considerado como un desarrollo fundamental en área tecnológica. En la actualidad, este tipo de tecnología, se aplica en varias áreas de la vida cotidiana, como por ejemplo: en salud, industria, transporte y entre otros. Sin embargo, al conectarse a internet, los diversos dispositivos que forman parte de esta infraestructura tecnológica recogen información de las personas que hacen uso de ellos.

Como referencia se ha tomado en cuenta los sistemas de protección de datos personales con los estándares más altos, de modo que sea posible identificar cuál de ellos podría aplicarse en la realidad ecuatoriana.

En el Ecuador, el derecho a la protección de datos personales, se encuentra respaldado por una acción constitucional denominada como *hábeas data*, esta acción tiene como principal objetivo proteger la información de las personas, además de que otorga a los titulares la facultad para conocer qué tipo de información suya se recoge por diversos medios y cuál es el trato que se les dará.

ABSTRACT

Technology, in recent years, has advanced by leaps and bounds; So that the internet has become an indispensable element in people's lives. Every day, more are the number of electronic devices that make use of the internet. To this technological infrastructure of devices interconnected to internet in any time and place, has been denominated like Internet of things, also call Internet of things, by its name in English.

The origin of this type of technology brings with it a series of benefits for the users, as well, it can unleash a series of risks, which creates the need to take measures that protect the personal data that are collected in the devices that make use Of internet of the things, as much from the design of the product, as well as the norm that regulates the territory where the devices have been used.

The internet of things, is considered as a fundamental development in technological area. At present, this type of technology is applied in several areas of daily life, such as in health, industry, transportation and among others. However, when connecting to the internet, the various devices that are part of this technological infrastructure gather information from the people who make use of them.

As a reference has taken into account the systems of protection of personal data with the highest standards, so that it is possible to identify which of them could be applied in the Ecuadorian reality.

In Ecuador, the right to the protection of personal data is backed by a constitutional action to known as habeas data, this action has as main objective to protect the information of the people, besides that it gives the holders the power to know what Type of information is collected by various means and what is the treatment that will be given.

ÍNDICE

INTRODUCCIÓN 1
1 CAPITULO I. PROTECCIÓN DE DATOS PERSONALES EN EL INTERNET DE LAS COSAS 3
1.1 Definición de dato personal: 3
1.2 Conductas lesivas comunes: 4
1.3 Protección de datos personales: 7
1.3.1 Antecedentes 9
1.4 Reglamento Europeo 12
1.5 La protección de datos en España con referencia al *IoT* 14
1.6 La Protección de datos en el Ecuador 16
2 CAPITULO II. EL INTERNET DE LAS COSAS 20
2.1 Antecedentes y evolución del internet de las cosas 20
2.2 El impacto del internet de las cosas en la sociedad y ámbitos de aplicación: 22
2.3 Problemática que se deriva del crecimiento del *IoT* 25
2.4 Privacidad por diseño, la alternativa para la protección de datos personales más apegada a la realidad: 28
3 CONCLUSIONES 34
REFERENCIAS 36
ANEXOS 40

INTRODUCCIÓN

El ensayo aborda el estudio del internet de las cosas, también conocido por las siglas *IoT*, como una nueva amenaza implícita en la tecnología que vulnera la protección de datos personales, debido a que propone nuevas formas de conexión que llevan en sí mismas, peligros ocultos para las personas, naturales o jurídicas, que hacen uso de la tecnología de éste tipo, de forma voluntaria o involuntaria.

El problema fundamental de este tipo de tecnología, radica en que, a través del uso de esta infraestructura tecnológica se generan y transmiten grandes cantidades de datos personales cuya confidencialidad, titularidad y protección, pueden ser vulnerables, generando como consecuencia, que los titulares pierdan el control sobre ellos, poniendo en riesgo la información personal e inclusive otros derechos relacionados a ella como la intimidad o la privacidad.

El problema comprende aspectos como la falta de conocimiento sobre los datos personales contenidos en la infraestructura que forma el internet de las cosas, además de la falta de control por parte de los titulares de los ficheros en cuanto a la captación, tratamiento, circulación y difusión de los mismos.

Este tipo de tecnología ya se utiliza en el Ecuador, por lo que, es necesario adoptar en la legislación ecuatoriana, normas que regulen el tratamiento de los datos personales contenidos en el internet de las cosas, a pesar de que el tamaño del mercado nacional sea pequeño.

El método que fue empleado, para la investigación del problema planteado, fue un análisis exegético sobre la protección de datos personales en el internet de las cosas, además del estudio de literatura y doctrina especializada en el tema que permitió definir conceptos, aplicaciones y usos del internet de las cosas, además de identificar qué tipo de datos personales puede contener esta infraestructura tecnológica. Principalmente, el análisis del Reglamento europeo, ayuda a determinar, qué principios pueden ser adoptados y adaptados a la realidad ecuatoriana, tomando en cuenta, el acelerado avance tecnológico del cual también es parte el Ecuador.

El desarrollo del presente trabajo académico se encuentra estructurado de la siguiente forma: El primer tema hace un acercamiento a la normativa nacional e internacional vigente, dónde se reconoce el derecho a la protección de datos personales. El segundo tema desarrolla el concepto de internet de las cosas y su crecimiento en la actualidad, así como la incidencia en la vida de las personas, y del mismo modo, las alternativas que pueden ser aplicables en el país para la protección de los datos personales, tomando en cuenta la realidad del Ecuador.

La conclusión principal arroja que, en base a la realidad ecuatoriana, es difícil que una normativa estatal exija a las grandes compañías productoras de tecnología, a tener un trato diferenciado con el país. Esto se debe a que el mercado ecuatoriano no es tan significativo, además cabe reconocer que el país no es productor de tecnología sino es importador de ella, por lo tanto no tendría sentido crear una norma que carezca de aplicabilidad. Sin embargo, existen otras alternativas que transcienden de la misma tecnología que permite salvaguardar la protección de los datos personales de los ciudadanos.

1 CAPITULO I. PROTECCIÓN DE DATOS PERSONALES EN EL INTERNET DE LAS COSAS

1.1 Definición de dato personal:

A simples rasgos, un dato personal puede entenderse como un tipo de información que permite identificar concretamente a una persona, ya sea su nombre completo, su número de identificación y hasta sus rasgos faciales.

El Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE del Parlamento Europeo en su Dictamen número 4/2007, para construir una definición sobre datos personales parte de cuatro elementos, entre los que están: toda información, sobre, identificada o identificable y persona física. Es decir una información debe contar con estos cuatro elementos para ser considerada como un dato personal.

Cuando se habla del elemento “toda información” puede entenderse que el concepto comprende a la información objetiva y subjetiva, es decir, aquella que permite identificar al sujeto que es titular de los datos, como también, los datos financieros de la persona, que permiten conocer el perfil completo del titular, independientemente de que si la información es verídica o no. (Grupo de Trabajo sobre Protección de Datos, 2000, pág. 6)

En cambio, el elemento “sobre” se relaciona a que la información está relacionada directamente con la persona, en otras palabras, es el vínculo de la información que se une a la persona. (Grupo de Trabajo sobre Protección de Datos, 2000, págs. 9-10)

Por otra parte, el componente “identificada o identificable”, se refiere a la persona cuyas características específicas la distinguen de los demás y la hacen única. Una persona es identificada, directa o indirectamente, gracias a ciertos datos, llamados identificadores, que guardan relación estrecha con la persona, titular de ellos. (Grupo de Trabajo sobre Protección de Datos, 2000, págs. 12-13)

Finalmente, en el componente “persona física”, el Grupo de Trabajo parte desde la premisa de que el derecho a la protección de datos personales es un derecho

exclusivo de los seres humanos tomando en cuenta al Art.8 de la declaración Universal de los Derechos Humanos que determina el derecho de las personas al reconocimiento de su personalidad jurídica. (Grupo de Trabajo sobre Protección de Datos, 2000, pág. 24)

En conclusión, se puede decir que los datos personales no son aquella información que la persona desea guardar en secreto de los demás, sino que por el contrario, es la información que forma parte de la naturaleza de la persona o que a través de ella puede ser concretamente identificada. Este tipo de información en muchos casos es utilizada para fines ilegales, por lo que los titulares deben contar con medios efectivos para su protección.

1.2 Conductas lesivas comunes:

Con la acelerada evolución que ha tenido el internet, la información, sobre todo personal, se ha convertido en el principal objetivo no solo de la cyberdelincuencia, sino de empresas que buscan posicionar sus productos e interferir en la decisión de consumo. Además, esta intromisión en la privacidad de los usuarios, principalmente, respecto de la seguridad y titularidad de sus datos. El internet ha generado un nuevo espacio donde sujetos y medios, por varios motivos, son capaces de vulnerar las seguridades de los dispositivos para extraer la información personal de los consumidores para fines, generalmente ilícitos, lo que crea cierta desconfianza en el usuario.

Téllez sostiene que los datos personales recopilados bajo ayuda de dispositivos electrónicos, no son vulnerables *per se*, es decir, que dependerá de la finalidad con que se recolecten los datos, de forma que, se consideran vulnerados cuando sean utilizados para fines comerciales, fiscales, policiales, etc., constituyéndose como medios de opresión y de lucro para quienes lo poseen sin consentimiento del titular. (Téllez, 1996)

Si bien es cierto, resulta cada vez más útil el uso de la tecnología en actividades de la vida diaria; sin embargo, esto trae consigo una serie de riesgos que pueden perjudicar a los usuarios. Es decir, los datos personales contenidos en el internet de las cosas, podrían ser vulnerados con fines ilícitos. Para ello, entidades de

cooperación mundial, así también, como los gobiernos de algunos Estados, han determinado ciertas normativas en las que se establece: qué conducta se considera como lesiva; y, cuál sería la sanción para el sujeto que la ejecutó, irrespetando el derecho de la protección de datos personales del sujeto afectado.

Antes de determinar qué conductas son consideradas como lesivas a la protección de datos personales en el internet de las cosas, es necesario identificar a los sujetos que intervienen para que se configure un acto dañino. La doctrina plantea que existen dos sujetos que se involucran en un acto lesivo como son los usuarios y los prestadores de servicios como sujetos pasivos o afectados y quienes cometen los actos perjudiciales como sujetos activos, sin embargo, es necesario conocer de qué forma y a través de qué medios se han ejecutado los hechos lesivos que afectan a los sujetos pasivos, para emitir sanciones y vías efectivas de protección de datos personales, siendo considerado a este como un derecho fundamental de todas las personas. (Parker, 1989, pág. 2)

Como consecuencia del acelerado avance tecnológico, la protección de los datos personales, enfrenta cada vez mayores riesgos de ser vulnerados, lo que ha obligado a los gobiernos y a los productores de tecnología, a desarrollar mecanismos de protección de datos personales más avanzados, para evitar la vulneración de los información personal de los usuarios contenida en dispositivos electrónicos.

En la actualidad, tanto a Estados Unidos como a los países que conforman la Unión Europea, se les considera como los precursores en el desarrollo de norma legal aplicable, en materia de protección de datos personales en internet de las cosas. Sin embargo, Europa va a la vanguardia, y por ende plantea sanciones a actos que perjudiquen a las personas, debido a la vulneración de su información personal en el ámbito informático. Para ello, es necesario conocer la normativa y las conductas que se consideran lesivas.

Según el análisis que realiza Donn Parker, la clasificación de las conductas lesivas en el área informática, se determina en base a la variedad y tipos de

medios por los que los actos lesivos son ejecutados. El autor clasifica estos actos tomando en cuenta varios aspectos que son: las formas en que ocurre la pérdida de la información, el tipo de pérdida, el rol que desempeñan los dispositivos, el tipo de acto relativo a los datos, programas y servicios, tipo de delito, *modus operandi* y habilidades requeridas. Además, señala que los delitos que se cometen por medios electrónicos son ejecutados por personas cuyos conocimientos en el área tecnológica son especializados. (Parker, 1989, págs. 3-4)

Por su parte, las Naciones Unidas, ha establecido una serie de conductas perjudiciales para las personas que hacen uso de la tecnología. Entre estas conductas se encuentran: el cometimiento de fraudes mediante la manipulación de computadores, del mismo modo, a los daños o modificaciones de programas o datos computarizados, también el acceso no autorizado a servicios y sistemas informáticos. (Naciones Unidas, 2005)

En la Unión Europea, se considera como una referencia clave el sistema de protección de datos personales, a pesar de ser un sistema que se adoptó de forma tardía. A través del Convenio Europeo de Protección de datos personales se determina que, las partes, deben comprometerse a establecer sanciones contra las infracciones de modo que, se cumplan con los principios para la protección de datos. (Ordónez, 2011)

Las conductas lesivas, en el caso de internet de las cosas, generalmente, van más allá de los delitos comunes, es decir, en ciertos casos, se cometen estos actos con la finalidad de conseguir chantajear a las grandes empresas, demostrando que sus métodos de seguridad son débiles y vulnerables.

En conclusión, el cometimiento de actos en contra de la información personal, contenida en el internet de las cosas, se ha hecho cada vez más frecuente. Resultado de ello, las industrias mejoran sus procesos adoptando medidas de protección mucho más seguras para implementarlas en sus productos dando más confianza a sus clientes y por otro lado, posicionándose mejor en el mercado.

1.3 Protección de datos personales:

De acuerdo a la forma en que es tratada, la información personal que viaja a través de medios tecnológicos, puede ser vulnerada y en consecuencia lo son también ciertos derechos fundamentales de los ciudadanos. Por su parte, cada vez más, los Estados han creado conciencia de los riesgos que corre la información personal de sus ciudadanos. Así también, la información confidencial propia, contenida en los dispositivos que forman parte de la infraestructura tecnológica actual, lo que los obliga a crear medios de protección legales, en caso de que se produzcan hechos que haciendo uso de estas vías interconectadas afecten a los usuarios.

Los sistemas jurídicos europeos y los norteamericanos se diferencian desde el punto de vista de los titulares, por una parte, el sistema norteamericano determina que es legal que los titulares de los ficheros posean los datos personales, ya que son considerados como una cosa de propiedad, por lo que no son de ámbito constitucional, y únicamente, si existe una transgresión a la privacidad, el titular tiene la potestad de solicitar el retiro de estos del fichero que posee el prestador de servicios. (Gregorio, 2014)

En la búsqueda de medios de protección de datos personales, surge un derecho al cual se lo ha nombrado como autodeterminación informativa, que de forma general, puede entenderse como la potestad de cada usuario sobre su información personal.

Varios autores, definen a la autodeterminación informativa como un derecho, relativamente reciente, cuyo origen más aceptable se remonta al año 1890 a través de la obra llamada *The right to be alone*, o el derecho a estar solo, misma que fue publicada a través de la *Harvard Law Review*, en la cual se plantea a ésta como el derecho de las personas de que otros no conozcan temas personales. Esto se lo hace como una propuesta al *common law*, por parte de sus autores que fueron Warren y Brandeis, en razón de que la esposa de uno de ellos fue víctima de invasión de su vida privada por parte de un grupo de periodistas. (Nieves, 2012)

Por su parte, Lucas Murillo, define a la autodeterminación informativa como el control que cada persona debería tener sobre su información personal. Esto se debe, a que el autor considera que la información debe ser conservada como parte de la identidad, libertad y dignidad de las personas, y para ello, se busca otorgar poderes al titular de la información para que éste pueda determinar qué aspectos de su vida no deben hacerse públicos, así también, que los datos manejados por otros hayan sido obtenidos de forma legal y lícita. (Murillo, 2008)

La autodeterminación informativa, últimamente, es objeto de varios estudios e investigaciones, por la influencia de la tecnología en los últimos años. Nace como un medio de protección de la privacidad de las personas, el cual, se ha visto bastante afectado en los últimos años, por el cometimiento de actos ilícitos en contra de los medios informáticos con fines ilícitos.

Sin embargo, la protección de datos personales no es un tema tan actual. Se puede decir, que el derecho de la autodeterminación informativa, nace en Europa, como una figura totalmente diferente e independiente del *right to privacy*, en donde hasta el momento, se siguen creando medios para la protección de datos personales.

En un principio, la normativa europea determina una serie de principios que deben respetarse durante los procesos de recolección, tratamiento y almacenamiento de los datos personales, de forma que estos datos sean de buena calidad que garanticen la veracidad de los mismos. (Garriga, 1999). Estos principios son: Principio de calidad de datos en este principio se comprende la obligación de cancelación de los datos que son innecesarios. (Guerrero, 2006, pág. 238). Por otra parte, el principio de transparencia, dentro de este principio, este principio se refiere al derecho que posee el usuario para conocer el tratamiento al que se someten sus datos. (Guerrero, 2006, pág. 250). Así también, son principios de suma importancia la seguridad y el consentimiento, dado que, especialmente los datos que contienen información acerca de la salud, sexualidad y raza debe tener ser obtenidos bajo el consentimiento expreso de sus titulares. (Santos, 2005, pág. 64)

Por su parte, la Ley española determina una serie de principios sobre los cuales se basará la protección de datos que brindan a sus ciudadanos, entre ellos se encuentran: la calidad de los datos que se refiere a la recolección de datos de forma válida estableciendo cuando son adecuados, pertinentes y justos para el fin que se desea. Por otra parte, se encuentran el derecho de información. Es decir, que los titulares de la información conozcan el proceso de la misma así como el fin para el que serán utilizados. El consentimiento, también, se constituye como un pilar fundamental, por cuanto, la persona deberá otorgar autorización para que un tercero pueda manejar sus datos personales, salvo excepciones establecidas en la respectiva normativa. En cuanto a los datos especialmente protegidos, se puede decir que está prohibido su tratamiento sin que el titular no haya expresado su consentimiento. (Nieves, 2012)

En conclusión, la autodeterminación informativa es un derecho inherente de las personas, el cual lleva impregnado en sí mismo otros derechos como son, el derecho a la libertad de expresión o el derecho a ser informado. Por su parte, los proveedores de los servicios, deberán según los principios, manejar de manera adecuada la información personal de sus usuarios. También, los Estados han creado estos mecanismos de tal forma que, el usuario tenga una protección jurídica en caso de que hayan sido víctimas de actos que afecten su integridad a través del mal manejo de su información personal. Sin embargo, es importante que los usuarios tengan conciencia sobre la información, que de forma voluntaria o involuntaria, entregan a los proveedores de servicios, así también, que se tenga presente la forma en que se otorgó el consentimiento para la recolección de la misma.

1.3.1 Antecedentes

En el sistema americano, la protección de datos personales, tiene como antecedente directo el derecho a la privacidad, establecido dentro de la enmienda XIV, también conocido como *right to privacy*, este derecho, en un principio, estaba orientado hacia la privacidad en la sexualidad como en *Warren y Brandeis*. (Nieves, 2012) Sin embargo, no es sino, hasta el caso *Whalen Vs. Roe*, donde se reconoce el conflicto que existe entre el interés personal, que

busca impedir que se divulguen datos personales; y el interés colectivo de que se lo haga en razón de una importante toma de decisiones. Esto se dio, debido a que en el Estado de Nueva York existía un sistema computarizado de registro médico que contenía información detallada y completa que permitía identificar plenamente a los pacientes. (Gregorio, 2014)

En un principio, el sistema americano, enfocado en la *privacy,* posee varias normas para su regulación. Respecto de la protección de datos, ha adoptado una posición de autorregulación, es decir, las compañías privadas dedicadas al tratamiento de datos personales, responden a las necesidades de información de las grandes empresas como también a la de los consumidores, aumentando la confianza entre las partes. (Hernández, 2012) La política que emplea Estados Unidos, ha logrado regular ciertos aspectos que se consideran vulnerables como puede ser la privacidad de datos de salud de las personas, siguiendo una ideología más liberal. (Hernández, 2012)

En el sistema americano, los datos personales se entienden como un bien de las personas, es decir, este tipo de datos pueden ser libremente recolectados y manejados, siempre y cuando sean utilizados únicamente para el fin con el que son recolectados. De modo que, en caso de que los datos sean mal utilizados el procedimiento determina en sus normas las sanciones que van entre el orden de retiro de datos o sanciones pecuniarias. (Levin & Nicholson, 2005, pág. 357)

Por otra parte, el sistema europeo de datos personales, es mucho más estricto que el sistema americano. En Europa el derecho de protección de datos personales parte desde la privacidad en el ámbito de la prohibición de la intervención arbitraria en la vida privada de las personas, sin que exista una orden judicial previa. Posterior a esto, aproximadamente en el año de 1990, la Unión Europea, reconoce la necesidad de una protección de datos que permita el adecuado funcionamiento del mercado convirtiéndose así, en una meta orientada hacia lo comercial. (Gregorio, 2014)

En el año de 1995, la Unión Europea aprueba la Directiva y el Parlamento europeo respecto a protección de datos personales y la libre circulación de los

mismos, con la finalidad de otorgar a los países miembros una referencia normativa. (Hernández, 2012)

Como se refleja, el sistema de protección de datos europeo guarda muchas diferencias con el sistema americano, estas diferencias condujeron a que se produzca el llamado conflicto de los puertos seguros o *safe harbor*.

El conflicto de puertos seguros se desarrolla aproximadamente desde 1999, a raíz de lo que entra en vigencia la directiva relativa a la protección de datos en Europa, por lo tanto, se origina un problema con Estados Unidos. Esto se debe a que la mayoría de prestadores de servicios en el área de la informática son estadounidenses, y que el sistema europeo de protección de datos personales sólo permitía la transmisión de datos a otros países siempre y cuando los estándares de protección de datos de estos sean altos, en base a esta afirmación, se dedujo que Estados Unidos no contaba con un sistema de protección de datos adecuado. (Guasch & Soler, 2016, pág. 342)

Para la solución de este conflicto, Estados Unidos, por su parte, propuso establecer los principios de puerto seguro; dentro de esta propuesta Estados Unidos se adhería a las exigencias de la Directiva europea, de modo que, la transferencia de los datos entre países europeos y Estados Unidos sea posible. (Guasch & Soler, 2016)

Por otra parte, la Unión Europea, a través de su grupo de trabajo sobre protección de datos del artículo 29, aprueba el dictamen 4/2000 acerca del nivel de protección de los principios de puerto seguro. Dentro de esta resolución contempla varios puntos de gran importancia; entre ellos, mantener las relaciones comerciales, siempre y cuando estos intereses no vayan en contra de los derechos fundamentales de las personas. (Grupo de Trabajo sobre Protección de Datos, 2000, pág. 2)

Sin embargo, Estados Unidos, ha determinado que estos principios sólo serán aplicables para la información proveniente de Europa, mas no ha manifestado el tratar de la misma forma a la información proveniente de otros países.

En conclusión, el avance tecnológico es cada vez más acelerado, lo que ha generado preocupación en las autoridades gubernamentales a nivel mundial obligándolos a buscar medidas tanto técnicas como jurídicas que garanticen la protección de los datos personales que son manejados por medios tecnológicos bajo el poder de los responsables de los ficheros.

1.4 Reglamento Europeo

La necesidad de una norma acorde a la protección de datos personales en el internet de las cosas, ya ha sido tomada en cuenta en varios países del mundo, la mayoría de estos países son muy adelantados en el área tecnológica. Especialmente, la Unión Europea que realizó un dictamen sobre el internet de las cosas, dentro del dictamen del Grupo de Trabajo del Artículo 29, se toman en cuenta varios aspectos de la tecnología como:

> "El documento analiza tres escenarios: la tecnología para llevar puesta *(wearable computing),* los dispositivos capaces de registrar información relacionada con la actividad física de las personas y la domótica.
>
> El Dictamen identifica y alerta de los riesgos que estos productos y servicios pueden plantear para la privacidad de las personas, definiendo un marco de responsabilidades y realizando recomendaciones
>
> A pesar de que los objetos que conforman la internet de las cosas recogen piezas aisladas de información, los datos recogidos de diferentes fuentes y analizados de otra forma o en conjunción con otros pueden revelar auténticos patrones de la vida de las personas.
>
> Un ejemplo destacado en el Dictamen es la información recogida por el acelerómetro y el giroscopio de un *smartphone*, que podría ser utilizada para obtener información sobre los hábitos de conducción del individuo." (Agencia Española de Protección de Datos, 2014)

Este dictamen marca un precedente para las demás normativas, como una referencia de que la tecnología está en más dispositivos de los que se conoce. Además, Europa en el año 2016 aprueba el reglamento sobre protección de

datos relativo a las personas físicas acorde al tratamiento y circulación de datos con el cual se derogaba, también, a la directiva 95/46/CE. (Parlamento y consejo de la unión europea, 2016)

Dentro de este reglamento, existe un artículo en especial, en el cual se relaciona la protección de datos personales desde el punto de vista legal y la seguridad en el diseño que los proveedores de servicios deben brindar. El artículo en concreto se expresa de la siguiente forma:

> **“Artículo 25 Protección de datos desde el diseño y por defecto**
>
> 1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.
>
> 2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.
>
> 3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42, como elemento que acredite el cumplimiento de las

> obligaciones establecidas en los apartados 1 y 2 del presente artículo.” (Parlamento y consejo de la unión europea, 2016)

En este artículo se puede resaltar varios puntos de suma importancia, mediante los cuales la norma europea obliga a los fabricantes de los productos que hacen uso de tecnología, a generar medios de protección de los datos personales de sus usuarios dentro de sus productos.

Además, tienen la responsabilidad de garantizar al usuario que nadie, excepto el proveedor, puede acceder a esa información y que la misma será utilizada, únicamente, para los fines que se recogieron, así como, debe conseguir el consentimiento del titular para hacerlo.

A pesar de que la normativa europea ha marcado un precedente en la protección de datos personales en el internet de las cosas, la regulación del *IoT* aún se considera como una brecha normativa que no es tomada en cuenta, con la suficiente atención que se debería. Por otra parte, es necesario que para la creación de una norma adecuada para la protección de datos personales no sólo el Estado en conjunto con las compañías prestadoras de servicios, establezcan medios de protección adecuados para proteger el interés de los usuarios.

1.5 La protección de datos en España con referencia al *IoT*

De acuerdo al análisis de los dos sistemas de protección de datos usados como referencia en el presente trabajo, se puede deducir que, el sistema de protección de datos personales, que podría adecuarse de mejor forma al sistema ecuatoriano es el que existe en Europa, entre ellos especialmente el sistema español, esto se debe a que el sistema español considera al derecho de protección de datos personales, como un derecho irrenunciable de las personas, por lo tanto, brinda mayor seguridad y mayor garantía; a diferencia del sistema americano que, como ya se lo mencionó, es un sistema más liberal, dónde sólo se crea normas basadas en la *privacy*.

Por lo tanto, es necesario tomar en cuenta ciertos aspectos principales de la normativa española, de modo que, sea posible determinar qué principios podrían incluirse en la normativa ecuatoriana.

En primer lugar, la norma española que regula la protección de datos personales, es la Ley Orgánica de Protección de Datos de Carácter Personal. Esta norma, exige por lo menos la intervención de dos sujetos en el tratamiento de los datos como son: el que trata los datos y el otro, cuyos objetos son tratados. Por otra parte, dentro de la normativa española, el consentimiento juega un papel fundamental dentro de la protección de datos personales, y se constituye como una obligación del responsable del fichero, obtener el consentimiento del titular, para recolectar y tratar los datos personales. (Grimalt, 2008, págs. 323-327)

La normativa europea, respecto del tratamiento de los datos personales, sostiene que la defensa de los derechos de las personas, en este caso de la protección de datos personales, no servirá como medio para impedir otros derechos, como por ejemplo, la protección de la intimidad, no burlará intereses dudosos. Por lo que se debe buscar el equilibrio entre los intereses que sí son legítimos. (Davara, 1998)

Es así, que la normativa española marca un precedente donde considera a la protección de datos como un derecho fundamental, que otorga la máxima protección a los ciudadanos. Entre otros importantes aportes que realiza la norma europea y que adopta España como es la creación de los derechos ARCO (acceso, rectificación, cancelación y oposición). El ejercicio de estos derechos es exclusivamente personal, por lo que sólo el afectado podrá exigir su cumplimiento. Además, de que su ejercicio es gratuito e independiente, es decir que no depende de otros derechos previos. (Veleiro, 2008, págs. 88-89)

Como se pudo palpar, el sistema español de protección de datos personales, es un sistema ideado para adaptarse a todo tipo de casos que se relacionen con el tratamiento de la información personal en cualquier área de la vida de las personas.

A pesar de las garantías que ofrece el sistema de protección de datos español, el sistema que existe en el Ecuador, continúa siendo insuficiente de tal forma que genera varios inconvenientes y falta de normas en ciertos aspectos dónde se involucran los datos personales y la tecnología.

1.6 La Protección de datos en el Ecuador

El Ecuador, a través de convenios internacionales, busca mejorar la industria nacional, especialmente, en el ámbito tecnológico. Esto se traduce a la necesidad, de crear una norma interna que proteja la información personal de los ecuatorianos, contenida en la infraestructura tecnológica llamada internet de las cosas o *IoT* por sus siglas en inglés.

Actualmente, varias empresas de gran tamaño han llegado al país con la finalidad de realizar sus procesos de producción en el Ecuador, en varias áreas, como por ejemplo: en el ámbito automotor, *Aymesa* es una de las compañías más grandes en el país, encargada del ensamblamiento de vehículos, mismos que en la actualidad, cuentan con tecnología que hace uso de internet ya sea por vía de GPS o por el sistema mecánico de los automotores. Actualmente ésta compañía tiene convenios con marcas de nombre mundial como son Hyundai, Kia y Volskwagen. (Aymesa, 2013) De igual forma, en el país, la industria de los televisores se encuentra presente, como es el caso *Audioelec*, empresa encargada del ensamblaje de televisores *smart* de las marcas Sony y LG en Ecuador. (Astudillo, 2015)

De lo anteriormente expuesto, puede decirse que el avance tecnológico en el Ecuador es una realidad, que en unos años puede incrementarse por el fenómeno de la globalización. Por lo tanto, el sistema legal interno, respecto de la protección de datos personales, tarde o temprano debe mejorar. De modo que, es necesario tomar en cuenta lo que otros países, han hecho al respecto de esta problemática.

En el caso de Ecuador, si bien, el avance tecnológico, no es tan adelantado en comparación a otros países con economías de gran tamaño, el Ecuador, busca mejorar los procesos de la industria implementando tecnología de última generación, gracias a las alianzas que ha hecho con países que cuentan con tecnología de punta.

Por una parte, la Constitución ecuatoriana en el artículo 66 numeral 19 con respecto a la protección de datos personales, determina lo siguiente:

> **“Art. 66.-** Se reconoce y garantizará a las personas:
>
> 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.” (Constitución de la República del Ecuador , 2008)

Es decir, la protección de datos personales, es un derecho reconocido constitucionalmente, en el cual, cada titular podrá conocer y aceptar el tratamiento de los datos personales que son entregados a los responsables de los ficheros, públicos o privados, de modo que, en caso de vulneración de este derecho, la misma Constitución le confiere mecanismos de protección. Así mismo, para la protección de los datos personales la Constitución plantea al *Hábeas data* de la siguiente forma:

> **“Art. 92.-** Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.
>
> Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley.
>
> La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su

> solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados.” (Constitución de la República del Ecuador , 2008)

Es decir que, en base a esta acción, la persona que vea vulnerado su derecho a la protección de datos personales, podrá demandar el cumplimiento de su derecho, así también, que se impongan sanciones en contra de los responsables de este acto vulnerable.

En otras palabras, el *hábeas data*, otorga a los ciudadanos una acción que hace efectivo el derecho de protección de su información personal. Además, pueden hacer uso de esta acción todas las personas, naturales y jurídicas, que se sientan afectadas en cuanto al manejo de su información personal contenida en bases de datos tanto públicas como privadas.

De modo que, “a través del *hábeas data* el legitimado (persona física o jurídica) puede acceder al conocimiento de sus datos personales y los referidos a sus bienes y al destino de tal información que se encuentren asentados en archivos, registros, bancos de datos u otros medios técnicos, electrónicos y ópticos, de carácter público o privado, de soporte, procesamiento y provisión de la información; y, en determinadas hipótesis (por ejemplo, falsedad o uso discriminatorio de tales datos), exigir la supresión, rectificación, actualización o el sometimiento a confidencialidad de los mismos.” (Bazán, 2009)

Por lo tanto, los ciudadanos ecuatorianos tienen el derecho de conocer y acceder a la información propia, así también, tienen derecho a conocer la legalidad en la recopilación de sus datos, teniendo la posibilidad de que, en caso de haberse recabado de forma ilegal los datos personales, puedan exigir la correspondiente sanción en contra de los responsables.

En conclusión, el *hábeas data* busca precautelar a la titularidad privacidad y seguridad de la información personal de los ciudadanos, así también, busca la protección de otros derechos como el derecho de la información, aquí también, juega un papel importante el consentimiento, puesto que si la persona titular de los datos, está al tanto de la finalidad que se busca conseguir, con la recopilación

de sus datos, podrá tener mayor control sobre su información personal. La intención principal, de ésta acción establecida en la Constitución es transparentar el acceso y manejo de la información personal de los ciudadanos, así como delimitar la responsabilidad de los sujetos que tienen el acceso y control de los ficheros.

Es así que, la Constitución mediante la expresión de esta acción constitucional busca mejorar el nivel de transparencia en el acceso a la información, así como el tratamiento a personas naturales y jurídicas que son responsables de ficheros o que acceden a ellos.

Si bien es cierto, en el Ecuador, el derecho en el área de protección de datos personales, no existe, sin embargo, el paso del tiempo obligará a tomar medidas tanto técnicas como jurídicas para salvaguardar los derechos de los ciudadanos, para ello, podría ser una vía adecuada tomar como modelo las legislaciones de alto estándar, como la española, que han desarrollado en gran parte, normas que regulan a proveedores de servicios o a responsables de ficheros.

2 CAPITULO II. EL INTERNET DE LAS COSAS

2.1 Antecedentes y evolución del internet de las cosas

El internet de las cosas, también conocido como *IoT (Internet of things)* por su nombre y siglas en inglés, es un reflejo de la fuerte influencia que han logrado, tanto la tecnología como el internet, en la vida diaria de todas las personas.

El Internet de las cosas, en la actualidad se ha constituido como objeto principal de varios estudios sobre tecnología, sin embargo no cuenta con un concepto empleado a nivel general, a pesar de ello, ha sido definido de diversas formas, que en esencia son similares, entre ellas, una de las más representativas es la dada por el *McKinsey Global Institute,* que define al *IoT* como la conexión que puede haber entre máquinas, equipos y otros elementos con sensores y servidores, normalmente no considerados computadores, conectados a una red los cuales permiten generar, receptar e intercambiar datos con mínima intervención humana. (Internet Society Org., 2015)

Hay autores que afirman que:

> “Con el Internet de las cosas, el planeta está siendo instrumentado e interconectado, al tiempo que se vuelve más inteligente. Esto ocurre porque los mil millones de personas y una lista interminable de objetos conectados a Internet (coches, electrodomésticos, teléfonos, cámaras, etc.) ahora pueden interactuar, traspasando las barreras del tiempo y el espacio. A su alrededor, se construyen entornos «inteligentes» capaces de analizar, diagnosticar y ejecutar funciones. Por ejemplo, una red eléctrica «inteligente» es capaz de detectar sobretensiones y de dirigir la electricidad por caminos alternativos para minimizar apagones.” (Fundación Bankinder, 2009, p.3)

El internet de las cosas, a partir del año 2008, hasta la actualidad, se ha convertido en una infraestructura tecnológica de gran influencia en la sociedad, y de la misma manera se puede predecir que tomará más fuerza con el transcurso de los años. Como un antecedente a esto, cabe mencionar que en los años 70’s el control y manejo remoto de dispositivos ya se encontraba en uso

a través de las líneas telefónicas. Un poco más allá, ya por los años 90's la tecnología *wireless*es creada y empleada dentro del ámbito industrial con la finalidad de expandir las operaciones de monitoreo y manejo de la maquinaria. Con la implementación de este tipo de tecnología lo que se buscaba no era que los dispositivos puedan conectarse a computadores, por el contrario, el verdadero objetivo era que a través de ciertos estándares un dispositivo de uso común pueda ser manejado mediante el uso de internet. Es así que, en 1990 en la conferencia sobre Internet se presenta un tostador que podía ser encendido y apagado vía internet. De modo que, en los años posteriores varias universidades tanto de Estados Unidos como del Reino Unido crearon productos también llamados *smart object networking,* que se fueron implementando en la vida diaria de las personas. (Internet Society Org., 2015)

Sin embargo, el origen del término proviene aproximadamente en el año 1999 en manos del pionero tecnológico, el británico Kevin Ashton, el cual describe al *IoT* como un sistema en el cual objetos del mundo físico puedan ser conectados a internet a través de sensores. (Internet Society Org., 2015)

Como punto referencial el IBSG *Internet Business Solutions Group* de Cisco determina que "en 2003, había aproximadamente 6,3 mil millones de personas en el planeta, y había 500 millones de dispositivos conectados a Internet. Si dividimos la cantidad de dispositivos conectados por la población mundial, el resultado indica que había menos de un dispositivo (0,08) por persona. De acuerdo a la definición de Cisco IBSG, *IoT* aún no existía en 2003 porque la cantidad de cosas conectadas era relativamente escasa, dado que apenas comenzada la invasión de los dispositivos omnipresentes, como los smartphones." (Cisco IBSG, 2011)

Como sucesos relevantes de la evolución del Internet de las cosas, a partir del año 2000, la revista Forbes ha realizado un listado de sucesos tecnológicos que permiten verificar la influencia del *IoT* en la sociedad entre los cuales se encuentran: en el año 2000 la empresa LG ingresa al mercado su primera nevera conectada a internet, en los años 2003-2004 se usa en gran parte el término *IoT* en publicaciones acerca de tecnología, en el año del 2005 la UIT (organismo

especializado de las Naciones Unidas para las tecnologías de la información y la comunicación) elabora el primer informe sobre el *IoT* donde se determina el crecimiento que ha tenido este tipo de tecnología y la proyección que tendrá en el futuro. Finalmente, en el transcurso de los años 2006 al 2009 el *Internet of the things* es reconocido por la Unión Europea y nace oficialmente al superar el número de dispositivos conectados a internet en comparación al número de seres humanos. (Bliznakoff, 2014)

Actualmente, es más popular el uso de dispositivos electrónicos que se conectan a internet. De modo que, con la creación de esta tecnología los productores buscan facilitar ciertas actividades de la vida diaria, que a pesar de ser de gran utilidad pueden representar una amenaza en contra de la protección de datos personales, generando problemas en los consumidores.

2.2 El impacto del internet de las cosas en la sociedad y ámbitos de aplicación:

El internet de las cosas, en la actualidad, tiene varias áreas de aplicación dentro de la vida cotidiana, su presencia puede notarse en objetos de diversos tipos, no solamente en computadores como se cree popularmente.

Como consecuencia de ello, el mundo ha experimentado un incremento impresionante de la tecnología, por lo tanto, cada vez es más cercano el hecho de que se vivirá en un mundo completamente automatizado, en donde, si se produce un accidente de tránsito las cámaras de vigilancia emitirían la alerta a los servicios médicos y los semáforos se configurarían, de tal forma que eviten congestionamientos en el tráfico. Es así, que la economía, actualmente se ha volcado a nuevos modelos de negocios basados en la tecnología, que ofrecen servicios, generalmente, de telecomunicaciones con el objetivo principal de buscar eficiencia en sus labores a través de la utilización de sistemas de autocorrección. (Fundación Bankinder, 2009, p.3)

Para el ser humano moderno, es técnicamente imposible no hacer uso de la tecnología, como consecuencia de ello, a continuación, se realizará una mención

a las áreas en las que es habitual el uso de la infraestructura tecnológica llamada Internet de las cosas.

La *Revista Chilena sobre Derecho y Tecnología* que es emitida por la Facultad de Derecho de la Universidad de Chile en su volumen 4, abarca al internet de las cosas y los ámbitos en los que es aplicado. Entre ellos se puede destacar los siguientes:

Medicina: El campo médico es una de las áreas con mayor relevancia para la aplicación del internet de las cosas, actualmente los dispositivos, como los marcapasos, podrán dar a conocer la situación del paciente al centro médico que lo esté controlando, así como permitir y prevenir alguna emergencia. Existen también otros dispositivos que ayudan a monitorear el bienestar de los pacientes a partir de la recolección de datos que se envían a sus respectivos historiales clínicos. (Enrile, 2015)

Seguridad: Actualmente, el incremento de la delincuencia en la sociedad, ha requerido la creación de dispositivos que permitan salvaguardar la integridad de las personas y a su vez, la de sus bienes, por ejemplo, ahora es muy común el uso y colocación de dispositivos de rastreo de los vehículos, así como también, la instalación de sensores de movimiento o sistemas de circuitos cerrados en el hogar, los cuales notifican a los propietarios, e inclusive a la policía, sobre cualquier tipo de actividad inusual que se suscite dentro de los inmuebles. Por ejemplo, en Corea del Sur, es muy utilizado un sistema electrónico de apertura de puertas a través de códigos numéricos, que a su vez notifican a su propietario a apertura del bien inmueble, reemplazando así a las llaves tradicionales. (Enrile, 2015)

Hogar: La tecnología ha avanzado, de tal forma que ha permitido crear aparatos electrónicos que brinden comodidad a las personas en la vida diaria. También conocida como domótica, actualmente, el mercado mundial cuenta con refrigeradores capaces de detectar la falta de abastecimiento de alimentos, así también, existen controladores de temperatura y purificadores de agua con la finalidad de evitar que la persona lo haga de forma manual. (Enrile, 2015)

Deporte y accesorios: Aquí se pueden clasificar los instrumentos utilizados por deportistas para el control de sus actividades, por ejemplo, hay relojes especiales, que permiten determinar el recorrido que ha realizado el deportista así como también los chips que permiten determinar el tiempo en que los corredores han cruzado la meta, así también, el peso y ritmo cardiaco. (Enrile, 2015)

Entretenimiento: El internet de las cosas ha incursionado con éxito en el campo de los videojuegos y es que se han creado juegos que se asemejan más a la realidad, a su vez que estos producen información que crean un perfil de la persona que hace uso de ellos. (Enrile, 2015)

Transporte: En la actualidad, existen dispositivos colocados tanto en vehículos que permiten indicar al fabricante si se ha sufrido algún desperfecto, así como, en transporte marítimo a través de GPS que ayudan a determinar la ruta por la que se encuentra navegando la embarcación. (Enrile, 2015)

Agroindustria: Este es un campo realmente no tan explotado, pero según investigaciones se prevé crear maquinaria que facilite el desempeño de las actividades industriales, que a su vez, permitan un mayor control de la producción y así mejorar la industria. (Enrile, 2015)

Como fue mencionado anteriormente, se puede decir que el Internet de las cosas se encuentra presente en la vida de todas las personas que hacen uso de él de manera consciente o inconsciente.

Es así que, como resultado de la creciente influencia tecnológica, el *IoT* técnicamente se constituye como un método de generación, trasmisión y recepción de datos con mínima intervención humana, de tal forma que se vuelve indispensable el conocer y comprender la manera en que los datos son transmitidos a través del Internet de las cosas, ya que como consecuencia de ello surgen una serie de problemas legales, debido a que se carece de normativa suficiente para el control y manejo de información transmitida por medio de esta infraestructura tecnológica.

Por lo tanto, puede concluirse que el impacto que ha tenido el *IoT* en la sociedad ha producido efectos tomados como avances que puede aportar a la humanidad hasta las amenazas a la seguridad y a la privacidad de las personas que pueden producirse, y que constituyen una problemática sobre la cual los gobiernos de distintos países, organismos no gubernamentales y sociedad civil están muy atentos.

2.3 Problemática que se deriva del crecimiento del *IoT*

De las características que presenta el internet de las cosas puede deducirse que el problema principal que se deriva de la influencia del *IoT* en la vida diaria, es la mínima intervención que tienen los seres humanos al momento de que esta infraestructura tecnológica genera, transmite o reproduce datos sobre el perfil de la persona que hace uso de ella.

Es importante saber, que los datos obtenidos en el *IoT* son el resultado de todo un proceso en el que intervienen varios agentes. Partiendo de la recolección de datos desde su origen, pasando por el transporte, el cual, los trasladará al lugar o entidad de almacenamiento, hasta llegar al lugar de destino, donde a más de almacenar la información, se administrará y analizará esa información con diversas finalidades, como por ejemplo, el interés de las empresas de luz en determinar el nivel de consumo de energía. (Enrile, 2015)

El riesgo que puede correr la información personal en el internet de las cosas, dentro del proceso anteriormente mencionado, depende, en un inicio, del dispositivo que la contenga y la función que desempeña. Se puede decir que, la información personal en el internet de las cosas, se ve afectada, principalmente, en tres aspectos de gran interés para el ser humano, que son: la privacidad, la seguridad y la titularidad de sus datos personales. (Centro de Seguridad TIC de la Comunidad Valenciana, S.F)

Para reflejar esta problemática, cabe mencionar algunos hechos que se producen en la actualidad, en razón de los datos que se procesan en el internet

de las cosas. Es entonces, el acceso libre a la información personal contenida en el *IoT*, tal vez, el aspecto que más problemas produce a los usuarios.

En la actualidad, es mayor el número de dispositivos que se conectan a internet, por lo tanto, ha aumentado la cantidad de información trasmitida en el *IoT*, en la mayoría de casos, sin embargo, los datos e información recolectada, enfrentan una serie de riesgos, por ejemplo pueden ser vulnerados por los hackers, piratas informáticos o estafadores virtuales, los cuales perjudican a los usuarios, robando la información y usándola para fines ilícitos. Por otra parte, la seguridad de la información personal, depende también de la pérdida de cualquier dispositivo que haga uso del *Iot*, ya que, cada vez son más los dispositivos que hacen uso del internet y, por tanto, el riesgo de pérdida también aumenta. (Centro de Seguridad TIC de la Comunidad Valenciana, S.F)

En cuanto a seguridad, se puede decir que, las compañías fabricantes se encargan, en un principio, de crear mecanismos que protejan a sus dispositivos, esto depende de varios procesos previos que incluyen la valoración del riesgo que afecta la seguridad de la información de las personas contenidas en el *IoT,* posterior a ello, las empresas buscan minimizar la cantidad de datos personales recolectados y conservados, así como, realizar previamente pruebas a la seguridad de los dispositivos antes de que estos sean comercializados. (FTC Staff Report, 2015)

Por ejemplo, en estos días, es normal el uso de GPS tanto en los teléfonos móviles así como en automóviles o incluso en dispositivos que se cuelgan a las cosas con la finalidad de conocer la ubicación de los mismos, generalmente estos dispositivos pueden ser de gran utilidad, así mismo, pueden ser perjudiciales, por cuanto los proveedores pueden revelar y almacenar en algún lugar desconocido de la web, la ubicación exacta de las personas, así como las rutas que toman a diario. Por otra parte, dependiendo del uso y finalidad con que se utilice el dispositivo, se podría acceder a esa información para manipularla sin que el titular legítimo de los datos tenga conocimiento de ello afectando su privacidad. (Centro de Seguridad TIC de la Comunidad Valenciana, S.F)

Por lo tanto, puede decirse que los usuarios al implementar esta infraestructura tecnológica, de forma voluntaria o involuntaria, a su vida diaria ceden parte de su privacidad, es decir que, se hace público cierto tipo de información, esto se contrapone, a que la privacidad se constituye como un derecho inherente de las personas, por lo tanto, se busca crear mecanismos, no sólo técnicos, sino legales a través de la creación de normas específicas destinadas a proteger a las personas y a su información personal contenida en *IoT* de actos que puedan perjudicarlos directamente, como consecuencia de la libre circulación, manejo o comercialización de los mismos y sin intervención ni conocimiento de sus titulares.

Es en base a esta hipótesis, que en el año 2014, Hewlett Packard encabezó un estudio en el cual se realizó varios análisis a un grupo de equipos más populares que hacen uso del internet de las cosas, el cual, arrojó como resultados que, el 90% de ellos de alguna forma recolectaban información de tipo personal como son: el nombre, la dirección, fecha de nacimiento e incluso el número de las tarjetas de crédito, además de que el 70% de los mismos transporta esa información sin ningún tipo de encriptación, y que el 80% del grupo no requiere de claves complejas para poder acceder a ellos, y por último que el 60% eran susceptibles de debilidades en relación a la interfaces de la web. Es decir, que la mayoría de equipos que hacen uso del internet de las cosas, no existe conocimiento y consentimiento de los usuarios que hacen uso de esta infraestructura tecnológica (Alcaraz, S.F)

Claramente, se puede constatar que el uso de éste tipo de tecnología, si bien, puede ser de gran utilidad en la vida diaria, su empleo desata una serie de inconvenientes, vinculados principalmente con la privacidad y seguridad de los datos que se obtienen dentro del internet de las cosas. Como consecuencia de ello, las compañías fabricantes de éste tipo de productos ha buscado implementar medios que permitan al usuario asegurarse en parte, de que su privacidad e intimidad no se vean afectadas por el transporte de la información personal a destinos desconocidos por el usuario y conocidos por los proveedores

de los servicios, de tal forma, que estos no puedan utilizar a los datos para fines distintos a los que el usuario conoce.

Muchos países todavía consideran al *IoT* como parte del futuro, por lo tanto, las violaciones de la privacidad a través del uso del internet de las cosas, no tiene la suficiente atención para ser sujeto de investigaciones y análisis. Sin embargo, se espera que para el año 2020, se conectarán a internet aproximadamente entre 20 a 50 millones de cosas, este crecimiento, en gran parte, se debe a la búsqueda de la reducción de costos para el procesamiento de datos. (Unión Internacional de Telecomunicaciones, 2015) En base a esto, se dice que el mayor impacto del *Iot* podría darse cuando se implemente el internet de las cosas a áreas de la vida diaria y sumamente personales, como el uso de la energía que podría determinar los momentos en que la vivienda se encuentra sola. (Unión Internacional de Telecomunicaciones, 2015)

En conclusión, la sociedad internacional está adaptándose a éste tipo de evolución tecnológica, lo que es un aspecto positivo para los usuarios en general. Si bien es cierto, la tecnología, significa en la actualidad un modo de facilitar la vida de las personas y ahorrar tiempo en procesos ahora sistematizados, cuyo defecto, tomando en cuenta el estudio anterior, es el origen de un conflicto en cuanto a titularidad, transporte, manejo y almacenamiento de los datos que se recolectan dentro del internet de las cosas, de modo que, específicamente en el ámbito legal, surgen varias interrogantes sobre quién es el sujeto titular de los datos obtenidos mediante el uso de la infraestructura tecnológica llamada como el internet de las cosas.

2.4 Privacidad por diseño, la alternativa para la protección de datos personales más apegada a la realidad:

Frente a los constantes riesgos que enfrentan los datos personales en la actualidad, y debido a la falta de protección jurídica suficiente, se ha creado un mecanismo de protección para el usuario que se ha denominado como la privacidad por diseño, o también conocida como *privacy by design*, que puede decirse, es una innovación que va más allá en el derecho de protección de datos personales.

La privacidad por diseño o *PbD*, por sus siglas en inglés, puede definirse como una estructura de diseño de sistemas de información, procesos físicos y de negocio, basados en la integración de la privacidad en el diseño del funcionamiento de sistemas informáticos, infraestructura y prácticas empresariales. Su origen se debe a la Comisionada de Información y Privacidad de Ontario (Canadá), la doctora Ann Cavoukian, la cual, busca promover la idea de que en un futuro cercano la privacidad no puede estar asegurada únicamente por los entornos jurídicos, sino que la seguridad de la privacidad debe someterse a varios análisis para determinar los riesgos que puedan traer consigo las nuevas tecnologías. (Cavoukian, 2011)

A través del empleo de esta estructura, se pretende que todas las acciones que estén relacionadas con el manejo y tratamiento de los datos personales sean identificados, analizados, y a su vez, se incorporen en los sistemas y entornos digitales. Sin embargo, la incorporación de la *PbD*, aún no aparece en ningún caso como un imperativo legal, es decir que carece todavía de un obligación determinada legalmente, sino que se constituye como una condición del prestador de servicios que decide añadir un “plus” de objetivos que se comprometan con la sociedad. (Alonso, 2009, pág. 115)

En razón de que la era digital es un fenómeno de acelerado avance, el que prácticamente se encuentra presente en el entorno de todas las personas, puede decirse que la privacidad por diseño, es un medio encaminado para la protección de datos, en el cual, el usuario sea quien tenga el mayor control posible sobre su información personal, así también, permite a los proveedores de servicios, mejorar sus estructuras, haciéndose más competitivos en el mercado tecnológico. Se puede decir, que lo que se busca a través de la implementación de este sistema, también se busca que las normas jurídicas tengan mayor respaldo, debido a que en muchos casos, la norma existente no es suficiente.

Varios autores creen que durante el empleo de los medios tecnológicos se pierde gran parte de la privacidad, es por ello, que se genera la necesidad de la creación de una estructura llamada privacidad por diseño, misma que se debe a varios factores, entre los cuales se pueden destacar los siguientes:

Globalización: La globalización es un fenómeno que avanza a gran escala, el cual, crea la necesidad de compartir información, poniendo en riesgo la seguridad de la información, por la difusión voluntaria o involuntaria de la información. (Ryerson University, S.F, págs. 1-2)

Límites organizacionales no estáticos: Los límites al manejo de la información no son estáticos, es decir, que en la actualidad, es sumamente complicado el poder detectar dónde, cómo y quién, ha vulnerado la seguridad de los datos personales y de qué forma están siendo administrados y con qué finalidad. (Ryerson University, S.F, págs. 1-2)

Vulnerabilidad en las herramientas: El uso y colaboración de las *social networkings tools* pueden constituirse como nuevas posibilidades para la seguridad, sin embargo, potencialmente pueden ser más riesgosas que si no son gestionadas proactivamente. (Ryerson University, S.F, págs. 1-2)

En base a las necesidades anteriormente mencionadas, en la aplicación del diseño se plantean una serie de principios que determinan el desarrollo de los entornos tecnológicos que manejen los datos de tipo personal, entre los cuales se encuentran:

1. **Principio Proactivo, no reactivo- Preventivo no correctivo:** Determina que debe anticiparse, identificarse y prevenirse todo tipo de eventos invasivos antes de que sucedan, eso significa que se debe tomar medidas antes de que ocurran. Por ejemplo, si va a crearse un dispositivo que haga uso de internet, se debe tomar en cuenta, qué formas de protección se debe implementar en él. (Cavoukian, 2011)
2. **Privacidad como configuración predeterminada:** La privacidad debe estar asegurada de forma previa, de modo que el usuario no deba realizar ninguna acción para que su información sea protegida, sino que desde el principio se encuentre asegurada. Por ejemplo, si una compañía de distribución de energía, desea hacer un control de los datos sobre el consumo que hacen las personas, debe adoptar medidas de seguridad para garantizar a los usuarios su privacidad,

puesto que esta información puede determinar las actividades que realizan las personas en la vida diaria. (Cavoukian, 2011)

3. **Privacidad incrustada en el diseño:** La privacidad debe incluirse directamente como un componente esencial de la arquitectura de los dispositivos. Por ejemplo, en un equipo de control médico se debe integrar el *Privacy by design*, para evitar la filtración de información sensible del paciente, como son sus dolencias o estado de salud. (Ryerson University, S.F)
4. **Funcionalidad Total- "Todos ganan", no "Si alguien gana, otro pierde":** La privacidad por diseño emplea el ganar – ganar, busca dejar atrás la idea de que una de las partes debe perder para que la otra gane, es decir, se permite que dentro de los sistemas puedan coexistir tanto la seguridad como la privacidad evitando lo que llaman falsas dualidades. (Cavoukian, 2011)
5. **Seguridad de extremo a extremo:** Si la seguridad ha sido implementada desde el principio los datos deben estar asegurados dentro de todo el proceso que atraviesen los datos hasta el fin. Garantizado su almacenamiento seguro, y que una vez cumplida la finalidad con la que los datos fueron recogidos, puedan ser eliminados de manera segura. (Ryerson University, S.F)
6. **Visibilidad y transparencia – mantenerlo abierto:** A través de ella se busca que cualquier forma en que se encuentre involucrada la tecnología sus componentes o partes se encuentren visibles tanto a sus usuarios como a los proveedores. (Cavoukian, 2011)
7. **Respeto a la privacidad de los usuarios:** Se requiere que, tanto los proveedores de servicios, como los fabricantes deben tener como principal prioridad la seguridad de los datos personales de los usuarios, facilitando medidas de protección de la privacidad y seguridad. (Ryerson University, S.F)

La aplicación de este tipo de protección, tiene como objetivo involucrar más al usuario en el manejo de su propia información; es por eso, que las autoridades europeas de protección de datos comparten este método y buscan aplicarlo en

los entornos digitales, tomando en cuenta como prioridad principal la protección y seguridad en el manejo de datos personales.

Es así, que el año 2010 durante la Conferencia Internacional número 32 de Autoridades de Protección de datos y Privacidad, realizada en Jerusalén, se adopta en la resolución el *Privacy by design*, de forma unánime en la que se deben tomar en cuenta varios aspectos, entre ellos, que no es una resolución vinculante, es decir, que no cuenta con una obligación determinada en una norma específica, por otra parte, cabe mencionar que es una resolución aprobada por autoridades a nivel internacional, y por último la resolución no hace referencia específica a la protección de datos, por cuanto quienes han participado en ella tienen diferentes sistemas jurídicos, por lo que su aplicación variaría de acuerdo a la forma en que esté estructurado el sistema jurídico de cada país. (GEV Asesores Internacionales, S.C., 2014)

Por su parte, la Unión Europea, también ha generado medidas de seguridad que puedan ser aplicables para los datos en el área tecnológica y lo expresa en la Recomendación 2012/148/UE de la comisión, que plantea que la protección de datos desde el diseño debería formar parte de las metodologías empleadas por las partes para dentro del desarrollo de las estructuras tecnológicas, siempre que dentro de los procesos, se vean involucrados datos personales. Así también, plantea que la protección de datos personales desde el diseño debe aplicarse por medio de legislación, incorporando normativa sobre la privacidad por diseño, reconociéndola así como un derecho de los usuarios. (Comisión Europea, 2012, pág. 73/12)

En conclusión, la protección de datos mediante el uso de la privacidad por diseño va más allá del ámbito legal, busca generar un entorno transparente en el que sus partes, tanto usuarios como proveedores, verifiquen la seguridad de los datos recolectados durante todo el proceso, desde su inicio hasta su fin, y que al final sean eliminados de forma segura, esto puede complementarse con las normas jurídicas existentes, de modo que se crea un entorno completamente seguro para los usuarios.

3 CONCLUSIONES

La tecnología que hace uso del internet, en las últimas décadas, ha ido tomando un lugar importante para las personas, así como también, para los gobiernos. Es habitual, el uso de internet en dispositivos móviles, sin embargo, internet de las cosas va más allá. Éste, es un concepto escasamente conocido, que está cada vez más involucrado en la vida de todos, ya que encontramos al *IoT*, en objetos de uso común como pueden ser las lavadoras o tan importantes como un marcapasos en el área de la salud.

El derecho a la protección de datos personales, es un derecho independiente que guarda relación con otros derechos fundamentales como son el derecho a la privacidad e intimidad. A pesar de que, en el Ecuador los reconoce como derechos fundamentales no existe norma legal especializada que establezca un sistema de protección, prevención y aplicación de los principios del derecho a la protección de los datos personales, a pesar de que otras normas internas como la Ley del Sistema Nacional de Registros Públicos, que también lo mencionan.

A lo largo del desarrollo del presente trabajo, se refleja que el internet de las cosas, es una realidad en el país, para ello, se ha tomado en cuenta las normativas existentes y las más desarrolladas sobre protección de datos personales a fin de identificar de qué forma se podría implementar normativa en el país que sea lo suficientemente efectiva para proteger la información personal de los ciudadanos.

En la actualidad, puede considerarse a la norma europea como el mayor referente sobre regulación acerca del derecho de la protección de datos personales. Esta normativa, puede ser tomada como ejemplo a seguir, sin embargo, el mercado europeo en comparación al ecuatoriano, es significativo ya que lo conforman varios países, por lo que sería viable exigir en bloque a las compañías de tecnología un nivel adecuado de protección de datos personales en sus dispositivos.

Dentro de la norma ecuatoriana, la Constitución reconoce el derecho a la protección de datos personales y reconoce al *Habeas data* como una acción para

la protección de la información personal de los personas, naturales o jurídicas, a través de esta acción se busca proteger la información personal de los ciudadanos. Esta acción podrá ser ejercida por el titular siempre que se haya considerado vulnerado su derecho a la protección de sus datos personales.

En el país, varias normas hacen mención a la protección de datos personales, sin embargo, no existe una norma específica que regule las acciones y dictamine medidas para la protección de datos personales, a consecuencia de que el Ecuador es un país pequeño, lo que quiere decir, que el mercado no es significativo ni en la región mucho menos a escala internacional, por lo que crear una normativa ecuatoriana sobre internet de las cosas, carecería de aplicabilidad en la realidad nacional.

Una solución a la falta de aplicabilidad de una norma sobre protección de datos personales en el internet de las cosas puede ser la privacidad por diseño, para ello, a través de convenios internacionales, los países latinoamericanos, siguiendo el ejemplo de Europa, puede unirse para exigir a los productores de tecnología implementar mayor seguridad en el área de internet de las cosas, de tal forma que los usuarios posean mayor control y protección de sus datos personales.

REFERENCIAS

Constitución de la República del Ecuador . (2008). Quito: CEP.

Agencia Española de Protección de Datos. (2014). Las Autoridades europeas de protección de datos aprueban el primer Dictamen conjunto sobre internet de las cosas.

Alcaraz, M. (S/A). *Internet de las Cosas.* Asunción: Universidad Católica Nuestra Señora de Asunción.

Alonso, J. (2009). *La protección de datos personales: Soluciones en entornos Microsoft.* Madrid: Microsoft Ibérica Unipersonal S.R.L.

Astudillo, G. (2015). La TV ensamblada en el país es más competitiva. *El comercio*.

Aymesa. (2013). *AYMESA*. Recuperado el 11 de Diciembre de 2016, de http://www.aymesa.ec/index.php/es/empresa

Bazán, V. (2009). *EL HÁBEAS DATA Y EL DERECHO DE AUTODETERMINACIÓN INFORMATIVA EN PERSPECTIVA DE DERECHO COMPARADO.*

Bliznakoff, D. (2014). *IoT: Tecnologías, usos, tendencias y desarrollo futuro.*

Cavoukian, A. (2011). *Privacy by Design.* Recuperado el 08 de Noviembre de 2016, de Association of Corporate Counsel : https://www.acc.com/chapters/euro/upload/7foundationalprinciples-spanish.pdf

Centro de Seguridad TIC de la Comunidad Valenciana. (S.F). *Seguridad en el Internet de las Cosas.* Valencia: Generalitat Valenciana.

Cisco IBSG. (2011). *Internet de las cosas como próxima evolución de Internet lo cambia todo.* Recuperado el 19 de Agosto de 2016, de http://www.cisco.com/c/dam/global/es_mx/solutions/executive/assets/pdf/internet-of-things-iot-ibsg.pdf

Comisión Europea. (2012). Recomendación de la Comisión . *Diario Oficial de la Unión Europea*, pág. 73/12.

Davara, M. (1998). *La protección de datos en Europa.* Madrid: Grupo Asnef Equifax.

Enrile, C. (2015). *Internet de las cosas: todo un mundo por regular.*

FTC Staff Report. (2015). Privacy and Security in a Connected World. *Internet of things*, I.

Garrido, R. (2013). *El hábeas data y la Ley de protección de datos en Chile.* Santiago de Chile: UTEM.

Garriga, A. (1999). *La protección de datos personales en el derecho español.* Madrid: Dikinson .

GEV Asesores Internacionales, S.C. (2014). Privacy by Design para fomentar la figura del encargado. México D.F.

Gregorio, C. (2014). *Protección de datos personales: Europa Vs. Estados Unidos.* México D.F.: Instituto de Investigaciones Jurídicas .

Grimalt, P. (2008). Servicios de la Sociedad de la información y protección de datos personales. En A. Recalde, *Derecho de la Empresa y Protección de datos* (p.p. 326-327). Navarra: Aranzadi S.A.

Grupo de Trabajo sobre Protección de Datos. (2000). *Dictamen 4/2000.* Bruselas: Comisión Europea.

Guasch, V., & Soler, J. (2016). Computación en la Nube y Puerto Seguro. *Revista de Derecho UNED*, 342.

Guerrero, M. d. (2006). *El impacto del internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal.* Navarra: Aranzadi S.A.

Hernández, J. (2012). La protección de datos personales en el internet y el habeas data. *Revista Derecho y Tecnología*, 65-66.

Internet Society Org. (2015). *The Internet of things.*

Levin, A., & Nicholson, M. J. (2005). Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground. *University of Ottawa law & technology journal*, 357.

Murillo, L. (2008). *El derecho a la autodeterminación informativa y la protección de datos personales.* Azpilcueta: BIBLID.

Naciones Unidas. (2005). Delitos Informáticos. *Undécimo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal*, (págs. 6-7). Bankok.

Nieves, M. (2012). The Right to Privacy. *Revista de Derecho Político UNED*, 197-198.

Ordónez, D. (2011). *Privacidad y Protección Judicial de los Datos Personales.* Barcelona: Bosch S.A.

Parker, D. (1989). Computer Crime. En *Criminal Justice Resource Manual* (págs. 3-4). Washington D.C.: National Institute of Justice.

Parlamento y consejo de la unión europea. (2016). Reglamento general de protección de datos.

Ryerson University. (S.F). Privacy by Design Setting a new standard for privacy certification. *Deloitte*, 1-2.

Sala de Prensa. (2016). *Asamblea Nacional* . Recuperado el 12 de Diciembre de 2016, de http://www.asambleanacional.gob.ec/es/noticia/45994-proyecto-de-ley-de-proteccion-de-datos-no-restringira

Santos, D. (2005). *Nociones Generales de la Ley Orgánica de Protección de Datos .* Madrid: TECNOS.

Téllez, J. (1996). *Derecho Informártico.* México D.F.: Interamericana de México, S.A de C.V.

Unión Internacional de Telecomunicaciones. (2015). Regulación y la Internet de las Cosas. *Actualidades de la UIT*, 12-14.

Veleiro, B. (2008). *Protección de datos de carácter personal.* Madrid: Estudios Jurídicos 12.

ANEXOS

Aprobación de la Directiva 95/46/CE y el Parlamento europeo respecto a protección de datos personales y la libre circulación de los mismos

DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995

On the protection of individuals with regard to the processing of personal data and on the free movement of such data

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 100a thereof,

Having regard to the proposal from the Commission (1),

Having regard to the opinion of the Economic and Social Committee (2),

Acting in accordance with the procedure referred to in Article 189b of the Treaty (3),

(1) Whereas the objectives of the Community, as laid down in the Treaty, as amended by the Treaty on European Union, include creating an ever closer union among the peoples of Europe, fostering closer relations between the States belonging to the Community, ensuring economic and social progress by common action to eliminate the barriers which divide Europe, encouraging the constant improvement of the living conditions of its peoples, preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognized in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms;

(2) Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;

(3) Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded;

(4) Whereas increasingly frequent recourse is being had in the Community to the processing of personal data in the various spheres of economic and

social activity; whereas the progress made in information technology is making the processing and exchange of such data considerably easier;

(5) Whereas the economic and social integration resulting from the establishment and functioning of the internal market within the meaning of Article 7a of the Treaty will necessarily lead to a substantial increase in cross-border flows of personal data between all those involved in a private or public capacity in economic and social activity in the Member States; whereas the exchange of personal data between undertakings in different Member States is set to increase; whereas the national authorities in the various Member States are being called upon by virtue of Community law to collaborate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State within the context of the area without internal frontiers as constituted by the internal market;

(6) Whereas, furthermore, the increase in scientific and technical cooperation and the coordinated introduction of new telecommunications networks in the Community necessitate and facilitate cross-border flows of personal data;

(7) Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; whereas this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law; whereas this difference in levels of protection is due to the existence of a wide variety of national laws, regulations and administrative provisions;

(8) Whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States; whereas this objective is vital to the internal market but cannot be achieved by the Member States alone, especially in view of the scale of the divergences which currently exist between the relevant laws in the Member States and the need to coordinate the laws of the Member States so as to ensure that the cross-border flow of personal data is regulated in a consistent manner that is in keeping with the objective of the internal market as provided for in Article 7a of the Treaty; whereas Community action to approximate those laws is therefore needed;

(9) Whereas, given the equivalent protection resulting from the approximation of national laws, the Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, and in

particular the right to privacy; whereas Member States will be left a margin for manoeuvre, which may, in the context of implementation of the Directive, also be exercised by the business and social partners; whereas Member States will therefore be able to specify in their national law the general conditions governing the lawfulness of data processing; whereas in doing so the Member States shall strive to improve the protection currently provided by their legislation; whereas, within the limits of this margin for manoeuvre and in accordance with Community law, disparities could arise in the implementation of the Directive, and this could have an effect on the movement of data within a Member State as well as within the Community;

(10) Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;

(11) Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data;

(12) Whereas the protection principles must apply to all processing of personal data by any person whose activities are governed by Community law; whereas there should be excluded the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, such as correspondence and the holding of records of addresses;

(13) Whereas the acitivities referred to in Titles V and VI of the Treaty on European Union regarding public safety, defence, State security or the acitivities of the State in the area of criminal laws fall outside the scope of Community law, without prejudice to the obligations incumbent upon Member States under Article 56 (2), Article 57 or Article 100a of the Treaty establishing the European Community; whereas the processing of personal data that is necessary to safeguard the economic well-being of the State does not fall within the scope of this Directive where such processing relates to State security matters;

(14) Whereas, given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and

image data relating to natural persons, this Directive should be applicable to processing involving such data;

(15) Whereas the processing of such data is covered by this Directive only if it is automated or if the data processed are contained or are intended to be contained in a filing system structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question;

(16) Whereas the processing of sound and image data, such as in cases of video surveillance, does not come within the scope of this Directive if it is carried out for the purposes of public security, defence, national security or in the course of State activities relating to the area of criminal law or of other activities which do not come within the scope of Community law;

(17) Whereas, as far as the processing of sound and image data carried out for purposes of journalism or the purposes of literary or artistic expression is concerned, in particular in the audiovisual field, the principles of the Directive are to apply in a restricted manner according to the provisions laid down in Article 9;

(18) Whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; whereas, in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State;

(19) Whereas establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect; whereas, when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities;

(20) Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice;

(21) Whereas this Directive is without prejudice to the rules of territoriality applicable in criminal matters;

(22) Whereas Member States shall more precisely define in the laws they enact or when bringing into force the measures taken under this Directive the general circumstances in which processing is lawful; whereas in particular Article 5, in conjunction with Articles 7 and 8, allows Member States, independently of general rules, to provide for special processing conditions for specific sectors and for the various categories of data covered by Article 8;

(23) Whereas Member States are empowered to ensure the implementation of the protection of individuals both by means of a general law on the protection of individuals as regards the processing of personal data and by sectorial laws such as those relating, for example, to statistical institutes;

(24) Whereas the legislation concerning the protection of legal persons with regard to the processing data which concerns them is not affected by this Directive;

(25) Whereas the principles of protection must be reflected, on the one hand, in the obligations imposed on persons, public authorities, enterprises, agencies or other bodies responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the right conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances;

(26) Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible;

(27) Whereas the protection of individuals must apply as much to automatic processing of data as to manual processing; whereas the scope of this protection must not in effect depend on the techniques used, otherwise this would create a serious risk of circumvention; whereas, nonetheless, as regards manual processing, this Directive covers only filing systems, not unstructured files; whereas, in particular, the content of a filing system must be structured according to specific criteria relating to individuals allowing easy access to the personal data; whereas, in line with the definition in Article 2 (c), the different criteria for determining the

constituents of a structured set of personal data, and the different criteria governing access to such a set, may be laid down by each Member State; whereas files or sets of files as well as their cover pages, which are not structured according to specific criteria, shall under no circumstances fall within the scope of this Directive;

(28) Whereas any processing of personal data must be lawful and fair to the individuals concerned; whereas, in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and legitimate and must be determined at the time of collection of the data; whereas the purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified;

(29) Whereas the further processing of personal data for historical, statistical or scientific purposes is not generally to be considered incompatible with the purposes for which the data have previously been collected provided that Member States furnish suitable safeguards; whereas these safeguards must in particular rule out the use of the data in support of measures or decisions regarding any particular individual;

(30) Whereas, in order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject or be necessary for the conclusion or performance of a contract binding on the data subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person, provided that the interests or the rights and freedoms of the data subject are not overriding; whereas, in particular, in order to maintain a balance between the interests involved while guaranteeing effective competition, Member States may determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies; whereas Member States may similarly specify the conditions under which personal data may be disclosed to a third party for the purposes of marketing whether carried out commercially or by a charitable organization or by any other association or foundation, of a political nature for example, subject to the provisions allowing a data subject to object to the processing of data regarding him, at no cost and without having to state his reasons;

(31) Whereas the processing of personal data must equally be regarded as lawful where it is carried out in order to protect an interest which is essential for the data subject's life;

(32) Whereas it is for national legislation to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another

natural or legal person governed by public law, or by private law such as a professional association;

(33) Whereas data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the data subject gives his explicit consent; whereas, however, derogations from this prohibition must be explicitly provided for in respect of specific needs, in particular where the processing of these data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy or in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms;

(34) Whereas Member States must also be authorized, when justified by grounds of important public interest, to derogate from the prohibition on processing sensitive categories of data where important reasons of public interest so justify in areas such as public health and social protection - especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system - scientific research and government statistics; whereas it is incumbent on them, however, to provide specific and suitable safeguards so as to protect the fundamental rights and the privacy of individuals;

(35) Whereas, moreover, the processing of personal data by official authorities for achieving aims, laid down in constitutional law or international public law, of officially recognized religious associations is carried out on important grounds of public interest;

(36) Whereas where, in the course of electoral activities, the operation of the democratic system requires in certain Member States that political parties compile data on people's political opinion, the processing of such data may be permitted for reasons of important public interest, provided that appropriate safeguards are established;

(37) Whereas the processing of personal data for purposes of journalism or for purposes of literary of artistic expression, in particular in the audiovisual field, should qualify for exemption from the requirements of certain provisions of this Directive in so far as this is necessary to reconcile the fundamental rights of individuals with freedom of information and notably the right to receive and impart information, as guaranteed in particular in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; whereas Member States should therefore lay down exemptions and derogations necessary for the purpose of balance between fundamental rights as regards general measures on the legitimacy of data processing, measures on the transfer of data to third countries and the power of the supervisory authority; whereas this should not, however, lead Member States to lay down

exemptions from the measures to ensure security of processing; whereas at least the supervisory authority responsible for this sector should also be provided with certain ex-post powers, e.g. to publish a regular report or to refer matters to the judicial authorities;

(38) Whereas, if the processing of data is to be fair, the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection;

(39) Whereas certain processing operations involve data which the controller has not collected directly from the data subject; whereas, furthermore, data can be legitimately disclosed to a third party, even if the disclosure was not anticipated at the time the data were collected from the data subject; whereas, in all these cases, the data subject should be informed when the data are recorded or at the latest when the data are first disclosed to a third party;

(40) Whereas, however, it is not necessary to impose this obligation of the data subject already has the information; whereas, moreover, there will be no such obligation if the recording or disclosure are expressly provided for by law or if the provision of information to the data subject proves impossible or would involve disproportionate efforts, which could be the case where processing is for historical, statistical or scientific purposes; whereas, in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration;

(41) Whereas any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing; whereas, for the same reasons, every data subject must also have the right to know the logic involved in the automatic processing of data concerning him, at least in the case of the automated decisions referred to in Article 15 (1); whereas this right must not adversely affect trade secrets or intellectual property and in particular the copyright protecting the software; whereas these considerations must not, however, result in the data subject being refused all information;

(42) Whereas Member States may, in the interest of the data subject or so as to protect the rights and freedoms of others, restrict rights of access and information; whereas they may, for example, specify that access to medical data may be obtained only through a health professional;

(43) Whereas restrictions on the rights of access and information and on certain obligations of the controller may similarly be imposed by Member States in so far as they are necessary to safeguard, for example, national security, defence, public safety, or important economic or financial interests of a Member State or the Union, as well as criminal investigations

and prosecutions and action in respect of breaches of ethics in the regulated professions; whereas the list of exceptions and limitations should include the tasks of monitoring, inspection or regulation necessary in the three last-mentioned areas concerning public security, economic or financial interests and crime prevention; whereas the listing of tasks in these three areas does not affect the legitimacy of exceptions or restrictions for reasons of State security or defence;

(44) Whereas Member States may also be led, by virtue of the provisions of Community law, to derogate from the provisions of this Directive concerning the right of access, the obligation to inform individuals, and the quality of data, in order to secure certain of the purposes referred to above;

(45) Whereas, in cases where data might lawfully be processed on grounds of public interest, official authority or the legitimate interests of a natural or legal person, any data subject should nevertheless be entitled, on legitimate and compelling grounds relating to his particular situation, to object to the processing of any data relating to himself; whereas Member States may nevertheless lay down national provisions to the contrary;

(46) Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected;

(47) Whereas where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services; whereas, nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service;

(48) Whereas the procedures for notifying the supervisory authority are designed to ensure disclosure of the purposes and main features of any processing operation for the purpose of verification that the operation is in accordance with the national measures taken under this Directive;

(49) Whereas, in order to avoid unsuitable administrative formalities, exemptions from the obligation to notify and simplification of the notification required may be provided for by Member States in cases where processing is unlikely adversely to affect the rights and freedoms of data subjects, provided that it is in accordance with a measure taken by a Member State specifying its limits; whereas exemption or simplification may similarly be provided for by Member States where a person appointed by the controller ensures that the processing carried out is not likely adversely to affect the rights and freedoms of data subjects; whereas such a data protection official, whether or not an employee of the controller, must be in a position to exercise his functions in complete independence;

(50) Whereas exemption or simplification could be provided for in cases of processing operations whose sole purpose is the keeping of a register intended, according to national law, to provide information to the public and open to consultation by the public or by any person demonstrating a legitimate interest;

(51) Whereas, nevertheless, simplification or exemption from the obligation to notify shall not release the controller from any of the other obligations resulting from this Directive;

(52) Whereas, in this context, ex post facto verification by the competent authorities must in general be considered a sufficient measure;

(53) Whereas, however, certain processing operation are likely to pose specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, such as that of excluding individuals from a right, benefit or a contract, or by virtue of the specific use of new technologies; whereas it is for Member States, if they so wish, to specify such risks in their legislation;

(54) Whereas with regard to all the processing undertaken in society, the amount posing such specific risks should be very limited; whereas Member States must provide that the supervisory authority, or the data protection official in cooperation with the authority, check such processing prior to it being carried out; whereas following this prior check, the supervisory authority may, according to its national law, give an opinion or an authorization regarding the processing; whereas such checking may equally take place in the course of the preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing and lays down appropriate safeguards;

(55) Whereas, if the controller fails to respect the rights of data subjects, national legislation must provide for a judicial remedy; whereas any damage which a person may suffer as a result of unlawful processing must be compensated for by the controller, who may be exempted from liability

if he proves that he is not responsible for the damage, in particular in cases where he establishes fault on the part of the data subject or in case of force majeure; whereas sanctions must be imposed on any person, whether governed by private of public law, who fails to comply with the national measures taken under this Directive;

(56) Whereas cross-border flows of personal data are necessary to the expansion of international trade; whereas the protection of individuals guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third countries which ensure an adequate level of protection; whereas the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations;

(57) Whereas, on the other hand, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited;

(58) Whereas provisions should be made for exemptions from this prohibition in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where protection of an important public interest so requires, for example in cases of international transfers of data between tax or customs administrations or between services competent for social security matters, or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest; whereas in this case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients;

(59) Whereas particular measures may be taken to compensate for the lack of protection in a third country in cases where the controller offers appropriate safeguards; whereas, moreover, provision must be made for procedures for negotiations between the Community and such third countries;

(60) Whereas, in any event, transfers to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to this Directive, and in particular Article 8 thereof;

(61) Whereas Member States and the Commission, in their respective spheres of competence, must encourage the trade associations and other representative organizations concerned to draw up codes of conduct so as to facilitate the application of this Directive, taking account of the specific characteristics of the processing carried out in certain sectors, and respecting the national provisions adopted for its implementation;

(62) Whereas the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data;

(63) Whereas such authorities must have the necessary means to perform their duties, including powers of investigation and intervention, particularly in cases of complaints from individuals, and powers to engage in legal proceedings; whereas such authorities must help to ensure transparency of processing in the Member States within whose jurisdiction they fall;

(64) Whereas the authorities in the different Member States will need to assist one another in performing their duties so as to ensure that the rules of protection are properly respected throughout the European Union;

(65) Whereas, at Community level, a Working Party on the Protection of Individuals with regard to the Processing of Personal Data must be set up and be completely independent in the performance of its functions; whereas, having regard to its specific nature, it must advise the Commission and, in particular, contribute to the uniform application of the national rules adopted pursuant to this Directive;

(66) Whereas, with regard to the transfer of data to third countries, the application of this Directive calls for the conferment of powers of implementation on the Commission and the establishment of a procedure as laid down in Council Decision 87/373/EEC (1);

(67) Whereas an agreement on a modus vivendi between the European Parliament, the Council and the Commission concerning the implementing measures for acts adopted in accordance with the procedure laid down in Article 189b of the EC Treaty was reached on 20 December 1994;

(68) Whereas the principles set out in this Directive regarding the protection of the rights and freedoms of individuals, notably their right to privacy, with regard to the processing of personal data may be supplemented or clarified, in particular as far as certain sectors are concerned, by specific rules based on those principles;

(69) Whereas Member States should be allowed a period of not more than three years from the entry into force of the national measures transposing this Directive in which to apply such new national rules progressively to all processing operations already under way; whereas, in order to facilitate their cost-effective implementation, a further period expiring 12 years after the date on which this Directive is adopted will be allowed to Member States to ensure the conformity of existing manual filing systems with certain of the Directive's provisions; whereas, where data contained in such filing systems are manually processed during this extended transition

period, those systems must be brought into conformity with these provisions at the time of such processing;

(70) Whereas it is not necessary for the data subject to give his consent again so as to allow the controller to continue to process, after the national provisions taken pursuant to this Directive enter into force, any sensitive data necessary for the performance of a contract concluded on the basis of free and informed consent before the entry into force of these provisions;

(71) Whereas this Directive does not stand in the way of a Member State's regulating marketing activities aimed at consumers residing in territory in so far as such regulation does not concern the protection of individuals with regard to the processing of personal data;

(72) Whereas this Directive allows the principle of public access to official documents to be taken into account when implementing the principles set out in this Directive,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I GENERAL PROVISIONS

Article 1

Object of the Directive

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

Article 2

Definitions

For the purposes of this Directive:

(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(c) 'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

(e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(f) 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;

(g) 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;

(h) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

Article 3

Scope

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Directive shall not apply to the processing of personal data:

- in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

- by a natural person in the course of a purely personal or household activity.

Article 4

National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

CHAPTER II GENERAL RULES ON THE LAWFULNESS OF THE PROCESSING OF PERSONAL DATA

Article 5

Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful.

SECTION I

PRINCIPLES RELATING TO DATA QUALITY

Article 6

1. Member States shall provide that personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with.

SECTION II

CRITERIA FOR MAKING DATA PROCESSING LEGITIMATE

Article 7

Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

SECTION III

SPECIAL CATEGORIES OF PROCESSING

Article 8

The processing of special categories of data

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

2. Paragraph 1 shall not apply where:

(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or

(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or

(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national

provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.

Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority.

6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.

7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

Article 9

Processing of personal data and freedom of expression

Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

SECTION IV

INFORMATION TO BE GIVEN TO THE DATA SUBJECT

Article 10

Information in cases of collection of data from the data subject

Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing for which the data are intended;

(c) any further information such as

- the recipients or categories of recipients of the data,

- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,

- the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Article 11

Information where the data have not been obtained from the data subject

1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing;

(c) any further information such as

- the categories of data concerned,

- the recipients or categories of recipients,

- the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.

SECTION V

THE DATA SUBJECT'S RIGHT OF ACCESS TO DATA

Article 12

Right of access

Member States shall guarantee every data subject the right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,

- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

SECTION VI

EXEMPTIONS AND RESTRICTIONS

Article 13

Exemptions and restrictions

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

(g) the protection of the data subject or of the rights and freedoms of others.

2. Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

SECTION VII

THE DATA SUBJECT'S RIGHT TO OBJECT

Article 14

The data subject's right to object

Member States shall grant the data subject the right:

(a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

(b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).

Article 15

Automated individual decisions

1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:

(a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or

(b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

SECTION VIII

CONFIDENTIALITY AND SECURITY OF PROCESSING

Article 16

Confidentiality of processing

Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

Article 17

Security of processing

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

- the processor shall act only on instructions from the controller,

- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

SECTION IX

NOTIFICATION

Article 18

Obligation to notify the supervisory authority

1. Member States shall provide that the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.

2. Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:

- where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored, and/or

- where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:

- for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive

- for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2),

thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

3. Member States may provide that paragraph 1 does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person demonstrating a legitimate interest.

4. Member States may provide for an exemption from the obligation to notify or a simplification of the notification in the case of processing operations referred to in Article 8 (2) (d).

5. Member States may stipulate that certain or all non-automatic processing operations involving personal data shall be notified, or provide for these processing operations to be subject to simplified notification.

Article 19

Contents of notification

1. Member States shall specify the information to be given in the notification. It shall include at least:

(a) the name and address of the controller and of his representative, if any;

(b) the purpose or purposes of the processing;

(c) a description of the category or categories of data subject and of the data or categories of data relating to them;

(d) the recipients or categories of recipient to whom the data might be disclosed;

(e) proposed transfers of data to third countries;

(f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

2. Member States shall specify the procedures under which any change affecting the information referred to in paragraph 1 must be notified to the supervisory authority.

Article 20

Prior checking

1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.

2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.

3. Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.

Article 21

Publicizing of processing operations

1. Member States shall take measures to ensure that processing operations are publicized.

2. Member States shall provide that a register of processing operations notified in accordance with Article 18 shall be kept by the supervisory authority.

The register shall contain at least the information listed in Article 19 (1) (a) to (e).

The register may be inspected by any person.

3. Member States shall provide, in relation to processing operations not subject to notification, that controllers or another body appointed by the Member States make available at least the information referred to in Article 19 (1) (a) to (e) in an appropriate form to any person on request.

Member States may provide that this provision does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can provide proof of a legitimate interest.

CHAPTER III JUDICIAL REMEDIES, LIABILITY AND SANCTIONS

Article 22

Remedies

Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.

Article 23

Liability

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.

2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

Article 24

Sanctions

The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.

CHAPTER IV TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

Article 25

Principles

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for

processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's decision.

Article 26

Derogations

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.

If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2).

Member States shall take the necessary measures to comply with the Commission's decision.

4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.

CHAPTER V CODES OF CONDUCT

Article 27

1. The Member States and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to this Directive, taking account of the specific features of the various sectors.

2. Member States shall make provision for trade associations and other bodies representing other categories of controllers which have drawn up draft national codes or which have the intention of amending or extending existing national codes to be able to submit them to the opinion of the national authority.

Member States shall make provision for this authority to ascertain, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives.

3. Draft Community codes, and amendments or extensions to existing Community codes, may be submitted to the Working Party referred to in Article 29. This Working Party shall determine, among other things, whether the drafts submitted to it are in accordance with the national provisions adopted pursuant to this Directive. If it sees fit, the authority shall seek the views of data subjects or their representatives. The Commission may ensure appropriate publicity for the codes which have been approved by the Working Party.

CHAPTER VI SUPERVISORY AUTHORITY AND WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Article 28

Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

These authorities shall act with complete independence in exercising the functions entrusted to them.

2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

3. Each authority shall in particular be endowed with:

- investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,

- effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,

- the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.

5. Each supervisory authority shall draw up a report on its activities at regular intervals. The report shall be made public.

6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

7. Member States shall provide that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

Article 29

Working Party on the Protection of Individuals with regard to the Processing of Personal Data

1. A Working Party on the Protection of Individuals with regard to the Processing of Personal Data, hereinafter referred to as 'the Working Party', is hereby set up.

It shall have advisory status and act independently.

2. The Working Party shall be composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission.

Each member of the Working Party shall be designated by the institution, authority or authorities which he represents. Where a Member State has designated more than one supervisory authority, they shall nominate a joint representative. The same shall apply to the authorities established for Community institutions and bodies.

3. The Working Party shall take decisions by a simple majority of the representatives of the supervisory authorities.

4. The Working Party shall elect its chairman. The chairman's term of office shall be two years. His appointment shall be renewable.

5. The Working Party's secretariat shall be provided by the Commission.

6. The Working Party shall adopt its own rules of procedure.

7. The Working Party shall consider items placed on its agenda by its chairman, either on his own initiative or at the request of a representative of the supervisory authorities or at the Commission's request.

Article 30

1. The Working Party shall:

(a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures;

(b) give the Commission an opinion on the level of protection in the Community and in third countries;

(c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;

(d) give an opinion on codes of conduct drawn up at Community level.

2. If the Working Party finds that divergences likely to affect the equivalence of protection for persons with regard to the processing of personal data in the Community are arising between the laws or practices of Member States, it shall inform the Commission accordingly.

3. The Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community.

4. The Working Party's opinions and recommendations shall be forwarded to the Commission and to the committee referred to in Article 31.

5. The Commission shall inform the Working Party of the action it has taken in response to its opinions and recommendations. It shall do so in a report which shall also be forwarded to the European Parliament and the Council. The report shall be made public.

6. The Working Party shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Community and in third countries, which it shall transmit to the Commission, the European Parliament and the Council. The report shall be made public.

CHAPTER VII COMMUNITY IMPLEMENTING MEASURES

Article 31

The Committee

1. The Commission shall be assisted by a committee composed of the representatives of the Member States and chaired by the representative of the Commission.

2. The representative of the Commission shall submit to the committee a draft of the measures to be taken. The committee shall deliver its opinion on the draft within a time limit which the chairman may lay down according to the urgency of the matter.

The opinion shall be delivered by the majority laid down in Article 148 (2) of the Treaty. The votes of the representatives of the Member States within the committee shall be weighted in the manner set out in that Article. The chairman shall not vote.

The Commission shall adopt measures which shall apply immediately. However, if these measures are not in accordance with the opinion of the committee, they shall be communicated by the Commission to the Council forthwith. It that event:

- the Commission shall defer application of the measures which it has decided for a period of three months from the date of communication,

- the Council, acting by a qualified majority, may take a different decision within the time limit referred to in the first indent.

FINAL PROVISIONS

Article 32

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive at the latest at the end of a period of three years from the date of its adoption.

When Member States adopt these measures, they shall contain a reference to this Directive or be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by the Member States.

2. Member States shall ensure that processing already under way on the date the national provisions adopted pursuant to this Directive enter into force, is brought into conformity with these provisions within three years of this date.

By way of derogation from the preceding subparagraph, Member States may provide that the processing of data already held in manual filing systems on the date of entry into force of the national provisions adopted in implementation of this Directive shall be brought into conformity with Articles 6, 7 and 8 of this Directive within 12 years of the date on which it is adopted. Member States shall, however, grant the data subject the right to obtain, at his request and in particular at the time of exercising his right of access, the rectification, erasure or blocking of data which are incomplete, inaccurate or stored in a way incompatible with the legitimate purposes pursued by the controller.

3. By way of derogation from paragraph 2, Member States may provide, subject to suitable safeguards, that data kept for the sole purpose of historical research need not be brought into conformity with Articles 6, 7 and 8 of this Directive.

4. Member States shall communicate to the Commission the text of the provisions of domestic law which they adopt in the field covered by this Directive.

Article 33

The Commission shall report to the Council and the European Parliament at regular intervals, starting not later than three years after the date referred to in Article 32 (1), on the implementation of this Directive, attaching to its report, if necessary, suitable proposals for amendments. The report shall be made public.

The Commission shall examine, in particular, the application of this Directive to the data processing of sound and image data relating to natural persons and shall submit any appropriate proposals which prove to be necessary, taking account of developments in information technology and in the light of the state of progress in the information society.

Article 34

This Directive is addressed to the Member States.

Done at Luxembourg, 24 October 1995.

For the European Parliament

The President

K. HAENSCH

For the Council

The President

L. ATIENZA SERNA

(1) OJ No C 277, 5. 11. 1990, p. 3 and OJ No C 311, 27. 11. 1992, p. 30.

(2) OJ No C 159, 17. 6. 1991, p 38.

(3) Opinion of the European Parliament of 11 March 1992 (OJ No C 94, 13. 4. 1992, p. 198), confirmed on 2 December 1993 (OJ No C 342, 20. 12. 1993, p. 30); Council common position of 20 February 1995 (OJ No C 93, 13. 4. 1995, p. 1) and Decision of the European Parliament of 15 June 1995 (OJ No C 166, 3. 7. 1995).

(1) OJ No L 197, 18. 7. 1987, p. 33.