



UNIVERSIDAD PRIVADA DEL NORTE
Laureate International Universities

FACULTAD DE
DERECHO Y CIENCIAS POLÍTICAS

TÍTULO DE LA TESIS

TESIS
PARA OPTAR AL TÍTULO PROFESIONAL DE:
ABOGADO

AUTOR:
Bach. Lucía Alejandra Vargas Fernández

ASESOR:
Guhtember Pacherres Pérez

CAJAMARCA – PERÚ
2012

A Carlos Manuel, aunque no me deje trabajar
y sólo quiera jugar, porque él
nunca dejará de ser niño
y nunca dejará de soñar

¿Qué les queda por probar a los jóvenes en este mundo de consumo y humo?
¿vértigo? ¿asaltos? ¿discotecas? también les queda discutir con dios
tanto si existe como si no existe tender manos que ayuden a abrir puertas
entre el corazón propio y el ajeno sobre todo les queda hacer futuro
a pesar de los ruines de pasado y los sabios granujas del presente.

- Mario Benedetti-

TABLA DE CONTENIDO

Ítem	Página
Dedicatoria	(i)
Epígrafe	(ii)
Tabla de Contenido	(iii)
Agradecimientos	(ix)
Lista de Abreviaciones	(x)
Glosario	(xi)
Página de Resumen	(xii)
Abstract	(xiii)
Introducción	(xiv)

CAPÍTULO I

DE LOS ASPECTOS METODOLÓGICOS

1. ÁREA	1
2. PLANTEAMIENTO Y DESCRIPCIÓN DE LA SITUACIÓN PROBLEMÁTICA	1
3. FORMULACIÓN Y SISTEMATIZACIÓN	4
4. FUNDAMENTACIÓN	4
5. DELIMITACIÓN	5
6. LIMITACIONES	5
7. OBJETIVOS	6
8. ANTECEDENTES DEL PROBLEMA	6
9. FUNDAMENTO TEÓRICO	6
10. ASUNCIONES	11
11. TÉRMINOS FUNDAMENTALES	11

12. HIPÓTESIS.....	
	12
13. OPERACIONALIZACIÓN DE VARIABLES.....	
	13
14. CUADRO DE DETERMINACIÓN DEL PROBLEMA.....	
	13
15. TIPOLOGÍA.....	
	14
16. ENFOQUE.....	
	14
17. ALCANCE.....	
	14
18. DISEÑO.....	
	14
19. MÉTODOS.....	
	14
20. TÉCNICAS E INSTRUMENTOS.....	
	14
21. MUESTREO.....	
	14
22. REVISIÓN DE LITERATURA PRECEDENTE.....	
	15

CAPÍTULO II

DE LA SOCIEDAD DE LA INFORMACIÓN Y

LAS PÁGINA WEB DE CONTENIDO SOCIAL O REDES SOCIALES

SUB CAPÍTULO I

LA SOCIEDAD DE LA INFORMACIÓN

1. GENERALIDADES.....	
	16
2. CONCEPTO DE LA SOCIEDAD DE LA INFORMACIÓN.....	
	17

2.1. CONTRASTE ENTRE SOCIEDAD DE LA INFORMACIÓN Y SOCIEDAD DEL CONOCIMIENTO.....	18
2.1.1. La Sociedad del Conocimiento.....	18
2.2. ELEMENTOS CONSTITUTIVOS DE LA SOCIEDAD DE LA INFORMACIÓN.....	21
• Las redes.....	21
• Los servicios básicos.....	21
• Las aplicaciones.....	21
2.2.1. LOS SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN....	21
2.3. LA SEGURIDAD: REQUISITO NECESARIO EN LA NUEVA SOCIEDAD DE LA INFORMACIÓN.....	23
• Seguridad física.....	24
• Seguridad lógica.....	24
• Seguridad organizo- administrativa.....	24
• Seguridad jurídica.....	25
2.3.1. PRINCIPALES CARACTERÍSTICAS DE LA NECESIDAD	

DE SEGURIDAD EN LA SOCIEDAD DE LA INFORMACIÓN.....
25

- La confidencialidad.....
25
- La integridad.....
25
- La disponibilidad.....
25
- Con la autenticación.....
25
- El control de accesos.....
25
- El sellado del tiempo.....
25

2.3.1.1. JUSTIFICACIÓN DE LA SEGURIDAD EN
LA SOCIEDAD DE LA INFORMACIÓN.....
27

2.3.2. LOS DATOS DE CARÁCTER PERSONAL.....
28

SUB CAPÍTULO II

LAS PÁGINAS WEB DE CONTENIDO SOCIAL

O REDES SOCIALES DEL INTERNET

1. JUSTIFICACIÓN.....
30

2. GENERALIDADES.....
30

3. LAS PÁGINAS WEB DE CONTENIDO SOCIAL
O REDES SOCIALES Y SU OBJETIVO
RESPECTO DE ESTA INVESTIGACIÓN.....
31

CAPÍTULO III
DE LOS CONTRATOS VÍA INTERNET

1. GENERALIDADES.....	
34	
1.1. LA SOCIEDAD DE MASAS.....	
34	
1.2. TRÁFICO CONTRACTUAL MASIVO.....	
36	
1.2.1. EL CARÁCTER SOCIAL DEL CONTRATO.....	
36	
1.3. LA AUTONOMÍA PRIVADA Y EL CONTRATO POR ADHESIÓN.....	
38	
1.3.1. LA AUTONOMÍA PRIVADA.....	
38	
1.3.2. EL CONTRATO POR ADHESIÓN.....	
41	
2. LOS CONTRATOS VÍA INTERNET.....	
42	
• CONTRATO INFORMÁTICO.....	
43	
• CONTRATO ELECTRÓNICO.....	
43	
• CONTRATO TELEMÁTICO.....	
45	
• CONTRATOS ON LINE.....	
46	
• CONTRATO DIGITAL.....	
46	

3. LAS CLÁUSULAS AMENAZADORAS DE DERECHOS.....
48

- Hi5.....
50
- BADOO.....
50
- REDDIT.....
50
- DIGG.....
51

3.1. LAS CLÁUSULAS AMENAZADORAS RESPECTO DEL
DERECHO DE AUTODETERMINACIÓN INFORMATIVA.....
53

CAPITULO IV

LA SOLUCIÓN LEGAL QUE SE DEBE ADOPTAR FRENTE A LAS CLÁUSULAS
AMENAZADORAS DE DERECHO DE AUTODETERMINACIÓN INFORMATIVA
CONTENIDA EN LOS CONTRATOS ON LINE EN LAS PÁGINAS WEB DE
CONTENIDO SOCIAL O REDES SOCIALES

1. GENERALIDADES.....
56
2. EL POR QUÉ DE UN ORGANISMO INTERNACIONAL.....
56
 - El conflicto de jurisdicción.....
56
 - La cooperación internacional.....
57
 - La supranacionalidad de los organismos internacionales..... 57
 - El beneficio de la integración.....
58
 - La Capacidad de los organismos internacionales.....
58

3. EL ORGANISMO INTERNACIONAL PROPIAMENTE DICHO: ORGANIZACIÓN MUNDIAL DE REVISIÓN DE CONTRATOS VÍA INTERNET Y SALVAGUARDA DE LOS DERECHOS DE LOS USUARIOS.....	58
1. Objetivos.....	59
2. Miembros integrantes.....	59
3. Comisiones integrantes.....	60
4. Áreas de acción.....	60
5. Funciones.....	60
6. Políticas.....	60
7. Proyectos y Fondos.....	61
8. Relaciones internacionales.....	61
 4. LA NORMATIVIDAD SOBRE LA CUAL DEBERÁ REGIRSE EL ORGANISMO INTERNACIONAL, DE LAS DIRECTIVAS DE LA UNIÓN EUROPEA.....	 61
• Directiva 95/46/CE del Parlamento Europeo y del Consejo de la Unión Europea, del 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.....	63
• Directiva 97/66/CE del Parlamento Europeo y del Consejo de la Unión Europea, del 15 de diciembre de 1997 relativa al tratamiento	

de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.....

69

- Directiva 2002/58/CE, del Parlamento Europeo y del Consejo de la Unión Europea, del 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.....

71

CAPITULO V

BASES EN LAS QUE SE SUSTENTA EL ORGANISMO INTERNACIONAL PROPUESTO 73

1. GENERALIDADES.....
73
2. SUSTENTOS PARA LA CREACIÓN
DE UN ORGANISMO INTERNACIONAL.....
74
 - SUSTENTO LEGAL.....
74
 - SUSTENTO ECONÓMICO.....
76
 - SUSTENTO ADMINISTRATIVO.....
77
 - a. La Comisión General.....
77
 - b. El Directorio.....
77
 - Comisión de asesoría y orientación al usuario..... 78
 - Comisión revisora.....
78
 - Comisión de atención de reclamos y denuncias..... 78

○ Comisión de asuntos legales.....	78
○ Comisión de arbitraje.....	78
○ Comisión fiscalizadora.....	79
○ Comisión sancionadora.....	79
c. Programas y Fondos.....	79

CONCLUSIONES.....	80
RECOMENDACIONES.....	81
LISTA DE REFERENCIAS.....	82
ANEXOS.....	84

AGRADECIMIENTOS

Agradezco esta Tesis:

A mis Padres y Abuelos, por el cariño, la confianza, el apoyo y por saber tolerar el carácter y el mal genio heredado, gracias por todo y por lo que vendrá.

A Ofelia, en la distancia, a los 2 Carlos, Manuel y Daniel y al pequeño Jano, por no dejarme trabajar, pero están ahí siempre, diciéndome que me admiran indirectamente.

A Dios, gracias por los retos, las penas, las dichas y todo lo que nos ofrece en esta vida prestada.

A mi estimado asesor de Tesis, el doctor Guhtember Pacherras Pérez, por su paciencia y su tiempo.

Y a los Docentes, que encontré en la Universidad Privada del Norte por la disposición y confianza depositados en nosotros sus alumnos.

LISTA DE ABREVIACIONES

- PYME: Pequeña y Mediana Empresa.
- MARCs Métodos alternativos de Resolución de Conflictos.

GLOSARIO

- Métodos criptográficos: El método criptográfico, criptosistema o algoritmo de encriptación, define dos transformaciones:
 - La encriptación: conversión el texto en claro (plaintext) en el texto cifrado o criptograma (ciphertext) mediante el empleo de la denominada clave de encriptación; y
 - La desencriptación: proceso inverso al primero, donde se emplea la llamada clave de desencriptación.

PÁGINA DE RESUMEN

La presente investigación presenta los problemas de los contratos a través de Internet, debido a que algunas redes sociales vinculadas a contenidos de Internet, lo que en la presente investigación denominamos las cláusulas que amenazadoras al derecho de autodeterminación informativa.

Pero, ¿qué derechos pueden ser dañados en una red social? En general las personas que utilizan estas redes sociales son personas naturales que comparten su información personal, esta información que se comparte en Internet, está protegida por un derecho que nuestro tribunal constitucional conoce como derecho a la autodeterminación informativa.

Estos nuevos tipos derechos son los que nacieron de los usos de Internet, y el desarrollo de la nueva tecnología, y sería más difícil para protegerlos debido a la fácil accesibilidad y el uso adecuado de Internet.

Si estos derechos son difíciles de proteger, por el simple uso de Internet, lo que va a suceder cuando las cláusulas que pretenden vulnerar los derechos a los que las redes sociales tienen acceso (a través de sus contratos on line), dichas cláusulas pretenden dañar nuestro ya mencionado derecho a la autodeterminación informativa.

Para evitar esta circunstancia, el presente trabajo se ha propuesto la creación de un organismo internacional que regularice esta situación y resuelva los posibles conflictos a través de los denominados MARCs (métodos alternativos de resolución de conflictos)

ABSTRACT

The present investigation presents the problems of contracts through internet, because of some social networks linked to internet contents what we call clauses that pretend to damage rights.

But, which rights would pretend to cause damage in a social network? In general people who use these social networks are natural people who share their personal information, this information that is shared on the Internet, is protected with a right that our constitutional tribunal know as informative at determinative right.

These rights are the new kinds which were born from the uses of the Internet, and the development of technology, and it would be more difficult to protect them because of the accessibility and the proper use of Internet.

If these rights are difficult to protect by the simple use of Internet, what is going to happen when the clauses that pretend to damage rights that the social networks use (through their On Line contracts), those clauses pretend to damage informative at determinative rights.

For avoiding this circumstance, the present work had proposed the creation of an international organism which would regularize the situations the electronic contracts might present, and resolve the conflicts through what are called MARCs (term used in Spanish for alternative methods for solving conflicts)

INTRODUCCION

La presente investigación tiene como antecedentes a la sociedad de la información que nació por el vertiginoso crecimiento de la información y la nueva tecnología, de ella nacieron las formas de contratación a través de internet, de las cuales derivaron la directivas de la unión europea para el tratamiento de los datos personales, conocidos en esta tesis como derecho de autodeterminación informativa.

Las fuentes utilizadas para la recolección de la información, son libros electrónicos en su mayoría, así como también nos agenciamos de libros físicos, revistas y por supuesto, páginas web.

De otro lado, para el desarrollo del presente trabajo, se encontraron algunas dificultades, como la variedad de información encontrada, la misma que, tuvo que ser sometida a juicios de contrastación para poder desarrollarla de manera uniforme, de otro lado nos encontramos con textos en inglés, los mismos que tuvieron la necesidad de ser traducidos para su inclusión, por último nos encontramos con que, la doctrina utilizada en su mayoría es foránea, por lo que debió utilizarse dolo aquella información que fuere susceptible de aplicarse.

¿Pero qué derechos pueden estar en amenaza en una red social? Para efectos de la presente investigación el derecho que puede ser vulnerado es el de autodeterminación informativa, puesto que con la inclusión de las cláusulas amenazadoras en en los contratos on line de las redes sociales, en cualquier momento, el usuario puede perder el control sobre la información vertida en las redes, sobre la cual solo él debiera tener control, para ser utilizada por los dueños de la red social de la manera en que a estos les convenga.

CAPÍTULO I

DE LOS ASPECTOS METODOLÓGICOS

23. ÁREA: Derechos Humanos y Derecho de Contratos Vía Internet.

24. PLANTEAMIENTO Y DESCRIPCIÓN DE LA SITUACIÓN PROBLEMÁTICA:

En la actualidad, el vertiginoso avance de la tecnología, la inserción de la computadora como herramienta de trabajo de uso diario, los teléfonos celulares, el internet, entre otros, ha logrado que el hombre cambie su perspectiva de la vida y el desarrollo en todos sus sentidos. ¿Quién imaginaría hace apenas una décadas la revolución tecnológica que acontece en la actualidad? Nos atrevemos a especular que nadie que creció en la décadas anteriores a los 70's adivinaría que para el siglo XXI uno tendría que depender de la tecnología para el desarrollo de sus actividades cotidianas. Desde los hornos microondas, hasta las computadoras y los celulares, cada día aparecen nuevos equipos que desfasan a los anteriores y nos crean nuevas relaciones de dependencia.

La ciencia jurídica no escapa a esta nueva realidad, los abogados dependemos de los nuevos fenómenos que está creando la revolución tecnológica respecto de muchos aspectos, si nos refiriésemos a uno específico, escogeríamos hablar respecto de la contratación, el tradicionalismo de contratar en persona, negociar, llegar a un acuerdo en común y firmar un contrato ha variado. El mundo moderno nos está exigiendo la creación de nuevas modalidades de contratación debido al fenómeno de la globalización y el uso del internet, si nos referimos al último en particular, la nueva contratación se denomina contratación vía internet, (Menéndez Mato 2008, 168), mediante los cuales ya no es necesaria la presencia física de las partes contratantes en un lugar determinado, ahora sólo basta la intermediación de un computador, o algún otro medio electrónico, hacer click en un determinado enlace electrónico y listo; puedes adquirir productos, contratar servicios, e incluso formar parte de redes sociales.

Esta fenomenología ha permitido al internet tener el poder, a futuro, de adueñarse de la contratación, hasta este punto no existiría una posible discrepancia de facilitar las

medidas de contratación y dejar fluir el comercio, pero el detalle de la despersonalización contractual, es que, si existe una falta de control o regulación respecto de la misma, podrían surgir problemas respecto de la parte más débil de la relación contractual, en este caso los destinatarios aceptantes (en una relación entre el creador o administrador de una página web y la otra persona quien sea que usa la página, contratante o no, a la segunda se le denominará destinatario).

La contratación vía internet se divide en varias categorías: contrato informático, contrato electrónico, contrato telemático, contrato on line y contrato digital (del Peso Navarro 2004, 7), los cuales pueden ser unilaterales o bilaterales, en el estricto sentido de las prestaciones. Esta nueva forma de contratación está desarrollándose con una tendencia en masa, la cual además, permitió la formación de la denominada sociedad de la información, esta idea engloba un conjunto de actividades industriales y económicas, comportamientos sociales, actividades individuales, y formas de organización política y administrativa, de importancia creciente en las naciones situadas en la vanguardia económica y cultural, a la que no pueden sustraerse los poderes públicos (Real Decreto 1289/1999 de 23 de julio. Creación de la comisión interministerial de la sociedad de la información y de las nuevas tecnologías. Exposición de Motivos).

Ahora bien, dentro de la contratación vía internet nació, como se dijo en el párrafo que antecede, el contrato on line, el cual es específicamente el que atrae a nuestra investigación, y sería aquel perfeccionado desde una página web y practicable en masa gracias a los programas informáticos de contratación (Menéndez Mato 2008, 169).

De la definición planteada acerca de los contratos on line se agrega que, todos son de adhesión, puesto que no existe negociación alguna entre las partes contratantes, pues son las páginas web quienes pre redactan unilateralmente dichos contratos y el destinatario puede aceptar o rechazar totalmente (Peralta Andía y Peralta Zecharro 2005, 147) aquello en él contenido.

Se ha brindado los conceptos precedentes con la finalidad de acercarnos a los contenidos de la situación problemática, entonces, se plantea lo siguiente: existen

determinadas cláusulas contenidas en los contratos on line que, en potencia, podrían afectar el derecho de autodeterminación informativa.

Pero, ¿qué es el derecho a la autodeterminación informativa? En el transcurso de la presente investigación nos preguntamos qué clase de derecho es aquel que la persona tiene sobre información personal que está contenida en medios electrónicos, que a pesar de ser compartida a través del internet sigue siendo propia; fue así que encontramos una resolución del Tribunal Constitucional, que define este derecho como, el que tiene por objeto proteger la intimidad, personal o familiar, la imagen y la identidad frente al peligro que representa el uso y la eventual manipulación de los datos a través de los ordenadores electrónicos (Caso Wilo Rodríguez Gutiérrez, Resolución N. ° 01797-2002-HD/TC, 29/09/2003), de los destinatarios de los servicios de las páginas web de contenido social, las cuales son páginas que ofrecen cuentas de usuario a los destinatarios de su servicios a cambio de nada, es decir, no existe contraprestación, en un sentido general se podría decir que el beneficio que obtienen estas páginas respecto de sus destinatarios es que los patrocinadores de las páginas web pueden bombardear a sus destinatarios de publicidad.

La situación anteriormente expuesta no justifica la inclusión de cláusulas amenazadoras (que reportan una ventaja indiscriminada a favor de uno de los contratantes en posible menoscabo del otro (De la Puente y La Valle 2003, 784)) de derechos de autodeterminación informativa en contra de sus destinatarios. Entonces surgió la incógnita de si existía alguna clase de protección en contra de las cláusulas amenazadoras, a favor de los destinatarios. La respuesta es no, por lo que se necesita una solución.

Por otro lado, para poder llegar a entender el problema planteado, debemos establecer las diferencias más importantes que, para los investigadores, podríamos encontrar entre el contrato de adhesión civil y el on line (que como ya se afirmó siempre es de adhesión), éstas son dos: Primero, el contrato de adhesión civil es eminentemente mercantil, lo cual está ligado con el hecho de que existen prestaciones recíprocas por lo que se puede afirmar que se encuentra en la clasificación de bilateral, mientras que el segundo- para la delimitación de este proyecto al trabajar con los contratos para creación de cuentas en las página web de

contenido social- no lo es. Segundo, los contratos de adhesión (en sus modalidades bancarias y financieras) son revisados por la Superintendencia Nacional de Banca y Seguros (para evitar la adhesión de cláusulas lesivas y amenazadoras), mientras que al contrato on line en el Perú aún no lo revisa ninguna entidad.

Del párrafo, que antecede, podemos asegurar que existe un problema respecto de las redes sociales, que dentro de sus contratos on line (para acceder a una cuenta de usuario por parte de los destinatarios en dichas páginas web) contienen cláusulas amenazadoras en contra de derechos de autodeterminación informativa de sus aceptantes.

25. FORMULACIÓN Y SISTEMATIZACIÓN:

¿Qué solución legal debe adoptarse frente a las cláusulas amenazadoras contra derechos de autodeterminación informativa contenida en los contratos on line en las páginas web Hi5, Badoo, Reddit y Digg?

- ¿Qué son cláusulas amenazadoras?
- ¿Qué es el derecho de autodeterminación informativa?
- ¿Qué son los contratos on line?

26. FUNDAMENTACIÓN

En un mundo globalizado como el nuestro será pionero quien investigue sobre las nuevas modalidades de contratación en masa, y de su nueva categoría enunciada en el planteamiento: los contratos vía internet, y para nuestro caso en específico el contrato on line.

Este contrato es utilizado por las redes sociales dentro de la sociedad de la información, que abre la brecha de un supuesto no legislado, y por ende no vigilado, expresamente en nuestro ordenamiento jurídico.

Deducido del planteamiento, aquí se enuncia, donde se encuentran las cláusulas amenazadoras y explicamos él porque de su consideración como tales; en las redes sociales Hi5, Badoo, Reddit y Digg.

CLÁUSULAS AMENAZADORAS

- Hi5 (CONTENIDO EN SU POLÍTICA DE PRIVACIDAD-
http://www.hi5.com/terms_of_service.html?#privacy_policy)
- Badoo (CONTENIDO EN SU POLÍTICA DE PRIVACIDAD-
<http://badoo.com/privacy/>)
- REDDIT (CONTENIDO EN SU POLITICA DE PRIVACIDAD-
<http://www.reddit.com/help/privacypolicy>)
- DIGG (CONTENIDO EN LA POLITICA DE PRIVACIDAD DE DIGG
<http://about.digg.com/privacy>)

De una lectura textual de estas cláusulas podemos concluir que, a pesar que las mismas políticas de uso o privacidad de las páginas anteriormente mencionadas, dicen que sus usuarios no poseen derechos sobre los contenidos (datos) o fotografías adheridas a su red; también incluyen estas otras cláusulas que autorizan a los dueños de las páginas desde volver anónima la información en ellas contenidas y hacer uso de ella a su discreción (en el caso de Hi5) pasando seleccionar información de las zonas de libre acceso o simplemente transmitida a la página, para uso comercial o promocional de los socios de las mismas (en el caso de Badoo), recalando que el usuario conoce los términos y los acepta; hasta la situación de tomar la información otorgada por el usuario como activo de la página web y que, si esta es vendida, la información pasará a ser vendida al adquirente de la página (en los casos de Reddit y Digg).

Podemos afirmar entonces que estas cláusulas contenidas en las políticas de privacidad de las páginas web, se configuran como amenazadoras por el hecho de atentar contra el derecho de autodeterminación informativa, por el solo hecho de encontrarse inmersas en estos contratos on line.

27. DELIMITACIÓN:

- TEMÁTICA: Contrato on line de prestaciones unilaterales en las páginas web de contenido social respecto de las redes.
- TEMPORAL: De Agosto de 2009 a Enero de 2012.

- **ESPACIAL:** La sociedad de la información en su extremo específico de servicios.
- **POBLACIONAL O DEMOGRÁFICA OBJETIVA:** Contratos on line de las páginas web: Hi5, Badoo, Reddit y Digg.

28. LIMITACIONES:

La falta de Investigación precedente sobre el tema específico (cláusulas amenazadoras en contratos on line).

La literatura que tiene mayor alcance para la investigación o es más completa es de autores extranjeros.

29. OBJETIVOS:

- **GENERAL:** Proponer la solución legal frente a las cláusulas amenazadoras del derecho a la autodeterminación informativa contenidas en los contratos on line en las redes sociales: Hi5, Badoo Reddit y Digg.
- **ESPECÍFICOS:**
 - Determinar que es la sociedad de la información en general, y que aspecto juega en ella las páginas web de contenido social o redes sociales.
 - Determinar que son los contratos vía internet, en especial el contrato on line y su utilización en las páginas web de contenido social o redes sociales.
 - Determinar que son las cláusulas amenazadoras de derechos, y su posible menoscabo frente a los destinatarios de las redes sociales Hi5, Badoo, Reddit y Digg.
 - Determinar que es el derecho a la autodeterminación informativa y porque debe ser protegido.

30. ANTECEDENTES DEL PROBLEMA:

- Historia de la computación y documentos informáticos, es un libro que nos ilustra sobre la explosión informática nació en los años 90s, pero se

consolidó según la historia en 1995, año en el que las empresas se instalan en la red de redes y empiezan a ofrecer sus servicios en el ciberespacio.

- Los servicios de la sociedad de la información es un libro del profesor Emilio del Peso Navarro, versa acerca del concepto de la sociedad de la información, su evolución, el tratamiento de sus servicios en Europa y sus incidencias en las personas jurídicas y naturales.
- El contrato vía internet es doctrina del Profesor Juan Carlos Menéndez Mato, que realiza un estudio y análisis profundo del contrato vía internet, su clasificación y su tratamiento en Europa.

31. FUNDAMENTO TEÓRICO:

El Profesor Johan Muñoz M. en su libro Historia de la computación y documentos informáticos, señala que en 1995 se produce la aparición de la internet comercial, las empresas se instalan en la red y ofrecen todo tipo de servicios on line, tiendas, banco, todo el mundo se instala en el ciberespacio.(Muñoz Johan 2009, 13).

Veamos ahora, se ha venido hablando de muchos términos que en lenguaje común podrían decirnos algo, una noción que cualquier persona partidaria del internet podría identificar, pero la configuración de este trabajo es jurídica por lo que analizaremos cada figura y cada variable de modo individual para poder entender el objetivo del presente trabajo, así también explicaremos la hipótesis en juego para determinar una concreción de solución legal frente al problema planteado.

Lo más conveniente es iniciar por los términos más técnicos, de esos que no surge la deducción tan fácilmente, así que iniciaremos dando el concepto de sociedad de la información, que es fundamental para entender la contratación a través de internet.

La sociedad de la información representa una etapa evolutiva más dentro de la historia económica global de la sociedad. Tras las etapas correspondientes a la sociedad industrial y posindustrial se da paso a la sociedad de la información, los rasgos caracterizadores de este nuevo estadio se asientan en 2 conceptos: información y nueva tecnología. La nueva tecnología- distinta de la industrial- se fundamenta en los avances y las convergencias operados en los sectores de las telecomunicaciones y la informática. De este modo, también se denomina a esta nueva etapa era digital. Por su parte la información se distingue de la existente

previamente debido al importe de valor económico y social que ha adquirido. Los elementos constitutivos de la sociedad de la información son: Las redes, los servicios básicos y las aplicaciones, éstas últimas relacionadas al comercio electrónico (Menéndez Mato 2008, 168). Para los fines de este trabajo sólo tomaremos en cuenta a las redes (donde están incluidas las páginas web) puesto que sobre ellas se puede contratar con o sin fin lucrativo.

Ahora que se clarificaron los términos sociedad de la información y, como se evidencia, es relevante para la presente investigación, nos gustaría pasar al concepto de contratos vía internet (contenidos dentro de la vertiginosa y cambiante sociedad de la información), que son el género de los denominados contratos on line.

Como ya mencionamos con anterioridad, debemos decir que, los contratos vía internet se clasifican en los siguientes: contrato informático, contrato electrónico, contrato telemático, contrato on line y contrato digital; el primero contiene a los siguientes, el segundo contiene al tercero, cuarto y quinto, el tercero al cuarto y al quinto y, por último, el cuarto contiene al quinto; son un tipo de género y especie sucesivo e inclusivo.

Lo más lógico sería ahora incluir los conceptos de cada contrato, que son los siguientes: El contrato informático es el que tiene como objeto un bien o servicio informático. En cambio el contrato electrónico es el concluido mediante el empleo de medios electrónicos, como por ejemplo la comunicación mediante ordenadores en una red. Ya sea abierta o cerrada- o el empleo del télex o fax. Un contrato informático puede ser también electrónico cuando es concluido por dichos medios electrónicos (del Peso Navarro 2004, 158).

Los contratos electrónicos pueden perfeccionarse mediante partes físicamente presentes o a distancia. Cuando los contratos electrónicos se perfeccionan a distancia mediante técnicas de procesamiento de datos y su envío, sin necesidad del empleo del papel para la comprensión del contenido del mensaje, reciben el nombre de contratos telemáticos (del Peso Navarro 2004, 158).

Finalmente, un contrato será digital, cuando para su conclusión se haya empleado la firma digital. Un contrato digital será siempre un contrato electrónico, pero no viceversa; además no tiene por qué ser un contrato a distancia, ni telemático, aunque siempre será un contrato on line, ya que este adjetivo no hace por sí referencia de la presencia o ausencia de las partes, sino a la realización a través de una red de ordenadores, lo cual es indispensable para firmar electrónicamente un documento (del Peso Navarro 2004, 158-165).

Con estos conceptos de contratación clarificados podemos dar el concepto extenso de contrato on line; en un primer momento, el contrato en línea u on line se reconoció como un acuerdo negocial, el cual para su conclusión, todas las partes, o una de ellas, utilizan modalidades ligadas a los protocolos técnicos de transmisión telemática de datos (tales son aquellos utilizados por internet) (Apud. Menendez Mato 2005, 168-169). Por otro lado, pueden señalarse dos acepciones distintas respecto de este contrato. La primera, más genérica, entendería por contrato on line a todo aquel cuya perfección ha tenido lugar en línea o red. De esta forma lo serían todos los concluidos a través de internet o desde una intranet. Para la segunda acepción más restrictiva, un contrato on line sería aquel perfeccionado desde una página web y practicable en masa gracias a los programas informáticos de contratación, podría de este modo decirse que un contrato concluido entre dos sujetos directamente mediante intercambio de sus respectivas oferta y aceptación mediante el uso de correo electrónico o videoconferencia o chat no son contratos on line (Menéndez Mato 2008, 168). Además, como ya se dedujo, es importante recalcar que consideramos a los contratos on line en los casos de las páginas web Hi5, Badoo y Six Apart. Como contratos de adhesión pues no existe negociación alguna entre las partes, son las páginas web quienes los pre redactan unilateralmente y el usuario o destinatario puede aceptar o rechazar totalmente (Peralta Andía y Peralta Zecharro 2005, 147-149) las condiciones en ellos estipulados.

Todo lo antes expuesto está relacionado con los contratos on line, como lo podemos deducir de la formulación del problema. Ahora podríamos agregar de nuestra propia cosecha, que los contratos on line en las páginas web de contenido social, son de prestaciones unilaterales, puesto que, una sola parte de la relación contractual ofrece un bien o servicio a favor de la otra, en este caso el ejemplo sería las páginas web de

contenido social que ofrecen una cuenta de usuario al aceptante, en donde el aceptante sólo tiene que decidir si acceder a una cuenta o no. Frente a este aspecto nos encontramos con una posición doctrinaria, la cual afirma que los contratos on line no son contratos, frente a ella nos planteamos la siguiente interrogación: ¿un contrato on line, por ser de prestaciones unilaterales, deja de ser un contrato? La respuesta es no, por el sólo hecho de ser de prestaciones unilaterales el contrato on line no pierde su naturaleza contractual, sino ¿qué pasaría en los casos civiles como la donación?.

De otro lado, nuestro siguiente tema es la solución legal frente al problema planteado, sobre lo cual podemos decir lo siguiente: La solución legal que planteamos, contenida en la hipótesis, es que tendría que constituirse un organismo internacional que se encargue de las posibles circunstancias que se presentarían por culpa de las cláusulas amenazadoras. Ahora bien, ¿Por qué la necesidad de un organismo internacional? Porque no se puede solucionar los problemas a través de tratados, o tal vez a través de legislación nacional. La respuesta, para nosotros, radica en dos bases fundamentales, si bien es cierto que ningún organismo internacional goza aún de universalidad, es decir, en el sentido del derecho internacional público, no existe aún ningún organismo internacional al que se le hayan afiliado todos los países del mundo; pero a pesar de ello existen organismos que tienen afiliados un gran número de países.

Esta capacidad de los organismos internacionales permite que se afilie a él, cualquier país, tenga el ordenamiento que tenga, las bases filosóficas o influencia de cualquier otra índole; lo que beneficia a quien sea que se afilie a él. Este sería entonces el primer punto a favor, mediante un organismo internacional se podría beneficiar a cualquier país que se afilie. Por otro lado en el caso específico de nuestro país, aquellos fallos que pronuncie un organismo internacional contará con supremacía, pues estará sujeto al derecho internacional público.

Respecto de cláusulas amenazadoras debemos clarificar que el término doctrinariamente hablando aún no existe, es un término que nació de la disertación en clase de proyecto de tesis acerca de la tesis que hoy se expone en particular; pero podemos afirmar que la noción que se expone nació de la idea de las cláusulas

lesivas. Entonces se puede afirmar que desarrollamos el término cláusulas amenazadoras en forma de asunción.

Por último, respecto al derecho a la autodeterminación informativa, como ya se dijo, tiene por objeto proteger la intimidad, personal o familiar, la imagen y la identidad frente al peligro que representa el uso y la eventual manipulación de los datos a través de los ordenadores electrónicos.

Por otro lado, aunque su objeto sea la protección de la intimidad, el derecho a la autodeterminación informativa no puede identificarse con el derecho a la intimidad, personal o familiar, reconocido por el inciso 7) del artículo 2° de la Constitución. Ello se debe a que mientras que el segundo protege el derecho a la vida privada, esto es, el poder jurídico de rechazar intromisiones ilegítimas en la vida íntima o familiar de las personas, el primero garantiza la facultad de todo individuo de poder preservarla controlando el registro, uso y revelación de los datos que les conciernen (Caso Wilo Rodríguez Gutiérrez, Resolución N. ° 01797-2002-HD/TC, 29/09/2003).

Tampoco el derecho a la autodeterminación informativa debe confundirse con el derecho a la imagen, reconocido en el inciso 7) del artículo 2° de la Constitución, que protege, básicamente la imagen del ser humano, derivada de la dignidad de la que se encuentra investido; mientras que el derecho a la autodeterminación informativa, en este extremo, garantiza que el individuo sea capaz de disponer y controlar el tipo de datos que sobre él se hayan registrado, a efectos de preservar su imagen derivada de su inserción en la vida en sociedad (Caso Wilo Rodríguez Gutiérrez, Resolución N. ° 01797-2002-HD/TC, 29/09/2003).

Finalmente, también se diferencia del derecho a la identidad personal, esto es, del derecho a que la proyección social de la propia personalidad no sufra interferencias o distorsiones a causa de la atribución de ideas, opiniones, o comportamientos diferentes de aquellos que el individuo manifiesta en su vida en sociedad (Caso Wilo Rodríguez Gutiérrez, Resolución N. ° 01797-2002-HD/TC, 29/09/2003).

32. ASUNCIONES:

- Cláusulas amenazadoras.- cláusulas que reportan una ventaja indiscriminada a favor de uno de los contratantes en posible menoscabo del otro.

33. TÉRMINOS FUNDAMENTALES:

- Sociedad de la información: Sociedad de la información engloba un conjunto de actividades industriales y económicas, comportamientos sociales, actividades individuales, y formas de organización política y administrativa, de importancia creciente en las naciones situadas en la vanguardia económica y cultural, a la que no pueden sustraerse los poderes públicos” (Real Decreto 1289/1999 de 23 de julio. Creación de la comisión Interministerial de la Sociedad de la Información y de las Nuevas Tecnologías. Exposición de Motivos)

- Contratos vía de internet:
 - Un contrato on line sería aquel perfeccionado desde una página web y practicable en masa gracias a los programas informáticos de contratación
(Menéndez Mato 2008, 158-165).

- Páginas web de contenido social o redes sociales: Aquellos sitios web creados específicamente para contener redes de información (pueden contener diarios, fotos digitales, escritos, videos digitales, links, entre otros), en las cuales cualquier destinatario puede convertirse en usuario al aceptar el contrato on line que es prerequisite fundamental para la creación de una cuenta en dichas páginas.

- Cláusulas amenazadoras.- cláusulas que reportan una ventaja indiscriminada a favor de uno de los contratantes en posible menoscabo del otro.

- Derecho de autodeterminación informativa.- Tiene por objeto proteger la intimidad, personal o familiar, la imagen y la identidad frente al peligro que representa el uso y la eventual manipulación de los datos a través de los ordenadores electrónicos. Garantiza la facultad de todo individuo de poder preservar la intimidad controlando el registro, uso y revelación de los datos que les conciernen. Garantiza que el individuo sea capaz de disponer y controlar el tipo de datos que sobre él se hayan registrado, a efectos de

preservar su imagen derivada de su inserción en la vida en sociedad. Se diferencia del derecho a la identidad personal, esto es, del derecho a que la proyección social de la propia personalidad no sufra interferencias o distorsiones a causa de la atribución de ideas, opiniones, o comportamientos diferentes de aquellos que el individuo manifiesta en su vida en sociedad (Caso Wilo Rodríguez Gutiérrez, Resolución N. ° 01797-2002-HD/TC, 29/09/2003).

34. HIPÓTESIS:

La solución legal ante las cláusulas amenazadoras al derecho de autodeterminación informativa contenida en contratos on line sería:

La creación de un ente internacional encargado de:

- Prohibir la inclusión de cláusulas amenazadoras o lesivas de derechos (para incluir un ámbito más amplio que el del presente campo de investigación).
- Revisar los contratos on line de acceso abierto, para acceder a estas redes sociales.
- Establecer fórmulas de solución de conflictos.
- Establecer sanciones cuando no se cumplan alguno de los 3 supuestos anteriores.

35. OPERACIONALIZACIÓN DE VARIABLES:

Denominación	Definición Conceptual
<p data-bbox="236 331 552 528">La solución legal sería: La creación de un ente internacional encargado de:</p> <ul data-bbox="288 555 552 1742" style="list-style-type: none"><li data-bbox="288 555 552 860">• Prohibir la inclusión de cláusulas amenazadoras o lesivas de derechos.<li data-bbox="288 887 552 1137">• Revisar los contratos a través de internet de acceso abierto.<li data-bbox="288 1164 552 1361">• Establecer fórmulas de solución de conflictos.<li data-bbox="288 1388 552 1742">• Establecer sanciones cuando no se cumplan alguno de los 3 supuestos anteriores.	<p data-bbox="576 331 1453 582">Ente internacional.- Organismo supra nacional que se encargue de velar por la seguridad jurídica de los miembros de la sociedad de la información que celebren contratos a través de Internet (para este trabajo contratos on line específicamente), el velar incluiría específicamente:</p> <ul data-bbox="628 609 1511 1639" style="list-style-type: none"><li data-bbox="628 609 1511 806">• Prohibición.- La inclusión expresa de una prohibición de cláusulas amenazadoras, implicaría una norma imperativa, frente a la cual en teoría, los miembros de la sociedad de la información no podrían incumplir.<li data-bbox="628 833 1511 1084">• Revisión.- Sería el modo de prevenir la inclusión de cláusulas amenazadoras (pues las prohibiciones no siempre serían respetadas) u otras que pudieran atentar contra los derechos de los usuarios de los servicios que ofrece la contratación vía internet.<li data-bbox="628 1111 1078 1146">• Acceso abierto.- público, libre.<li data-bbox="628 1173 1511 1424">• Solución de conflictos.- En los casos en que sea imposible determinar de primera mano si una cláusula es amenazadora o no, sería este ente el que solucionaría la controversia, y de ese mismo modo, todos los posibles conflictos que se presentarían en la contratación a través de Internet.<li data-bbox="628 1451 1511 1639">• El ente podría establecer sanciones ante el reiterado incumplimiento de algún supuesto como por ejemplo que tras revisar los contratos a través de internet encuentren reiteradamente una cláusula amenazadora.

36. CUADRO DE DETERMINACIÓN DEL PROBLEMA:

<p>El Problema:</p> <p>¿Qué solución legal debe adoptarse frente a las cláusulas amenazadoras contra derechos de autodeterminación informativa contenida en los contratos on line en las páginas web Hi5, Badoo, Reddit y Digg?</p>
<p>La Hipótesis:</p> <p>La solución legal frente a la existencia de cláusulas amenazadoras al derecho de autodeterminación informativa en los contratos on line para el acceso a cuentas en las redes sociales Hi5, Badoo, Reddit y Digg, es la creación de un organismo internacional que se encargue de prohibir la inclusión de cláusulas amenazadoras, revisar los contratos on line de acceso abierto, para acceder a estas redes sociales, establecer fórmulas de solución de conflictos y establecer sanciones cuando no se cumplan alguno de los 3 supuestos anteriores.</p>

37. TIPOLOGÍA: eminentemente DOGMÁTICA pues la investigación es teórica, basada en libros (DOCTRINA) y la solución es PROPOSITIVA respecto de una solución legal.

38. ENFOQUE: CUALITATIVO: la realidad sujeta a examen crítico.

39. ALCANCE: DESCRIPTIVO Y PROPOSITIVO: Descriptivo porque señala como es el tratamiento actual de las cláusulas amenazadoras de derecho a la autodeterminación informativa en contratos on line; y propositivo por el hecho de proponer una solución legal frente a la existencia de las mismas cláusulas amenazadoras.

40. DISEÑO: No experimental- las ciencias jurídicas no permiten experimentar, sólo se ven resultados reales, o de aplicación.

41. MÉTODOS:

MÉTODO DOGMÁTICO COMPARATIVO.-

Dogmático propiamente dicho, análisis de la doctrina europea respecto de la sociedad de la información y en comparación con doctrinas europeas e internacional acerca de la contratación vía internet.

42. TÉCNICAS E INSTRUMENTOS:

RECOPILACIÓN Y ANÁLISIS DOCUMENTAL.- se han utilizado libros en soporte electrónico y la bibliografía de contratación en general y vía internet.

43. MUESTREO:

Revisión, análisis y estructuración de las cláusulas amenazadoras en concordancia con la doctrina europea acerca de la sociedad de la información y la contratación vía internet.

44. REVISIÓN DE LITERATURA PRECEDENTE:

De la revisión hemos encontrado lo siguiente que es relevante para nuestra investigación:

La investigación se encuentra inmersa en la denominada sociedad de la información, dado que las páginas web de contenido social se encuentran inmersas en los servicios de dicha sociedad (Los servicios de la sociedad de la información, Emilio del Peso Navarro).

Además los servicios de las páginas web de contenido social se perfeccionan a través de contratos on line (Contratos vía internet, Juan Carlos Menéndez Mato)

CAPÍTULO II
DE LA SOCIEDAD DE LA INFORMACIÓN Y
LA PÁGINA WEB DE CONTENIDO SOCIAL O REDES SOCIALES

SUB CAPÍTULO I

LA SOCIEDAD DE LA INFORMACIÓN

3. GENERALIDADES.-

No podríamos hablar de contratación a través de internet, o de sus implicancias sin antes saber que es el internet y que nuevas incidencias ha tenido en nuestro entorno, sus nuevos alcances y la figura que ha creado, aquella que traspasa fronteras; la nueva sociedad de la información.

El internet, ha sido denominada como la “red de redes”; es decir, una red que no sólo interconecta computadoras, sino que interconecta redes de computadoras entre sí. Una red de computadoras es un conjunto de máquinas que se comunican a través de algún medio con el objeto de compartir recursos (http://www.cad.com.mx/que_es_internet.htm).

Dentro del objeto de compartir recursos han surgido diferentes facetas donde los que navegan en el internet han desarrollado una serie de actos, la gente comparte información, intercambia ideas, comercializa productos, entre otros; para el desarrollo de estos actos se desarrolló lo que denominamos la sociedad de la información.

El profesor Juan Carlos Menéndez Mato, nos señala que, el término sociedad de la información aparece en Japón durante la crisis de inicios de los años 70. Afirma también que por su parte el proyecto europeo nace de iniciativa estadounidense, con interesantes perspectivas positivas para alcanzar a través de ella una mayor cohesión e integración entre los distintos Estados miembros – objetivos fundamentales de esta organización- además de permitirle un acceso directo con todos sus agentes sociales – incluso con los ciudadanos- y de éstos con las instituciones (Menéndez Mato 2008, 103).

Tras esa breve introducción acerca de cómo es que aparece el término la pregunta objetiva vendría a ser ¿qué es la sociedad de la información propiamente dicha?

4. CONCEPTO DE LA SOCIEDAD DE LA INFORMACIÓN.-

Según la exposición de motivos española de creación de la comisión interministerial de la sociedad de la Información y de las nuevas tecnologías del Real Decreto 1289/1999 de 23 de julio, la idea de sociedad de la información engloba un conjunto de actividades industriales y económicas, comportamientos sociales, actividades individuales, y formas de organización política y administrativa, de importancia creciente en las naciones situadas en la vanguardia económica y cultural, a la que no pueden sustraerse los poderes públicos.

Para la presente investigación de todas las actividades que engloba la sociedad de la información, nos interesan los comportamientos sociales que en ella se desarrollan; ya que, como veremos en el sub capítulo siguiente, el tema de estudio son las páginas web de contenido social o redes sociales.

Ahora bien, la doctrina española concuerda en que los dos conceptos fundamentales de la sociedad de la información son la información y la nueva tecnología, (las que obviamente inciden en todas las actividades que conforman la sociedad de la información) y que se encuentran desarrolladas a continuación: Primero, la información es un conjunto de datos acerca de algún suceso, hecho, fenómeno o situación, que organizados en un contexto determinado tienen su significado, cuyo propósito puede ser el de reducir la incertidumbre o incrementar el conocimiento acerca de algo (www.promonegocioS.net). De otro lado, la nueva tecnología- distinta de la industrial- se fundamenta en los avances y las convergencias operados en los sectores de las telecomunicaciones y la informática. De este modo, también se denomina a esta nueva etapa “era digital”. Por su parte la información se distingue de la existente previamente debido al importe de valor económico y social que ha adquirido (Menéndez Mato 2008, 105).

4.1. CONTRASTE ENTRE SOCIEDAD DE LA INFORMACIÓN Y SOCIEDAD DEL CONOCIMIENTO:

4.1.1. La Sociedad del Conocimiento.-

En el transcurso de la historia, un sin fin de innovaciones e inventos han transformado y alterado los hábitos y las prácticas de las comunidades más simples a las sociedades más complejas, las llamadas civilizadas y evolucionadas (Rodríguez de Almeida y Davara Rodríguez 2006, 372).

Si el progreso debe valorarse en un acto continuo, en movimiento diacrónico lato, desde los albores de las sociedades organizadas, también es cierto que “la gran ruptura” tuvo lugar en plena revolución científica del siglo xvi, en la que “el camino hacia” permitió estructurar capacidades cognitivas y automatismos hoy universalizados (Rodríguez de Almeida y Davara Rodríguez 2006, 373).

De esta revolución científica y consiguiente revolución industrial a la aparición del ordenador, encontramos un pequeño gran paso que trajo mutaciones profundas, a escala planetaria, independientemente de las capacidades, e incluso, de las voluntades, de cualquier grupo o nación (Rodríguez de Almeida y Davara Rodríguez 2006, 373).

“La sociedad de la información” o cibersociedad se sustenta en el hecho de que la información es un recurso o un bien económico fundamental y base del desarrollo social actual (Rodríguez de Almeida y Davara Rodríguez 2006, 373).

La información es un bien que no agota con su consume, es más, puede que se enriquezca en un desarrollo ideal y utópico hasta valores incalculables, naciendo otra nueva y rica información que cada vez va produciendo más información. El centro de atención de las autopistas de la información es la propia información, quedando la llamada autopista y el ordenador en sí como el medio a través del cual se comunica o localiza dicha información” (Apud. Rodríguez de Almeida y Davara Rodríguez 2006, 373).

Aquello que hoy denominamos Informática, surge de forma creciente, no como un ramo del saber en un compartimento estanco, sino como una herramienta social que confiere visibilidad creciente al concepto “tecnoantropo”, llevando a la vida cotidiana convicciones apriorísticas de “e” - algo (e-learning, e-commerce), en un caminar imparable de la “aldea global” a la sociedad del conocimiento (Rodríguez de Almeida y Davara Rodríguez 2006, 374).

Las tecnologías de la información y la comunicación son un marco insustituible de la actual sociedad humana. La sociedad del conocimiento designa otro paradigma social en el que la alianza entre el conocimiento y la información ocupa el trono destinado a los monarcas que orientan el destino del hombre (Rodríguez de Almeida y Davara Rodríguez 2006, 374).

El conocimiento que da nombre a esta sociedad, se multiplica, rápidamente, mostrando una gravidez permanente donde nacen frutos que, rápidamente, superan los anteriores modelos a tal velocidad, que cada vez hay más científicos e investigadores en una perpetua y cotidiana búsqueda de metodologías, análisis, experimentaciones u observaciones con la certeza de que su tarea es infinita (Rodríguez de Almeida y Davara Rodríguez 2006, 381).

Ya no pretendemos únicamente adquirir conocimiento para utilizarlo en la fabricación de utensilios y herramientas o en la elaboración procesada de mercancías. Pretendemos poseer conocimientos para actuar en todos los frentes que nos puedan afectar y en aquellos en los que voluntariamente dejamos huella. Es decir, el paradigma mental clásico debe ser revisado y alterado para perfilar nuevas herramientas que puedan encaminar nuestro aprendizaje, para que no seamos excluidos de la sociedad del conocimiento (Rodríguez de Almeida y Davara Rodríguez 2006, 381).

La Sociedad del Conocimiento tiene múltiples personalidades y nos compete a cada uno de nosotros observarla desde perspectivas diferentes, opuestas, iluminada y en la oscuridad, para que entonces sí se pueda hacer la luz. Y la luz, de hecho, es necesaria. Véase la matriz conceptual de la identificación de la sociedad del conocimiento que nos lleva a reconocerla con los más variados apellidos, de la información, digital, de consumo, virtual, posindustrial, cibernética y todo un sinfín de denominaciones (Rodríguez de Almeida y Davara Rodríguez 2006, 381).

De todo lo expuesto por Rodríguez y Davara, se puede concluir entonces que la sociedad del conocimiento, encuentra su sustento en dos premisas inseparables, la información y el conocimiento, los cuales a lo largo de la historia humana se han desarrollado de modo paralelo y conjunto, al mismo tiempo, se habla ahora de esta sociedad puesto que, sus dos componentes son fuente inagotable para nuestro desarrollo.

De otro lado, se puede llegar a una segunda conclusión, en el sentido que, la sociedad del conocimiento, no es otra que la sociedad de la información, como se vio en este título cuando los autores Rodríguez y Davara, citan que los otros apellidos de la sociedad del conocimiento, serán de la Información, digital, de consumo, entre otras; lo cual nos reporta taxativamente que se tratan de sinónimos. Si conjugamos esta premisa con lo señalado con anterioridad, esto es que los componentes principales de la sociedad de la información, son precisamente información y nueva tecnología; y contrastamos que los componentes principales de la sociedad del conocimiento son información y conocimiento, tendremos pues, que la diferencia sustancial entre los conceptos de ambas, son sus componentes, los cuales se diferencian únicamente en: conocimiento y nuevas tecnologías.

Entonces, de lo expuesto en los párrafos anteriores podemos concluir que, para la doctrina las sociedades, tanto de conocimiento como de información son en teoría equivalentes, pero sí de sus componentes nos referimos, se diferenciarán respecto de conocimiento y nuevas tecnologías.

Para los efectos prácticos de la presente investigación, se ha preferido trabajar con la denominada sociedad de la información debido a que, se ciñe a los conceptos propuestos en el problema, goza de sustento jurídico por parte de la comunidad europea y encaja dentro de la solución propuesta en la hipótesis.

4.2. ELEMENTOS CONSTITUTIVOS DE LA SOCIEDAD DE LA INFORMACIÓN:

Los elementos constitutivos de la sociedad de la información (Menéndez Mato 2008, 105-106) son:

- Las redes.- Permiten la transmisión de la información y, gracias a ellas, las limitaciones temporales y espaciales han desaparecido (por ejemplo: teléfonos, satélites, cables).
- Los servicios básicos.- son aquellos servicios que permiten la utilización de las redes. Son ejemplos de ellos: el correo electrónico, la transferencia de ficheros, los multimedia interactivos, o los servicios de videos.
- Las aplicaciones.- éstas ofrecen soluciones específicas para grupos de usuarios. Los ejemplos son diez: teletrabajo, educación a distancia, red de universidades y centros de investigación; servicios telemáticos para las PYME; gestión del tráfico por carretera: control del tráfico aéreo; redes de asistencia sanitaria; licitación electrónica; red transeuropea de administraciones públicas (programas de intercambio de datos entre administraciones); y autopistas urbanas de la información (aplicación centrada en los beneficios que obtienen los consumidores en la sociedad de la información: tele compra, transacciones bancarias, educación a distancia, etc.).

Como se puede notar de lo expresado anteriormente, en la sociedad de la información se encuentran inmersos muchos supuestos del desarrollo humano;

para la presente investigación se ha de desarrollar específicamente las actividades referidas a los servicios básicos o simplemente servicios.

4.2.1. LOS SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN.-

Si en la presente, nos referimos a los comportamientos sociales de las personas en la sociedad de la información, será necesario referirnos específicamente a los servicios de la sociedad de la información.

La directiva 98/48/CE del Parlamento Europeo y del consejo de 20 de Julio de 1998. artículo 1, punto 2, prescribe que por servicio de la sociedad de la información se entiende todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios.

Según la directiva 2000/31/CE del Parlamento Europeo y del consejo de 8 de junio de 2000- considerando 18, los servicios de la sociedad de la información pretenden cubrir una amplia variedad de actividades económicas que se desarrollan en línea; dichas actividades en particular consiste en la venta de mercancías en línea.

Si bien en principio los servicios de la sociedad de la información tienen una naturaleza de contraprestación, concordamos con el profesor del Peso Navarro cuando agrega que también lo son, en la medida que representan una actividad económica, los servicios no remunerados por sus destinatarios, como aquellos que consisten en:

- Ofrecer información en línea o
- Comunicaciones comerciales o
- Los que ofrecen instrumentos de búsqueda, acceso y recopilación de datos.

Además agrega, que los servicios de la sociedad de la información también consisten en transmitir información a través de una red de comunicación o albergar información facilitada por el destinatario del servicio.

El concepto de servicio de la sociedad de la información comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios.

Son servicios de la sociedad de la información, entre otros, y siempre que representen una actividad económica, los siguientes (Barral Viñals 2004, 34-35):

- La contratación de bienes o servicios por vía electrónica.
- La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales.
- La gestión de compras en la red por grupos de personas.
- El envío de comunicaciones comerciales.
- El suministro de información vía telemática.
- El video bajo demanda, como servicio en que el usuario puede seleccionar a través de la red, tanto el programa deseado como el momento de su suministro y recepción, y, en general, la distribución de contenidos previa petición individual.

Nos gustaría que de todo lo expresado acerca de los servicios de la sociedad de la información se tomara en cuenta, especialmente aquellos relacionados con los servicios no remunerados que ofrecen recopilación de datos y las que consisten en transmitir información de una red de comunicación o albergar información facilitada por el destinatario del servicio.

De otro lado, según la comunicación de la comisión del Parlamento Europeo y el consejo sobre el programa plurianual de la comunidad para fomentar el desarrollo de la industria europea de los contenidos multimedia y la utilización de éstos en la naciente sociedad de la información, los contenidos informáticos son una de las dimensiones clave de la sociedad de la información.

Por contenido se entienden los datos, textos, sonidos, imágenes o combinaciones multimedios de ello, representados en formato analógico o digital sobre diversos tipos de soportes, tales como papel, microfilm o dispositivos de almacenamiento magnético u óptico (del Peso Navarro 2004, 8).

Como podemos observar, los contenidos informáticos en los servicios de la sociedad de la información gozan de un contenido fundamental por lo que su seguridad también se conformará como esencial para efectos del trabajo que se viene desarrollando.

4.3. LA SEGURIDAD: REQUISITO NECESARIO EN LA NUEVA SOCIEDAD DE LA INFORMACIÓN.-

Es necesario citar la Sentencia del Tribunal Supremo Español, del 10 de diciembre de 1980, la cual inspiro, en parte el presente título, la cual dicta textualmente: La protección de los derechos no se contrae a la reparación de los perjuicios originados, sino que ha de extenderse a las medidas de prevención que razonablemente impidan ulteriores lesiones (Molina Mateos y otros 2005, 371)

La evolución de la importancia de la protección de la información y las comunicaciones en la sociedad de la información, ha ido incrementándose.

La conveniencia inicial de proteger se ha transformado en necesidad, que deviene en obligación cuando se refiere a la protección de derechos.

La seguridad de la información como instrumento efectivo, coadyuva con el derecho y el poder como instrumentos de ordenación social y, juridificada se sitúa en el pórtico de su reconocimiento como deber (Molina Mateos y otros 2005, 373).

Ahora bien, existen diferentes clases de seguridad en la sociedad de la información, las cuales cito a continuación (del Peso Navarro 2004, 34-35):

- Seguridad física.- comprende todas las medidas que tratan de proteger los sistemas de información de amenazas físicas (inundaciones, fuego, cortes del fluido eléctrico, interferencias, atentados, robos, hurtos, etc.) originadas tanto en la naturaleza como en los propios medios y en el ser humano.
- Seguridad lógica.- pretende proteger el patrimonio informacional que se compone tanto de aplicaciones informáticas como del contenido de las bases y de los ficheros.

La protección de este tipo se puede realizar a través de contraseñas, conocimientos y hábitos del usuario, firmas digitales y principalmente la utilización de métodos criptográficos.

- Seguridad organizo- administrativa.- la gran olvidada de muchos autores, pretende cubrir el hueco dejado por las anteriores y que viene, en cierto modo a complementarlas.

Difícilmente se puede lograr de forma eficaz la seguridad de la información si no existen claramente definidas:

- Políticas de seguridad.
 - Políticas de personal.
 - Políticas de contratación.
 - Análisis de riesgos.
 - Planes de contingencias.
- Seguridad jurídica.- a través de la aportación de normas legales, fijar el marco jurídico necesario para proteger los bienes informáticos.

4.3.1. PRINCIPALES CARACTERÍSTICAS DE LA NECESIDAD DE SEGURIDAD EN LA SOCIEDAD DE LA INFORMACIÓN.-

El profesor del Peso Navarro, asegura que se define la seguridad de la información como el conjunto de sistemas y procedimientos que garantizan la confidencialidad, la integridad y la disponibilidad de la información. Éstas son las tres características que hasta el presente han venido definiendo lo que es la seguridad de la información, pero la irrupción de internet ha hecho que estas características no sean ya suficientes y que, junto a ellas, aparezcan otras como: autenticación o autentificación; no repudio, tanto en origen como en destino; control de acceso y sellado de tiempo (del Peso Navarro 2004, 35).

Analicemos pues, a continuación, lo que significa cada una de ellas según el profesor del Peso Navarro:

- La confidencialidad, pretende que la información sea conocida exclusivamente por los usuarios autorizados en la forma y tiempo determinados previamente.
- La integridad, pretende que la información sea creada, alterada, modificada o borrada sólo por los usuarios autorizados.
- La disponibilidad, pretende que la información se pueda utilizar cuando y como lo requieran los usuarios autorizados.
- Con la autenticación, se pretende acreditar que el remitente del mensaje es quien dice ser y no otra persona.
La autenticación tiene dos funciones básicas: identificar al autor del mensaje y verificar que dicho autor se obliga legalmente con el mismo (del Peso Navarro 2004, 36).
- El control de accesos, prohíbe que los usuarios no autorizados accedan a los recursos del sistema.

- El sellado del tiempo, nos permite verificar la fecha y el momento en que se ha enviado el mensaje.

En resumen, podemos decir que lo que se pretende es que sea imposible alterar los (texto original mensajes) –para nuestros datos- y si los son, que quede constancia de ello, su autoría ha de ser inequívoca y deben tener valor probatorio en caso necesario (del Peso Navarro 2004, 37).

Podríamos concluir que para conservar la confidencialidad de nuestros datos, sean estos del carácter que sean, vendría a ser un procedimiento largo y costoso. Como se verá un poco más adelante, no debería ser excesivamente onerosa la inversión para proteger la información; aquí estamos refiriéndonos a información en general, de cualquier sujeto (persona natural o persona jurídica), más adelante nos referiremos a los datos de carácter personal, que, lógicamente respectan únicamente a personas naturales.

Entonces, ¿para que el parangón? Para notar que inclusive en el ámbito precautorio, las personas jurídicas cuentan con posibilidades más amplias para proteger sus datos que las personas naturales, y si las personas naturales quisieran usar estos métodos para proteger su información, resultaría en alto oneroso, y por ende, sería sólo para algunos sectores de la población.

Invirtamos la figura, que sucedería entonces cuando es la persona jurídica quien aprovecha su posición privilegiada respecto de los datos de las personas naturales, veremos qué consecuencias negativas se pueden acarrear respecto de los datos de carácter personal.

4.3.1.1. JUSTIFICACIÓN DE LA SEGURIDAD EN LA SOCIEDAD DE LA INFORMACIÓN.-

Veamos entonces, del desarrollo de la necesidad de la seguridad en la sociedad de la información, y, según el profesor del Peso Navarro, la

información es la materia prima de la sociedad de la información con la que trabajan millones de ciudadanos de todos los países del mundo (del Peso Navarro 2004, 37).

Entonces, si la información es tan importante en la sociedad de la información, es también importante su protección, pero los doctrinarios afirman que es allí donde surgen los problemas.

Si damos un vistazo al pasado, en una primera época de la informática, la información se encontraba confinada en grandes centros de datos, donde era relativamente fácil protegerla, pues su salida de esos lugares estaba claramente prefijada.

Ahora, afirma el profesor del Peso Navarro, que posteriormente, con la incorporación de las redes de comunicaciones, el problema creció, pero se podía solventar. Añade que después, tras la aparición de los ordenadores personales acrecentó el problema, pues la información ya no se encontraba tan sólo distribuida, sino estaba prácticamente desparramada (del Peso Navarro 2004, 37).

La aparición y utilización masiva de internet ha hecho que el tema de la seguridad en la sociedad de la información sea el propietario mismo de la información quien deba buscar soluciones.

Es el mismo Profesor del Peso Navarro, quien recomienda algunas pautas para solucionar el problema de la seguridad en la sociedad de la información: no se debe caer en exagerados histerismos cuando tratemos de resolver este problema, ni entrar en el juego de aquellos que, con el afán de vender, nos quieren convencer de que todo hay que protegerlo con medidas de seguridad excesivamente costosas.

A la hora de implantar medidas de seguridad, es preciso tener hecha una clasificación de la información conociendo lo que realmente debemos proteger y lo que no, y no adoptando iguales medidas para

todo nuestro patrimonio informacional, cuando, en muchos casos, parte de él no merece que realicemos ningún gasto en su seguridad.

A nuestro parecer, debería protegerse especialmente aquellos datos que involucren ámbitos de la vida personal, familiar y amical; contenidos de carácter personalísimo que sólo debieran ser utilizados por los dueños del patrimonio informacional. Además debe tomarse en cuenta que los contenidos de estos datos deben ser relevantes para cada persona natural que los exhiba en el internet, un criterio que pueda ser sustentado y plausible de ser defendido frente a terceros; para que así, pueda ser justificable su protección. A continuación el desarrollo de los datos que pueden ser vulnerables y que pertenecen a las personas naturales.

4.3.2. LOS DATOS DE CARÁCTER PERSONAL.-

Hemos venido hablando de la información, vimos entonces que se podría tomar mecanismos precautorios para su protección y que ellos podían ser alcanzados en generalidad por empresas o personas jurídicas por motivos de su onerosidad.

¿Qué pasa entonces con las personas naturales? Bueno, es aquí donde desarrollamos como son tratados los datos de carácter personal en la sociedad de la información.

No nos parece complicado decir que son datos de carácter personal, de una manera simple podríamos empezar con el nombre, el sexo, la edad, el estado civil; andando un poco más, podríamos agregarle gustos, preferencias, las cuales podrían enmarcarse desde las culinarias, hasta las políticas, artísticas, literarias, entre otras; también podrían calzar en este concepto, para la sociedad de la información, las fotografías, videos, slides u otros similares que una persona tenga, o (en el caso de los slides) elabore, de sí misma.

La Ley Orgánica de Protección de Datos, 15/1999 del 13 de diciembre, en su artículo 31, califica como datos de carácter personal a cualquier información concerniente a personas físicas identificadas o identificables (Apud. Del Peso Navarro y otros 2010, 15).

En este sentido, la misma Ley Orgánica, en su artículo 5.1.f, califica los mismos datos como, toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión, concerniente a una persona física identificada o identificable (Apud. Del Peso Navarro y otros 2010, 15).

Se dice que, en un hipotético peligro a la información de carácter personal cada vez parece más probable y la intimidad (se tratará del derecho propiamente dicho que hemos considerado en el capítulo que relata de la autodeterminación informativa) de las personas queda con más facilidad al descubierto y la protección de estos datos cada vez resulta más difícil de realizar; nos gustaría que se tome especial énfasis en que la protección de los datos es cada vez más difícil de consumir. Nos encontramos una vez más ante la posible colisión de derechos, algo que, por otra parte, no nos debe escandalizar, pues en otras áreas del derecho es habitual: el derecho a la intimidad de las personas, el derecho a la protección de sus datos de carácter personal y por otro lado frente al derecho a la libre circulación de mercancías y servicios, lo que hace necesaria la libre circulación también de los datos personales (del Peso Navarro 2004, 58).

Concordamos con el Profesor en ambos aspectos, por lo que podríamos añadir algo al segundo. En primer lugar es verdad que la protección de los datos de carácter personal será cada vez más difícil, un ejemplo sencillo de ello es que si una persona cualquiera entra a su buscador favorito, como por ejemplo Google, Yahoo, AltaVista, etc. y coloca el nombre de algún conocido, inmediatamente aparecerá por lo menos sus nombre completo, algunos datos de carácter personal y en determinados casos su fotografía, esto se debe a que las personas responden a los fenómenos causados por la

sociedad de la información, uno de ellos son las páginas web de contenido social o redes sociales desarrolladas en el sub capítulo a continuación.

Por otro lado, es muy normal que las ciencias jurídicas tengan derechos que se contravengan, los encontramos en todas su ramas; pero es deber del legislador saber distinguir cual es aquel que prevalece respecto del otro. Por otro lado, es igualmente cierto que se ha vuelto necesaria la libre circulación de datos personales, pero esto no da derecho a otras entidades o personas de utilizar los mismos de manera inescrupulosa.

SUB CAPÍTULO II

LAS PÁGINAS WEB DE CONTENIDO SOCIAL O REDES SOCIALES DEL INTERNET

4. JUSTIFICACIÓN.-

Nos gustaría comentar en primer término, que se desarrolló en este primer capítulo la sociedad de la información, algunos de sus componentes y el desarrollo de los mismos pues el objeto de nuestro estudio, es decir los contratos on line para acceder a los servicios de las páginas web de contenido social o redes sociales; estas últimas están contenidas en dicha sociedad.

Era necesario incluir el tratamiento de cómo las empresas o personas jurídicas en lugares como España o la Unión Europea se hacían cargo de la importancia de la seguridad en sus redes y cuan oneroso pueden llegar a ser las mismas, como mencionamos en el capítulo anterior.

En línea con lo expresado anteriormente, creímos importante incluir también el tratamiento de los datos de carácter personal dentro de la sociedad de la información puesto que más adelante desarrollaremos en pleno, el derecho que el Tribunal Constitucional peruano decidió denominar el derecho a la autodeterminación informativa, que, como veremos en el capítulo tercero de los contratos vía internet, algunas redes sociales pretenden vulnerar.

5. GENERALIDADES.-

Veamos, antes de ver lo específico, empecemos con lo general, es decir, las páginas web. En un sentido técnico, se reconoce que las páginas web son aquellos documentos adaptados para la web, siendo su principal característica los enlaces con otras páginas de la misma naturaleza.

Estas páginas pueden ser de muchas categorías, en realidad no hemos encontrado ningún trabajo que involucre una clasificación oficial; pero podríamos encontrar entre las más comunes, desde los buscadores, que sirven para encontrar o, si se quiere, averiguar cualquier tipo de información (como Google, Yahoo, AltaVista, entre otros); las páginas de correo electrónico las cuales te ofrecen un servicio de correo, para poder trasladar e intercambiar información (como Hotmail, Yahoo, Gmail, etc.); otras pueden ser las empresariales que, brindan información básica acerca de empresas o personas jurídicas que sirven principalmente para publicitar a las empresas dueñas, informando a los posibles clientes de sus productos y servicios (como las páginas web de las universidades, las de los consorcios, los grupos, entre otras), hasta las que recopilan datos de sus usuarios, y comparten esta información con los usuarios de su misma red (en principio) como lo son las páginas web de contenido social o redes sociales (como lo son Hi5, Badoo, SixApart, Facebook, Twitter, Tagged, Sonico, MySpace, entre muchas otras).

6. LAS PÁGINAS WEB DE CONTENIDO SOCIAL O REDES SOCIALES Y SU OBJETIVO RESPECTO DE ESTA INVESTIGACIÓN.-

Como afirmamos en el párrafo anterior a este título, las páginas web de contenido social o redes sociales, se encargan, como la primera de sus características, de recopilar datos de los usuarios que las utilizan; pero ¿cómo es que en realidad funcionan? Bien, en la actualidad en el ámbito de los servicios de la sociedad de la información, las páginas web de contenido social, por lo general pertenecen a una empresa o consorcio que, a través de ellas realizan investigaciones de mercado para su propio aprovechamiento o el de sus clientes.

El profesor del Peso Navarro afirma que la creación de nuevos mercados, inexistentes hace pocos años, como es de los teléfonos móviles por ejemplo, y su rápido desarrollo hace que el empleo de los medios tradicionales de captación y de

fidelización de clientes ya no son válidos y es necesario emplear nuevas técnicas que nos permitan un tratamiento masivo, rápido y, a poder ser, barato.

Esto da lugar a la creación de bases de datos en las que se almacenan cuantos más datos mejor para lograr con ello un perfil de quien compra o puede comprar en el futuro (del Peso Navarro 2004, 57).

Estas nuevas bases de datos, para la recopilación de los mismos, se desarrollan a través de las, ya mencionadas y modernas redes sociales. Su sistema funciona de la siguiente manera: configuran y hacen pública a través de internet una página web en donde cualquier persona, en este caso denominada destinatario o usuario, crea una cuenta a través de la página (a través de un contrato on line, que será desarrollado en el capítulo III) y empieza a utilizar sus servicios; estos servicios (los de contar con una cuenta) en su mayoría son de carácter gratuito.

De estos usuarios, recopilan una gran cantidad de datos de carácter personal desde nombres, apellidos, dirección, países de origen y de residencia hasta gustos, preferencias, opiniones personales, políticas y todas las demás imaginables. Si vamos un poco más allá, existen inclusive páginas que tienen anuncios publicitarios para que el usuario decida si es de su agrado o no.

Entonces podemos concluir que estas páginas son en realidad agentes de mercado que analizan un público objetivo, para saber que ofertar en determinados lugares, a determinadas personas y en qué circunstancias, de esta información personal pueden deducir clase social, preferencias, necesidades, capacidad adquisitiva entre otros factores de marketing.

Muy aparte de lo antes indicado, se puede señalar que las redes sociales tienen también un lado positivo, como lo es el permitir la promoción de productos y servicios en el Internet, cualquier tipo de empresa puede valerse de los medios electrónicos contenidos en estas páginas. Esto permite un ciclo económico puesto que las fuentes confiables de información permiten a los receptores de esta su análisis y consiguiente resultado, lo que permite desarrollar mejores productos y servicios. En esta línea de ideas podemos agregar que también puede tener efectos

sociales, sociológicos y psicológicos, los mismos que no son materia de la presente investigación, pero vale la pena mencionarlos.

Para agregar información sobre estas páginas web, y como fenómeno social propiamente dicho, el público objetivo que las usa es en su mayoría joven, que en algunos casos no asume los riesgos que podría implicar la publicidad, en el sentido del libre acceso, respecto de su datos de carácter personal; es más existen algunos jóvenes que publican datos que podrían resultar comprometedores, como ejemplos clásicos podemos citar a las jovencitas que cuelgan en las redes su fotos digitales en ropa de baño o en ropa interior; estas situaciones podría ir más allá del peligro que reporta la presente investigación, podrían mancillar también su honor y buena reputación tema que podría ser muy discutible también.

De lo dicho en el párrafo anterior podemos decir, que ante el avance vertiginoso de la era digital, debemos estar preparados y preparar a las futuras generaciones para que sepan cómo proteger sus datos de carácter personal, su intimidad y demás derechos que el famoso fenómeno de internet pudiera afectar o poner en peligro de afectación a sus diferentes derechos.

Por último, veremos más adelante que existen creadores de redes sociales que podrían pretender aprovecharse de la situación de disponer de estos datos de carácter personal de sus usuarios, en otros aspectos que no están necesariamente relacionados al marketing.

CAPÍTULO III

DE LOS CONTRATOS VÍA INTERNET

4. GENERALIDADES.-

Para hablar de los contratos vía internet, primero debemos referirnos a la contratación en masa y a la contratación por adhesión que son conceptos previos e incluyentes de la referida contratación, pues, valga la redundancia, es practicable en masa y casi siempre por adhesión.

4.1. LA SOCIEDAD DE MASAS.-

Para poder referirnos a la contratación en masa debemos reseñarnos a cómo es que surgió, cuáles son sus aspectos y características. Según el Profesor Carlos Alberto Soto Coaguila, el fenómeno trascendente que continua año tras año es la explosión demográfica. Desde fines del siglo XIX hasta la fecha se ha producido una progresiva aceleración y un incontrolable aumento de la población (Soto Coaguila 2005, 2).

Este aumento considerable de la población ha tenido efectos en todas las ciencias humanas, no podía escapar de ella las ciencias jurídicas, y en el presente trabajo nos concentraremos específicamente en la influencia que ha operado sobre el derecho de los contratos y la contratación.

Ahora, este aumento de la población ha venido a crear, según el Profesor Soto Coaguila, el nuevo paradigma: la masificación de la sociedad. El incremento de los seres humanos en el mundo ha generado las llamadas “masas humanas” (Soto Coaguila 2005, 2).

¿Pero que son las masas?, según Philip Lersch (Apud. Soto Coaguila 2005, 3) la masa es pura cantidad, una acumulación o conglomerado sin trabazón interna y sin forma externa; implica la homogeneidad de sus partes componentes. A nuestro entender lo que el profesor Lersch quiso decir con masa es que esta es un concepto numérico, que solo se trata de cantidad, que no tiene una forma

definida puesto que crece sin control y que, dentro de ella todos los seres humanos que la conformamos debemos ser tratados como iguales.

Ahora, tras haber aclarado el concepto de masas podemos abordar el de sociedad de masas, según Juan Vallet de Gortisoló (Apud. Soto Coaguila, 2005, 3) la sociedad de masas es un conjunto inorgánico de individuos despersonalizados, la agregación física y compacta de seres humanos orientados hacia un contenido directo, temporal y organizado, y que en su mayoría reaccionan ante los mismos estímulos y de una manera semejante.

En conclusión la sociedad de masas está formada por conglomerados de seres humanos totalmente despersonalizados. Sus principales características son: la uniformidad, la carencia de estructura, la manipulación externa y la ausencia de responsabilidad (Soto Coaguila 2005, 4).

Desarrollaremos cada una de las características a continuación, tal y como las describe (Soto Coaguila 2005, 5):

- La uniformidad.- en la sociedad de masas determina una extrema igualación del individuo que conforma la masa. Se trata de una igualdad imaginaria, pues cada ser humano es distinto psíquica y físicamente. Empero, no hay distinción de rango o características, pues todos los individuos se consideran iguales a sí mismos. Hay igualdad de gustos y formas de ser, y las costumbres siguen el mismo derrotero. Como consecuencia de esta uniformidad y tendencia a igualarse se genera una carencia de estructuras, ya que los individuos componentes de la masa se presentan iguales, desapareciendo de toda jerarquía o rango.
- La manipulación externa.- se presenta como consecuencia de la falta de vida y estructuras propias del hombre-masa. De allí que el poder de los medios de comunicación condiciona y manipula a las masas generando en ellas nuevas necesidades y costumbres, lo que convierte al hombre en un simple espectador de la vida.

- La ausencia o falta de responsabilidad.- surge como consecuencia de las características anteriores, pues al no tener participación directa en la sociedad de masas es movido externamente a través de los medios de comunicación por lo que no es responsable de sus actos. (Soto Coaguila 2005, 4-5)

En este contexto según Recasens Siches (Apud. Soto Coaguila 2005, 5) aparece el hombre-masa quien se caracteriza por su deseo excesivo de disfrute y su falta de sentido de responsabilidad.

Una vez que hemos ubicado a la sociedad de masas y sus características, corresponde abordar el tema de los fenómenos masivos o masificados, que a entender de Díez Picazo (Apud. Soto Coaguila 2005, 5) son todos los hechos donde intervienen masas de personas y en los cuales se traban relaciones circunstanciales y donde, además, los integrantes de la masa entablan relaciones sin llegar a poseer un conocimiento exacto de la identidad de los otros sujetos. Existe un riguroso anonimato.

Como vimos en la sociedad de la información, muchos de estos fenómenos masivos son en puridad sociales. Podemos ubicar entre los que tiene relevancia jurídica aquellos contractuales.

4.2. TRÁFICO CONTRACTUAL MASIVO.-

Como pudimos ver de la sociedad de masas, los fenómenos provocados por la explosión demográfica han repercutido en todo; ahora bien, para poder desarrollar cual fue su repercusión en materia contractual, primero nos gustaría referirnos al carácter social del contrato, desarrollado a continuación.

4.2.1. EL CARÁCTER SOCIAL DEL CONTRATO.-

Para nuestra investigación es importante que se sepa lo siguiente: El contrato no es una institución que únicamente cumple funciones jurídicas o económicas, también funciones de carácter social. (Soto Coaguila 2005, 36).

Según Carlos Cárdenas (Apud. Soto Coaguila 2005, 36), si bien la persona está en aptitud de realizar sus aspiraciones, objetivos e intereses a través de la contratación, debe hacerlo necesariamente en armonía con las aspiraciones, objetivos e intereses de los otros. Dentro de esta perspectiva, según el mismo profesor peruano, el contrato se convierte en un medio de cooperación social y se produce lo que cabe calificar como la “humanización del contrato”. Ello implica concebir el contrato como un medio integrador, armonizador y cooperador de las relaciones sociales, no como vehículo de explotación, de imposición, de abuso de una parte sobre otra.

Nos interesa especialmente la afirmación del profesor Cárdenas en lo referido a que si el contrato se ve de la óptica: humanización; es esencial que ambas partes en la relación contractual tengan derechos de carácter invulnerable, que exista respeto mutuo y que una no se aproveche o ni siquiera intente aprovecharse de su situación de ventaja respecto de la otra.

Por otro lado, para el profesor Soto Coaguila, un aspecto importante del carácter social de los contratos radica en el conflicto entre los intereses individuales y colectivos. Existen dos posiciones sobre este respecto:

- Para los defensores de las tesis liberales el interés individual debe primar, en razón de ser de la -autonomía privada- ley entre partes, por lo tanto, ningún tercero ajeno a la relación contractual puede alterar su normal ejecución o frustrar su cumplimiento. En otras palabras los contratos son intangibles, intocables, de allí la razón de su inmutabilidad, que algunos califican de santidad.
- Por otro lado, se encuentran los que sostienen que el interés social se antepone al interés individual, y que el contrato debe estar al servicio del bien común, es decir del bien estar de cada uno pero también de los demás miembros de la sociedad.

El mismo Profesor Soto Coaguila Considera que, teóricamente, una u otra postura, es válida, dependiendo de la orientación ideológica que siga el

legislador. Sin embargo, recordemos que no son los particulares los que deciden cuáles serán las reglas de la contratación; es el Estado que en ejercicio del ius imperium, conferido por el pueblo y a través del legislador, establece el marco legal mediante el cual los particulares tendrán la facultad de crear, relaciones contractuales. De la misma forma, el Estado dispone que las relaciones contractuales de los particulares se respeten y se garanticen su cumplimiento, pero conforme a los límites y restricciones que el mismo Estado, mediante la ley, decide establecer a los contratos. (Soto Coaguila 2005, 37-38).

Ahora bien, nosotros afirmamos que así como los Estados delimitan como deberán ser las relaciones contractuales entre particulares; para la misma salvaguarda del bien común; alguna entidad internacional encargada de velar por ello, delimitará la contratación vía internet que obviamente es de carácter internacional.

Queremos agregar que, pretender prever todas las formas de contratación es casi imposible. El progreso de la sociedad mediante los descubrimientos de la ciencia, el surgimiento de la tecnología y la producción estandarizada de los bienes y servicios han generado que la contratación privada no sea uniforme en el tiempo. En esta medida, es ingenuo pensar que las legislaciones puedan aprehender todos los supuestos o variantes de la contratación privada (Soto Coaguila 2005, 40).

Para nosotros, cuando la sociedad de masas pasa al ámbito de internet, será reconocida como la sociedad de la información (física: sociedad de masas, virtual o a través de internet: sociedad de la información); y cuando el tráfico contractual masivo pasa al internet formará parte de los denominados contratos vía internet, desarrollados a continuación.

4.3. LA AUTONIMÍA PRIVADA Y EL CONTRATO POR ADHESIÓN.-

4.3.1. LA AUTONOMIA PRIVADA.-

Se entiende por “autonomía”, en general, el poder de darse normas de por sí, por lo cual el concepto de autonomía viene, en cierta forma, a identificarse con el concepto de “soberanía” (Apud. De la Puente y La Valle 2003, 197). Esta autonomía puede ser concedida por el Estado a una autoridad, caso en el cual estamos frente a las normas que constituyen el ordenamiento jurídico, que son obligatorias para todos, o bien atribuida a los sujetos privados, quienes de esta manera pueden dictar normas para regular sus propias conductas. Tal segunda potestad recibe el nombre de “Autonomía privada” (Apud. De la Puente y La Valle 2003, 197). Se dice, por ello, que en virtud de esta autonomía los hombres son soberanos para vincularse obligatoriamente entre sí, dentro de los cauces del ordenamiento jurídico.

No siempre la expresión “autonomía privada” ha sido plenamente acogida. La literatura jurídica ha preferido utilizar el término “autonomía de la voluntad”, por entenderse que la potestad, que es el contenido de la autonomía, se confiere a la voluntad humana, para que sea ella la que gobierne las voluntades entre las personas que la exteriorizan (De la Puente y La Valle 2003, 197).

Esto es comprensible por cuanto, siendo la autonomía concedida a los particulares el fundamento del acto jurídico, durante todo el periodo histórico en el que se consideró el acto jurídico como la expresión de la voluntad de sus otorgantes resultaba consecuente que se atribuyera a la voluntad el principio rector de las relaciones humanas (De la Puente y La Valle 2003, 197). Era el auge de la teoría de la voluntad.

Pero tras el transcurso de muchas otras teorías, se pensó que la autonomía debía recaer en el elemento que daba lugar a la existencia del acto jurídico, que no era necesariamente de la voluntad, sino el poderío privado de crear (regular, modificar o extinguir) relaciones jurídicas, cualquiera que fuere el criterio que hiciera efectivo ese poderío. Por ello, se consideró más apropiada la expresión “autonomía privada” (De la Puente y La Valle 2003, 198).

Sin entrar, por el momento, a juzgar el fundamento de la autonomía privada, esto es, si es la libertad humana (De la Puente y La Valle 2003, 198), o

individual, la que justifica que las personas tengan la potestad de regular privadamente sus intereses, o si por el contrario, es el Estado el que, desprendiéndose de parte de su propia soberanía, confiere a los particulares el poder de dictar normas aplicables a su relación entre sí, conviene estudiar cual es el concepto de autonomía privada.

Podemos llegar a la conclusión que la noción de libertad individual se traduce en la libertad de contratar, o sea la libertad concedida a las personas para que, de común acuerdo puedan crear, regular, modificar o extinguir entre sí relaciones jurídicas patrimoniales. Tal es el concepto escrito de autonomía privada (De la Puente y La Valle 2003, 199).

Obsérvese que este concepto de la autonomía privada, la libertad adquiere un nuevo sentido, pues sin dejar de ser la ausencia de ataduras para obligarse, se convierte también en poder de crear relaciones jurídicas obligacionales. La persona jurídica es no solo libre para contratar sino también soberana para ser obligatorias las relaciones jurídicas producto del contrato (De la Puente y La Valle 2003, 199).

Podemos decir, pues, que la autonomía privada es el poder reconocido a las personas para regular, dentro del ordenamiento jurídico, sus propios intereses y crear libremente relaciones jurídicas entre sí (Apúd. De la Puente y La Valle 2003, 199).

El principio de la autonomía privada tiene un doble contenido (Apúd. De la Puente y La Valle 2003, 199):

- En primer lugar, la libertad de contratar, llamada más propiamente libertad de conclusión, que es la facultad de decidir como cuando y con quien se contrata, sabiendo que con ello se va a crear derechos y obligaciones;
- En segundo lugar, la libertad contractual, llamada también más propiamente libertad de configuración interna, que es el determinar el contenido del contrato, o sea el modelado del mismo. Debe destacarse que la segunda libertad presupone la primera.

De lo anteriormente expuesto, respecto de la teoría de la autonomía privada se desprende el concepto de contrato negociado, llamado también paritario o discrecional, el cual es el contrato tradicional que crea relaciones contractuales y nace del consentimiento libre entre dos o más partes perfectamente identificadas (oferente y aceptante), y existe además participación de ambas en el contenido contractual (Soto Coaguila 2005, 40).

En la actualidad la perspectiva de la negociación se encuentra vigente, pero también nos encontramos ante un nuevo escenario: la contratación paritaria ha dejado de ser la regla en la contratación (Soto Coaguila 2005, 40). Este nuevo escenario ha dado paso a la contratación por adhesión desarrollada a continuación.

4.3.2. EL CONTRATO POR ADHESIÓN.-

Actualmente la contratación masiva, estandarizada o predispuesta es la forma común de contratar. En este nuevo sistema de contratación, los contratantes no elaboran el contenido del contrato, éste es predispuesto por uno de ellos con anticipación a su celebración. La doctrina Nacional concuerda en que, se le denomina contrato por adhesión desde que ésta no es el objeto del contrato, sino la manera de celebrarlo.

Concordamos con el Profesor Soto Coaguila cuando afirma en el tráfico contractual masivo, los contratos o relaciones jurídicas contractuales se desarrollan bajo otro esquema, un sistema de contratación distinto al tradicional o paritario. Este sistema contractual tiene un carácter masivo y estandarizado. Uno de los contratantes (denominado “predisponente”) predispone integra o parcialmente el contenido del contrato y la otra parte (denominada “adherente”) acepta contratar adhiriéndose a las condiciones preestablecidas por el contratante predisponente. El adherente se encuentra en la disyuntiva de: contratar bajo dichas condiciones o no contratar. Cuando el predisponente redacta íntegramente el contrato surge lo que la doctrina conoce como ya se dijo, con el nombre de contrato por adhesión.

En ese orden de ideas, es preciso acotar que el art. 1390° de nuestro Código Civil establece que el contrato es por adhesión cuando una de las partes, colocada en la alternativa de aceptar o rechazar íntegramente las estipulaciones fijadas por la otra parte, declara su voluntad de aceptar.

El primer elemento que tipifica el contrato por adhesión es que una de las partes fija unilateralmente las estipulaciones contractuales, sin participación de la otra. Esta fijación puede ser, en teoría, previa a la oferta, aunque debe tomarse en consideración que la predisposición de las estipulaciones no es una característica del contrato por adhesión (como si lo es de las cláusulas generales de contratación), de tal manera que normalmente el oferente fija sus estipulaciones al momento de declarar su oferta (De la Puente y La Valle 2003, 652).

El segundo elemento característico de la definición legal del contrato por adhesión es que la parte que redacta o fija las estipulaciones plantea a la otra una alternativa inmodificable entre la aceptación íntegra de tales estipulaciones, o sea la oferta, y el rechazo también íntegro, de ella (De la Puente y La Valle 2003, 654).

Obsérvese que no se trata de una imposición, en el sentido que el redactante u oferente presiona o somete al destinatario para que acepte su oferta, sino únicamente lo coloca en una disyuntiva ante la cual el destinatario tiene, en principio, amplia libertad de elección entre la aceptación y el rechazo (De la Puente y La Valle 2003, 654).

Recapitulando lo expuesto, cabe decir que el contrato por adhesión, considerado en sí mismo, es una manera de contratar en la cual, sin perderse la autonomía privada manifestada por la libertad de conclusión del contrato, la determinación de las conclusiones del mismo es hecha unilateralmente y exclusivamente por una de las partes y plasmada en su oferta, para que la otra parte, o sea el destinatario, decida a su solo criterio contratar o no en tales

condiciones. En el primer caso, aceptará la oferta; en el segundo caso, la rechazará (De la Puente y La Valle 2003, 655).

5. LOS CONTRATOS VÍA INTERNET.-

El Profesor Menéndez Mato, indica que no es conveniente utilizar una clasificación cerrada de aquel tipo de contratación que pueda realizarse a través de internet, pero en su libro el contrato vía internet, ofrece una clasificación que será relevante para la presente Investigación.

Según el autor antes citado, que analiza al contrato informático, contrato electrónico, contrato telemático, contrato on line y contrato digital. Todos ellos salvo el denominado contrato informático se encuentran en una relación más o menos concéntrica. Es decir, el más amplio de ellos, que englobaría, a los restantes por su mayor especificidad, sería el contrato electrónico y así sucesivamente respetando el orden en que han sido enunciados. El presente desarrollo es una copia literal del libro citado en este párrafo (Menéndez Mato 2008, 159-170):

- **CONTRATO INFORMÁTICO.-** Inicialmente resultaba usual el empleo de la expresión “contrato informático” para referirse a aquel tipo de contratación en el que el objeto está representado por un bien o un servicio de carácter informático. En cuanto al tipo contractual en sí mismo no resulta tan relevante, pudiendo tratarse de compraventas, arrendamientos, así como otras figuras nuevas nacidas de las prácticas más recientes. Por lo que respecta al objeto del contrato, podría tratarse de bienes- como de hardware como de software-como de servicios.

Sin embargo pronto aparecieron autores que se centraron en distinguir entre contrato informático y contrato con objeto informático y contrato de informática. Este último correspondería en el descrito en el párrafo precedente, en cuanto al primero, denominan como tal al contrato que se ha perfeccionado mediante ayuda de medios informáticos.

Sin embargo hay otro sector de la doctrina que prefiere mantener el significado original asignado al “contrato informático”- es decir, en cuanto a poseedores de un objeto informático- y decide calificar de “contrato electrónico” a aquel cuya conclusión se ha operado gracias a la intervención de procedimientos informáticos u otros medios electrónicos. Esta opción será la escogido en este trabajo, de modo que cuando se hable de contrato informático se hará referencia a aquel cuyo objeto es de naturaleza informática, por lo que se respeta el origen histórico de la denominación “contrato informático”.

- **CONTRATO ELECTRÓNICO.-** Se ha reservado la expresión “contrato electrónico” para referirse aquel conjunto de contratos para cuya conclusión se emplean medios o procedimiento electrónicos. Pese a la aparente claridad de la definición, ha de hacerse referencia al menos a tres cuestiones respecto del calificativo “electrónico” aplicado a un contrato.

En primer lugar, cabría plantearse si cuando se habla de procedimientos informáticos sería lo mismo que decir medios o procedimientos electrónicos. La segunda de las cuestiones es la de si cabe ofrecer otra aceptación del significado de la expresión de acuerdo a la cual por el “contrato electrónico” se haría referencia al contrato propio de comercio electrónico, para concluir afirmando que cuando se contrate en el entorno de dicho comercio se dará nacimiento a un contrato electrónico. Finalmente, la tercera de las cuestiones surge en relación a si debe entenderse por contrato electrónico necesariamente un contrato concluido a distancia.

Respecto de esta última puede ya responderse afirmando que una cosa no tiene porqué conllevar la otra. Es decir, existen contratos perfeccionados mediante procedimientos electrónicos entre partes que se encuentran físicamente presentes, y por el contrario otros contratos electrónicos se concluyen a distancia. A este último tipo de

contrato se le aplicará la específica denominación de “contrato telemático”. Además podría, incluso, hablarse de “contrato recogido en forma electrónica”, pese a que su conclusión haya sido previamente mediante un intercambio verbal de la oferta y la aceptación entre partes físicamente presentes. De todos modos, cuando para la perfección de un contrato se recurre a técnicas electrónicas, es porque ésta tiene lugar entre las partes que no se hallan físicamente presentes.

En cuanto al primer tema, el hecho es que cuando se habla de procedimientos se está haciendo referencia a un fenómeno más amplio que el correspondiente a los medio informáticos. De este modo, los últimos se englobarían dentro de la categoría de los medios electrónicos, en la que además de integrarse, por ejemplo la comunicación entre ordenadores, también estará presentes los medios como el fax o el télex.

Se puede decir que el adjetivo “electrónico” finalmente reduce su aplicación a la existencia de tratamiento o almacenamiento de datos; y que esto no lo hace ni el fax ni el télex. Pero esto no quiere decir que no sean medios de comunicación electrónicos, por lo que en sentido genérico también ellos serían contratos electrónicos.

Se manifiesta en principio, en desacuerdo a concebir al contrato electrónico en el seno del comercio electrónico. Por un lado, debido a los problemas que ha planteado, plantea y planteara el concepto de “comercio electrónico”; por lo que estos mismos problemas se trasladarían a esta acepción contractual. Por otro, un contrato sobre comercio electrónico podría concluirse mediante una contratación típica, entre partes presentes físicamente y tras meses de negociación.

Una síntesis contenida en la Ley de Servicios de la Sociedad de la Información nos informa que, el contrato celebrado por vía electrónica o contrato electrónico, es todo aquel contrato, en el que la

oferta y la aceptación se transmiten por medio de equipos electrónicos de tratamiento y almacenamiento de datos, conectados a una red de telecomunicaciones (Apúd. Del Peso Navarro y otros 2010, 14).

En cuanto a la manifestación de voluntad en que consiste la aceptación, existen en la red variadas posibilidades, entre las cuales encontramos el pulsar “click” sobre el icono de aceptación, que deben siempre conllevar la expresión de consentimiento expreso y por último, en ningún caso permiten dar relevancia al silencio como forma de aceptación (Barral Viñals 2004, 47).

- **CONTRATO TELEMÁTICO.-** Todo contrato electrónico cuya perfección es operada a distancia recibe la calificación de “contrato telemático”. En cuanto al adjetivo “telemático”, indica que es el resultado de la contracción semántica de los términos de “telecomunicaciones” e “informática”; y sería ejemplos de contratos telemáticos los concluidos mediante el empleo de internet o intranet entre partes físicamente distantes.

Sobre esta figura, no importa tanto detenerse acerca de la determinación del momento exacto de la aparición de la telemática sino de nuevo, poner énfasis en la duda de si es apropiado incluir todas las técnicas electrónicas (no solo las informáticas) de comunicación a distancia para la calificación del contrato como “telemático”. En este caso el empleo de telemático se circunscribe al empleo de medios de procesamiento de datos y al envío de estos datos directamente, siendo accesible su contenido sin necesidad de ser reproducidos sobre un papel, por lo que no lo serían ni los incluidos vía télex ni mediante fax.

- **CONTRATOS ON LINE.-** Pueden señalarse dos acepciones distintas respecto de este contrato. La primera, más genérica, entendería por contrato on line a todo aquel cuya perfección ha tenido

lugar en línea o red. De esta forma lo serían todos los concluidos a través de internet o desde una intranet.

Para la segunda acepción más restrictiva, un contrato on line sería aquel perfeccionado desde una página web y practicable en masa gracias a los programas informáticos de contratación, podría de este modo decirse que un contrato concluido entre dos sujetos directamente mediante intercambio de sus respectivas oferta y aceptación mediante el uso de correo electrónico o videoconferencia o chat no son contratos on line.

- **CONTRATO DIGITAL.-** La expresión “contrato digital” quedará reservada en el presente estudio al contrato que para su conclusión haya acudido al uso de la firma digital.

Como se advirtió en el capítulo II, para poder acceder a una cuenta en una página web de contenido social o red social, las mismas páginas se agencian de contratos vía internet; pero no cualquiera de estos contratos, en el desarrollo de este trabajo llegamos a la conclusión de que el contrato que estás necesitan son estrictamente los contratos on line.

Ahora bien, nos encontramos en la doctrina con el detalle que algunos autores consideran que los contratos on line cuya naturaleza no sea contraprestativa, no son contratos propiamente dichos; a continuación nuestra postura al respecto:

Aclaremos primero la definición concreta de lo que es un contrato: por definición es un acto jurídico, por el que, a través de un acuerdo de voluntades, entre 2 o más partes, donde una parte es el oferente, quien ofrece un producto o un servicio; mientras que la otra parte, el aceptante, una vez que, valga la redundancia, acepta la oferta se convierte en dueño del bien o acreedor de los servicios a cambio de una prestación dineraria, o en algunos casos de otra índole (como en especie por ejemplo).

En el mundo de la sociedad de la información, los contratos on line, que como se viene repitiendo es aquel perfeccionado a través de una página de internet, según nuestro desarrollo propio, inspirado en la sub-clasificación respecto de la prestación de los contratos, esbozada por el profesor peruano de la Puente y la Valle, podrían dividirse en dos Clases:

- Contratos on line de prestaciones bilaterales.- el que por tradición de clasificación contiene prestaciones recíprocas, por ejemplo, una página de internet que ofrece bienes, el aceptante decide comprar uno de aquellos bienes ofrecidos, para ello introduce el número de su tarjeta de crédito y la clave en la referida página y paga por el bien, mientras el transferente queda obligado a su entrega; entonces nos encontramos en el caso de bien a cambio de prestación dineraria.
- Contratos on line de prestaciones unilaterales.- son aquellos contratos en los que una sola parte de la relación contractual ofrece un bien o servicio a favor de la otra, sin mediar pago alguno por ello, en este caso el ejemplo sería las páginas web de contenido social o redes sociales que ofrecen una cuenta de usuario al aceptante, en donde el aceptante sólo tiene que decidir si acceder a una cuenta o no, sin contraprestación alguna a cambio.

¿Entonces, un contrato on line por ser de prestaciones unilaterales, deja de ser contrato?

La respuesta es no, por el sólo hecho de ser de prestaciones unilaterales el contrato on line no pierde su naturaleza contractual, sino ¿Qué pasaría en los casos civiles como la donación?.

De otra parte, el caso en discusión es diferente respecto de las redes sociales, pues, se sabe que no reciben prestación de ninguna índole por parte de los usuarios aceptantes en la relación contractual, pero si lo queremos ver desde el punto de vista lucrativo, estas páginas reciben buenas cantidades de dinero por parte de sus patrocinadores quienes publicitan sus productos y servicios a través de estas mismas

páginas a sus usuarios. Ergo, podemos concluir sobre este tema que, a pesar que los usuarios de las páginas web de contenido Social no aportan directamente una prestación dineraria a los administradores de las mismas, indirectamente contribuyen a su enriquecimientos pues, por lógica, mientras más usuarios tenga una página web, más patrocinadores tendrá y contará con más dinero.

Agregaremos que, como ya hemos venido afirmando existen páginas web de contenido social que pretenden aprovecharse de la información personal que les brindan sus usuarios, a continuación desarrollaremos como es que las redes sociales podrían hacerlo incluyendo determinadas cláusulas en sus contratos on line para acceder a una cuenta.

6. LAS CLÁUSULAS AMENAZADORAS DE DERECHOS.-

Primero, nos gustaría iniciar precisando que, tras la búsqueda del término cláusulas amenazadoras de derechos en la doctrina, lo más que encontramos fueron textos del derecho canónico donde se discutía sobre estas cláusulas respecto de amenazas directas respecto de derechos fundamentales; tales como reyes amenazando con despojar de la vida a sus fieles o monarcas amenazando con invadir territorios extranjeros, y otros casos similares (ubicándonos en el medievo y tiempos del renacimiento).

Lo relatado anteriormente no corresponde en lo que actualmente queremos delinear como cláusula amenazadora de derechos, aquellas eran amenazas propiamente dichas por parte de seres humanos, en aquel tiempo, con poder y dinero suficiente para amenazar y cumplir con las referidas amenazas a su antojo.

Nos avocaremos entonces, a desarrollar el concepto de cláusulas contractuales, para llegar así a la definición que hemos adoptado de cláusulas amenazadoras, y respecto de aquellas las que se encuentran contenidas en los contratos on line de las redes sociales.

El contrato, por ser la exteriorización de la voluntad común de las partes, debe tener una forma y un contenido. Esto es lo que se denomina la estructura del contrato (de la Puente y la Valle 2003, 39). Dentro de esta estructura contractual el contenido del

contrato se exterioriza con la manifestación de la voluntad a través de las cláusulas contractuales, que sirven además para ordenar el contenido contractual, con la peculiaridad que cada cláusula se configura como un precepto negocial autónomo, o sea que su verdadera utilidad radica en que cada una de ellas, pueden constar de uno o más párrafos o disposiciones, tengan determinado efecto jurídico (de la Puente y la Valle 2003, 39).

Existen distintas clasificaciones de cláusulas, respecto de las amenazadoras específicamente, no hemos encontrado un concepto doctrinario, distinto del mencionado al principio, sobre el cual nos podamos referir, pero nos hemos basado en el concepto conocido de cláusula abusiva para derivar en el de cláusula amenazadora.

Son cláusulas abusivas aquellas que, son interpretadas como cláusulas excesivas, demasiado onerosa, que reporta una ventaja indiscriminada a favor de uno de los contratantes en menoscabo del otro (de la Puente y la Valle 2003, 784).

Así es como concluimos que las cláusulas amenazadoras son aquellas que, reportan una ventaja indiscriminada a favor de uno de los contratantes en posible menoscabo del otro. Podemos entonces asegurar que el término “en posible”, reporta un daño en potencia, que podría manifestarse en un futuro incierto, que por atemporal, no deja de reportar peligro.

Lo antes expresado se explica con el siguiente cuadro:

Cláusulas Lesivas: Cláusulas que reportan una ventaja indiscriminada a favor de uno de los contratantes en posible menoscabo del otro.
Cláusulas Amenazadoras: Cláusulas que reportan una ventaja indiscriminada a favor de uno de los contratantes en menoscabo del otro.

Tenemos como objetivo de todo lo expresado hasta ahora, llegar a incluir cuales son las cláusulas amenazadoras de derechos que hemos encontrado en las páginas web de contenido social o redes sociales. Para la presente Investigación encontramos este tipo de cláusulas en las siguientes páginas web: Hi5, Badoo Reddit y Digg. Las cláusulas encontradas en dichas páginas fueron las siguientes:

- Hi5 (CONTENIDO EN SU POLÍTICA DE PRIVACIDAD-
http://www.hi5.com/terms_of_service.html?#privacy_policy)

Uso De La Información

(...) Hi5 puede analizar cualquier información recolectada para sus propios propósitos internos. Además, hi5 puede quitar información que identifique individualmente de la información recolectada para volverla anónima. hi5 puede usar la información anónima para cualquier propósito y revelar la información anónima a su sola discreción.

- Badoo (CONTENIDO EN SU POLÍTICA DE PRIVACIDAD-
<http://badoo.com/privacy/>)

Uso De Sus Datos Personales

(...) Finalmente, le informamos que Badoo puede utilizar el contenido que usted haya publicado en las zonas de libre acceso de la red social de Badoo para su incorporación en aquellos materiales publicitarios y promocionales que puedan publicarse en los sitios web de nuestros socios por lo que usted acepta esta posibilidad y autoriza a Badoo a utilizar tales contenidos con ese fin.

- REDDIT (CONTENIDO EN SU POLITICA DE PRIVACIDAD-
<http://www.reddit.com/help/privacypolicy>)

Contenido original:

In addition, we reserve the right to use the information we collect about your computer, which may at times be able to identify you, for any lawful business purpose, including without limitation to help diagnose problems with our servers, to gather broad demographic information, and to otherwise administer our Website.

While your personally identifying information is protected as outlined above, we reserve the right to use, transfer, sell, and share aggregated, anonymous data about our users as a group for any business purpose, such as analyzing usage trends and seeking compatible advertisers and partners.

In addition, as our business changes, we may buy or sell various assets. In the event all or a portion of the assets owned or controlled by Service Provider, its parent or any subsidiary or affiliated entity are sold, assigned, transferred or acquired by another company, the information from and/or about our Website users may be among the transferred assets.

Traducción:

Además, nos reservamos el derecho a utilizar la información que recopilamos de tu equipo, que, a veces, puede ser capaz de identificarte, para cualquier finalidad legal comercial, sin limitaciones, para ayudar a diagnosticar problemas con nuestros servidores, para recopilar información demográfica, y para administrar nuestro sitio web de cualquier manera.

Mientras que tu información personal este protegida como se describe anteriormente, nos reservamos el derecho a usar, transferir, vender y compartir datos agregados y anónimos de nuestros usuarios, para cualquier finalidad comercial, como el análisis de las tendencias de uso y la búsqueda compatibles de anunciantes y socios.

Además, conforma cambie nuestro negocio, podemos comprar o vender varios activos. En el caso de la totalidad o una parte de los activos propiedad o controlados por el proveedor de servicio, la empresa matriz, cualquier subsidiaria o entidad afiliada sean vendidos, cedidos, transferidos o adquiridos por otra empresa, la

información perteneciente y / o concerniente los usuarios de nuestro sitio web puede formar parte de los activos transferidos.

- DIGG (CONTENIDO EN LA POLITICA DE PRIVACIDAD DE DIGG <http://about.digg.com/privacy>)

Contenido original:

Digg Personnel: Digg personnel and authorized consultants and/or contractors may have access to user information if necessary in the normal course of Digg business.

Business Transfers: In some cases, we may choose to buy or sell assets. In these types of transactions, user information is typically one of the business assets that is transferred. Moreover, if Digg, or substantially all of its assets, were acquired, user information would be one of the assets that is transferred.

Social sharing of data: Digg allows other users to browse stories that you have Dugg, submitted or commented on. This information is made available publicly via your User Profile, on Digg Labs (labs.digg.com). Digg may choose to post this data on other site features.

Traducción:

Personal de Digg: El personal de Digg y sus consultores autorizados y / o contratistas podrán tener acceso a la información del usuario si es necesario en el curso normal del negocio de Digg.

Transferencias de negocio: En algunos casos, podemos optar por comprar o vender activos. En este tipo de transacciones, la información del usuario es típicamente uno de los activos del negocio que es transferido. Por otra parte, si Digg, o sustancialmente todos sus activos, fueren transferidos, la información del usuario será uno de los activos que se transfieran.

Datos compartidos en las redes sociales: Digg permite a otros usuarios navegar por las historias en ella contenidas (sentido figurativo de Dugg), que se hubiere publicado o comentado. Esta información está a disposición del público a través de tu perfil de

usuario, en Digg Labs (labs.digg.com). Digg puede elegir entre poner estos datos en las características de otros sitios.

De la lectura literal de éstas cláusulas podemos deducir que a pesar que las mismas políticas de uso o privacidad de las páginas anteriormente mencionadas, afirman, en principio que no poseen derechos sobre los contenidos o fotos digitales adheridas a su red; también incluyen éstas cláusulas que autorizan a los dueños de las páginas desde volver anónima la información y hacer uso de ella a su discreción (en el caso del Hi5) hasta seleccionar información de las zonas de libre acceso o simplemente transmitida a la página para uso comercial o promocional de los socios de las mismas páginas (en el caso Badoo), o comercializar tu información como un activo de la página (en los casos de Reddit y Digg) recalando que el usuario conoce los términos y los acepta.

Esto tiene relación directa con lo afirmado en el sub capítulo relacionado a las páginas web de contenido social o redes sociales respecto a que estas páginas se encargan de recopilar datos de carácter personal de sus usuarios, estos contenidos se vuelven amenazadores con la presencia de este tipo de cláusulas en sus contratos on line, esta es la base del problema encontrado por nosotros para la presente investigación.

6.1. LAS CLÁUSULAS AMENAZADORAS RESPECTO DEL DERECHO DE AUTODETERMINACIÓN INFORMATIVA.-

Ahora que sabemos que son las cláusulas amenazadoras, como se manifiestan en la sociedad de la información y en que redes sociales, es hora de preguntarnos, ¿Qué clase de derechos amenazan estas cláusulas?. Desarrollaremos a continuación una cita textual de lo que nuestro Tribunal Constitucional peruano ha denominado el derecho de autodeterminación informativa, en el expediente N° 1797-2002-HD/TC:

El derecho reconocido en el inciso 6) del artículo 2° de la Constitución es denominado por la doctrina derecho a la autodeterminación informativa y tiene por objeto proteger la intimidad, personal o familiar, la imagen y la

identidad frente al peligro que representa el uso y la eventual manipulación de los datos a través de los ordenadores electrónicos. Por otro lado, aunque su objeto sea la protección de la intimidad, el derecho a la autodeterminación informativa no puede identificarse con el derecho a la intimidad, personal o familiar, reconocido, a su vez, por el inciso 7) del mismo artículo 2° de la Constitución. Ello se debe a que mientras que este protege el derecho a la vida privada, esto es, el poder jurídico de rechazar intromisiones ilegítimas en la vida íntima o familiar de las personas, aquel garantiza la facultad de todo individuo de poder preservarla controlando el registro, uso y revelación de los datos que les conciernen.

Tampoco el derecho a la autodeterminación informativa debe confundirse con el derecho a la imagen, reconocido en el inciso 7) del artículo 2° de la Constitución, que protege, básicamente la imagen del ser humano, derivada de la dignidad de la que se encuentra investido; mientras que el derecho a la autodeterminación informativa, en este extremo, garantiza que el individuo sea capaz de disponer y controlar el tipo de datos que sobre él se hayan registrado, a efectos de preservar su imagen derivada de su inserción en la vida en sociedad.

Finalmente, también se diferencia del derecho a la identidad personal, esto es, del derecho a que la proyección social de la propia personalidad no sufra interferencias o distorsiones a causa de la atribución de ideas, opiniones, o comportamientos diferentes de aquellos que el individuo manifiesta en su vida en sociedad.

Del desarrollo y el análisis del derecho a la autodeterminación informativa, podemos asegurar que las cláusulas amenazadoras están dirigidas específicamente contra ese derecho de los usuarios de las páginas web de contenido social o redes sociales.

Pero, ¿Se justifica que las prestaciones unilaterales por parte de las páginas web de contenidos social incluyan cláusulas amenazadoras en sus contratos on line?

No, como ya dijimos en acápite anteriores, la falta de prestación dineraria directa, se justifica con la publicidad con la que bombardean a sus usuarios, como primer sustento de esta respuesta. Por otro lado, si lo analizamos de un punto de vista más jurídico, veremos que desde una perspectiva de los derechos humanos, uno evolutivo y vanguardista, pretende defender, en este caso a los usuarios de las redes sociales, del “peligro en potencia”, que es en sí lo que representan las cláusulas amenazadoras de derechos.

En un caso hipotético, encontramos el ejemplo que inspiró la presente tesis, en el cual una persona colgó una foto suya en una red social, una foto en la cual se encontraba sonriendo; unos meses después un amigo suyo le informo que su foto se encontraba circulando en la red, tras una breve búsqueda de productos de limpieza bucal, encontró su foto en una propaganda donde, el aparecía en la versión de “antes” de usar el producto y una joven agraciada luciendo una sonrisa con los dientes relucientes aparecía en la versión de “después”.

Se puede afirmar entonces, que desde ningún punto de vista se puede justificar la inclusión de estas cláusulas en ningún tipo de contratos on line. Tras esta afirmación ya hemos esbozado también cual podría ser la solución ante estos casos. En el capítulo siguiente desarrollaremos cual podría ser la solución legal a desarrollarse ante los casos de amenaza de los derechos de autodeterminación informativa con relación a los usuarios de las redes sociales.

CAPITULO IV

LA SOLUCIÓN LEGAL QUE SE DEBE ADOPTAR FRENTE A LAS CLÁUSULAS AMENAZADORAS DE DERECHO DE AUTODETERMINACIÓN INFORMATIVA CONTENIDA EN LOS CONTRATOS ON LINE EN LAS PÁGINAS WEB DE CONTENIDO SOCIAL O REDES SOCIALES

5. GENERALIDADES.-

En el desarrollo de nuestros aspectos metodológicos desarrollamos la hipótesis que surgió para hacer frente al problema de las cláusulas amenazadoras de derecho de autodeterminación informativa en los contratos on line de las redes sociales (Hi5, Badoo, Reddit y Digg), está sugiere la creación de un organismo internacional que se encargue de: prohibir la inclusión de cláusulas amenazadoras, e inclusive lesivas de derechos; revisar los contratos a través de internet, en especial los on line, establecer fórmulas de solución de conflictos (como veremos en este capítulo los denominados MARCs) y establecer sanciones cuando no se cumplan alguno de los 3 supuestos anteriores.

6. EL POR QUÉ DE UN ORGANISMO INTERNACIONAL

Ahora, nos concierne citar algunos de los principales problemas del uso del internet y que justifica nuestra proposición de un organismo internacional, el cual es:

- El conflicto de jurisdicción.-

Un sistema global ya abierto como el internet lleva implícita la realización entre personas que pueden encontrarse a miles de kilómetros de distancia y estar sujetas a leyes muy distintas. ¿Qué pasa si tenemos algún conflicto legal con alguna de ellas? ¿En qué país plantearíamos el reclamo? ¿Cuáles son los tribunales competentes? (Torres Álvarez 2005, 43)

Esta discusión no está cerrada. En la práctica se presentan muchos problemas y nada indica que vayan a desaparecer en corto plazo (Torres Álvarez 2005, 43).

De las tres primeras interrogantes planteadas por Torres Álvarez es de donde tomamos el primer punto de sustento de la necesidad de un organismo internacional para la solución de los conflictos que se configuran o podrían hacerlo a través de internet. Sería verdaderamente difícil que frente a un conflicto legal, alguna de las partes pudiera determinar la jurisdicción y competencia de los tribunales a los que les correspondería dirimir respecto del conflicto. Por otro lado en el hipotético caso de que lo anterior sucediera, la parte que determinaría la jurisdicción o competencia sería, probablemente, la mayoría de las veces, la parte más fuerte de la relación contractual, en estos casos los representantes de las páginas web de contenido social o redes sociales, lo que evidentemente dejaría en desventaja al usuario aceptante; por lo que, esta perspectiva no sería una solución justa.

- La cooperación internacional.-

Para entenderla debemos saber cuáles son sus características, porque es así que surge la cooperación internacional (Gómez 2004, 140):

- Asistencialista
- Asimétrica
- Dirigida a receptores pasivos
- Coyuntural
- Condicionada

La cooperación internacional juega para nosotros su labor en lo relacionado a su característica coyuntural; puesto que el fenómeno de internet es una circunstancia propia del desarrollo de la ciencia y la tecnología, entonces en la actualidad juega un papel importante por lo que deberá ser objeto de la cooperación internacional.

- La supranacionalidad de los organismos internacionales.-

Como sabemos de la definición de supranacionalidad, en el aspecto del derecho internacional, es aquella que puede tener incidencia o, como denominamos con anterioridad jurisdicción, sobre varios países; en este caso sobre aquellos que integren el organismo internacional.

Ahora bien dentro de la supranacionalidad encontramos que se resolvería el conflicto de jurisdicción que podría crear el uso de internet; agregaremos aquí lo que encontramos en estudios de índole diplomática sobre un beneficio de las políticas exteriores y, para la presente investigación, en extensión de los organismos de carácter supranacional:

- El beneficio de la integración.-

Permite una forma avanzada de cooperación y ayuda mutua, concede además la concertación de políticas y ampliación de mercados, por último es la única alternativa actualmente previsible y válida en fortalecimiento político y económico (García Bedoya 1992, 74).

Nos conviene resaltar que el organismo internacional que proponemos crear contará con este beneficio si se logra como lo dice el profesor García Bedoya, la forma avanzada de cooperación y ayuda mutua, si desarrolla las políticas necesarias para la protección de los usuarios de aquellas páginas que pretendan vulnerar el derecho de autodeterminación informativa; a través del consenso de sus Estados miembro; y el desarrollo del fortalecimiento político entre estos mismos Estados.

- La Capacidad de los organismos internacionales.-

De esta característica, podemos citar un ejemplo, la ONU tiene derechos y obligaciones distintos a los de los Estados, es decir, que goza de una personalidad internacional, lo que significa que es un sujeto de derecho internacional, que tiene capacidad de adquirir derechos, contraer obligaciones internacionales y que tiene competencia para prevalerse de sus derechos por la vía de reclamación internacional (Pinto 2009,15).

El ente propuesto por este trabajo, debería contar con la denominada personalidad internacional, especialmente en el sentido de contraer obligaciones.

7. EL ORGANISMO INTERNACIONAL PROPIAMENTE DICHO: ORGANIZACIÓN MUNDIAL DE REVISIÓN DE CONTRATOS VÍA INTERNET Y SALVAGUARDA DE LOS DERECHOS DE LOS USUARIOS.

Bien sabemos que, aún no existen organizaciones internacionales acogidas a nivel mundial, es decir, que engloben a todos los países contenidos en el globo, de los cursos de derecho internacional recordamos a aquella característica denominada como universalidad. Ahora bien, aunque la premisa que antecede es una verdad irrefutable, con el presente trabajo se pretende, un organismo que, aunque no sea acogido por todos los países del mundo, sea acogido por un número considerable, y en especial llame la atención de los países desarrollados para que de manera complementaría ayuden a aquellos en vías de desarrollo para la implementación de las normas que se requieren para poder acogerse a este organismo.

Como bien sabemos, una organización internacional debe tener premisas básicas para su constitución y organización, éstas serían las siguientes:

9. Objetivos

- a. Revisar de los contratos a on line contenidos en las redes sociales para el acceso a una cuenta, con la finalidad de evitar la inclusión de cláusulas amenazadoras contra el derecho de autodeterminación informativa.
- b. Mantener un centro de arbitraje, y otro de conciliación para la solución de conflictos derivados de cláusulas ambiguas, que en determinado momento pudieran llegar a ser amenazadoras contenidas en los contratos on line de las redes sociales.
- c. Contar con una comisión fiscalizadora, que se encargue de revisar periódicamente que las redes sociales no vuelvan a incluir estas cláusulas que sean explícitamente amenazadoras, de manera que, sí se diera el supuesto, se harían acreedores de sanciones.

- d. Sancionar a las páginas web que recaigan en la conducta amenazadora, sanciones que podrían llegar a ser pecuniarias.

10. Miembros integrantes

Serán aquellos países que se constituyan al momento de la creación del organismo, y los que se adhieran con el tiempo.

11. Comisiones integrantes:

- a. Comisión de asesoría y orientación al usuario
- b. Comisión revisora
- c. Comisión de atención de reclamos y denuncias
- d. Comisión de asuntos legales
- e. Comisión de conciliación
- f. Comisión de arbitraje
- g. Comisión fiscalizadora
- h. Comisión sancionadora

12. Áreas de acción

Geográfica:

- a. Latinoamérica.
- b. Norteamérica.
- c. Unión Europea (Europa).
- d. Asia (No Comunista).
- e. África.
- f. Australia.

13. Funciones

- a. Legislativas.- para proveer al órgano de normas y reglamentos que permitan su funcionamiento, dicten las directrices por ella trazadas para la inclusión de leyes que permitan su funcionamiento efectivo y eficaz en cada uno de los países y demás eventualidades que se presenten durante su funcionamiento.

- b. Sociales.- para la protección de los usuarios (personas naturales), frente a las redes sociales y el tratamiento de dichos usuarios como iguales respecto del amparo del derecho de autodeterminación informativa.
- c. De seguridad jurídica.- para establecer un orden frente a los posibles abusos que se pudieren cometer en contra de las personas naturales.

14. Políticas.-

- a. Igualdad
- b. Transparencia
- c. Buena fe

15. Proyectos y Fondos.-

Como todo ente internacional, para mantener a flote su organización, actualizado su trabajo, sus políticas y sus necesidades de acuerdo a cada circunstancia, los miembros del ente, en coordinación con sus países conformantes, deberá mantener actualizado un régimen de proyectos enfocados a la protección de los derechos que defiende.

16. Relaciones internacionales.-

Deberá mantener una coordinación cercana tanto con sus países miembro, como con aquellos otros entes internacionales encargados de la protección de otros derechos humanos y afines en general.

8. LA NORMATIVIDAD SOBRE LA CUAL DEBERÁ REGIRSE EL ORGANISMO INTERNACIONAL, DE LAS DIRECTIVAS DE LA UNIÓN EUROPEA:

Al haberse desarrollado el como deberá ser desarrollado el organismo internacional, ahora proponemos bajo que directrices debería trabajar, bajo que modalidades y sobre qué base debe erigirse.

Según nuestra hipótesis la primera labor que debiere efectuar nuestro organismo es la prohibición de la inclusión de cláusulas amenazadoras en cualquier

contrato on line de cualquier red social; claro está que éstas son las primeras en incluirse por ser la materia específica de nuestra investigación pero bien podría este mismo organismo, encargarse de cualquier otro tipo de cláusula o contenido contractual que pudiere perjudicar a los usuarios de las mismas, como ejemplos podríamos citar la inclusión de cláusulas lesivas, abusivas, leoninas, entre otras.

La segunda labor, y una de las principales, sería la revisión de todos y cada uno de los contratos on line para verificar que la prohibición señalada en el párrafo anterior sea cumplida. Esto sería la base fundamental de un sistema que forme parte de la sociedad de la información, el carácter restrictivo de las bases de nuestro organismo, permitiría la seguridad jurídica del derecho de autodeterminación informativa de los usuarios de las redes sociales.

Pero como sabemos, este control previo no siempre será suficiente para la salvaguarda de los derechos de los usuarios, y menos en un medio tan innovador y lleno de tecnologías de creación constante como lo es el internet, siempre habrá alguna manera de saltar el control previo que se pudiere establecer, por lo que también se contemplaría como parte de las funciones de nuestro organismo internacional la propuesta y solución de los conflictos que pudieran desprenderse de los daños que se pudiera cometer contra alguna persona usuaria. Pero, ¿Por qué decimos daños? Si bien el concepto de la cláusula amenazadora, que es la única que hemos desarrollado en el presente trabajo, reporta una ventaja indiscriminada a favor de una de las partes contratantes en posible menoscabo de la otra, cuando este posible menoscabo se materializa se convierte en un daño real. No es necesario explicar entonces que las demás cláusulas mencionadas en el primer párrafo de este subtítulo también son susceptibles de causar daños.

Para la solución de las controversias que pudieren presentarse debemos acudir a lo que la doctrina mejicana conoce como ciberjusticia, y dentro de ella le factor conocido como cibertribunales; los cuales tienen como propósito servir de mediadores en los litigios derivados de internet (comercio electrónico, propiedad intelectual, protección de la vida privada – lo que en la presente investigación venimos tratando con la autodeterminación informativa-, etc.). Estos tribunales

permiten a las partes interesadas elegir entre una cantidad de expertos (en ocasiones académicos) aquellos que pondrán soluciones a los conflictos, sustentados en los textos internacionales más avanzados de la materia (Téllez Valdés 2009, 42)

Pero ¿Cómo es que debieren operar los cibertribunales?, pues mediante los sistemas alternativos de solución de disputas, también conocidos como métodos alternativos de resolución de conflictos, a los cuales ya referimos como MARCs, como lo son; el arbitraje, la mediación y la conciliación, los cuales presentan claros beneficios y ventajas prácticas en relación con los procesos estatales, en particular para la solución de conflictos dentro de estructuras digitales (Téllez Valdés 2005, 43).

Algunos de sus principales beneficios son:

- Autonomía de la voluntad de las partes.
 - Posibilidad de elegir un conciliador o árbitro neutral entre otros países.
 - Posibilidad de utilizar tecnologías e infraestructuras tecnológicas muy avanzadas.
 - Procesos extrajudiciales muy cortos, simples y flexibles (manteniendo todos los derechos de las partes).
 - Trabajo y discusión en tiempo real al tratarse de solución de conflictos derivados de los contratos on line.
 - No hay posibilidad de prolongar los procesos mediante apelación.
 - Costos mucho más bajos.
 - Privacidad y confidencialidad durante el proceso y después de él.
- (Téllez Valdés 2005, 43)

Por último, para que las redes sociales que incurrieron en falta y provocaron daño a alguno de sus usuarios, el organismo internacional debiera proponer un sistema de sanciones muy aparte de la indemnización que debieren pagar a los usuarios; esto con el propósito de evitar que las redes sociales (o cualquier otro tipo de página web) reiteren en la comisión de daños hacía los usuarios.

La Comunidad Europea desarrollo algunas directivas respecto del tratamiento de los datos personales de las personas naturales (en este caso los usuarios de las páginas web de contenido social o redes sociales), por lo que el organismo internacional, debiere ceñirse a dichas directivas, las cuales se desarrollan a continuación:

- **Directiva 95/46/CE del Parlamento Europeo y del Consejo de la Unión Europea, del 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.**

Algunos alcances importantes respecto de esta directiva serían los siguientes:

Artículo 1.

Objeto de la Directiva

1. Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales.

La directiva refiere al derecho a la intimidad, que para nuestro caso podría ser reemplazado por el derecho de autodeterminación informativa, (ligado a los datos personales, que serían relevantes), que como ya se desarrollo con anterioridad, se trata de un derecho que cubre integralmente a los usuarios respecto de la información vertida en el internet; derecho desarrollado por nuestro Tribunal Constitucional, y en el presente trabajo en nuestro Capítulo III, parte 3, y que, también se trata de un derecho fundamental, por lo que se calzaría de modo más adecuado.

Además que sería correcta la aplicación del derecho de autodeterminación informativa, es necesario saber que entiende la directiva en comento respecto de los datos personales y los ligados a estos.

Artículo 2

Definiciones

- a) Datos personales.- toda información sobre una persona física identificada o identificable (el interesado); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social.

Estos datos personales, se encuentran inmersos en el derecho de autodeterminación informativa, si nos colocamos en un supuesto analógico, por lo que calzan de manera perfecta para el ámbito de nuestra investigación.

- b) Tratamiento de datos personales.- tratamiento: cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción.
- c) Fichero de datos personales (fichero): todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

Estos datos serán fundamentales en el tratamiento del organismo internacional, pues son aquellos conceptos que se manejan diariamente en las denominadas redes sociales y aquellos que podrían ser susceptibles de vulneración.

Por otro lado, otros aspectos relevantes de la directiva para el caso concreto están contenidos en el siguiente artículo:

Artículo 6

1. Los Estados miembros dispondrán que los datos personales sean:
 - a) Tratados de manera leal y lícita;

- b) Recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre Y cuando los Estados miembros establezcan las garantías oportunas.
- c) Adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente.
- d) Exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificadas.
- e) Conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos.

Los 5 principios aquí detallados permitirán un marco sólido respecto del tratamiento transparente, claro y conciso de los datos personales; para que así los usuarios sepan a que atenerse al ingresar este tipo de datos en una red social. Además sirve para que los acuerdos respecto de los datos de carácter personal sean tomados de forma bilateral (entre la persona natural o usuario aceptante y la red social) de manera que sea justa la utilización de estos datos, y con el conocimiento de la persona de los que podrían ser utilizados para fines específicos y que no le causarían perjuicio.

Ahora bien, esta directiva también dispone los supuestos específicos en que podrá disponer de los datos personales, detallados a continuación:

Artículo 7

Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si:

- a) El interesado ha dado su consentimiento de forma inequívoca.
- b) Es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado.
- c) Es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento.
- d) Es necesario para proteger el interés vital del interesado.

Estas normas son de carácter imperativo, prevén que los datos de carácter personal sean utilizados por las redes sociales (en una interpretación restrictiva que calza para nuestra investigación) solo en los casos exclusivos donde la persona dueña de los datos de autorización o para fines específicos que también requieran de su autorización, a nuestro entender, este artículo se encarga de proteger a los usuarios aceptantes de modo que su información sea utilizada de manera lícita.

La información presentada con anterioridad es la específica que nos interesa acerca del tratamiento y la protección de los datos personales que podrían ser tomados de esta directiva en beneficio del organismo internacional que proponemos. Esta directiva también nos propone los principios de seguridad y confidencialidad del tratamiento de los datos de carácter personal (contemplados en su Sección VIII), los cuales también consideramos importantes e incluimos a continuación:

Artículo 16. Confidencialidad del tratamiento

Las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, solo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento o salvo en virtud de un imperativo legal.

Artículo 17. Seguridad del tratamiento

1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de

organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales.

(...)

Por otro lado consideramos conveniente incluir la siguiente información:

TRANSFERENCIA DE DATOS PERSONALES A PAÍSES TERCEROS

Artículo 25. Principios

1. Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de derecho nacional adoptadas con arreglo a las demás disposiciones de la presente directiva, el país tercero de que se trate garantice un nivel de protección adecuado.
2. El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Estas consideraciones están referidas a los países terceros que no pertenezcan, en nuestro caso a nuestro organismo internacional, se debe tomar en consideración que si las redes sociales desean transmitir la información de carácter personal a

algún país o lugar, en donde no goce de suficiente protección deberá existir algún tipo de restricción (como esta) para evitar que los datos sean utilizados de manera errónea o hasta dañosa respecto de sus dueños, la presente consideración se tiene, debido a que existe un precedente de red social, la cual fue considerada en un principio para la presente investigación, denominada SixApart, la cual contenía dentro de sus políticas de privacidad, cláusulas amenazadoras al derecho de autodeterminación informativa, esta red social fue vendida a una compañía japonesa, lo cual no tiene nada de malos, siempre que se sepa, cual será el modo de operar respecto de los datos de carácter personal de los usuarios contenidos en la red social traspasada.

Para terminar con las cuestiones que podrían ser importantes de la presente directiva respecto de nuestra propuesta; nos encontramos con una disposición final que dicta textualmente:

Los Estados miembros adoptarán las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente directiva, a más tardar al final de un período de tres años a partir de su adopción.

No sabemos si el periodo tiempo considerado por esta directiva sea suficiente para la adopción de estas medidas en países como los latinoamericanos, africanos u otros en vías de desarrollo, cuya legislación no es tan avanzada como la europea, pero si consideramos que estas medidas deben ser tomadas en un tiempo prudencial para que la legislación y medidas nacionales se complementen y ayuden al organismo internacional, un periodo que a nuestro entender no debería ser menor a 5 años.

- **Directiva 97/66/CE del Parlamento Europeo y del Consejo de la Unión Europea, del 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.**

Tanto para esta directiva, como para la anterior, el derecho a la intimidad referido en ambas, está referido a lo que nosotros hemos venido desarrollando como el derecho de autodeterminación

informativa que se diferencia de lo que nuestra legislación conoce como intimidad propiamente dicha y nos parece más integral respecto del tratamiento de la información en el internet.

Ahora, lo que esta directiva propone y es relevante respecto de nuestra propuesta de organismo internacional es lo siguiente:

Artículo 2

Definiciones

Se entenderá por:

- a) (...)
- b) Usuario: la persona que utiliza un servicio público de telecomunicación con fines privados o comerciales, aunque no haya contratado dicho servicio.
- c) Red pública de telecomunicación: los sistemas de transmisión y, cuando proceda, los equipos de conmutación y otros recursos que permiten la transmisión de señales entre puntos de terminación definidos por cable, por medios radioeléctricos, por medios ópticos o por otros medios electromagnéticos que se utilizan, total o parcialmente, para la prestación de servicios públicos de telecomunicación.
- d) Servicio de telecomunicación: un servicio cuya prestación consiste total o parcialmente en la transmisión y el envío de señales a través de redes de telecomunicación, excepción hecha de la radiodifusión sonora y de la televisión.

Estas definiciones son más claras en comparación con la directiva anterior, nos brindan los nombres específicos de las partes y los servicios que intervienen en la relación contractual; en este caso las personas naturales serían los usuarios; y el internet será la red pública de telecomunicación; estos datos serán tomados como referenciales para poder entender el contenido que desarrollo la directiva y servirá para nuestra investigación.

Artículo 5

Confidencialidad de las comunicaciones

1. Los Estados miembros garantizarán, mediante normas nacionales, la confidencialidad de las comunicaciones realizadas a través de las redes públicas de telecomunicación y de los servicios de telecomunicación accesibles al público. En particular, prohibirán la escucha, la grabación, el almacenamiento u otros tipos de interceptación o vigilancia de las comunicaciones por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando esté autorizada legalmente.

Volvemos a encontrar aquí el principio de confidencialidad, que debe ser resguardado para que sean los usuarios exclusivamente quienes permitan su difusión o propagación. Entonces será nuestro organismo internacional el encargado de esta salvaguarda, y controlar que sus Estados miembros se sujeten a las referidas normas, e implementen sus supuestos.

- **Directiva 2002/58/CE, del Parlamento Europeo y del Consejo de la Unión Europea, del 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.**

En primer término nos interesa:

(...)

- (3) La confidencialidad de las comunicaciones está garantizada de conformidad con los instrumentos internacionales relativos a los derechos humanos.

Como hemos observado y repetido reiteradas veces, el derecho a la autodeterminación informativa puede considerarse parte de los derechos humanos (de carácter sui generis claro está), este sería el método para protegerlo de un modo internacional, para que calce en el concepto de protegido por instrumento internacional.

Además podríamos adicionar:

(7) En el caso de las redes públicas de comunicación, deben elaborarse disposiciones legales, reglamentarias y técnicas específicas con objeto de proteger los derechos y libertades fundamentales de las personas físicas y los intereses legítimos de las personas jurídicas, en particular frente a la creciente capacidad de almacenamiento y tratamiento informático de datos relativos a (...) y usuarios.

(8) Deben armonizarse las disposiciones legales, reglamentarias y técnicas adoptadas por los Estados miembros para proteger los datos personales, la intimidad y los intereses legítimos de las personas jurídicas en el sector de las comunicaciones electrónicas.

(...)

(26) Los datos (...) que son tratados en las redes de comunicaciones electrónicas para el establecimiento de conexiones y la transmisión de información contienen información sobre la vida privada de las personas físicas, y afectan al derecho de éstas al respecto de su correspondencia, o se refieren a los intereses legítimos de las personas jurídicas. Dichos datos sólo deben poder almacenarse en la medida en que resulten necesarios para la prestación del servicio (...) y durante un tiempo limitado.

Cualquier otro tratamiento de dichos datos que el proveedor de servicios de comunicaciones electrónicas disponibles al público pretenda llevar a cabo (...) para la prestación de servicios de valor añadido sólo puede permitirse si se ha manifestado su consentimiento fundado en una información plena y exacta facilitada por el proveedor de servicios de comunicaciones electrónicas.

CAPITULO V

BASES EN LAS QUE SE SUSTENTA EL ORGANISMO INTERNACIONAL PROPUESTO

La Declaración Universal de Derechos Humanos del 10 de diciembre de 1948 en su texto presenta: *“el ideal común por el que todos los pueblos y naciones deben esforzarse, a fin de que tanto los individuos como las instituciones, inspirándose constantemente en ella, promueven mediante la enseñanza y la educación, el respeto a estos derechos y libertades, y aseguren, por medidas progresivas de carácter nacional e internacional su reconocimiento y aplicación universales y efectivos...”*.

3. GENERALIDADES.-

La doctrina Internacional considera, que los organismos internacionales, poseen una existencia jurídica distinta a la del conjunto de Estados, es decir manifiestan una voluntad autónoma.

La institucionalización de las relaciones internacionales ha conducido a nuevas formas de negociar las normas de derecho internacional. En este sentido, se verifican procesos de negociación internacional que responden a patrones más o menos comunes, una trama de resoluciones de organismos internacionales que aporta la diversidad de entes que las generan y de los objetos que regulan por lo que perfilan un animus regulador (Pinto 2009, 12).

Existe un consenso en el mundo jurídico y en el de la historiografía jurídica en cuanto a que la Paz de Westfalia, en 1648, luego de la Guerra de Treinta Años cierra la etapa medioeval para dar lugar a un sistema de unidades políticas, Estados de algún modo embrionario del actual. En ese contexto, el derecho

internacional surge como el conjunto de pautas de conducta mutuamente aceptadas por los Estados para regir sus relaciones (Pinto 2009, 13).

Si nos remitiéramos específicamente a los Organismos Internacionales, estos gozan de una personalidad jurídica propia, en otras palabras, de la capacidad de ejercer derechos y asumir obligaciones en el marco de determinados sistemas jurídicos, de modo concreto: nacional o internacional.

4. SUSTENTOS PARA LA CREACIÓN DE UN ORGANISMO INTERNACIONAL.-

- **SUSTENTO LEGAL.-**

En primer lugar es necesario precisar que un organismo internacional es producto de un acto jurídico multilateral, concedido por un grupo de Estados que tienen un objetivo en común con su creación, con autonomía distinta a la de sus Estados creadores y bajo la luz de una conferencia internacional.

Como todo acto jurídico, su existencia está sujeta a su celebración; la misma que tendrá una entrada en vigencia, supeditada al consenso de sus creadores, es decir, dependerá de las condiciones en que se establezca su nacimiento, así como el número de países que se adhiera al mismo.

Dentro de este contexto, se deberá establecer el nombre, los objetivos, las finalidades, la organización, la duración, las disposiciones de su tratado constitutivo, miembros integrantes, las funciones de cada uno, las competencias, y todas aquellas disposiciones necesarias para el ejercicio pleno de su funcionamiento.

De otro lado, es bueno indicar, que el ente debe contar con la capacidad para contratar con terceros, quienes le permitan ejercer su funcionamiento cotidiano. Por lo general para el ejercicio de esta capacidad se designa algún funcionario de alto rango, quien, en conjunción con otros funcionarios tomarían las decisiones importantes.

En esta línea de ideas, por ejemplo, La ONU tiene derechos y obligaciones distintos a los de los Estados, es decir, que goza de una personalidad internacional, lo que significa que es un sujeto de derecho internacional, que tiene capacidad de adquirir derechos, contraer obligaciones internacionales y que tiene competencia para prevalerse de sus derechos por la vía de reclamación internacional (Pinto 2009, 15). El ente propuesto, entonces, podría gozar de esta misma personalidad internacional.

Este esquema de sujetos de derecho internacional, esto es, de centros de imputación normativa, coexiste con otro más amplio de actores de derecho internacional, conformado por entes no estatales de activa participación en el quehacer internacional (Pinto 2009, 15).

De otro lado, la subjetividad internacional del individuo queda planteada, parece claro que el individuo puede adquirir algún derecho y contraer ciertas obligaciones y adquirir algún derecho y contraer ciertas obligaciones en virtud del orden jurídico internacional y que, en ciertas condiciones, pueda prevalerse de sus derechos ante instancias internacionales, jurisdiccionales y no jurisdiccionales.

La capacidad del individuo en derecho internacional es restringida, en la medida en que no es agente generador de norma jurídica internacional, los derechos que tiene y las obligaciones que contrae son determinadas por los Estados (Pinto 2009, 17).

Todas las instancias internacionales son de procedimiento reglado, que resuelven con fundamento en derecho internacional las controversias que las partes planteen. El valor jurídico de sus decisiones es diverso- en algunos casos los textos que los rigen emplean el término “recomendaciones”-. Por otro lado, la opinión pública ha comenzado a hacer suya la cuestión de la observancia de las decisiones adoptadas (Pinto 2009, 19).

Una característica propia del conjunto normativo para un organismo internacional es la pluralidad de fuentes de una misma norma. Así, un derecho o una obligación puede alegarse respecto de más de un sujeto a título de distintas fuentes de derecho; lo que para uno será costumbre internacional, para otros consistirá en una estipulación de un tratado en vigor entre ellos y, eventualmente, para otros será un principio general del derecho (Pinto 2009, 23).

Los estándares de derechos humanos adquieren con la mundialización una difusión amplísima y permiten un debate sobre contenidos que, con sus más o menos, es de una riqueza incalculable para la calidad de vida cotidiana. En todo caso, vale la pena recordarlo, los derechos humanos deben servir para eso, para servir mejor (Pinto 2009, 27).

No es, pues, una internacionalización de nociones e institutos vigentes en los derechos constitucionales nacionales- lo que supone una traslación de normativa sin más- sino de una noción cualitativamente distinta que surge de un consenso mundial y que se apoya en las nociones de dignidad y libertad comunes a todas las culturas y civilizaciones (Pinto 2009, 27).

Por último, es pertinente recalcar que el ente funcionaria como instancia supranacional, esta solo causará efectos sobre sus países miembro, será de fácil acceso a los usuarios y sin fines de lucro.

- **SUSTENTO ECONÓMICO.-**

En primer lugar, para que un organismo internacional entre en vigencia, debe existir, como ya se dijo, una pluralidad de miembros en su constitución; estos miembros siempre serán Estados por la naturaleza jurídica internacional del mismo.

Sobre ese respecto, se puede deducir, que los miembros que lo conformaran serán de distintas clases, y cuando nos referimos a ellos

hablamos del ámbito económico, tanto los países del primer mundo, como los que se encuentran en vías de desarrollo, podrán formar parte de esta organización.

Entonces, serían los miembros que conformarán la organización, de acuerdo a sus posibilidades y contextos económicos, los cuales creen un fondo, es decir, reúnan dinero para el inicio de las operaciones del ente; después de ello, será el propio ente, a través de proyectos quien se sustente y pueda continuar con sus funciones.

De otro lado, como se verá más adelante, este organismo contará con una comisión sancionadora, sanciones que podrían tener también carácter pecuniario, de tal modo que permitan sustentar los gastos con los que contaría el ente.

No se descarta, por último, que empresas privadas, ONGs y algún tipo de asociación y conjunto de personas se encuentren en posición de apoyar al organismo de manera económica.

- **SUSTENTO ADMINISTRATIVO.-**

Para la existencia de cualquier organización, tenga el cariz que tenga, necesita de una estructura para su desarrollo. En este contexto, el organismo internacional propuesto podría contar con el siguiente esquema:

- a. La Comisión General.-**

El órgano central de nuestro ente internacional, deberá estar conformada por un representante oficial de cada uno de los Estados miembro, con derecho a voto, con la finalidad del consenso en la toma de decisiones.

Esta comisión será la encargada de la mencionada toma de decisiones a nivel macro, es decir atender a las necesidades de las demás comisiones conforme a la evolución del organismo.

b. El Directorio.-

La máxima instancia del ente, encargado de la toma de decisiones respecto de cada comisión a su cargo, las mismas que serán descritas a posteriori.

Deberá estar conformado por 5 personas, y sus respectivos suplentes en caso de faltar alguno de ellos, estos miembros deberían ser tres profesionales de derecho, un especialista en informática, y un especialista en sociología; todos con experiencia en niveles internacionales en relación al desarrollo de derechos humanos, derecho informático y nuevas tecnologías, dominio en el desarrollo de la sociedad de la información, además de contar con el requisito indispensable del conocimiento avanzado de cuatro idiomas como mínimo, entre los cuales deberán contarse de manera forzosa con el inglés y el español.

Ahora las subcomisiones que dependerán de directorio, son las siguientes:

- Comisión de asesoría y orientación al usuario.- la cual estará encargada de advertir a los usuarios de los riesgos de la contratación on line, cuales derechos podrán ser factibles de ser protegidos, que clase de información no debería compartirse en línea, entre otros.
- Comisión revisora.- encargada de estudiar que los contratos on line se abstengan de contener clausulas amenazadoras al derecho de determinación informativa.
- Comisión de atención de reclamos y denuncias.- ante la afectación de derechos de los usuarios, estos podrán enviar un correo electrónico para iniciar el procedimiento de reclamo o

denuncia, la misma que podrá terminar ante la comisión de conciliación o arbitraje.

- Comisión de asuntos legales.- esta comisión contará con profesionales del derecho dispuestos a asesorar a aquellos usuarios que necesiten de asesoría legal en cada caso particular que derive de un reclamo o denuncia.
- Comisión de conciliación.- encargada de establecer fórmulas para las soluciones de los conflictos generados por cláusulas ambiguas que pudieran llegar a ser amenazadoras, generaría un costo moderado.
- Comisión de arbitraje.- encargada de arbitrar frente a los conflictos generados por cláusulas ambiguas que pudieran llegar a ser amenazadoras, generaría un costo normal.
- Comisión fiscalizadora.- encargada de efectuar un control sobre las páginas web para que no incluyan o vuelvan a incluir las referidas cláusulas.
- Comisión sancionadora.- encargada de realizar la escala de sanciones que correspondería aplicar a las redes sociales que recaigan en inclusión de cláusulas amenazadoras.

Cada una de estas comisiones deberá contar con profesionales en derecho, que cuenten con el dominio de 4 idiomas como mínimo, tengan amplia experiencia en el manejo internacional de derechos humanos, en especial acerca del derecho de autodeterminación informativa, y por supuesto amplio conocimiento sobre las nuevas tecnologías.

c. Programas y Fondos.-

Todo organismo internacional, debe contar con una serie de programas y fondos que permitan su viabilidad económica a futuro; en este caso se podrían implementar una serie de estos proyectos para

que del producto de su desarrollo se extraiga dinero para el manejo del ente.

CONCLUSIONES

- La Sociedad de la Información es el nuevo ámbito donde se desarrollan y se desarrollaran los actos jurídicos, dentro de ella encontramos el fenómeno de la contratación masiva, que es mejor conocido como la contratación a través de Internet.
- La tendencia de contratación a través de Internet, es una que se encuentra en pleno apogeo, es claro, que, como todo acto humano iba a encontrar una situación inconveniente, la presencia de las cláusulas amenazadoras, es sólo una de las tantas posibles inconveniencias que se pudieren presentar. El presente trabajo sugiere una solución legal para este primer conflicto hallado en la contratación a través de Internet.
- La mejor solución legal que hemos podido proponer frente al problema de las clausulas amenazadoras fue la creación de un Organismo Internacional puesto que, este tendría facultades de solución a diferentes niveles tanto para evitar la inclusión de las clausulas, como para evitar los posibles conflictos, y solucionarlos de presentarse la oportunidad y establecer también un ranking de sanciones para las Redes Sociales que incumplan con lo que este Organismo disponga.
- Por último, este Organismo planteado deberá ceñirse a los fundamentos de las directivas Europeas que hablan de derecho a la intimidad (que nosotros conocemos como autodeterminación Informativa). Y si se presentaran nuevos problemas o conflictos, este Organismo podría adaptarse para la solución de posibles futuros conflictos como otras cláusulas que puedan vulnerar o vulneren

derechos y demás tratamientos que impliquen los datos de carácter personal.

RECOMENDACIONES

- Ante la evidente existencia de cláusulas amenazadoras de derechos en las redes sociales, se propone la creación de un Organismo Internacional, el cual debe contar con una serie de características, propuestas en el presente trabajo de investigación lo cual se resume en implementar normas de carácter previsor, regulador y sancionador.

LISTA DE REFERENCIAS

- Barral Viñals Inmaculada, La regulación del comercio electrónico, Editorial Dykinson, 2004.
- Caso Wilo Rodríguez Gutiérrez, Resolución N. ° 01797-2002-HD/TC, 29/09/2003.
- Cárdenas Quiroz, Carlos, Autonomía privada, Contrato y constitución, en Contrato y Mercado, Gaceta Jurídica Editoras, Lima, 2000.
- Del Peso Navarro, Emilio.2004. Servicios de la Sociedad de la Información. Ediciones Díaz de Santos.
- Del Peso Navarro Emilio, del Peso Ruiz Mar, Ruiz Gómez Asunción, del Peso Ruiz Nuria, Vocabulario español actualizado de iustecnología de la información (Bibliografía de las TICS por temas, autores y año de publicación), Ediciones Díaz de Santos, 2010.
- De la Puente y Lavalle, Manuel El contrato en General, tomo I, Palestra 2003.
- García Bedoya, Carlos; Política Exterior Peruana Teoría Y Practica (2da. Edición); 1992

- Gómez, Carlos H; Una mirada creativa al futuro de los organismos internacionales de cooperación multilateral; Editorial: Organización de Estados Iberoamericanos (OEI); 2004.
- Menéndez Mato, Juan Carlos; El Contrato Vía Internet; JM BOSCH EDITOR, 2008.
- Molina Mateos José María, Sánchez de Diego y Fernández de la Riva Manuel, Aspectos jurídicos de la protección criptológica de la información y las comunicaciones, Universidad Complutense de Madrid, 2005.
- Muñoz M. Johan, Historia de la computación y documentos informáticos; Editorial: El Cid Editor | apuntes, 2009.
- Pastor Ridruejo, José Antonio; Curso De Derecho Internacional Público Y Organizaciones Internacionales Octava Edición, curso de derecho Internacional público Y organizaciones Internacionales Octava edición, 2005.
- Peralta Andía, Javier Rolando y Peralta Zecharro Nilda, Fuentes de las Obligaciones en el Código Civil, IDEMSA, Lima, 2005.
- Pinto Mónica (Compiladora), Las Fuentes del Derecho Internacional en la era de la Globalización, Editorial Eudeba, 2009.
- Rodríguez de Almeida Reginaldo y Davara Rodríguez Javier, De la sociedad de la información a la sociedad del conocimiento: la sociedad bit, Editorial: Universidad Complutense de Madrid, 2006.
- Soto Coaguila, Carlos Alberto, Transformación del Derecho de Contratos, Editora Jurídica GRIJLEY, 2005.
- Torres Álvarez, Hernán; El Sistema de Seguridad Jurídica en el Comercio Electrónico; Fondo Editorial PUCP, 2005.

Sitios Web

- Política de privacidad de Badoo (en línea) consultado 22 mayo 2012. Disponible en <http://badoo.com/privacy/>
- Política de Privacidad (en línea) consultado 22 mayo 2012. Disponible en <http://about.digg.com/privacy>

- Políticas de Privacidad (en línea) consultado 22 mayo 2012. Disponible en http://www.hi5.com/terms_of_service.html?#privacy_policy
- ¿Qué es Internet? (en línea) consultado 22 mayo 2012. Disponible en http://www.cad.com.mx/que_es_internet.htm
- Reddit ayuda (en línea) consultado 22 mayo 2012. Disponible en <http://www.reddit.com/help/privacypolicy>
- Mercadotecnia, Qué es Información, Artículo Publicado en Octubre de 2010. Disponible en www.promonegocioS.net.

ANEXOS

**Directiva 95/46/CE del parlamento europeo y del consejo de 24 de octubre de 1995
relativa a la protección de las personas físicas en lo que respecta al tratamiento de
datos personales y a la libre circulación de estos datos.**

EL PARLAMENTO EUROPEO Y EL, CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado constitutivo de la Comunidad Europea, y, en particular, su artículo 100
A,

Vista la propuesta de la Comisión. 1

Visto el dictamen del Comité Económico y Social 2

De conformidad con el procedimiento establecido en el artículo 189 B del Tratado³,

Considerando que los objetivos de la Comunidad definidos en el Tratado, tal y como
quedó modificado por el Tratado de la Unión Europea, consisten en lograr una unión
cada vez más estrecha entre los pueblos europeos, establecer relaciones más estrechas
entre los Estados miembros de la Comunidad, asegurar, mediante una acción común, el
progreso económico y social, eliminando las barreras que dividen Europa, fomentar la
continua mejora de las condiciones de vida de sus pueblos, preservar y consolidar la paz
y la libertad y promover la democracia, basándose en los derechos fundamentales
reconocidos en las constituciones Y leyes de los Estados miembros y en el Convenio
Europeo para la Protección de los Derechos Humanos y de las Libertades
Fundamentales;

Considerando que los sistemas de tratamiento de datos están al servicio del hombre; que
deben, cualquiera que sea la nacionalidad o la residencia de las personas físicas, respetar
las libertades y derechos fundamentales de las personas físicas y, en particular, la
intimidad, y contribuir al progreso económico y social, al desarrollo de los
intercambios, así como al bienestar de los individuos;

(3) Considerando que el establecimiento y funcionamiento del mercado interior, dentro del cual está garantizada, con arreglo al artículo 7 A del Tratado, la libre circulación de mercancías, personas, servicios y capitales, hacen necesaria no sólo la libre circulación de datos personales de un Estado miembro a otro, sino también la protección de los derechos fundamentales de las personas; (4) Considerando que se recurre cada vez más en la Comunidad al tratamiento de datos personales en los diferentes sectores de actividad económica y social; que el avance de las tecnologías de la información facilita considerablemente el tratamiento y el intercambio de dichos datos;

(5) Considerando que la integración económica y social resultante del establecimiento y funcionamiento del mercado interior, definido en el artículo 7 A del Tratado, va a implicar necesariamente un aumento notable de los flujos transfronterizos de datos personales entre todos los agentes de la vida económica y social de los Estados miembros, ya se trate de agentes públicos o privados; que el intercambio de datos personales entre empresas establecidas en los diferentes Estados miembros experimentará un desarrollo; que las administraciones nacionales de los diferentes Estados miembros, en aplicación del Derecho comunitario, están destinadas a colaborar y a intercambiar datos personales a fin de cumplir su cometido o ejercer funciones por cuenta de las administraciones de otros Estados miembros, en el marco del espacio sin fronteras que constituye el mercado interior;

(6) Considerando, por lo demás, que el fortalecimiento de la cooperación científica y técnica, así como el establecimiento coordinado de nuevas redes de telecomunicaciones en la Comunidad exigen y facilitan la circulación transfronteriza de datos personales;

(7) Considerando que las diferencias entre los niveles de protección de los derechos y libertades de las personas y, en particular, de la intimidad, garantizados en los Estados miembros por lo que respecta al tratamiento de datos personales, pueden impedir la

transmisión de dichos datos del territorio de un Estado miembro al de otro; que, por lo tanto, estas diferencias pueden constituir un obstáculo para el ejercicio de una serie de actividades económicas a escala comunitaria, falsear la competencia e impedir que las administraciones cumplan los cometidos que les incumben en virtud del Derecho comunitario; que estas diferencias en los niveles de protección se deben a la disparidad existente entre las disposiciones legales, reglamentarias y administrativas de los Estados miembros;

(8) Considerando que, para eliminar los obstáculos a la circulación de datos personales, el nivel de protección de los derechos y libertades de las personas, por lo que se refiere al tratamiento de dichos datos, debe ser equivalente en todos los Estados miembros; que ese objetivo, esencial para el mercado interior, no puede lograrse mediante la mera actuación de los Estados miembros, teniendo en cuenta, en particular, las grandes diferencias existentes en la actualidad entre las legislaciones nacionales aplicables en la materia y la necesidad de coordinar las legislaciones de los Estados miembros para que el flujo transfronterizo de datos personales sea regulado de forma coherente y de conformidad con el objetivo del mercado interior definido en el artículo 7 A del Tratado; que, por tanto, es necesario que la Comunidad intervenga para aproximar las legislaciones;

(9) Considerando que, a causa de la protección equivalente que resulta de la aproximación de las legislaciones nacionales, los Estados miembros ya no podrán obstaculizar la libre circulación entre ellos de datos personales por motivos de protección de los derechos y libertades de las personas físicas, y, en particular, del derecho a la intimidad; que los Estados miembros dispondrán de un margen de maniobra del cual podrán servirse, en el contexto de la aplicación de la presente Directiva, los interlocutores económicos y sociales; que los Estados miembros podrán,

por lo tanto, precisar en su derecho nacional las condiciones generales de licitud del tratamiento de datos; que, al actuar así, los Estados miembros procurarán mejorar la protección que proporciona su legislación en la actualidad; que, dentro de los límites de dicho margen de maniobra y de conformidad con el Derecho comunitario, podrán surgir disparidades en la aplicación de la presente Directiva, y que ello podrá tener repercusiones en la circulación de datos tanto en el interior de un Estado miembro como en la Comunidad;

(10) Considerando que las legislaciones nacionales relativas al tratamiento de datos personales tienen por objeto garantizar el respeto de los derechos y libertades fundamentales, particularmente del derecho al respeto de la vida privada reconocido en el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, así como en los principios generales del Derecho comunitario; que, por lo tanto, la aproximación de dichas legislaciones no debe conducir a una disminución de la protección que garantizan sino que, por el contrario, debe tener por objeto asegurar un alto nivel de protección dentro de la Comunidad;

(11) Considerando que los principios de la protección de los derechos y libertades de las personas y, en particular, del respeto de la intimidad, contenidos en la presente Directiva, precisan y amplían los del Convenio de 28 de enero de 1981 del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales;

(12) Considerando que los principios de la protección deben aplicarse a todos los tratamientos de datos personales cuando las actividades del responsable del tratamiento entren en el ámbito de aplicación del Derecho comunitario; que debe excluirse el tratamiento de datos efectuado por una persona física en el ejercicio de actividades

exclusivamente personales o domésticas, como la correspondencia y la llevanza de un repertorio de direcciones;

(13) Considerando que las actividades a que se refieren los títulos V y VI del Tratado de la Unión Europea relativos a la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en el ámbito penal no están comprendidas en el ámbito de aplicación del Derecho comunitario, sin perjuicio de las obligaciones que incumben a los Estados miembros con arreglo al apartado 2 del artículo 56 y a los artículos 57 y 100 A del Tratado; del] tratamiento de los datos de carácter personal que sea necesario para la salvaguardia del bienestar económico del Estado no está comprendido en el ámbito de aplicación de la presente Directiva en los casos en que dicho tratamiento esté relacionado con la seguridad del Estado;

(14) Considerando que, habida cuenta de la importancia que, en el marco de la sociedad de la información, reviste el actual desarrollo de las técnicas para captar, transmitir, manejar, registrar, conservar o comunicar los datos relativos a las personas físicas constituidos por sonido e imagen, la presente Directiva habrá de aplicarse a los tratamientos que afectan a dichos datos;

(15) Considerando que los tratamientos que afectan a dichos datos sólo quedan amparados por la presente Directiva cuando están automatizados o cuando los datos a que se refieren se encuentran contenidos o se destinan a encontrarse contenidos en un archivo estructurado según criterios específicos relativos a las personas, a fin de que se pueda acceder fácilmente a los datos de carácter personal de que se trata;

(16) Considerando que los tratamientos de datos constituidos por sonido e imagen, como los de la vigilancia por videocámara, no están comprendidos en el ámbito de aplicación de la presente Directiva cuando se aplican con fines de seguridad pública, defensa, seguridad del Estado o para el ejercicio de las actividades del Estado relacionadas con

ámbitos del derecho penal o para el ejercicio de otras actividades que no están comprendidos en el ámbito de aplicación del Derecho comunitario;

(17) Considerando que en lo que respecta al tratamiento del sonido y de la imagen aplicados con fines periodísticos o de expresión literaria o artística, en particular en el sector audiovisual, los principios de la Directiva se aplican de forma restringida según lo dispuesto en el artículo 9;

(18) Considerando que, para evitar que una persona sea excluida de la protección garantizada por la presente Directiva, es necesario que todo tratamiento de datos personales efectuado en la Comunidad respete la legislación de uno de sus Estados miembros; que, a este respecto, resulta conveniente someter el tratamiento de datos efectuados por cualquier persona que actúe bajo la autoridad del responsable del tratamiento establecido en un Estado miembro a la aplicación de la legislación de tal Estado;

(19) Considerando que el establecimiento en el territorio de un Estado miembro implica el ejercicio efectivo y real de una actividad mediante una instalación estable; que la forma jurídica de dicho establecimiento, sea una simple sucursal o una empresa filial con personalidad jurídica, no es un factor determinante al respecto; que cuando un mismo responsable esté establecido en el territorio de varios Estados miembros, en particular por medio de una empresa filial, debe garantizar, en particular para evitar que se eluda la normativa aplicable, que cada uno de los establecimientos cumpla las obligaciones impuestas por el Derecho nacional aplicable a estas actividades;

(20) Considerando que el hecho de que el responsable del tratamiento de datos esté establecido en un país tercero no debe obstaculizar la protección de las personas contemplada en la presente Directiva; que en estos casos el tratamiento de datos debe regirse por la legislación del Estado miembro en el que se ubiquen los medios utilizados

y deben adaptarse garantías para que se respeten en la práctica los derechos y obligaciones contempladas en la presente Directiva;

(21) Considerando que la presente Directiva no afecta a las normas de territorialidad aplicables en materia penal;

(22) Considerando que los Estados miembros precisarán en su legislación o en la aplicación de las disposiciones adoptadas en virtud de la presente Directiva las condiciones generales de licitud del tratamiento de datos; que, en particular, el artículo 5 en relación con los artículos 7 y 8, ofrece a los Estados miembros la posibilidad de prever, independientemente de las normas generales, condiciones especiales de tratamiento de datos en sectores específicos, así como para las diversas categorías de datos contempladas en el artículo 8;

(23) Considerando que los Estados miembros están facultados para garantizar la protección de las personas tanto mediante una ley general relativa a la protección de las personas respecto del tratamiento, de los datos de carácter personal como mediante leyes sectoriales, como las relativas a los institutos estadísticos;

(24) Considerando que las legislaciones relativas a la protección de las personas jurídicas respecto del tratamiento de los datos que las conciernan no son objeto de la presente Directiva;

(25) Considerando que los principios de la protección tienen su expresión, por una parte, en las distintas obligaciones que incumben a las personas, autoridades públicas, empresas, agencias u otros organismos que efectúen tratamientos - obligaciones relativas, en particular, a la calidad de los datos, la seguridad técnica, la notificación a las autoridades de control y las circunstancias en las que se puede efectuar el 'tratamiento- y, por otra parte, en los derechos otorgados a las personas cuyos datos sean objeto de tratamiento de ser informadas acerca de dicho tratamiento, de poder acceder a

los datos, de poder solicitar su rectificación o incluso de oponerse a su tratamiento en determinadas circunstancias;

(26) Considerando que los principios de la protección deberán aplicarse a cualquier información relativa a una persona identificada o identificable; que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona; que los principios de la protección no se aplicarán a aquellos datos hechos anónimos de manera tal que ya no sea posible identificar al interesado; que los códigos de conducta con arreglo al artículo 27 pueden constituir un elemento útil para proporcionar indicaciones sobre los medios gracias a los cuales los datos pueden hacerse anónimos y conservarse de forma tal que impida identificar al interesado;

(27) Considerando que la protección de las personas debe aplicarse tanto al tratamiento automático de datos como a su tratamiento manual; que el alcance de esta protección no debe depender, en efecto, de las técnicas utilizadas, pues la contrario daría lugar a riesgos graves de alusión; que, no obstante, por lo que respecta al tratamiento manual, la presente Directiva sólo abarca los ficheros, y no se aplica a las carpetas que no están estructuradas; que, en particular, el contenido de un fichero debe estructurarse conforme a criterios específicos relativos a las personas, que permitan acceder fácilmente a los datos personales; que, de conformidad con la definición que recoge la letra c) del artículo 2, los distintos criterios que permiten determinar los elementos de un conjunto estructurado de datos de carácter personal y los distintos criterios que regulan el acceso a dicho conjunto de datos pueden ser definidos por cada Estado miembro; que, las carpetas y conjuntos de carpetas, así como sus portadas, que no estén estructuradas

conforme a criterios específicos no están comprendidas en ningún caso en el ámbito de aplicación de la presente Directiva;

(28) Considerando que todo tratamiento de datos personales debe efectuarse de forma lícita y leal con respecto al interesado; que debe referirse, en particular, a datos adecuados, pertinentes y no excesivos en relación con los objetivos perseguidos; que estos objetivos han de ser explícitos y legítimos, y deben estar determinados en el momento de obtener los datos; que los objetivos de los tratamientos posteriores a la obtención no pueden ser incompatibles con los objetivos originalmente especificados;

(29) Considerando que el tratamiento ulterior de datos personales, con fines históricos, estadísticos o científicos no debe por lo general considerarse incompatible con los objetivos para los que se recogieron los datos, siempre y cuando los Estados miembros establezcan las garantías adecuadas; que dichas garantías deberán impedir que dichos datos sean utilizados para tomar medidas o decisiones contra cualquier persona;

(30) Considerando que para ser lícito el tratamiento de datos personales debe basarse además en el consentimiento del interesado o ser necesario con vistas a la celebración o ejecución de un contrato que obligue al interesado, o para la observancia de una obligación legal o para el cumplimiento de una misión de interés público o para el ejercicio de la autoridad pública o incluso para la realización de un interés legítimo de una persona, siempre que no prevalezcan los intereses o los derechos y libertades del interesado; que, en particular, para asegurar el equilibrio de los intereses en juego, garantizando a la vez una competencia efectiva, los Estados miembros pueden precisar las condiciones en las que se podrán utilizar y comunicar a terceros datos de carácter personal, en el desempeño de actividades legítimas de gestión ordinaria de empresas y otras entidades; que los Estados miembros pueden asimismo establecer previamente las condiciones en que pueden efectuarse comunicaciones de datos personales a terceros

con fines de prospección comercial o de prospección realizada por una institución benéfica u otras asociaciones o fundaciones, por ejemplo de carácter político, dentro del respeto de las disposiciones que permiten a los interesados oponerse, sin alegar los motivos y sin gastos, al tratamiento de los datos que les conciernan;

(31) Considerando que un tratamiento de datos personales debe estimarse lícito cuando se efectúa con el fin de proteger un interés esencial para la vida del interesado;

(32) Considerando que corresponde a las legislaciones nacionales determinar si el responsable del tratamiento que tiene conferida una misión de interés público o inherente al ejercicio del poder público, debe ser una administración pública u otra persona de derecho público o privado, como por ejemplo una asociación profesional;

(33) Considerando, por lo demás, que los datos que por su naturaleza puedan atentar contra las libertades fundamentales o la intimidad no deben ser objeto de tratamiento alguno, salvo en caso de que el interesado haya dado su consentimiento explícito; que deberán constar de forma explícita las excepciones a esta prohibición para necesidades específicas, en particular cuando el tratamiento de dichos datos se realice con fines relacionados con la salud, por parte de personas físicas sometidas a una obligación legal de secreto profesional, o para actividades legítimas por parte de ciertas asociaciones o fundaciones cuyo objetivo sea hacer posible el ejercicio de libertades fundamentales;

(34) Considerando que también se deberá autorizar a los Estados miembros, cuando esté justificado por razones de interés público importante, a hacer excepciones a la prohibición de tratar categorías sensibles de datos en sectores como la salud pública y la protección social, particularmente en lo relativo a la garantía de la calidad y la rentabilidad, así como los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro enfermedad, la investigación científica y las estadísticas públicas; que a ellos corresponde, no obstante, prever las

garantías apropiadas y específicas a los fines de proteger los derechos fundamentales y la vida privada de las personas;

(35) Considerando, además, que el tratamiento de datos personales por parte de las autoridades públicas con fines, establecidos en el Derecho constitucional o en el Derecho internacional público, de asociaciones religiosas reconocidas oficialmente, se realiza por motivos importantes de interés público;

(36) Considerando que, si en el marco de actividades relacionadas con las elecciones, el funcionamiento del sistema democrático en algunos Estados miembros exige que los partidos políticos recaben datos sobre la ideología política de los ciudadanos, podrá autorizarse el tratamiento de estos datos por motivos importantes de interés público, siempre que se establezcan las garantías adecuadas;

(37) Considerando que para el tratamiento de datos personales con fines periodísticos o de expresión artística o literaria, en particular en el sector audiovisual, deben preverse excepciones o restricciones de determinadas disposiciones de la presente Directiva siempre que resulten necesarias para conciliar los derechos fundamentales de la persona con la libertad de expresión y, en particular, la libertad de recibir o comunicar informaciones, tal y como se garantiza en el artículo 10 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales; que por lo tanto, para ponderar estos derechos fundamentales, corresponde a los Estados miembros prever las excepciones y las restricciones necesarias en lo relativo a las medidas generales sobre la legalidad del tratamiento de datos, las medidas sobre la transferencia de datos a terceros países y las competencias de las autoridades de control sin que esto deba inducir, sin embargo, a los Estados miembros a prever excepciones a las medidas que garanticen la seguridad del tratamiento; que, igualmente, debería concederse a la autoridad de control responsable en la materia al menos una serie de competencias a

posteriori como por ejemplo publicar periódicamente un informe al respecto o bien iniciar procedimientos legales ante las autoridades judiciales;

(38) Considerando que el tratamiento leal de datos supone que los interesados deben estar en condiciones de conocer la existencia de los tratamientos y, cuando los datos se obtengan de ellos mismos, contar con una información precisa y completa respecto a las circunstancias de dicha obtención;

(39) Considerando que determinados tratamientos se refieren a datos que el responsable no ha recogido directamente del interesado; que, por otra parte, pueden comunicarse legítimamente datos a un tercero aún cuando dicha comunicación no estuviera prevista en el momento de la recogida de los datos del propio interesado; que, en todos estos supuestos, debe informarse al interesado en el momento del registro de los datos o, a más tardar, al comunicarse los datos por primera vez a un tercero;

(40) Considerando, no obstante, que no es necesario imponer esta obligación si el interesado ya está informado, si el registro o la comunicación están expresamente previstos por la ley o si resulta imposible informarle, o ello implica esfuerzos desproporcionados, como puede ser el caso para tratamientos con fines históricos, estadísticos o científicos; que a este respecto pueden tomarse en consideración el número de interesados, la antigüedad de los datos, y las posibles medidas compensatorias;

(41) Considerando que cualquier persona debe disfrutar del derecho de acceso a los datos que le conciernan y sean objeto de tratamiento, para cerciorarse, en particular, de su exactitud y de la licitud de su tratamiento; que por las mismas razones cualquier persona debe tener además el derecho de conocer la lógica que subyace al tratamiento automatizado de los datos que la conciernan, al menos en el caso de las decisiones automatizadas a que se refiere el apartado 1 del artículo 15; que este derecho no debe

menoscabar el secreto de los negocios ni la propiedad intelectual y en particular el derecho de autor que proteja el programa informática; que no obstante esto no debe suponer que se deniegue cualquier información al interesado;

(42) Considerando que, en interés del interesado de que se trate y para proteger los derechos y libertades de terceros, los Estados miembros podrán limitar los derechos de acceso y de información; que podrán, por ejemplo, precisar que el acceso a los datos de carácter médico únicamente pueda obtenerse a través de un profesional de la medicina;

(43) Considerando que los Estados miembros podrán imponer restricciones a los derechos de acceso e información y a determinadas obligaciones del responsable del tratamiento, en la medida en que sean estrictamente necesarias para, por ejemplo, salvaguardar la seguridad del Estado, la defensa, la seguridad pública, los intereses económicos o financieros importantes de un Estado miembro o de la Unión, así como para realizar investigaciones y entablar procedimientos penales y perseguir violaciones de normas deontológicas en las profesiones reguladas; que conviene enumerar, a efectos de excepciones y limitaciones, las tareas de control, inspección o reglamentación necesarias en los tres últimos sectores mencionados relativos a la seguridad pública, los intereses económicos o financieros y la represión penal; que esta enumeración de tareas relativas a los tres sectores citados no afecta a la legitimidad de las excepciones y restricciones establecidas por razones de seguridad del Estado o de defensa;

(44) Considerando que los Estados miembros podrán verse obligados, en virtud de las disposiciones del Derecho comunitario, a establecer excepciones a las disposiciones de la presente Directiva relativas al derecho de acceso, a la información de personas y a la calidad de los datos para garantizar algunas de las finalidades contempladas más arriba;

(45) Considerando que cuando se pudiera efectuar lícitamente un tratamiento de datos por razones de interés público o del ejercicio de la autoridad pública, o en interés

legítimo de una persona física, cualquier persona deberá, sin embargo, tener derecho a oponerse a que los datos que le conciernan sean objeto de un tratamiento, en virtud de motivos fundados y legítimos relativos a su situación concreta; que los Estados miembros tienen, no obstante, la posibilidad de establecer disposiciones nacionales contrarias;

(46) Considerando que la protección de los derechos y libertades de los interesados en lo que respecta a los tratamientos de datos personales exige la adopción de medidas técnicas y de organización apropiadas, tanto en el momento de la concepción del sistema de tratamiento como en el de la aplicación de los tratamientos mismos, sobre todo con objeto de garantizar la seguridad e impedir, por tanto, todo tratamiento no autorizado; que corresponde a los Estados miembros velar por que los responsables del tratamiento respeten dichas medidas; que esas medidas deberán garantizar un nivel de seguridad adecuado teniendo en cuenta el estado de la técnica y el coste de su aplicación en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse;

(47) Considerando que cuando un mensaje con datos personales sea transmitido a través de un servicio de telecomunicaciones o de correo electrónico cuyo único objetivo sea transmitir mensajes de ese tipo, será considerada normalmente responsable del tratamiento de los datos personales presentes en el mensaje aquella persona de quien proceda el mensaje y no la que ofrezca el servicio de transmisión; que, no obstante, las personas que ofrezcan estos servicios normalmente serán consideradas responsables del tratamiento de los datos personales complementarios y necesarios para el funcionamiento del servicio;

(48) Considerando que los procedimientos de notificación a la autoridad de control tienen por objeto asegurar la publicidad de los fines de los tratamientos y de sus

principales características a fin de controlarlos a la luz de las disposiciones nacionales adoptadas en aplicación de la presente Directiva;

(49) Considerando que para evitar trámites administrativos improcedentes, los Estados miembros pueden establecer exenciones o simplificaciones de la notificación para los tratamientos que no atenten contra los derechos y las libertades de los interesados, siempre y cuando sean conformes a un acto adoptado por el Estado miembro en el que se precisen sus límites; que los Estados miembros pueden igualmente disponer la exención o la simplificación cuando un encargado, nombrado por el responsable del tratamiento, se cerciore de que los tratamientos efectuados no pueden atentar contra los derechos Y libertades de los interesados; que la persona encargada de la protección de los datos, sea o no empleado del responsable del tratamiento de datos, deberá ejercer sus funciones con total independencia;

(50) Considerando que podrán establecerse exenciones o simplificaciones para los tratamientos cuya única finalidad sea el mantenimiento de registros destinados, de conformidad con el Derecho nacional, a la información del público y que sean accesibles para la consulta del público o de toda persona que justifique un interés legítimo;

(51) Considerando, no obstante, que el beneficio de la simplificación o de la exención de la obligación de notificación no dispensa al responsable del tratamiento de ninguna de las demás obligaciones derivadas de la presente Directiva;

(52) Considerando que, en este contexto, el control a *posteriori* por parte de las autoridades competentes debe considerarse, en general, una medida suficiente;

(53) Considerando, no obstante, que determinados tratamientos pueden presentar riesgos particulares desde el punto de vista de los derechos y las libertades de los interesados, ya sea por su naturaleza, su alcance o su finalidad, como los de excluir a los interesados

del beneficio de un derecho, de una prestación o de un contrato, 9 por el uso particular de una tecnología nueva; que es competencia de los Estados miembros, si así lo desean, precisar tales riesgos en sus legislaciones;

(54) Considerando que, a la vista de todos los tratamientos llevados a cabo en la sociedad, el número de los que presentan tales riesgos particulares debería ser muy limitado; que los Estados miembros deben prever, para dichos tratamientos, un examen previo a su realización por parte de la autoridad de control o del encargado de la protección de datos en cooperación con aquélla; que, tras dicho control previo, la autoridad de control, en virtud de lo que disponga su Derecho nacional, podrá emitir un dictamen o autorizar el tratamiento de datos; que este examen previo podrá realizarse también en el curso de la elaboración de una medida legislativa aprobada por el Parlamento nacional o de una medida basada en dicha medida legislativa, que defina la naturaleza del tratamiento y precise las garantías adecuadas;

(55) Considerando que las legislaciones nacionales deben prever un recurso judicial para los casos en los que el responsable del tratamiento de datos no respete los derechos de los interesados; que los daños que pueden sufrir las personas a raíz de un tratamiento ilícito han de ser reparados por el responsable del tratamiento de datos, el cual sólo podrá ser eximido de responsabilidad si demuestra que no le es imputable el hecho perjudicial, principalmente si demuestra la responsabilidad del interesado o un caso de fuerza mayor; que deben imponerse sanciones a toda persona, tanto de derecho privado como de derecho público, que no respete las disposiciones nacionales adoptadas en aplicación de la presente Directiva;

(56) Considerando que los flujos transfronterizos de datos personales son necesarios para el desarrollo del comercio internacional; que la protección de las personas garantizada en la Comunidad por la presente Directiva no se opone a la transferencia de

datos personales a terceros países que garanticen un nivel de protección adecuado; que el carácter adecuado del nivel de protección ofrecido por un país tercero debe apreciarse teniendo en cuenta todas las circunstancias relacionadas con la transferencia o la categoría de transferencias;

(57) Considerando, por otra parte, que cuando un país tercero no ofrezca un nivel de protección adecuado debe prohibirse la transferencia al mismo de datos personales;

(58) Considerando que han de establecerse excepciones a esta prohibición en determinadas circunstancias, cuando el interesado haya dado su consentimiento, cuando la transferencia sea necesaria en relación con un contrato o una acción judicial, cuando así lo exija la protección de un interés público importante, por ejemplo en casos de transferencia internacional de datos entre las administraciones fiscales o aduaneras o entre los servicios competentes en materia de seguridad social, o cuando la transferencia se haga desde un registro previsto en la legislación con fines de consulta por el público o por personas con un interés legítimo; que en tal caso dicha transferencia no debe afectar a la totalidad de los datos o las categorías de datos que contenga el mencionado registro; que, cuando la finalidad de un registro sea la consulta por parte de personas que tengan un interés legítimo, la transferencia sólo debería poder efectuarse a petición de dichas personas o cuando éstas sean las destinatarias;

(59) Considerando que pueden adaptarse medidas particulares para paliar la insuficiencia del nivel de protección en un tercer país, en caso de que el responsable del tratamiento ofrezca garantías adecuadas; que, por lo demás, deben preverse procedimientos de negociación entre la Comunidad y los países terceros de que se trate;

(60) Considerando que, en cualquier caso, las transferencias hacia países terceros sólo podrán efectuarse si se respetan plenamente las disposiciones adoptadas por los Estados miembros en aplicación de la presente Directiva, Y, en particular, de su artículo 8;

(61) Considerando que los Estados miembros y la Comisión, dentro de sus respectivas competencias, deben alentar a los sectores profesionales para que elaboren códigos de conducta a fin de facilitar, habida cuenta del carácter específico del tratamiento de datos efectuado en determinados sectores, la aplicación de la presente Directiva respetando las disposiciones nacionales adoptadas para su aplicación;

(62) Considerando que la creación de una autoridad de control que ejerza sus funciones con plena independencia en cada uno de los Estados miembros constituye un elemento esencial de la protección de las personas en lo que respecta al tratamiento de datos personales;

(63) Considerando que dicha autoridad debe disponer de los medios necesarios para cumplir su función, ya se trate de poderes de investigación o de intervención, en particular en casos de reclamaciones presentadas a la autoridad o de poder comparecer en juicio; que tal autoridad ha de contribuir a la transparencia de los tratamientos de datos efectuados en el Estado miembro del que dependa;

(64) Considerando que las autoridades de los distintos Estados miembros habrán de prestarse ayuda mutua en el ejercicio de sus funciones -, de forma que se garantice el pleno respeto de las normas de protección en toda la Unión Europea;

(65) Considerando que se debe crear, en el ámbito comunitario, un grupo de protección de las personas en lo que respecta al tratamiento de datos personales, el cual habrá de ejercer sus funciones con plena independencia; que, habida cuenta de este carácter específico, el grupo deberá asesorar a la Comisión y contribuir, en particular, a la aplicación uniforme de las normas nacionales adoptadas en aplicación de la presente Directiva;

(66) Considerando que, por lo que respecta a la transferencia de datos hacia países terceros, la aplicación de la presente Directiva requiere que se atribuya a la Comisión

competencias de ejecución y que se cree un procedimiento con arreglo a las modalidades establecidas en la Decisión 87/373/CEE del Consejo.⁴

(67) Considerando que el 20 de diciembre de 1994 se alcanzó un acuerdo sobre un *modus vivendi* entre el Parlamento Europeo, el Consejo y la Comisión concerniente a las medidas de aplicación de los actos adoptados de conformidad con el procedimiento establecido en el artículo 189 B del Tratado CE;

(68) Considerando que los principios de protección de los derechos y libertades de las personas v, en particular, del respeto de la intimidad en lo que se refiere al tratamiento de los datos personales objeto de la presente Directiva podrán completarse o precisarse, sobre todo en determinados sectores, mediante normas específicas conformes a estos principios;

(69) Considerando que resulta oportuno conceder a los Estados miembros un plazo que no podrá ser superior a tres años a partir de la entrada en vigor de las medidas nacionales de transposición de la presente Directiva, a fin de que puedan aplicar de manera progresiva las nuevas disposiciones nacionales mencionadas a todos los tratamientos de datos ya existentes; que, con el fin de facilitar una aplicación que presente una buena relación coste eficacia, se concederá a los Estados miembros un período suplementario que expirará a los doce años de la fecha en que se adopte la presente Directiva, para garantizar que los ficheros manuales existentes en dicha fecha se hayan ajustado a las disposiciones de la Directiva; que si los datos contenidos en dichos ficheros son tratados efectivamente de forma manual en ese período transitorio ampliado deberán, sin embargo, ser ajustados a dichas disposiciones cuando se realice tal tratamiento;

(70) Considerando que no es procedente que el interesado tenga que dar de nuevo su consentimiento a fin de que el responsable pueda seguir efectuando, tras la entrada en

vigor de las disposiciones nacionales adoptadas en virtud de la presente Directiva, el tratamiento de datos sensibles necesario para la ejecución de contratos celebrados previo consentimiento libre e informado antes de la entrada en vigor de las disposiciones mencionadas;

(71) Considerando que la presente Directiva no se opone a que un Estado miembro regule las actividades de prospección comercial destinadas a los consumidores que residan en su territorio, en la medida en que dicha regulación no afecte a la protección de las personas en lo que respecta a tratamientos de datos personales;

(72) Considerando que la presente Directiva autoriza que se tenga en cuenta el principio de acceso público a los documentos oficiales a la hora de aplicar los principios expuestos en la presente Directiva,

HAN ADOPTADO LA PRESENTE DIRECTIVA:

CAPÍTULO I - DISPOSICIONES GENERALES

Artículo 1

Objeto de la Directiva

1. Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales.

2. Los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los

Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1.

Artículo 2

Definiciones

A efectos de la presente Directiva, se entenderá por:

a)«datos personales»: toda información sobre una persona física identificada o identificable (el “interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social;

b)«tratamiento de datos personales,, («tratamiento,»: cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción;

c)"fichero de datos personales" ("fichero"): todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica; d)responsable del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos ,personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario; e)encargado del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento;

f)"tercero", la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento;

g)"destinatario": la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero. No obstante, las autoridades que puedan recibir una comunicación de datos en el marco de una investigación específica no serán considerados destinatarios;

h)"consentimiento del interesado".: toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan.

Artículo 3

Ámbito de aplicación

1. Las disposiciones de la presente Directiva se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

2. Las disposiciones de la presente Directiva no se aplicarán al tratamiento de datos personales:

- efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal;

- efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas.

Artículo 4

Derecho nacional aplicable

1. Los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando:

a) el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable;

b) el responsable del tratamiento no esté establecido en el territorio del Estado miembro, sino en un lugar en que se aplica su legislación nacional en virtud del Derecho internacional público;

c) el responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea.

2. En el caso mencionado en la letra c) del apartado 1, el responsable del tratamiento deberá designar un representante establecido en el territorio de dicho Estado miembro, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

CAPÍTULO II

Condiciones Generales Para La Licitud Del Tratamiento De Datos Personales

Artículo 5

Los Estados miembros precisarán, dentro de los límites de las disposiciones del presente capítulo, las condiciones en que son lícitos los tratamientos de datos personales.

Sección I. Principios Relativos A La Calidad De Los Datos

Artículo 6

1. Los Estados miembros dispondrán que los datos personales sean:

- a) tratados de manera leal y lícita;
- b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre Y cuando los Estados miembros establezcan las garantías oportunas;
- c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente;
- d) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificadas;
- e) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente.

Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos.

2. Corresponderá a los responsables del tratamiento garantizar el cumplimiento de lo dispuesto en el apartado

Sección II. Principios Relativos A La Legitimación Del Tratamiento De Datos

Artículo 7

Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si:

- a) el interesado ha dado su consentimiento de forma inequívoca,
- b) es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o
- c) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o
- d) es necesario para proteger el interés vital del interesado, o
- e) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o
- f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del Artículo 1 de la presente Directiva.

Sección III Categorías Especiales De Tratamientos

Artículo 8 Tratamiento de categorías especiales de datos

1. Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad.

2. Lo dispuesto en el apartado 1 no se aplicará cuando:

- a) el interesado haya dado su consentimiento explícito a dicho tratamiento, salvo en los casos en los que la legislación del Estado miembro disponga que la prohibición establecida en el apartado 1 no pueda levantarse con el consentimiento del interesado, o
- b) el tratamiento sea necesario para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho laboral en la medida en que esté autorizado por la legislación y ésta prevea garantías adecuadas, o
- c) el tratamiento sea necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento, o
- d) el tratamiento sea efectuado en el curso de sus actividades legítimas y con las debidas garantías por una fundación, una asociación o cualquier otro organismo sin fin de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera exclusivamente a sus miembros o a las personas que mantengan contactos regulares con la fundación, la asociación o el organismo por razón de su finalidad y con tal de que los datos no se comuniquen a terceros sin el consentimiento de los interesados, o
- e) el tratamiento se refiera a datos que el interesado haya hecho manifiestamente público o sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.

3. El apartado 1 no se aplicará cuando el tratamiento de datos resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto al secreto profesional sea en virtud de la legislación nacional, o de las normas establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto.

4. Siempre que dispongan las garantías adecuadas, los Estados miembros podrán, por motivos de interés público importantes, establecer otras excepciones, además de las previstas en el apartado 2, bien mediante su legislación nacional, bien por decisión de la autoridad de control.

5. El tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, sólo podrá efectuarse bajo el control de la autoridad pública o si hay previstas garantías específicas en el Derecho nacional, sin perjuicio de las excepciones que podrá establecer el Estado miembro basándose en disposiciones nacionales que prevean garantías apropiadas y específicas. Sin embargo, sólo podrá llevarse un registro completo de condenas penales bajo el control de los poderes públicos.

Los Estados miembros podrán establecer que el tratamiento de datos relativos a sanciones administrativas o procesos civiles se realicen asimismo bajo el control de los poderes públicos.

6. Las excepciones a las disposiciones del apartado 1 que establecen los apartados 4 y 5 se notificarán a la Comisión.

7. Los Estados miembros determinarán las condiciones en las que un número nacional de identificación o cualquier otro medio de identificación de carácter general podrá ser objeto de tratamiento.

Artículo 9

Tratamiento de datos personales y libertad de expresión

En lo referente al tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria, los Estados miembros establecerán, respecto de las disposiciones del presente capítulo, del capítulo IV y del capítulo VI, exenciones y excepciones sólo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión.

Sección IV. Información Del Interesado

Artículo 10

Información en caso de obtención de datos recabados del propio interesado

Los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán comunicar a la persona de quien se recaben los datos que le conciernan, por lo menos la información que se enumera a continuación, salvo si la persona ya hubiera sido informada de ello:

- a) la identidad del responsable del tratamiento y, en su caso, de su representante;
- b) los fines del tratamiento de que van a ser objeto los datos;
- c) cualquier otra información tal como:
 - los destinatarios o las categorías de destinatarios de los datos,
 - el carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder,
 - la existencia de derechos de acceso y rectificación de los datos que la conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que se obtengan los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado.

Artículo 11

Información cuando los datos no han sido recabados del propio interesado

1. Cuando los datos no hayan sido recabados del interesado, los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán, desde el momento del registro de los datos o, en caso de que se piense comunicar datos a un tercero, a más tardar, en el momento de la primera comunicación de datos, comunicar al interesado por lo menos la información que se enumera a continuación, salvo si el interesado ya hubiera sido informado de ello:

- a) la identidad del responsable del tratamiento y, en su caso, de su representante;
- b) los fines del tratamiento de que van a ser objeto los datos;
- c) cualquier otra información tal como:
 - las categorías de los datos de que se trate,
 - los destinatarios o las categorías de destinatarios de los datos,
 - la existencia de derechos de acceso y rectificación de los datos que la conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que se hayan obtenido los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado.

2. Las disposiciones del apartado 1 no se aplicarán, en particular para el tratamiento con fines estadísticos o de investigación histórica o científica, cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados o el registro o la comunicación a un tercero estén expresamente prescritos por ley. En tales casos, los Estados miembros establecerán las garantías apropiadas.

Sección V Derecho De Acceso Del Interesado A Los Datos

Artículo 12. Derecho de acceso

Los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento:

- a) libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos:
 - la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran Y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos;

- la comunicación, en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos;
 - el conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado, al menos en los casos de las decisiones automatizadas a que se refiere el apartado 1 del artículo 15;
- b) en su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos;
- c) la notificación a los terceros a quienes se hayan comunicado los datos de toda rectificación, supresión o bloqueo efectuado de conformidad con la letra b), si no resulta imposible o supone un esfuerzo desproporcionado.

Sección VI. Excepciones Y Limitaciones

Artículo 13 Excepciones y limitaciones

1. Los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones Y los derechos previstos en el apartado 1 del artículo 6, en el artículo 10, en el apartado 1 del artículo 11, y en los artículos 12 y 21 cuando tal limitación constituya una medida necesaria para la salvaguardia de:

- a) la seguridad del Estado;
- b) la defensa;
- c) la seguridad pública;
- d) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas;
- e) un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales;

f) una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e);

g) la protección del interesado o de los derechos y libertades de otras personas.

2. Sin perjuicio de las garantías legales apropiadas, que excluyen, en particular, que los datos puedan ser utilizados en relación con medidas o decisiones relativas a personas concretas, los Estados miembros podrán, en los casos en que manifiestamente no exista ningún riesgo de atentado contra la intimidad del interesado, limitar mediante una disposición legal los derechos contemplados en el artículo 12 cuando los datos se vayan a tratar exclusivamente con fines de investigación científica o se guarden en forma de archivos de carácter personal durante un período que no supere el tiempo necesario para la exclusiva finalidad de la elaboración de estadísticas.

Sección VII. Derecho De Oposición Del Interesado

Artículo 14. Derecho De Oposición Del Interesado

Los Estados miembros reconocerán al interesado el derecho a:

a) oponerse, al menos en los casos contemplados en las letras e) y f) del artículo 7, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos;

b) oponerse, previa petición y sin gastos, al tratamiento de los datos de carácter personal que le conciernan respecto de los cuales el responsable prevea un tratamiento destinado a la prospección; o ser informado antes de que los datos se comuniquen por primera vez a terceros o se usen en nombre de éstos a efectos de prospección, y a que se le ofrezca expresamente, el derecho de oponerse, sin gastos, a dicha comunicación o utilización.

Los Estados miembros adoptarán todas las medidas necesarias para garantizar que los interesados conozcan la existencia del derecho a que se refiere el párrafo primero de la letra b).

Artículo 15. Decisiones individuales automatizados

1. Los Estados miembros reconocerán a las personas el derecho a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc.

2. Los Estados miembros permitirán, sin perjuicio de lo dispuesto en los demás artículos de la presente Directiva, que una persona pueda verse sometida a una de las decisiones contempladas en el apartado 1 cuando dicha decisión:

a) se haya adoptado en el marco de la celebración o ejecución de un contrato, siempre que la petición de celebración o ejecución del contrato presentada por el interesado se haya satisfecho o que existan medidas apropiadas, como la posibilidad de defender su punto de vista, para la salvaguardia de su interés legítimo;

b) esté autorizada por una ley que establezca medidas que garanticen el interés legítimo del interesado.

Sección VIII Confidencialidad Y Seguridad Del Tratamiento

Artículo 16. Confidencialidad del tratamiento

Las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, solo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento o salvo en virtud de un imperativo legal.

Artículo 17. Seguridad del tratamiento

1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales.

Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse.

2. Los Estados miembros establecerán que el responsable del tratamiento, en caso de tratamiento por cuenta del mismo, deberá elegir un encargado del tratamiento que reúna garantías suficientes en relación con las medidas de seguridad técnica y de organización de los tratamientos que deban efectuarse, y se asegure de que se cumplen dichas medidas.

3. La realización de tratamientos por encargo deberá estar regulada por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento, y que disponga, en particular:

- que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento;
- que las obligaciones del apartado 1, tal como las define la legislación del Estado miembro en el que esté establecido el encargado, incumben también a éste.

4. A efectos de conservación de la prueba, las partes del contrato o del acto jurídico relativas a la protección de datos y a los requisitos relativos a las medidas a que hace referencia el apartado 1 constarán por escrito o en otra forma equivalente.

SECCIÓN IX

Notificación

Artículo 18. Obligación de notificación a la autoridad de control

1. Los Estados miembros dispondrán que el responsable del tratamiento o, en su caso, su representante, efectúe una notificación a la autoridad de control contemplada en el artículo 28, con anterioridad a la realización de un tratamiento o de un conjunto de tratamientos, total o parcialmente automatizados, destinados a la consecución de un fin o de varios fines conexos.

2. Los Estados miembros podrán disponer la simplificación o la omisión de la notificación, sólo en los siguientes casos y con las siguientes condiciones:

- cuando, para las categorías de tratamientos que no puedan afectar a los derechos y libertades de los interesados habida cuenta de los datos a que se refiere el tratamiento, los Estados miembros precisen los fines de los tratamientos, los datos o categorías de datos tratados, la categoría o categorías de los interesados, los destinatarios o categorías de destinatarios a los que se comuniquen los datos y el período de conservación de los datos y/o

- cuando el responsable del tratamiento designe, con arreglo al Derecho nacional al que está sujeto, un encargado de protección de los datos personales que tenga por cometido, en particular:

- hacer aplicar en el ámbito interno, de manera independiente, las disposiciones nacionales adoptadas en virtud de la presente Directiva,

- llevar un registro de los tratamientos efectuados por el responsable del tratamiento, que contenga la información enumerada en el apartado 2 del artículo 21, garantizando así que el tratamiento de los datos no pueda ocasionar una merma de los derechos y libertades de los interesados.

3. Los Estados miembros podrán disponer que no se aplique el apartado 1 a aquellos tratamientos cuya única finalidad sea la de llevar un registro que, en virtud de disposiciones legales o reglamentarias, esté destinado a facilitar información al público y estén abiertos a la consulta por el público en general o por toda persona que pueda demostrar un interés legítimo.

4. Los Estados miembros podrán eximir de la obligación de notificación o disponer una simplificación de la misma respecto de los tratamientos a que se refiere la letra d) del apartado 2 del artículo 5.

5. Los Estados miembros podrán disponer que los tratamientos no automatizados de datos de carácter personal o algunos de ellos sean notificados eventualmente de una forma simplificada.

Artículo 19. Contenido de la notificación

1. Los Estados miembros determinarán la información que debe figurar en la notificación, que será como mínimo:

a) el nombre y la dirección del responsable del tratamiento y, en su caso, de su representante;

b) el o los objetivos del tratamiento;

c) una descripción de la categoría o categorías de interesados y de los datos o categorías de datos a los que se refiere el tratamiento;

d) los destinatarios o categorías de destinatarios a los que se pueden comunicar los datos;

e) las transferencias de datos previstas a países terceros;

f) una descripción general que permita evaluar de modo preliminar si las medidas adoptadas en aplicación del artículo 17 resultan adecuadas para garantizar la seguridad del tratamiento.

2. Los Estados miembros precisarán los procedimientos por los que se notificarán a la autoridad de control las modificaciones que afecten a la información contemplada en el apartado 1.

Artículo 20. Controles previos

1. Los Estados miembros precisarán los tratamientos que puedan suponer riesgos específicos para los derechos y libertades de los interesados y velarán por que sean examinados antes del comienzo del tratamiento.

2. Estas comprobaciones previas serán realizadas por la autoridad de control una vez que haya recibido la notificación del responsable del tratamiento o por el encargado de la protección de datos quien, en caso de duda, deberá **consultar** a la autoridad de control.

3. Los Estados miembros podrán también llevar a cabo dicha comprobación en el marco de la elaboración de una norma aprobada por el Parlamento o basada en la misma norma, que defina el carácter del tratamiento y establezca las oportunas garantías.

Artículo 21. Publicidad de los tratamientos

1. Los Estados miembros adoptarán las medidas necesarias para garantizar la publicidad de los tratamientos.

2. Los Estados miembros establecerán que la autoridad de control lleve un registro de los tratamientos notificados con arreglo al artículo 18.

En el registro se harán constar, como mínimo, las informaciones a las que se refieren las letras a) a e) del apartado 1 del artículo 19.

El registro podrá ser consultado por cualquier persona.

3. Los Estados miembros dispondrán, en lo que respecta a los tratamientos no sometidos a notificación, que los responsables del tratamiento u otro órgano designado por los

Estados miembros comuniquen, en la forma adecuada, a toda persona que lo solicite, al menos las informaciones a que se refieren las letras a) a

e) del apartado 1 del artículo 19.

Los Estados miembros podrán establecer que esta disposición no se aplique a los tratamientos cuyo fin único sea llevar un registro, que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y que esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo.

Capítulo III. Recursos Judiciales, Responsabilidad Y Sanciones

Artículo 22. Recursos

Sin perjuicio del recurso administrativo que pueda interponerse, en particular ante la autoridad de control mencionada en el artículo 28, y antes de acudir a la autoridad judicial, los Estados miembros establecerán que toda persona disponga de un recurso judicial en caso de violación de los derechos que le garanticen las disposiciones de Derecho nacional aplicables al tratamiento de que se trate.

Artículo 23. Responsabilidad

1. Los Estados miembros dispondrán que toda persona que sufra un perjuicio como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la presente Directiva, tenga derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido.

2. El responsable del tratamiento podrá ser eximido parcial o totalmente de dicha responsabilidad si demuestra que no se le puede imputar el hecho que ha provocado el daño.

Artículo 24 Sanciones

Los Estados miembros adoptarán las medidas adecuadas para garantizar la plena aplicación de las disposiciones de la presente Directiva y determinarán, en particular, las sanciones que deben aplicarse en caso de incumplimiento de las disposiciones adoptadas en ejecución de la presente Directiva.

CAPÍTULO IV - TRANSFERENCIA DE DATOS PERSONALES A PAÍSES TERCEROS

Artículo 25. Principios

1. Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado.

2. El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurren en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

3. Los Estados miembros y la Comisión se informarán recíprocamente de los casos en que consideren que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2.

4. Cuando la Comisión compruebe, con arreglo al procedimiento establecido en el apartado 2 del artículo 31, que un tercer país no garantiza un nivel de protección

adecuado con arreglo al apartado 2 del presente artículo, los Estados miembros adoptarán las medidas necesarias para impedir cualquier transferencia de datos personales al tercer país de que se trate.

5. La Comisión iniciará en el momento oportuno las negociaciones destinadas a remediar la situación que se produzca cuando se compruebe este hecho en aplicación del apartado 4.

6. La Comisión podrá hacer constar, de conformidad con el procedimiento previsto en el apartado 2 del artículo 31, que un país tercero garantiza un nivel de protección adecuado de conformidad con el apartado

2 del presente artículo, a la vista de su legislación interna o de sus compromisos internacionales, suscritos especialmente al término de las negociaciones mencionadas en el apartado 5, a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas.

Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

Artículo 26. Excepciones

1. No obstante lo dispuesto en el artículo 25 y salvo disposición contraria del Derecho nacional que regule los casos particulares, los Estados miembros dispondrán que pueda efectuarse una transferencia de datos personales a un país tercero que no garantice un nivel de protección adecuado con arreglo a lo establecido en el apartado 2 del artículo 25, siempre y cuando:

a) el interesado haya dado su consentimiento inequívocamente a la transferencia prevista, o

- b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado, o
- c) la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero, o
- d) La transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, o
- e) la transferencia sea necesaria para la salvaguardia del interés vital del interesado, o
- f) la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta.

2. Sin perjuicio de lo dispuesto en el apartado 1, los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado con arreglo al apartado 2 del artículo 25, cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas.

3. Los Estados miembros informarán a la Comisión y a los demás Estados miembros acerca de las autorizaciones que concedan con arreglo al apartado 2.

En el supuesto de que otro Estado miembro o la Comisión expresaron su oposición y la justificaran debidamente por motivos derivados de la protección de la vida privada y de los derechos y libertades fundamentales de las personas, la Comisión adoptará las medidas adecuadas con arreglo al procedimiento establecido en el apartado 2 del artículo 31.

Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

4. Cuando la Comisión decida, según el procedimiento establecido en el apartado 2 del artículo 31, que determinadas cláusulas contractuales tipo ofrecen las garantías suficientes establecidas en el apartado 2, los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

CAPÍTULO V - CÓDIGOS DE CONDUCTA

Artículo 27

1. Los Estados miembros y la Comisión alentarán la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por los Estados miembros en aplicación de la presente Directiva.

2. Los Estados miembros establecerán que las asociaciones profesionales, y las demás organizaciones representantes de otras categorías de responsables de tratamientos, que hayan elaborado proyectos de códigos nacionales o que tengan la intención de modificar o prorrogar códigos nacionales existentes puedan someterlos a examen de las autoridades nacionales.

Los Estados miembros establecerán que dicha autoridad vele, entre otras cosas, por la conformidad de los proyectos que le sean sometidos con las disposiciones nacionales adoptadas en aplicación de la presente

Directiva. Si lo considera conveniente, la autoridad recogerá las observaciones de los interesados o de sus representantes.

3. Los proyectos de códigos comunitarios, así como las modificaciones o prórrogas de códigos comunitarios existentes, podrán ser sometidos a examen del grupo contemplado en el artículo 29. Éste se pronunciará, entre otras cosas, sobre la conformidad de los proyectos que le sean sometidos con las disposiciones nacionales adoptadas en aplicación de la presente Directiva. Si lo considera conveniente, el Grupo recogerá las observaciones de los interesados o de sus representantes. La Comisión podrá efectuar una publicidad adecuada de los códigos que hayan recibido un dictamen favorable del grupo.

CAPÍTULO VI - AUTORIDAD DE CONTROL Y GRUPO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES

Artículo 28

Autoridad de control

1. Los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva.

Estas autoridades ejercerán las funciones que les son atribuidas con total independencia.

2. Los Estados miembros dispondrán que se consulte a las autoridades de control en el momento de la elaboración de las medidas reglamentarias o administrativas relativas a la protección de los derechos y libertades de las personas en lo que se refiere al tratamiento de datos de carácter personal.

3. La autoridad de control dispondrá, en particular, de:

- poderes de investigación, como el derecho de acceder a los datos que sean objeto de un tratamiento y el de recabar toda la información necesaria para el cumplimiento de su misión de control;
- poderes efectivos de intervención, como, por ejemplo, el de formular dictámenes antes de realizar los tratamientos, con arreglo al artículo 20, y garantizar una publicación adecuada de dichos dictámenes, o el de ordenar el bloqueo, la supresión o la destrucción de datos, o incluso prohibir provisional o definitivamente un tratamiento, o el de dirigir una advertencia o amonestación al responsable del tratamiento o el de someter la cuestión a los parlamentos u otras instituciones políticas nacionales;
- capacidad procesal en caso de infracciones a las disposiciones nacionales adoptadas en aplicación de la presente Directiva o de poner dichas infracciones en conocimiento de la autoridad judicial.

Las decisiones de la autoridad de control lesivas de derechos podrán ser objeto de recurso jurisdiccional.

4. Toda autoridad de control entenderá de las solicitudes que cualquier persona, o cualquier asociación que

la represente, le presente en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales. Esa persona será informada del curso dado a su solicitud.

Toda autoridad de control entenderá, en particular, de las solicitudes de verificación de la licitud de un tratamiento que le presente cualquier persona cuando sean de aplicación las disposiciones nacionales tomadas en virtud del artículo 13 de la presente Directiva. Dicha persona será informada en todos los casos de que ha tenido lugar una verificación.

5. Toda autoridad de control presentará periódicamente un informe sobre sus actividades. Dicho informe será publicado.

6. Toda autoridad de control será competente, sean cuales sean las disposiciones de Derecho nacional aplicables al tratamiento de que se trate, para ejercer en el territorio de su propio Estado miembro los poderes que se le atribuyen en virtud del apartado 3 del presente artículo. Dicha autoridad podrá ser instada a ejercer sus poderes por una autoridad de otro Estado miembro.

Las autoridades de control cooperarán entre sí en la medida necesaria para el cumplimiento de sus funciones, en particular mediante el intercambio de información que estimen útil.

7. Los Estados miembros dispondrán que los miembros y agentes de las autoridades de control estarán sujetos, incluso después de haber cesado en sus funciones, al deber de secreto profesional sobre informaciones confidenciales a las que hayan tenido acceso.

Artículo 29

Grupo de protección de las personas en lo que respecta al tratamiento de datos personales.

1. Se crea un grupo de protección de las personas en lo que respecta al tratamiento de datos personales, en lo sucesivo denominado «Grupo».

Dicho Grupo tendrá carácter consultivo e independiente.

2. El Grupo estará compuesto por un representante de la autoridad o de las autoridades de control designadas por cada Estado miembro, por un representante de la autoridad o autoridades creadas por las instituciones y organismos comunitarios, y por un representante de la Comisión.

Cada miembro del Grupo será designado por la institución, autoridad o autoridades a que represente.

Cuando un Estado miembro haya designado varias autoridades de control, éstas nombrarán a un representante común. Lo mismo harán las autoridades creadas por las instituciones y organismos comunitarios.

3. El Grupo tomará sus decisiones por mayoría simple de los representantes de las autoridades de control.

4. El Grupo elegirá a su presidente. El mandato del presidente tendrá una duración de dos años. El mandato será renovable.

5. La Comisión desempeñará las funciones de secretaría del Grupo.

6. El Grupo aprobará su reglamento interno.

7. El Grupo examinará los asuntos incluidos en el orden del día por su presidente, bien por iniciativa de éste, bien previa solicitud de un representante de las autoridades de control, bien a solicitud de la Comisión.

Artículo 30

1. El Grupo tendrá por cometido:

a) estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la presente Directiva con vistas a contribuir a su aplicación homogénea;

b) emitir un dictamen destinado a la Comisión sobre el nivel de protección existente dentro de la Comunidad y en los países terceros;

c) asesorar a la Comisión sobre cualquier proyecto de modificación de la presente Directiva, cualquier proyecto de medidas adicionales o específicas que deban adaptarse para salvaguardar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales, así como sobre cualquier otro proyecto de medidas comunitarias que afecte a dichos derechos y libertades;

d) emitir un dictamen sobre los códigos de conducta elaborados a escala comunitaria.

2. Si el Grupo comprobaré la existencia de divergencias entre la legislación y la práctica de los Estados miembros que pudieren afectar a la equivalencia de la protección de las personas en lo que se refiere al tratamiento de datos personales en la Comunidad, informará de ello a la Comisión.
3. El Grupo podrá, por iniciativa propia, formular recomendaciones sobre cualquier asunto relacionado con la protección de las personas en lo que respecta al tratamiento de datos personales en la Comunidad.
4. Los dictámenes y recomendaciones del Grupo se transmitirán a la Comisión Y al Comité contemplado en el artículo 31.
5. La Comisión informará al Grupo del curso que haya dado a los dictámenes y recomendaciones. A tal efecto, elaborará un informe, que será transmitido asimismo al Parlamento Europeo y al Consejo. Dicho informe será publicado.
6. El Grupo elaborará un informe anual sobre la situación de la protección de las personas físicas en lo que respecta al tratamiento de datos personales en la Comunidad y en los países terceros, y lo transmitirá al Parlamento Europeo, al Consejo y a la Comisión. Dicho informe será publicado.

CAPÍTULO VII - MEDIDAS DE EJECUCIÓN COMUNITARIAS

Artículo 31

El Comité

1. La Comisión estará asistida por un Comité compuesto por representantes de los Estados miembros y presidido por el representante de la Comisión.
2. El representante de la Comisión presentará al Comité un proyecto de las medidas que se hayan de adoptar. El Comité emitirá su dictamen sobre dicho proyecto en un plazo que el presidente podrá determinar en función de la urgencia de la cuestión de que se trate.

El dictamen se emitirá según la mayoría prevista en el apartado 2 del artículo 148 del Tratado. Los votos de los representantes de los Estados miembros en el seno del Comité se ponderarán del modo establecido en el artículo anteriormente citado. El presidente no tomará parte en la votación.

La Comisión adoptará las medidas que serán de aplicación inmediata. Sin embargo, si dichas medidas no fueren conformes al dictamen del Comité, habrán de ser comunicadas sin demora por la Comisión al Consejo. En este caso: la Comisión aplazará la aplicación de las medidas que ha decidido por un período de tres meses a partir de la fecha de dicha comunicación; el Consejo, actuando por mayoría cualificada, podrá adoptar una decisión diferente dentro del plazo de tiempo mencionado en el primer guión.

DISPOSICIONES FINALES

Artículo 32

1. Los Estados miembros adoptarán las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva, a más tardar al final de un período de tres años a partir de su adopción.

Cuando los Estados miembros adopten dichas disposiciones, éstas harán referencia a la presente Directiva o irán acompañadas de dicha referencia en su publicación oficial. Los Estados miembros establecerán las modalidades de la mencionada referencia.

2. Los Estados miembros velarán por que todo tratamiento ya iniciado en la fecha de entrada en vigor de las disposiciones de Derecho nacional adoptadas en virtud de la presente Directiva se ajuste a dichas disposiciones dentro de un plazo de tres años a partir de dicha fecha.

No obstante lo dispuesto en el párrafo primero, los Estados miembros podrán establecer que el tratamiento de datos que ya se encuentren incluidos en ficheros manuales en la

fecha de entrada en vigor de las disposiciones nacionales adoptadas en aplicación de la presente Directiva, deba ajustarse a lo dispuesto en los artículos 6, 7 y 8 en un plazo de doce años a partir de la adopción de la misma. No obstante, los Estados miembros otorgarán al interesado, previa solicitud y, en particular, en el ejercicio de su derecho de acceso, el derecho a que se rectifiquen, supriman o bloqueen los datos incompletos, inexactos o que hayan sido conservados de forma incompatible con los fines legítimos perseguidos por el responsable del tratamiento.

3. No obstante lo dispuesto en el apartado 2, los Estados miembros podrán disponer, con sujeción a las garantías adecuadas, que los datos conservados únicamente a efectos de investigación histórica no deban ajustarse a lo dispuesto en los artículos 6, 7 y 8 de la presente Directiva.

4. Los Estados miembros comunicarán a la Comisión el texto de las disposiciones de Derecho interno que adopten en el ámbito regulado por la presente Directiva.

Artículo 33

La Comisión presentará al Consejo y al Parlamento Europeo periódicamente y por primera vez en un plazo de tres años a partir de la fecha mencionada en el apartado 1 del artículo 32 un informe sobre la aplicación de la presente Directiva, acompañado, en su caso, de las oportunas propuestas de modificación. Dicho informe será publicado.

La Comisión estudiará, en particular, la aplicación de la presente Directiva al tratamiento de datos que consistan en sonidos e imágenes relativos a personas físicas y presentará las propuestas pertinentes que puedan resultar necesarias en función de los avances de la tecnología de la información, y a la luz de los trabajos de la sociedad de la información.

Artículo 34

Los destinatarios de la presente Directiva serán los Estados miembros.

Hecho en Luxemburgo, el 24 de octubre de 1995.

Por el Parlamento Europeo Por el Consejo

El Presidente El Presidente

K. HANSCH L. ATIENZA SERNA

DO n° C 277 de 5. 11. 1990, p. 3 y DO n° C 311 de 27. 11. 1992, p. 30.

(2) DO n° 159 de 17. 6. 1991, p. 38.

(3) Dictamen del Parlamento Europeo de 11 de marzo de 1992 (DO no C 94 de 13. 4. 1992, p. 198), confirmado el 2 de diciembre de 1993 (DO n° C 342 de 20. 12. 1993, p. 30); posición común del Consejo de 20 de febrero de 1995 (DO n° C 93 de 13. 4. 1995, p. 1) y Decisión del Parlamento Europeo de 15 de junio de 1995 (DO n° C 166 de 3. 7. 1995).

1 DO n° C 277 de 5. 11. 1990, p. 3 y DO n° C 311 de 27. 11. 1992, p. 30.

2 DO n° 159 de 17. 6. 1991, p. 38.

3 Dictamen del Parlamento Europeo de 11 de marzo de 1992 (DO no C 94 de 13. 4. 1992, p. 198), confirmado el 2 de diciembre de 1993 (DO n° C 342 de 20. 12. 1993, p. 30); posición común del Consejo de 20 de febrero de 1995 (DO n° C 93 de 13. 4. 1995, p. 1) y Decisión del Parlamento Europeo de 15 de junio de 1995 (DO n° C 166 de 3. 7. 1995).

4 DO n° L197 de 18.7. 1987, p. 33.

Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado constitutivo de la Comunidad Europea y, en particular, su artículo 100 A,

Vista la propuesta de la Comisión (1)

Visto el dictamen del Comité Económico y Social (2),

De conformidad con el procedimiento establecido en el artículo 189 B del Tratado (3), a la vista del texto con junto aprobado el 6 de noviembre de 1997 por el Comité de conciliación,

(1) Considerando que la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos (4) insta a los Estados miembros a garantizar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de los datos personales y, en especial, su derecho a la intimidad, de forma que los datos personales puedan circular libremente en la Comunidad;

(2) Considerando que la confidencialidad de las comunicaciones está garantizada de conformidad con los instrumentos internacionales relativos a los derechos humanos (especialmente el Convenio europeo para la protección de los derechos humanos y de las libertades fundamentales) y las constituciones de los Estados miembros;

(1) DO C 200 de 22.7.1994, p. 4.

(2) DO C 159 de 17.6.1991, p. 38.

(3) Dictamen del Parlamento Europeo de 11 de marzo de 1992 (DO C 94 de 13.4.1992, p. 198), Posición común del Consejo de 12 de septiembre de 1996 (DO C 315 de 24.10.1996, p. 30) y Decisión del Parlamento Europeo de 16 de enero de 1997 (DO C 33 de 3.2.1997, p. 78). Decisión del Parlamento Europeo de 20 de noviembre de 1997 (DO C 371 de 8.12.1997). Decisión del Consejo de 1 de diciembre de 1997.

(4) DO L 281 de 23.11.1995, p. 31.

(3) Considerando que en la actualidad están apareciendo en la Comunidad Europea nuevas redes digitales públicas avanzadas de telecomunicación que crean necesidades específicas en materia de protección de datos personales y de la intimidad de los usuarios; que el desarrollo de la sociedad de la información se caracteriza por la introducción de nuevos servicios de telecomunicación; que el desarrollo transfronterizo de estos servicios, como el vídeo por pedido o la televisión interactiva, depende en parte de la confianza de los usuarios en que no se pondrá en peligro su intimidad;

(4) Considerando que esto está ocurriendo en especial con la introducción de la red digital de servicios integrados (RDSI) y las redes móviles digitales;

(5) Considerando que, en su Resolución, de 30 de junio de 1988, sobre el desarrollo del mercado común de los servicios y equipos de telecomunicación en el horizonte de 1992(5), el Consejo preconizó la adopción de medidas de protección de los datos personales con objeto de crear un marco adecuado para el futuro desarrollo de las telecomunicaciones dentro de la Comunidad; que el Consejo volvió a subrayar la importancia de la protección de los datos personales y de la intimidad en su Resolución, de 18 de julio de

1989, sobre una mayor coordinación en la introducción de la Red Digital de Servicios Integrados (RDSI) en la Comunidad Europea para 1992 (6);

(6) Considerando que el Parlamento Europeo subrayó la importancia de proteger los datos personales y la intimidad en las redes de telecomunicación, especialmente en relación con la introducción de la RDSI;

(7) Considerando que, en el caso de las redes públicas de telecomunicación, deben elaborarse disposiciones legales, reglamentarias y técnicas específicas con objeto de proteger los derechos y libertades fundamentales de las personas físicas y los intereses legítimos de las personas jurídicas, en particular frente a los riesgos crecientes derivados del almacenamiento y el tratamiento informático de datos relativos a abonados y usuarios;

(5) DO C 257 de 4.10.1988, p. 1.

(6) DO C 196 de 1.8.1989, p. 4.

(8) Considerando que las disposiciones legales, reglamentarias y técnicas adoptadas por los Estados miembros para proteger los datos personales, la intimidad y los intereses legítimos de las personas jurídicas, en el sector de la telecomunicación, deben armonizarse a fin de evitar obstáculos para el mercado interior de las telecomunicaciones de conformidad con el objetivo establecido en el artículo 7 A del Tratado; que una armonización se limitará a los requisitos necesarios para garantizar que no se obstaculice la promoción y el desarrollo de nuevos servicios de telecomunicación y nuevas redes entre Estados miembros;

(9) Considerando que los Estados miembros, los pro veedores y los usuarios afectados y las instancias comunitarias competentes deberían cooperar para el establecimiento y el desarrollo de las tecnologías pertinentes siempre que ello sea necesario para aplicar las garantías previstas por las disposiciones de la presente Directiva;

(10) Considerando que estos nuevos servicios incluyen la televisión interactiva y el vídeo por pedido;

(11) Considerando que en el sector de las telecomunicaciones se aplica la Directiva 95/46/CE, para todas las cuestiones relativas a la protección de los derechos y libertades fundamentales que no están cubiertas de forma específica por las disposiciones de la presente Directiva, incluidas las obligaciones del controlador y los derechos de las personas; que la Directiva 95/46/CE se aplica a los servicios de telecomunicaciones que no están disponibles para el público; (12) Considerando que la presente Directiva no aborda cuestiones en materia de protección de los derechos y libertades fundamentales relacionadas con actividades no regidas por la legislación comunitaria, de manera semejante a lo que dispone el artículo 3 de la Directiva 95/46/CE; que corresponde a los Estados miembros adoptar las medidas que consideren necesarias para la protección de la defensa de la seguridad pública, la seguridad del Estado (incluido el bienestar económico del Estado cuando las actividades tengan relación con asuntos de seguridad del Estado) y la aplicación del Derecho penal; que la presente Directiva no afectará a la capacidad de los Estados miembros a interceptar legalmente las telecomunicaciones para cualquiera de estos fines;

(13) Considerando que los abonados de un servicio público de telecomunicación pueden ser personas físicas o jurídicas; que las disposiciones de la presente Directiva están destinadas a proteger, como complemento de la Directiva 95/46/CE, los derechos fundamentales de las personas físicas y, en particular, su derecho a la intimidad, así como los intereses legítimos de las personas jurídicas; que dichas disposiciones no podrán en caso alguno conllevar una obligación por parte de los Estados miembros de extender la aplicación de la Directiva 95/46/CE a la protección de los intereses

legítimos de las personas jurídicas; que dicha protección está garantizada en el marco de la legislación comunitaria y nacional aplicable;

(14) Considerando que la aplicación de determinadas exigencias relativas a la presentación y a la limitación de la identificación de la línea llamante y de la línea conectada y a la presentación automática a las líneas de abonado conectadas a centrales analógicas no debe ser obligatoria en aquellos casos particulares en los que dicha aplicación resulte imposible técnicamente, o en los que requiera un esfuerzo económico desproporcionado; que es importante que las partes interesadas sean informadas de dichos casos, y que los Estados miembros deben notificarlos a la Comisión;

(15) Considerando que los proveedores de servicios deben tomar las medidas adecuadas para salvaguardar la seguridad de sus servicios, en su caso en conjunción con el proveedor de la red, e informar a los abonados de todo riesgo concreto de violación de la seguridad de la red; que la seguridad se valora a la luz de lo dispuesto en el artículo 17 de la Directiva 95/46/CE;

(16) Considerando que deben adoptarse medidas para evitar el acceso no autorizado a las comunicaciones a fin de proteger la confidencialidad de las mismas por medio de las redes públicas de telecomunicaciones y de servicios de telecomunicaciones a disposición pública; que la legislación nacional de algunos Estados miembros prohíbe solamente el acceso intencionado no autorizado a las comunicaciones;

(17) Considerando que los datos relativos a los abonados utilizados para el establecimiento de llamadas contienen información sobre la vida privada de las personas físicas y atañen a su derecho de respeto a la correspondencia, o afectan a los intereses legítimos de las personas jurídicas; que dichos datos sólo podrán almacenarse en la medida en que resulten necesarios para la prestación del servicio, para fines de facturación y para los pagos de interconexión, durante un período limitado; que

cualquier tratamiento que el proveedor del servicio público de telecomunicación pretenda llevar a cabo para la prospección de sus propios servicios de telecomunicaciones sólo puede permitirse si el abonado ha manifestado su acuerdo sobre la base de una información plena y exacta facilitada por el proveedor de servicios públicos de telecomunicaciones acerca del tipo de tratamiento que pretende llevar a cabo;

(18) Considerando que la introducción de facturas desglosadas ha mejorado las posibilidades para que el abonado pueda verificar que las tarifas aplicadas por el proveedor del servicio son correctas y que, al mismo tiempo, puede poner en peligro la intimidad de los usuarios de servicios públicos de telecomunicaciones; que por consiguiente, a fin de proteger la intimidad de los usuarios, los Estados miembros deben fomentar el desarrollo de opciones de servicios de telecomunicaciones, como posibilidades de pago que permitan el acceso anónimo o estrictamente privado a través del pago con tarjetas de crédito; considerando que los Estados miembros también podrán exigir, con el mismo fin, que se suprima un determinado número de cifras de los números a los que se haya llamado y mencionados en las facturas desglosadas;

(19) Considerando que es necesario, por lo que respecta a la identificación del número de la línea llamante, proteger el derecho del interlocutor que efectúa la llamada a reservarse la identificación de la línea desde la que realiza dicha llamada y el derecho del interlocutor llamado a rechazar llamadas de líneas no identificadas; que está justificado anular la eliminación de la presentación de la identificación de la línea llamante en casos particulares; que determinados abonados, en particular las líneas de auxilio y otras organizaciones similares, tienen interés en garantizar el anonimato de sus interlocutores; que es necesario, por lo que respecta a la identificación de la línea conectada, proteger el derecho y el interés legítimos de la persona llamada a impedir la

presentación de la identificación de la línea a la que la persona que llama está conectada realmente, en particular en el caso de los servicios de desvío de llamadas; que los proveedores de los servicios públicos de telecomunicaciones debe informar a sus abonados de la existencia de la identificación de líneas llamantes y conectadas en la red y de todos los servicios ofrecidos sobre la base de la identificación de las líneas llamantes y conectadas y sobre las opciones de confidencialidad disponibles; que esto permitirá a los abonados llevar a cabo una elección informada sobre las posibilidades de confidencialidad que deseen utilizar; que las opciones de confidencialidad ofrecidas caso por caso no tienen que estar disponibles necesariamente como servicio de la red automática, pero pueden obtenerse mediante simple solicitud al proveedor del servicio público de telecomunicaciones;

(20) Considerando que deben ofrecerse garantías a los abonados contra las molestias que puedan causar las llamadas desviadas automáticamente por otros; que en tales casos los abonados deben poder detener las llamadas desviadas hacia sus terminales mediante simple solicitud al proveedor de servicios públicos de telecomunicaciones;

(21) Considerando que las guías son ampliamente divulgadas y accesibles al público; que el derecho a la intimidad de las personas físicas y el interés legítimo de las personas jurídicas exigen que los abonados puedan decidir en qué medida se publican sus datos personales en dichas guías; que los Estados miembros podrán reservar esta posibilidad a los abonados que son personas físicas;

(22) Considerando que deben ofrecerse garantías a los abonados contra la intrusión en su intimidad mediante llamadas no solicitadas y por fax; que los Estados miembros podrán reservar estas protecciones a los abonados que son personas físicas;

(23) Considerando que debe garantizarse la armonización en la introducción de características técnicas de equipos de telecomunicación para la protección de datos, a fin de que sea compatible con la realización del mercado interior;

(24) Considerando, en particular, y de forma similar a lo establecido en el artículo 13 de la Directiva

95/46/CE, que los Estados miembros pueden restringir el ámbito de las obligaciones y los derechos de los abonados en determinadas circunstancias, por ejemplo, garantizando que el proveedor del servicio público de telecomunicaciones podrá anular la eliminación de la presentación de la identificación de la línea llamante de conformidad con la legislación nacional a efecto de evitar o detectar delitos o por razones de seguridad del Estado;

(25) Considerando que, en los casos en que no se respeten los derechos de los usuarios y abonados, el

Derecho nacional debe prever vías de recurso judiciales; que deben imponerse sanciones a aquellas personas, ya sean de derecho público o privado, que incumplan las medidas nacionales adoptadas en virtud de la presente Directiva;

(26) Considerando que resulta útil en el ámbito de aplicación de la presente Directiva aprovechar las experiencias del Grupo de protección de las personas en lo que respecta al tratamiento de datos personales, formado por representantes de las autoridades competentes de los Estados miembros, creado por el artículo 29 de la Directiva 95/46/CE;

(27) Considerando que, en vista de los desarrollos tecnológicos y de la evolución que se espera de los servicios ofrecidos, será necesario especificar técnicamente las categorías de datos enumeradas en el anexo de la presente Directiva para la aplicación de su artículo 6, con la asistencia del Comité formado por representantes de los Estados

miembros y creado por el artículo 31 de la Directiva 95/46/CE, a fin de garantizar una aplicación coherente de los requisitos que establece la presente Directiva, independientemente de los cambios de la tecnología; que este procedimiento se aplicará únicamente a las especificaciones necesarias para adaptar el anexo a nuevos avances tecnológicos teniendo en cuenta los cambios en la demanda del mercado y de los consumidores; que la Comisión deberá informar debidamente al Parlamento Europeo de su intención de aplicar este procedimiento; que en cualquier otro caso se aplicará el procedimiento establecido en el artículo 100 A del Tratado;

(28) Considerando que, para facilitar el cumplimiento de lo dispuesto en la presente Directiva, son necesarias determinadas disposiciones particulares para el tratamiento de datos ya iniciado en la fecha en que entre en vigor la legislación nacional de aplicación de la presente Directiva,

HAN ADOPTADO LA PRESENTE DIRECTIVA:

Artículo 1

Objeto y ámbito de aplicación

1. La presente Directiva establece la armonización de las disposiciones de los Estados miembros necesarios para garantizar un nivel equivalente de protección de las libertades y de los derechos fundamentales y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales en el sector de las telecomunicaciones, así como la libre circulación de tales datos y de los equipos y servicios de telecomunicación en la Comunidad.

2. A los efectos mencionados en el apartado 1, las disposiciones de la presente Directiva especificarán y completarán la Directiva 95/46/CE. Además, protegerán los intereses legítimos de los abonados que sean personas jurídicas.

3. La presente Directiva no se aplicará a las actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos y y VI del Tratado de la Unión Europea y, en cualquier caso, a las actividades que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dichas actividades estén relacionadas con la seguridad del Estado) y a las actividades del Estado en materia penal.

Artículo 2

Definiciones

A los efectos de la presente Directiva y además de las definiciones recogidas en la Directiva 95/46/CE, se entenderá por:

- a) «abonado»: la persona física o jurídica que sea parte en un contrato con el proveedor en un servicio público de telecomunicaciones para la prestación de tales servicios;
- b) «usuario»: la persona que utiliza un servicio público de telecomunicación con fines privados o comerciales, aunque no haya contratado dicho servicio;
- c) «red pública de telecomunicación»: los sistemas de transmisión y, cuando proceda, los equipos de conmutación y otros recursos que permiten la transmisión de señales entre puntos de terminación definidos por cable, por medios radioeléctricos, por medios ópticos o por otros medios electromagnéticos que se utilizan, total o parcialmente, para la prestación de servicios públicos de telecomunicación;
- d) «servicio de telecomunicación»: un servicio cuya prestación consiste total o parcialmente en la transmisión y el envío de señales a través de redes de telecomunicación, excepción hecha de la radiodifusión sonora y de la televisión.

Artículo 3

Servicios regulados

1. La presente Directiva se aplicará al tratamiento de datos personales en relación con la prestación de servicios públicos de telecomunicación en las redes públicas de telecomunicación en la Comunidad y, especialmente, a través de la red digital de servicios integrados (RDSI) y las redes móviles digitales públicas.
2. Los artículos 8, 9 y 10 se aplicarán a las líneas de abonado conectadas a centrales digitales y, siempre y cuando sea técnicamente posible y no exija un esfuerzo económico desproporcionado, a las líneas de abonado conectadas a centrales analógicas.
3. Los Estados miembros notificarán a la Comisión aquellos casos en los que no sea posible técnicamente cumplir los requisitos de los artículos 8, 9 y 10, o que exijan una inversión desproporcionada para ello.

Artículo 4

Seguridad

1. El proveedor de un servicio público de telecomunicación deberá adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios, de ser necesario en colaboración con el proveedor de la red pública de telecomunicación por lo que respecta a la seguridad de la red. Considerando las técnicas más avanzadas y el coste de su aplicación, dichas medidas garantizarán un nivel de seguridad adecuado para el riesgo existente.
2. En caso de que exista un riesgo concreto de violación de la seguridad de la red, el proveedor de un servicio público de telecomunicación deberá informar a los abonados sobre dicho riesgo y sobre las posibles soluciones, incluidos los costes necesarios.

Artículo 5

Confidencialidad de las comunicaciones

1. Los Estados miembros garantizarán, mediante normas nacionales, la confidencialidad de las comunicaciones realizadas a través de las redes públicas de telecomunicación y de los servicios de telecomunicación accesibles al público. En particular, prohibirán la escucha, la grabación, el almacenamiento u otros tipos de interceptación o vigilancia de las comunicaciones por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando esté autorizada legalmente, de conformidad con el apartado 1 del artículo 14.

2. El apartado 1 no se aplicará a las grabaciones legalmente autorizadas de comunicaciones en el marco de una práctica comercial lícita destinada a aportar pruebas de una transacción comercial o de cualquier otra comunicación comercial.

Artículo 6

Tráfico y facturación

1. Sin perjuicio de lo dispuesto en los apartados 2, 3 y 4, los datos sobre tráfico relacionados con los usuarios y abonados tratados para establecer comunicaciones y almacenados por el proveedor de una red o servicio público de telecomunicación deberán destruirse o hacerse anónimos en cuanto termine la comunicación.

2. A los efectos de la facturación de los usuarios y de los pagos de las interconexiones, podrán ser tratados los datos indicados en el anexo. Se autorizará este tratamiento únicamente hasta la expiración del plazo durante el cual pueda impugnarse legalmente la factura o exigirse el pago.

3. El proveedor de un servicio público de telecomunicación podrá tratar los datos a que se hace referencia en el apartado 2 para la promoción comercial de sus propios servicios de telecomunicación siempre y cuando el abonado haya dado su consentimiento.

4. El tratamiento de los datos de tráfico y facturación deberá limitarse a las personas que actúen bajo las órdenes del proveedor de la red o del servicio público de

telecomunicación que se ocupe de la gestión de la facturación o del tráfico, de las solicitudes de información de los clientes y de la detección de fraudes y promoción comercial de los propios servicios del proveedor, y deberá limitarse a lo necesario para realizar tales actividades.

5. Los apartados 1, 2, 3 y 4 se aplicarán sin perjuicio de la posibilidad de que las autoridades competentes sean informadas de los datos sobre facturación o tráfico con arreglo a la legislación aplicable, con vistas a resolver litigios, en particular los litigios relativos a la interconexión o a la facturación.

Artículo 7

Facturación desglosada

1. Los abonados tendrán el derecho a recibir facturas no desglosadas.
2. Los Estados miembros aplicarán las disposiciones nacionales a fin de reconciliar los derechos de los abonados que reciban facturas desglosadas con el derecho a la intimidad de los usuarios que efectúen llamadas y de los abonados que reciban llamadas, por ejemplo, garantizando que dichos usuarios y abonados dispongan de suficientes otras modalidades de comunicación o de pago.

Artículo 8

Presentación y limitación de la identificación de la línea llamante y conectada

1. Cuando se ofrezca la posibilidad de presentar la identificación de la línea llamante, el usuario que origine la llamada deberá poder suprimir en cada llamada, mediante un procedimiento sencillo y gratuito, la identificación de la línea llamante. El abonado que origine la llamada deberá tener esta posibilidad por línea.
2. Cuando se ofrezca la posibilidad de presentar la identificación de la línea llamante, el abonado que reciba la llamada deberá tener la posibilidad, mediante un procedimiento

sencillo y gratuito siempre que haga un uso correcto de esta función, de impedir la presentación de la identificación de la línea llamante en las llamadas entrantes.

3. Cuando se ofrezca la posibilidad de presentar la identificación de la línea llamante y ésta se presente con anterioridad a que se establezca la llamada, el abonado que reciba la llamada deberá tener la posibilidad, mediante un procedimiento sencillo, de rechazar las llamadas entrantes procedentes de usuarios o abonados que hayan suprimido la presentación de la identificación de la línea que origina la llamada.

4. Cuando se ofrezca la posibilidad de presentar la identificación de la línea conectada, el abonado que reciba la llamada deberá tener la posibilidad, por un procedimiento sencillo y gratuito, de suprimir la presentación de la identificación de la línea conectada a la parte llamante.

5. Las disposiciones establecidas en el apartado 1 se aplicarán también a las llamadas efectuadas desde la

Comunidad a terceros países; las disposiciones establecidas en los apartados 2, 3 y 4 se aplicarán también a las llamadas entrantes procedentes de terceros países.

6. Los Estados miembros velarán por que, cuando se ofrezca la posibilidad de presentar la identificación de la línea llamante o de la línea conectada, los proveedores de servicios públicos de telecomunicaciones informen al público sobre dicha posibilidad y sobre las que se establecen en los apartados 1, 2, 3 y 4.

Artículo 9

Excepciones

Los Estados miembros velarán por que existan procedimientos transparentes que determinen la forma en que el proveedor de una red pública de telecomunicación y/o de un servicio de telecomunicación accesible al público puede anular la supresión de la presentación de la identificación de la línea llamante:

- a) por un período de tiempo limitado, a instancia del abonado que solicite la identificación de llamadas maliciosas o molestas; en tal caso, los datos que incluyan la identificación del abonado que origina la llamada serán almacenados y puestos a disposición por el proveedor de la red pública de telecomunicación o del servicio público de telecomunicación, de acuerdo con el Derecho nacional;
- b) por línea, para las entidades reconocidas por un Estado miembro que atiendan las llamadas de urgencia, incluidos los cuerpos de policía, los servicios de ambulancia y los cuerpos de bomberos, para que puedan responder a tales llamadas.

Artículo 10

Desvío automático de llamadas

Los Estados miembros velarán por que se ofrezca a todo abonado, por un procedimiento sencillo y gratuito, la posibilidad de poner fin al desvío automático de llamadas a su terminal por parte de un tercero.

Artículo 11

Guías

1. Los datos personales recogidos en las guías impresas o electrónicas accesibles al público o que pueden obtenerse a través de servicios de información deberán limitarse a lo estrictamente necesario para identificar a un abonado concreto, a menos que el abonado haya dado su consentimiento inequívoco para que se publiquen otros datos personales. El abonado tendrá derecho, de forma gratuita, a que se le excluya de una guía impresa o electrónica a petición propia, a indicar que sus datos personales no se utilicen para fines de venta directa, a que se omita parcialmente su dirección y a que no exista referencia que revele su sexo, cuando ello sea aplicable lingüísticamente.
2. Sin perjuicio de lo dispuesto en el apartado 1, los Estados miembros podrán permitir a los operadores exigir un pago a los abonados que deseen hacer que sus datos

personales no figuren en una guía, siempre que la cantidad en cuestión no sea disuasoria del ejercicio de este derecho y siempre que, teniendo en cuenta las exigencias de calidad de la guía pública respecto del servicio universal, dicha cantidad se limite a los costes reales ocasionados al operador por la adaptación y actualización de la lista de abonados que no hayan de incluirse en la guía pública.

3. Los derechos conferidos en virtud del apartado 1 se aplicarán a los abonados que sean personas físicas.

Los Estados miembros garantizarán asimismo, en el marco del Derecho comunitario y de las legislaciones nacionales aplicables, la suficiente protección de los intereses legítimos de los abonados que no sean personas físicas en lo que se refiere a su inclusión en guías públicas.

Artículo 12

Llamadas no solicitadas

1. La utilización de sistemas de llamada automática sin intervención humana (aparatos de llamada automática) o facsímil (fax) con fines de venta directa sólo se podrán autorizar respecto de aquellos abonados que hayan dado su consentimiento previo.

2. Los Estados miembros tomarán las medidas adecuadas para garantizar, gratuitamente, que no se permitan las llamadas no solicitadas con fines de venta directa por medios que no sean los mencionados en el apartado 1 sin el consentimiento de los abonados de que se trate o respecto de los abonados que no deseen recibir dichas llamadas. La elección entre estas posibilidades será la que determine la legislación nacional.

3. Los derechos conferidos en virtud de los apartados 1 y 2 se aplicarán a los abonados que sean personas físicas. Los Estados miembros garantizarán asimismo, en el marco del Derecho comunitario y de las legislaciones nacionales aplicables, la suficiente

protección de los intereses legítimos de los abonados que no sean personas físicas en lo que se refiere a llamadas no solicitadas.

Artículo 13

Características técnicas y normalización

1. Al aplicar las disposiciones de la presente Directiva, los Estados miembros velarán, con arreglo a los apartados 2 y 3, por que no se impongan exigencias obligatorias respecto de características técnicas específicas relativas a las terminales u otros equipos de telecomunicaciones que puedan obstaculizar la colocación del equipo en el mercado y la libre circulación de dichos equipos en los Estados miembros y entre estos últimos.

2. Cuando las disposiciones de la presente Directiva sólo puedan aplicarse mediante la implantación de características técnicas específicas, los Estados miembros informarán a la Comisión de conformidad con los procedimientos establecidos en la Directiva 83/189/CEE del Consejo, de 28 de marzo de 1983, por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas

(1).

3. Cuando proceda, la Comisión garantizará la elaboración de normas europeas comunes para la aplicación de las características técnicas específicas, de conformidad con la legislación comunitaria en materia de aproximación de la legislación de los Estados miembros relativa al equipo terminal de telecomunicaciones, incluido el reconocimiento mutuo de su conformidad, y con la Decisión 87/95/CEE del Consejo, de 22 de diciembre de 1986, relativa a la normalización en el campo de la tecnología de la información y de las telecomunicaciones (2).

Artículo 14

Extensión del ámbito de aplicación de determinadas disposiciones de la Directiva 95/46/CE

1. Los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones y derechos que se establecen en los artículos 5 y 6 y en los apartados 1, 2, 3 y 4 del artículo 8, cuando dichas limitaciones constituyan una medida necesaria para proteger la seguridad nacional, la defensa, la seguridad pública, la prevención, la investigación, la detección y la persecución de delitos o la utilización no autorizada del sistema de telecomunicación a que se hace referencia en el apartado 1 del artículo 13 de la

Directiva 95/46/CE.

2. Las disposiciones del capítulo III sobre recursos judiciales, responsabilidad y sanciones de la Directiva

95/46/CE se aplicarán a las disposiciones de Derecho nacional adoptadas con arreglo a la presente

Directiva y relativa a los derechos individuales derivados de la presente Directiva.

3. El Grupo de protección de las personas en lo que respecta al tratamiento de datos personales establecido con arreglo al artículo 29 de la Directiva 95/46/CE ejercerá las funciones especificadas en el artículo 30 de la citada Directiva también por lo que se refiere a la protección de los derechos y libertades fundamentales y de los intereses legítimos en el sector de las telecomunicaciones, que son objeto de la presente Directiva.

4. La Comisión, asistida por el Comité creado por el artículo 31 de la Directiva 95/46/CE, procederá a la adaptación técnica del anexo con arreglo al procedimiento mencionado en el presente artículo. Dicho

Comité se reunirá específicamente para tratar de las cuestiones cubiertas por la presente Directiva.

(1) DO L 109 de 26.4.1983, p. 8; Directiva cuya última modificación la constituye la Directiva 94/10/CE (DO L 100 de 19.4.1994, p. 30).

(2) DO L 36 de 7.2.1987, p. 31; Decisión cuya última modificación la constituye el Acta de adhesión de 1994.

Artículo 15

Aplicación de la Directiva

1. Los Estados miembros pondrán en vigor las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva a más tardar el 24 de octubre de 1998.

No obstante lo dispuesto en el párrafo primero, los Estados miembros pondrán en vigor las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento al artículo 5 de la presente Directiva a más tardar el 24 de octubre de 2000.

Cuando los Estados miembros adopten dichas disposiciones, éstas harán referencia a la presente Directiva

o irán acompañadas de dicha referencia en su publicación oficial. Los Estados miembros establecerán las modalidades de la mencionada referencia.

2. No obstante lo dispuesto en el apartado 3 del artículo 6, no será necesario el consentimiento respecto al tratamiento en curso el día de entrada en vigor de las disposiciones nacionales adoptadas con arreglo a la presente Directiva. En tales casos se informará a los abona dos sobre este tratamiento y, si no expresan su reprobación en un

período que determinará el Estado miembro, se considerará que han dado su consentimiento.

3. El artículo 11 no se aplicará a las guías que se hayan publicado antes de que entren en vigor las disposiciones nacionales adoptadas con arreglo a la presente Directiva.

4. Los Estados miembros comunicarán a la Comisión el texto de las disposiciones de Derecho nacional que adopten en el ámbito regulado por la presente Directiva.

Artículo 16

Destinatarios

Los destinatarios de la presente Directiva serán los Estados miembros.

Hecho en Bruselas, el 15 de diciembre de 1997.

Por el Parlamento Europeo

El Presidente

J. M. GIL-ROBLES

Por el Consejo

El Presidente

J. C. JUNCKER

ANEXO

Lista de datos

A los efectos a que se hace mención en el apartado 2 del artículo 6, podrán procesarse los siguientes datos

que incluyan:

- el número o la identificación de la estación del abonado,
- la dirección del abonado y el tipo de estación,
- el número total de unidades que deben facturarse durante el ejercicio contable,
- el número del abonado que recibe la llamada,

— el tipo, la hora de comienzo y la duración de las llamadas realizadas o el volumen de datos transmitido,

— la fecha de la llamada o del servicio,

— otros datos relativos a los pagos, tales como pago anticipado, pagos a plazos, desconexión y notificaciones de recibos pendientes.

Directiva 2002/58/CE, de 12 de julio, relativa al tratamiento de los datos personales

y

a la protección de la intimidad en el sector de las comunicaciones electrónicas

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado constitutivo de la Comunidad Europea y, en particular, su artículo 95,

Vista la propuesta de la Comisión (1),

Visto el dictamen del Comité Económico y Social(2),

Previa consulta al Comité de las Regiones,

De conformidad con el procedimiento establecido en el artículo 251 del Tratado(3),

Considerando lo siguiente:

(1) La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos(4), insta a los Estados miembros a garantizar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de los datos personales y, en especial, su derecho a la intimidad, de forma que los datos personales puedan circular libremente en la Comunidad.

(2) La presente Directiva pretende garantizar el respeto de los derechos fundamentales y observa los principios consagrados, en particular, en la Carta de los Derechos Fundamentales de la Unión

Europea. Señaladamente, la presente Directiva pretende garantizar el pleno respeto de los derechos enunciados en los artículos 7 y 8 de dicha Carta.

(3) La confidencialidad de las comunicaciones está garantizada de conformidad con los instrumentos internacionales relativos a los derechos humanos, especialmente el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales y las constituciones de los Estados miembros.

(4) La Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones(5), tradujo los principios establecidos en la Directiva 95/46/CE en normas concretas para el sector de las telecomunicaciones. La Directiva 97/66/CE debe ser adaptada al desarrollo de los mercados y de las tecnologías de los servicios de comunicaciones electrónicas para que el nivel de protección de los datos personales y de la intimidad ofrecido a los usuarios de los servicios de comunicaciones electrónicas disponibles al público sea el mismo, con independencia de las tecnologías utilizadas. Procede, pues, derogar dicha Directiva y sustituirla por la presente.

(5) Actualmente se están introduciendo en las redes públicas de comunicación de la Comunidad nuevas tecnologías digitales avanzadas que crean necesidades específicas en materia de protección de datos personales y de la intimidad de los usuarios. El desarrollo de la sociedad de la información se caracteriza por la introducción de nuevos servicios de comunicaciones electrónicas. El acceso a las redes móviles digitales está ya disponible y resulta asequible para un público muy amplio. Estas redes digitales poseen gran capacidad y muchas posibilidades en materia de tratamiento de los datos personales. El éxito del desarrollo transfronterizo de estos servicios depende en parte de la confianza de los usuarios en que no se pondrá en peligro su intimidad.

(6) Internet está revolucionando las estructuras tradicionales del mercado al aportar una infraestructura común mundial para la prestación de una amplia gama de servicios de comunicaciones electrónicas. Los servicios de comunicaciones electrónicas disponibles al público a través de Internet introducen nuevas posibilidades para los usuarios, pero también nuevos riesgos para sus datos personales y su intimidad.

(7) En el caso de las redes públicas de comunicación, deben elaborarse disposiciones legales, reglamentarias y técnicas específicas con objeto de proteger los derechos y libertades fundamentales de las personas físicas y los intereses legítimos de las personas jurídicas, en particular frente a la creciente capacidad de almacenamiento y tratamiento informático de datos relativos a abonados y usuarios.

(8) Deben armonizarse las disposiciones legales, reglamentarias y técnicas adoptadas por los

Estados miembros para proteger los datos personales, la intimidad y los intereses legítimos de las personas jurídicas en el sector de las comunicaciones electrónicas, a fin de evitar obstáculos para el mercado interior de las comunicaciones electrónicas de conformidad con el artículo 14 del Tratado.

La armonización debe limitarse a los requisitos necesarios para garantizar que no se vean obstaculizados el fomento y el desarrollo de los nuevos servicios y redes de comunicaciones electrónicas entre Estados miembros.

(9) Los Estados miembros, los proveedores y usuarios afectados y las instancias comunitarias competentes deben cooperar para el establecimiento y el desarrollo de las tecnologías pertinentes cuando sea necesario para aplicar las garantías previstas en la presente Directiva y teniendo especialmente en cuenta el objetivo de reducir al mínimo el tratamiento de los datos personales y de tratar la información de forma anónima o mediante seudónimos cuando sea posible.

(10) En el sector de las comunicaciones electrónicas es de aplicación la Directiva 95/46/CE, en particular para todas las cuestiones relativas a la protección de los derechos y las libertades fundamentales que no están cubiertas de forma específica por las disposiciones de la presente

Directiva, incluidas las obligaciones del responsable del tratamiento de los datos y los derechos de las personas. La Directiva 95/46/CE se aplica a los servicios de comunicaciones electrónicas que no sean de carácter público.

(11) Al igual que la Directiva 95/46/CE, la presente Directiva no aborda la protección de los derechos y las libertades fundamentales en relación con las actividades no regidas por el Derecho comunitario. Por lo tanto, no altera el equilibrio actual entre el derecho de las personas a la intimidad y la posibilidad de que disponen los Estados miembros, según se indica en el apartado 1 del artículo 15 de la presente Directiva, de tomar las medidas necesarias para la protección de la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando las actividades tengan relación con asuntos de seguridad del Estado) y la aplicación del

Derecho penal. En consecuencia, la presente Directiva no afecta a la capacidad de los Estados miembros para interceptar legalmente las comunicaciones electrónicas o tomar otras medidas, cuando sea necesario, para cualquiera de estos fines y de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, según la interpretación que se hace de éste en las sentencias del Tribunal Europeo de Derechos Humanos.

Dichas medidas deberán ser necesarias en una sociedad democrática y rigurosamente proporcionales al fin que se pretende alcanzar y deben estar sujetas, además, a salvaguardias adecuadas, de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

(12) Los abonados de un servicio de comunicaciones electrónicas disponible para el público pueden ser personas físicas o jurídicas. Al complementar la Directiva 95/46/CE, la presente Directiva pretende proteger los derechos fundamentales de las personas físicas y, en particular, su derecho a la intimidad, así como los intereses legítimos de las

personas jurídicas. La presente Directiva no supone obligación alguna por parte de los Estados miembros de hacer extensiva la aplicación de la

Directiva 95/46/CE a la protección de los intereses legítimos de las personas jurídicas, que está garantizada en el marco de la legislación comunitaria y nacional.

(13) La relación contractual entre un abonado y un proveedor de servicios puede implicar un pago periódico o único por el servicio prestado o por prestar. Las tarjetas de prepago se consideran asimismo un contrato.

(14) Los datos de localización pueden referirse a la latitud, la longitud y la altitud del equipo terminal del usuario, a la dirección de la marcha, al nivel de precisión de la información de la localización, a la identificación de la célula de red en la que está localizado el equipo terminal en un determinado momento o a la hora en que la información de localización ha sido registrada.

(15) Una comunicación puede incluir cualquier dato relativo a nombres, números o direcciones facilitado por el remitente de una comunicación o el usuario de una conexión para llevar a cabo la comunicación. Los datos de tráfico pueden incluir cualquier conversión de dicha información efectuada por la red a través de la cual se transmita la comunicación a efectos de llevar a cabo la transmisión. Los datos de tráfico pueden referirse, entre otras cosas, al encaminamiento, la duración, la hora o el volumen de una comunicación, al protocolo utilizado, a la localización del equipo terminal del remitente o destinatario, a la red en que se origina o concluye la transmisión, al principio, fin o duración de una conexión. También pueden referirse al formato en que la red conduce la comunicación.

(16) La información que forma parte de un servicio de radiodifusión suministrado en una red pública de comunicaciones y está dirigida a una audiencia potencialmente ilimitada no constituye una comunicación con arreglo a la presente Directiva. No

obstante, en casos en que se pueda identificar al abonado o usuario individual que recibe dicha información, por ejemplo con servicios de vídeo a la carta, la información conducida queda incluida en el significado del término

"comunicación" a efectos de la presente Directiva.

(17) A efectos de la presente Directiva, el consentimiento de un usuario o abonado, independientemente de que se trate de una persona física o jurídica, debe tener el mismo significado que el consentimiento de la persona afectada por los datos tal como se define y se especifica en la

Directiva 95/46/CE. El consentimiento podrá darse por cualquier medio apropiado que permita la manifestación libre, inequívoca y fundada de la voluntad del usuario, por ejemplo mediante la selección de una casilla de un sitio web en Internet.

(18) Los servicios con valor añadido pueden consistir, por ejemplo, en recomendaciones sobre las tarifas menos costosas, orientación vial, información sobre tráfico, previsiones meteorológicas o información turística.

(19) La aplicación de determinados requisitos relativos a la presentación y a restricciones en la identificación de la línea de origen y de la línea conectada y al desvío automático de las llamadas a las líneas de abonado conectadas a centrales analógicas no debe ser obligatoria en aquellos casos particulares en los que dicha aplicación resulte imposible técnicamente, o en los que requiera un esfuerzo económico desproporcionado. Es importante que las partes interesadas sean informadas de dichos casos, y por consiguiente los Estados miembros deben notificarlos a la Comisión.

(20) Los proveedores de servicios deben tomar las medidas adecuadas para salvaguardar la seguridad de sus servicios, de ser necesario en conjunción con el suministrador de la red, e informar a los abonados de todo riesgo especial relativo a la seguridad de la red. Tales riesgos pueden presentarse especialmente en el caso de los servicios de

comunicaciones electrónicas a través de una red abierta como Internet o de una red de telefonía móvil analógica. Resulta particularmente importante que los abonados y usuarios de tales servicios sean plenamente informados por su proveedor de servicios de los riesgos para la seguridad que escapan a posibles soluciones adoptadas por dicho proveedor de servicios. Los proveedores de servicios que ofrecen servicios de comunicaciones electrónicas disponibles al público a través de Internet deben informar a usuarios y abonados de las medidas que pueden adoptar para proteger la seguridad de sus comunicaciones, por ejemplo utilizando determinados tipos de soporte lógico o tecnologías de cifrado. La exigencia de informar a los abonados de riesgos de seguridad particulares no exime al proveedor del servicio de la obligación de tomar a sus expensas medidas inmediatas y adecuadas para solucionar cualesquiera riesgos nuevos e imprevistos de seguridad y restablecer el nivel normal de seguridad del servicio. El suministro de información sobre riesgos de seguridad al abonado debe ser gratuito, salvo los costes nominales en que pueda incurrir el abonado al recibir o recoger la información, por ejemplo al cargar un mensaje de correo electrónico. La seguridad se valora a la luz del artículo 17 de la

Directiva 95/46/CE.

(21) Deben adoptarse medidas para evitar el acceso no autorizado a las comunicaciones a fin de proteger la confidencialidad de las mismas, incluidos tanto sus contenidos como cualquier dato relacionado con ellas, por medio de las redes públicas de comunicaciones y los servicios de comunicaciones electrónicas disponibles al público. La legislación nacional de algunos Estados miembros prohíbe solamente el acceso intencionado no autorizado a las comunicaciones.

(22) Al prohibirse el almacenamiento de comunicaciones, o de los datos de tráfico relativos a éstas, por terceros distintos de los usuarios o sin su consentimiento no se

pretende prohibir el almacenamiento automático, intermedio y transitorio de esta información, en la medida en que sólo tiene lugar para llevar a cabo la transmisión en la red de comunicaciones electrónicas, y siempre que la información no se almacene durante un período mayor que el necesario para la transmisión y para los fines de la gestión del tráfico, y que durante el período de almacenamiento se garantice la confidencialidad. Cuando resulte necesario para hacer más eficaz la transmisión de toda información públicamente asequible a otros destinatarios del servicio a solicitud de los mismos, la presente Directiva no debe evitar que dicha información siga almacenada más tiempo, siempre que la misma sea, en cualquier caso, asequible al público sin restricciones y que se eliminen todos los datos relativos a los abonados o usuarios individuales que pidan tal información.

(23) La confidencialidad de las comunicaciones debe garantizarse también en el curso de las prácticas comerciales lícitas. Cuando sea necesario y esté legalmente autorizado, las comunicaciones podrán grabarse al objeto de proporcionar la prueba de una transacción comercial.

La Directiva 95/46/CE es de aplicación a este tipo de tratamiento. Los interlocutores en las comunicaciones deben ser informados con anterioridad a la grabación sobre la misma, su objeto y la duración de su almacenamiento. La comunicación grabada debe ser eliminada en cuanto sea posible y en cualquier caso a más tardar al concluir el plazo durante el cual dicha transacción puede ser impugnada jurídicamente.

(24) Los equipos terminales de los usuarios de redes de comunicaciones electrónicas, así como toda información almacenada en dichos equipos, forman parte de la esfera privada de los usuarios que debe ser protegida de conformidad con el Convenio Europeo para la Protección de los Derechos

Humanos y de las Libertades Fundamentales. Los denominados "programas espía" (spyware), web bugs, identificadores ocultos y otros dispositivos similares pueden introducirse en el terminal del usuario sin su conocimiento para acceder a información, archivar información oculta o rastrear las actividades del usuario, lo que puede suponer una grave intrusión en la intimidad de dichos usuarios. Sólo debe permitirse la utilización de tales dispositivos con fines legítimos y con el conocimiento de los usuarios afectados.

(25) No obstante, los dispositivos de este tipo, por ejemplo los denominados "chivatos" (cookies), pueden constituir un instrumento legítimo y de gran utilidad, por ejemplo, para analizar la efectividad del diseño y de la publicidad de un sitio web y para verificar la identidad de usuarios partícipes en una transacción en línea. En los casos en que estos dispositivos, por ejemplo los denominados "chivatos" (cookies), tengan un propósito legítimo, como el de facilitar el suministro de servicios de la sociedad de la información, debe autorizarse su uso a condición de que se facilite a los usuarios información clara y precisa al respecto, de conformidad con la Directiva 95/46/CE, para garantizar que los usuarios están al corriente de la información que se introduce en el equipo terminal que están utilizando. Los usuarios deben tener la posibilidad de impedir que se almacene en su equipo terminal un "chivato" (cookie) o dispositivo semejante. Esto es particularmente importante cuando otros usuarios distintos al usuario original tienen acceso al equipo terminal y, a través de éste, a cualquier dato sensible de carácter privado almacenado en dicho equipo. La información sobre la utilización de distintos dispositivos que se vayan a instalar en el equipo terminal del usuario en la misma conexión y el derecho a impedir la instalación de tales dispositivos se pueden ofrecer en una sola vez durante una misma conexión y abarcar asimismo cualquier posible utilización futura de dichos dispositivos en conexiones posteriores. La presentación de

la información y del pedido de consentimiento o posibilidad de negativa debe ser tan asequible para el usuario como sea posible. No obstante, se podrá supeditar el acceso a determinados contenidos de un sitio web a la aceptación fundada de un "chivato" (cookie) o dispositivo similar, en caso de que éste tenga un propósito legítimo.

(26) Los datos relativos a los abonados que son tratados en las redes de comunicaciones electrónicas para el establecimiento de conexiones y la transmisión de información contienen información sobre la vida privada de las personas físicas, y afectan al derecho de éstas al respeto de su correspondencia, o se refieren a los intereses legítimos de las personas jurídicas. Dichos datos sólo deben poder almacenarse en la medida en que resulten necesarios para la prestación del servicio, para fines de facturación y para los pagos de interconexión, y durante un tiempo limitado.

Cualquier otro tratamiento de dichos datos que el proveedor de servicios de comunicaciones electrónicas disponibles al público pretenda llevar a cabo para la comercialización de servicios de comunicaciones electrónicas o para la prestación de servicios de valor añadido sólo puede permitirse si el abonado ha manifestado su consentimiento fundado en una información plena y exacta facilitada por el proveedor de servicios de comunicaciones electrónicas disponibles al público acerca del tipo de tratamiento que pretende llevar a cabo y sobre el derecho del abonado a denegar o a retirar su consentimiento a dicho tratamiento. Los datos sobre tráfico utilizados para la comercialización de los servicios de comunicaciones o para la prestación de servicios de valor añadido deben también eliminarse o hacerse anónimos tras la prestación del servicio. Los proveedores de servicios deben mantener siempre informados a los abonados de los tipos de dato que están tratando y de la finalidad y duración del tratamiento.

(27) El momento exacto en que finaliza la transmisión de una comunicación, tras el cual los datos de tráfico deberán eliminarse salvo a efectos de facturación, puede depender del tipo de servicio de comunicaciones electrónicas que se suministre. Por ejemplo, para una llamada de telefonía vocal la transmisión finalizará en cuanto uno de los usuarios interrumpa la conexión; para el correo electrónico la transmisión finaliza en cuanto el destinatario recoge el mensaje, en general del servidor de su proveedor de servicios.

(28) La obligación de eliminar datos de tráfico o de hacerlos anónimos cuando ya no se necesiten para la transmisión de una comunicación no entra en conflicto con procedimientos existentes en

Internet como la prelectura en soporte rápido (caching), en el sistema de nombres de dominio, de direcciones IP o el caching de una dirección IP vinculada a una dirección física, o la utilización de información relativa al usuario para controlar el derecho de acceso a redes o servicios.

(29) De ser necesario, el proveedor del servicio puede tratar, en casos concretos, los datos de tráfico relacionados con los abonados y usuarios, a fin de detectar fallos o errores técnicos en la transmisión de las comunicaciones. El proveedor también puede tratar los datos de tráfico necesarios a efectos de facturación a fin de detectar y frenar el fraude consistente en la utilización sin pago de servicios de comunicaciones electrónicas.

(30) Los sistemas para el suministro de redes y servicios de comunicaciones electrónicas deben diseñarse de modo que se limite la cantidad de datos personales al mínimo estrictamente necesario.

Cualesquiera actividades relacionadas con el suministro del servicio de comunicaciones electrónicas que vayan más allá de la transmisión de una comunicación y su facturación debe basarse en datos de tráfico acumulados que no puedan referirse a abonados o

usuarios. Cuando dichas actividades no puedan basarse en datos acumulados, deben considerarse servicios con valor añadido para los cuales se requiere el consentimiento del abonado.

(31) El consentimiento que deberá obtenerse para el tratamiento de datos personales a efectos de proporcionar un particular servicio con valor añadido debe ser el del abonado o el del usuario, en función de los datos que deban tratarse y el tipo de servicio que se suministre y de que sea posible desde el punto de vista técnico, de procedimiento y del contrato distinguir la persona que utiliza un servicio de comunicaciones electrónicas de la persona física o jurídica que ha suscrito el mismo.

(32) Si el proveedor de un servicio de comunicaciones electrónicas o de un servicio con valor añadido subcontrata el tratamiento de datos personales necesario para la prestación de dichos servicios a otra entidad, dicha subcontratación y el tratamiento de datos subsiguiente deben cumplir plenamente los requisitos relativos a los responsables y a los encargados del tratamiento de datos personales que establece la Directiva 95/46/CE. Si la prestación de un servicio con valor añadido requiere que los datos de tráfico o de localización sean transmitidos por un proveedor de servicios de comunicaciones electrónicas hacia un proveedor de servicios con valor añadido, los abonados o usuarios a los que se refieran dichos datos deben asimismo estar plenamente informados sobre dicha transmisión antes de dar su consentimiento al tratamiento de los datos.

(33) La introducción de facturas desglosadas ha aumentado la posibilidad de que el abonado pueda comprobar que las tarifas aplicadas por el proveedor del servicio son correctas, pero, al mismo tiempo, puede poner en peligro la intimidad de los usuarios de servicios de comunicaciones electrónicas disponibles al público. Por consiguiente, a fin de proteger la intimidad de los usuarios, los Estados miembros deben fomentar el

desarrollo de opciones de servicios de comunicaciones electrónicas tales como posibilidades de pago alternativas que permitan el acceso anónimo o estrictamente privado a los servicios de comunicaciones electrónicas disponibles al público, por ejemplo tarjetas de llamada y posibilidad de pago con tarjetas de crédito. Con idéntico propósito, los Estados miembros podrán pedir a los operadores que ofrezcan a sus abonados otro tipo de factura detallada en la que se omita cierto número de cifras del número llamado.

(34) Es necesario, por lo que respecta a la identificación de la línea de origen, proteger el derecho del interlocutor que efectúa la llamada a reservarse la identificación de la línea desde la que realiza dicha llamada y el derecho del interlocutor llamado a rechazar llamadas procedentes de líneas no identificadas. Está justificado anular la eliminación de la presentación de la identificación de la línea de origen en casos particulares. Determinados abonados, en particular las líneas de ayuda y otras organizaciones similares, tienen interés en garantizar el anonimato de sus interlocutores. Es necesario, por lo que respecta a la identificación de la línea conectada, proteger el derecho y el interés legítimo del interlocutor llamado a impedir la presentación de la identificación de la línea a la que está conectado realmente el interlocutor llamante, en particular en el caso de las llamadas que han sido desviadas. Los proveedores de servicios de comunicaciones electrónicas disponibles al público deben informar a sus abonados de la existencia de la identificación de líneas llamantes y conectadas en la red y de todos los servicios ofrecidos a partir de la identificación de las líneas llamantes y conectadas, así como sobre las opciones de confidencialidad disponibles. Esto permitirá a los abonados decidir con conocimiento de causa las posibilidades de confidencialidad que deseen utilizar. Las opciones de confidencialidad ofrecidas caso por caso no tienen que estar disponibles necesariamente como servicio de la red automática, pero sí obtenerse

mediante simple solicitud al proveedor del servicio de comunicaciones electrónicas disponibles al público.

(35) En las redes móviles digitales se tratan los datos sobre localización que proporcionan la posición geográfica del equipo terminal del usuario móvil para hacer posible la transmisión de las comunicaciones. Tales datos constituyen datos sobre tráfico a los que es aplicable el artículo 6 de la presente Directiva. Sin embargo, además, las redes móviles digitales pueden tener la capacidad de tratar datos sobre localización más precisos de lo necesario para la transmisión de comunicaciones y que se utilizan para la prestación de servicios de valor añadido tales como los servicios que facilitan información sobre tráfico y orientaciones individualizadas a los conductores. El tratamiento de tales datos para la prestación de servicios de valor añadido sólo debe permitirse cuando los abonados hayan dado su consentimiento. Incluso en los casos en que los abonados hayan dado su consentimiento, éstos deben contar con un procedimiento sencillo y gratuito de impedir temporalmente el tratamiento de los datos sobre localización.

(36) Los Estados miembros podrán restringir el derecho a la intimidad de los usuarios y abonados por lo que se refiere a la identificación de la línea de origen en los casos en que ello sea necesario para rastrear llamadas malevolentes, y en lo tocante a la identificación y localización de dicha línea cuando sea preciso para que los servicios de socorro cumplan su cometido con la máxima eficacia posible. Para ello, los Estados miembros podrán adoptar disposiciones específicas que permitan a los proveedores de servicios de comunicaciones electrónicas ofrecer el acceso a la identificación y localización de la línea de origen sin el consentimiento previo de los usuarios o abonados de que se trate.

(37) Deben ofrecerse garantías a los abonados contra las molestias que puedan causar las llamadas desviadas automáticamente por otros. Además en tales casos, los abonados deben poder detener las llamadas desviadas hacia sus terminales mediante simple solicitud al proveedor de servicios de comunicaciones electrónicas disponibles al público.

(38) Las guías de abonados a los servicios de comunicaciones electrónicas alcanzan gran difusión y tienen carácter público. El derecho a la intimidad de las personas físicas y el interés legítimo de las personas jurídicas exigen que los abonados puedan decidir si se hacen públicos sus datos personales en dichas guías y, caso de hacerse públicos, cuáles de ellos. Los suministradores de guías públicas deben informar a los abonados que vayan a incluirse en tales guías acerca de la finalidad de las mismas y de cualquier uso particular que pueda hacerse de las versiones electrónicas de las guías públicas, especialmente a través de funciones de búsqueda incorporadas al soporte lógico, tales como las funciones de búsqueda inversa que permiten al usuario de la guía averiguar el nombre y la dirección del abonado a partir exclusivamente de un número de teléfono.

(39) Debe imponerse a quien recoja datos para ser incluidos en las guías públicas en las que figuren los datos personales de los abonados la obligación de informar a estos últimos acerca de los objetivos de dichas guías. Cuando los datos puedan ser transmitidos a una o más terceras partes, debe informarse al abonado de esta posibilidad, así como acerca del destinatario o de las categorías de posibles destinatarios. Cualquier transmisión debe estar sujeta a la condición de que los datos no puedan utilizarse para otros fines más que aquéllos para los que se recojan. Si quien recoge datos del usuario o cualquier tercero a quien se hayan transmitido los datos desea utilizarlos con un fin suplementario, la renovación del consentimiento del abonado

deberá obtenerla ya sea quien recogió inicialmente los datos o el tercero a quien se hayan transmitido.

(40) Deben ofrecerse garantías a los abonados contra la intrusión en su intimidad mediante comunicaciones no solicitadas con fines de venta directa, especialmente a través de llamadores automáticos, faxes y mensajes de correo electrónico, incluidos los de SMS. Por una parte, el envío de estas formas de comunicaciones comerciales no solicitadas puede resultar relativamente sencillo y económico, y por otra, puede conllevar una molestia e incluso un coste para el receptor. Además, en algunos casos su volumen puede dar lugar a dificultades en las redes de comunicaciones electrónicas y en los equipos terminales. Se justifica, para este tipo de comunicaciones no solicitadas con fines de venta directa, la exigencia de obtener el consentimiento expreso previo de los receptores antes de que puedan dirigírseles comunicaciones de esta índole. El mercado único requiere un planteamiento armonizado que garantice la existencia de normas sencillas aplicadas a escala comunitaria, tanto para las empresas como para los usuarios.

(41) En el contexto de una relación preexistente con el cliente, es razonable admitir el uso de las señas electrónicas del cliente con objeto de ofrecer productos o servicios similares, pero exclusivamente por parte de la misma empresa que haya obtenido las señas electrónicas de conformidad con la Directiva 95/46/CE. En el momento de recabarse las señas electrónicas, debe informarse al cliente de manera clara e inequívoca sobre su uso ulterior con fines de venta directa, y debe dársele la posibilidad de negarse a dicho uso. Debe seguir ofreciéndose al cliente esta posibilidad cada vez que reciba un mensaje ulterior de venta directa, sin cargo alguno salvo los posibles costes de transmisión de esta negativa.

(42) El caso de otras formas de venta directa que resultan más onerosas para el remitente y no implican costes financieros para los abonados y usuarios, como las

llamadas personales de telefonía vocal, se puede justificar el mantenimiento de un sistema que dé a los abonados o usuarios la posibilidad de indicar que no desean recibir llamadas de ese tipo. Sin embargo, a fin de no disminuir los niveles actuales de protección de la intimidad, debe facultarse a los Estados miembros para mantener sus sistemas nacionales que únicamente autoricen ese tipo de llamadas cuando los abonados y usuarios hayan dado su consentimiento previo.

(43) Para facilitar la aplicación efectiva de las normas comunitarias en materia de mensajes no solicitados con fines de venta directa, es preciso prohibir el uso de identidades falsas y de domicilios y números de contacto falsos cuando se envían mensajes no solicitados con fines de venta directa.

(44) Determinados sistemas de correo electrónico ofrecen al usuario la posibilidad de ver la identidad del remitente y el asunto del mensaje, así como borrar el mensaje, sin tener que descargar el resto del contenido ni los ficheros anexos, reduciendo con ello los costes que podrían derivarse de descargar mensajes o ficheros no solicitados. Estas modalidades de funcionamiento pueden seguir siendo útiles en determinados casos, como instrumento añadido a las obligaciones generales que se establecen en la presente Directiva.

(45) La presente Directiva no afecta a las disposiciones tomadas por los Estados miembros para proteger los intereses legítimos de las personas jurídicas en lo que se refiere a las comunicaciones no solicitadas con fines de venta directa. En caso de que los Estados miembros establezcan un registro de autoexclusión de dicho tipo de comunicaciones con destino a las personas jurídicas, en su mayor parte usuarios comerciales, serán de plena aplicación las disposiciones del artículo 7 de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en

particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico)(6).

(46) Las funcionalidades para la prestación de servicios de comunicaciones electrónicas pueden estar integradas en la red o en cualquier parte del equipo terminal del usuario, incluido el soporte lógico. La protección de los datos personales y la intimidad del usuario de los servicios de comunicaciones electrónicas disponibles al público debe ser independiente de la configuración de los distintos componentes necesarios para prestar el servicio y de la distribución de las funcionalidades necesarias entre dichos componentes. La Directiva 95/46/CE cubre cualquier forma de tratamiento de datos personales con independencia de la tecnología utilizada. La existencia de normas específicas para los servicios de comunicaciones electrónicas, junto a las normas generales para los demás componentes necesarios para la prestación de tales servicios, podría no facilitar la protección de los datos personales y la intimidad de modo tecnológicamente neutro. Por consiguiente, puede resultar necesario adoptar medidas que exijan a los fabricantes de determinados tipos de equipos utilizados en los servicios de comunicaciones electrónicas que fabriquen sus productos de manera que incorporen salvaguardias para garantizar la protección de los datos personales y la intimidad del usuario y el abonado. La adopción de dichas medidas de conformidad con la Directiva 1999/5/CE del Parlamento Europeo y del Consejo, de 9 de marzo de 1999, sobre equipos radioeléctricos y equipos terminales de telecomunicación y reconocimiento mutuo de su conformidad(7), garantizará que la introducción de características técnicas en los equipos de comunicaciones electrónicas, incluido el soporte lógico, para fines de protección de datos esté armonizada a fin de que sea compatible con la realización del mercado interior.

(47) En los casos en que no se respeten los derechos de los usuarios y abonados, el Derecho nacional debe prever vías de recurso judiciales. Deben imponerse sanciones a aquellas personas, ya sean de Derecho público o privado, que incumplan las medidas nacionales adoptadas en virtud de la presente Directiva.

(48) Resulta útil en el ámbito de aplicación de la presente Directiva aprovechar las experiencias del

Grupo de protección de las personas en lo que respecta al tratamiento de datos personales, compuesto por representantes de las autoridades de control de los Estados miembros y creado por el artículo 29 de la Directiva 95/46/CE.

(49) Para facilitar el cumplimiento de lo dispuesto en la presente Directiva, son necesarias determinadas disposiciones particulares para el tratamiento de datos ya en curso el día en que entre

en vigor la legislación nacional de aplicación de la presente Directiva.

HAN ADOPTADO LA PRESENTE DIRECTIVA:

Artículo 1

Ámbito de aplicación y objetivo

1. La presente Directiva armoniza las disposiciones de los Estados miembros necesarias para garantizar un nivel equivalente de protección de las libertades y los derechos fundamentales y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas, así como la libre circulación de tales datos y de los equipos y servicios de comunicaciones electrónicas en la Comunidad.

2. Las disposiciones de la presente Directiva especifican y completan la Directiva 95/46/CE a los efectos mencionados en el apartado 1. Además, protegen los intereses legítimos de los abonados que sean personas jurídicas.

3. La presente Directiva no se aplicará a las actividades no comprendidas en el ámbito de aplicación del Tratado constitutivo de la Comunidad Europea, como las reguladas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea, ni, en cualquier caso, a las actividades que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dichas actividades estén relacionadas con la seguridad del mismo) y a las actividades del Estado en materia penal.

Artículo 2

Definiciones

Salvo disposición en contrario, serán de aplicación a efectos de la presente Directiva las definiciones que figuran en la Directiva 95/46/CE y en la Directiva 2002/21/CE del Parlamento

Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco)(8).

Además, a efectos de la presente Directiva se entenderá por:

- a) "usuario": una persona física que utiliza con fines privados o comerciales un servicio de comunicaciones electrónicas disponible para el público, sin que necesariamente se haya abonado a dicho servicio;
- b) "datos de tráfico": cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma;
- c) "datos de localización": cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público;

- d) "comunicación": cualquier información intercambiada o conducida entre un número finito de interesados por medio de un servicio de comunicaciones electrónicas disponible para el público. No se incluye en la presente definición la información conducida, como parte de un servicio de radiodifusión al público, a través de una red de comunicaciones electrónicas, excepto en la medida en que la información pueda relacionarse con el abonado o usuario identificable que reciba la información;
- e) "llamada": una conexión establecida por medio de un servicio telefónico disponible para el público que permita la comunicación bidireccional en tiempo real;
- f) "consentimiento" de un usuario o abonado: el consentimiento del interesado, con arreglo a la definición de la Directiva 95/46/CE;
- g) "servicio con valor añadido": todo servicio que requiere el tratamiento de datos de tráfico o datos de localización distintos de los de tráfico que vayan más allá de lo necesario para la transmisión de una comunicación o su facturación;
- h) "correo electrónico": todo mensaje de texto, voz, sonido o imagen enviado a través de una red de comunicaciones pública que pueda almacenarse en la red o en el equipo terminal del receptor hasta que éste acceda al mismo.

Artículo 3

Servicios afectados

1. La presente Directiva se aplicará al tratamiento de datos personales en relación con la prestación de servicios de comunicaciones electrónicas disponibles al público en las redes públicas de comunicaciones de la Comunidad.
2. Los artículos 8, 10 y 11 se aplicarán a las líneas de abonado conectadas a centrales digitales y, siempre y cuando sea técnicamente posible y no exija un esfuerzo económico desproporcionado, a las líneas de abonado conectadas a centrales analógicas.

3. Los Estados miembros notificarán a la Comisión aquellos casos en los que no sea posible técnicamente o exija un esfuerzo económico desproporcionado cumplir los requisitos de los artículos 8, 10 y 11.

Artículo 4

Seguridad

1. El proveedor de un servicio de comunicaciones electrónicas disponible para el público deberá adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios, de ser necesario en colaboración con el proveedor de la red pública de comunicaciones por lo que respecta a la seguridad de la red. Considerando las técnicas más avanzadas y el coste de su aplicación, dichas medidas garantizarán un nivel de seguridad adecuado al riesgo existente.

2. En caso de que exista un riesgo particular de violación de la seguridad de la red, el proveedor de un servicio de comunicaciones electrónicas disponible para el público deberá informar a los abonados sobre dicho riesgo y, cuando el riesgo quede fuera del ámbito de las medidas que deberá tomar el proveedor del servicio, sobre las posibles soluciones, con una indicación de los posibles costes.

Artículo 5

Confidencialidad de las comunicaciones

1. Los Estados miembros garantizarán, a través de la legislación nacional, la confidencialidad de las comunicaciones, y de los datos de tráfico asociados a ellas, realizadas a través de las redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público. En particular, prohibirán la escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y los datos de tráfico asociados a ellas por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando dichas

personas estén autorizadas legalmente a hacerlo de conformidad con el apartado 1 del artículo 15. El presente apartado no impedirá el almacenamiento técnico necesario para la conducción de una comunicación, sin perjuicio del principio de confidencialidad.

2. El apartado 1 no se aplicará a las grabaciones legalmente autorizadas de comunicaciones y de los datos de tráfico asociados a ellas cuando se lleven a cabo en el marco de una práctica comercial lícita con el fin de aportar pruebas de una transacción comercial o de cualquier otra comunicación comercial.

3. Los Estados miembros velarán por que únicamente se permita el uso de las redes de comunicaciones electrónicas con fines de almacenamiento de información o de obtención de acceso a la información almacenada en el equipo terminal de un abonado o usuario a condición de que se facilite a dicho abonado o usuario información clara y completa, en particular sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Directiva 95/46/CE y de que el responsable del tratamiento de los datos le ofrezca el derecho de negarse a dicho tratamiento. La presente disposición no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar o facilitar la transmisión de una comunicación a través de una red de comunicaciones electrónicas, o en la medida de lo estrictamente necesario a fin de proporcionar a una empresa de información un servicio expresamente solicitado por el usuario o el abonado.

Artículo 6

Datos de tráfico

1. Sin perjuicio de lo dispuesto en los apartados 2, 3 y 5 del presente artículo y en el apartado 1 del artículo 15, los datos de tráfico relacionados con abonados y usuarios que sean tratados y almacenados por el proveedor de una red pública de comunicaciones o de un servicio de comunicaciones electrónicas disponible al público deberán eliminarse

o hacerse anónimos cuando ya no sea necesario a los efectos de la transmisión de una comunicación.

2. Podrán ser tratados los datos de tráfico necesarios a efectos de la facturación de los abonados y los pagos de las interconexiones. Se autorizará este tratamiento únicamente hasta la expiración del plazo durante el cual pueda impugnarse legalmente la factura o exigirse el pago.

3. El proveedor de un servicio de comunicaciones electrónicas disponible para el público podrá tratar los datos a que se hace referencia en el apartado 1 para la promoción comercial de servicios de comunicaciones electrónicas o para la prestación de servicios con valor añadido en la medida y durante el tiempo necesarios para tales servicios o promoción comercial, siempre y cuando el abonado o usuario al que se refieran los datos haya dado su consentimiento. Los usuarios o abonados dispondrán de la posibilidad de retirar su consentimiento para el tratamiento de los datos de tráfico en cualquier momento.

4. El proveedor del servicio deberá informar al abonado o al usuario de los tipos de datos de tráfico que son tratados y de la duración de este tratamiento a los efectos mencionados en el apartado 2 y, antes de obtener el consentimiento, a los efectos contemplados en el apartado 3.

5. Sólo podrán encargarse del tratamiento de datos de tráfico, de conformidad con los apartados 1,

2, 3 y 4, las personas que actúen bajo la autoridad del proveedor de las redes públicas de comunicaciones o de servicios de comunicaciones electrónicas disponibles al público que se ocupen de la facturación o de la gestión del tráfico, de las solicitudes de información de los clientes, de la detección de fraudes, de la promoción comercial de los servicios de comunicaciones electrónicas o de la prestación de un servicio con valor

añadido, y dicho tratamiento deberá limitarse a lo necesario para realizar tales actividades.

6. Los apartados 1, 2, 3 y 5 se aplicarán sin perjuicio de la posibilidad de que los organismos competentes sean informados de los datos de tráfico con arreglo a la legislación aplicable, con vistas a resolver litigios, en particular los relativos a la interconexión o a la facturación.

Artículo 7

Facturación desglosada

1. Los abonados tendrán derecho a recibir facturas no desglosadas.
2. Los Estados miembros aplicarán las disposiciones nacionales a fin de conciliar los derechos de los abonados que reciban facturas desglosadas con el derecho a la intimidad de los usuarios que efectúen las llamadas y de los abonados que las reciban, por ejemplo, garantizando que dichos usuarios y abonados dispongan de suficientes modalidades alternativas de comunicación o de pago que potencien la intimidad.

Artículo 8

Presentación y restricción de la identificación de la línea de origen y de la línea conectada

1. Cuando se ofrezca la posibilidad de visualizar la identificación de la línea de origen, el proveedor del servicio deberá ofrecer al usuario que efectúe la llamada la posibilidad de impedir en cada llamada, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de la línea de origen. El abonado que origine la llamada deberá tener esta posibilidad para cada línea.
2. Cuando se ofrezca la posibilidad de visualizar la identificación de la línea de origen, el proveedor del servicio deberá ofrecer al abonado que reciba la llamada la posibilidad, mediante un procedimiento sencillo y gratuito, siempre que haga un uso razonable de

esta función, de impedir la presentación de la identificación de la línea de origen en las llamadas entrantes.

3. Cuando se ofrezca la posibilidad de visualizar la identificación de la línea de origen y ésta se presente antes de que se establezca la llamada, el proveedor del servicio deberá ofrecer al abonado que reciba la llamada la posibilidad, mediante un procedimiento sencillo, de rechazar las llamadas entrantes procedentes de usuarios o abonados que hayan impedido la presentación de la identificación de la línea de origen.

4. Cuando se ofrezca la posibilidad de visualizar la identificación de la línea conectada, el proveedor del servicio deberá ofrecer al abonado que reciba la llamada la posibilidad, por un procedimiento sencillo y gratuito, de impedir la presentación de la identificación de la línea conectada al usuario que efectúa la llamada.

5. Las disposiciones del apartado 1 se aplicarán también a las llamadas efectuadas desde la Comunidad a terceros países. Las disposiciones de los apartados 2, 3 y 4 se aplicarán también a las llamadas entrantes procedentes de terceros países.

6. Los Estados miembros velarán por que, cuando se ofrezca la posibilidad de visualizar la identificación de la línea de origen o de la línea conectada, los proveedores de servicios de comunicaciones electrónicas disponibles al público informen al público sobre dicha posibilidad y sobre las que se establecen en los apartados 1 a 4.

Artículo 9

Datos de localización distintos de los datos de tráfico

1. En caso de que puedan tratarse datos de localización, distintos de los datos de tráfico, relativos a los usuarios o abonados de redes públicas de comunicaciones o de servicios de comunicaciones electrónicas disponibles al público, sólo podrán tratarse estos datos si se hacen anónimos, o previo consentimiento de los usuarios o abonados, en la medida

y por el tiempo necesarios para la prestación de un servicio con valor añadido. El proveedor del servicio deberá informar a los usuarios o abonados, antes de obtener su consentimiento, del tipo de datos de localización distintos de los datos de tráfico que serán tratados, de la finalidad y duración del tratamiento y de si los datos se transmitirán a un tercero a efectos de la prestación del servicio con valor añadido. Se deberá ofrecer a los usuarios y abonados la posibilidad de retirar en todo momento su consentimiento para el tratamiento de los datos de localización distintos de los datos de tráfico.

2. Cuando se haya obtenido el consentimiento de un usuario o abonado para el tratamiento de datos de localización distintos de los datos de tráfico, el usuario o abonado deberá seguir contando con la posibilidad, por un procedimiento sencillo y gratuito, de rechazar temporalmente el tratamiento de tales datos para cada conexión a la red o para cada transmisión de una comunicación.

3. Sólo podrán encargarse del tratamiento de datos de localización distintos de los datos de tráfico de conformidad con los apartados 1 y 2 personas que actúen bajo la autoridad del proveedor de las redes públicas de comunicaciones o de servicios de comunicaciones electrónicas disponibles al público o del tercero que preste el servicio con valor añadido, y dicho tratamiento deberá limitarse a lo necesario a efectos de la prestación del servicio con valor añadido.

Artículo 10

Excepciones

Los Estados miembros velarán por que existan procedimientos transparentes que determinen la forma en que el proveedor de una red pública de comunicaciones o de un servicio de comunicaciones electrónicas disponible al público podrá anular:

a) la supresión de la presentación de la identificación de la línea de origen por un período de tiempo limitado, a instancia de un abonado que solicite la identificación de

llamadas malevolentes o molestas; en tal caso, los datos que incluyan la identificación del abonado que origina la llamada serán almacenados y facilitados por el proveedor de la red pública de comunicaciones o del servicio de comunicaciones electrónicas disponible para el público, de acuerdo con el Derecho nacional;

b) la supresión de la presentación de la identificación de la línea de origen y el rechazo temporal o la ausencia de consentimiento de un abonado o un usuario para el tratamiento de los datos de localización, de manera selectiva por línea, para las entidades reconocidas por un Estado miembro para atender llamadas de urgencia, incluidos los cuerpos de policía, los servicios de ambulancias y los cuerpos de bomberos, para que puedan responder a tales llamadas.

Artículo 11

Desvío automático de llamadas

Los Estados miembros velarán por que todo abonado tenga la posibilidad, por un procedimiento sencillo y gratuito, de detener el desvío automático de llamadas a su terminal por parte de un tercero.

Artículo 12

Guías de abonados

1. Los Estados miembros velarán por que se informe gratuitamente a los abonados antes de ser incluidos en las guías acerca de los fines de las guías de abonados, impresas o electrónicas, disponibles al público o accesibles a través de servicios de información sobre las mismas, en las que puedan incluirse sus datos personales, así como de cualquier otra posibilidad de uso basada en funciones de búsqueda incorporadas en las versiones electrónicas de la guía.

2. Los Estados miembros velarán por que los abonados tengan oportunidad de decidir si sus datos personales figuran en una guía pública, y en su caso cuáles de ellos, en la

medida en que tales datos sean pertinentes para la finalidad de la guía que haya estipulado su proveedor, y de comprobar, corregir o suprimir tales datos. La no inclusión en una guía pública de abonados, así como la comprobación, corrección o supresión de datos personales de una guía, no deberán dar lugar al cobro de cantidad alguna.

3. Los Estados miembros podrán exigir que para cualquier finalidad de una guía pública distinta de la búsqueda de datos de contacto de personas a partir de su nombre y, si resulta necesario, de un mínimo de otros identificadores, se recabe el consentimiento específico de los abonados.

4. Los apartados 1 y 2 se aplicarán a los abonados que sean personas físicas. Los Estados miembros velarán asimismo, en el marco del Derecho comunitario y de las legislaciones nacionales aplicables, por la suficiente protección de los intereses legítimos de los abonados que no sean personas físicas en lo que se refiere a su inclusión en guías públicas.

Artículo 13

Comunicaciones no solicitadas

1. Sólo se podrá autorizar la utilización de sistemas de llamada automática sin intervención humana (aparatos de llamada automática), fax o correo electrónico con fines de venta directa respecto de aquellos abonados que hayan dado su consentimiento previo.

2. No obstante lo dispuesto en el apartado 1, cuando una persona física o jurídica obtenga de sus clientes la dirección de correo electrónico, en el contexto de la venta de un producto o de un servicio de conformidad con la Directiva 95/46/CE, esa misma persona física o jurídica podrá utilizar dichas señas electrónicas para la venta directa de sus propios productos o servicios de características similares, a condición de que se

ofrezca con absoluta claridad a los clientes, sin cargo alguno y de manera sencilla, la posibilidad de oponerse a dicha utilización de las señas electrónicas en el momento en que se recojan las mismas y, en caso de que el cliente no haya rechazado inicialmente su utilización, cada vez que reciban un mensaje ulterior.

3. Los Estados miembros tomarán las medidas adecuadas para garantizar, que, sin cargo alguno, no se permitan las comunicaciones no solicitadas con fines de venta directa en casos que no sean los mencionados en los apartados 1 y 2, bien sin el consentimiento del abonado, bien respecto de los abonados que no deseen recibir dichas comunicaciones. La elección entre estas dos posibilidades será determinada por la legislación nacional.

4. Se prohibirá, en cualquier caso, la práctica de enviar mensajes electrónicos con fines de venta directa en los que se disimule o se oculte la identidad del remitente por cuenta de quien se efectúa la comunicación, o que no contengan una dirección válida a la que el destinatario pueda enviar una petición de que se ponga fin a tales comunicaciones.

5. Los apartados 1 y 3 se aplicarán a los abonados que sean personas físicas. Los Estados miembros velarán asimismo, en el marco del Derecho comunitario y de las legislaciones nacionales aplicables, por la suficiente protección de los intereses legítimos de los abonados que no sean personas físicas en lo que se refiere a las comunicaciones no solicitadas.

Artículo 14

Características técnicas y normalización

1. Al aplicar las disposiciones de la presente Directiva, los Estados miembros velarán, sin perjuicio de los apartados 2 y 3, por que no se impongan requisitos obligatorios respecto de características técnicas específicas a los equipos terminales u otros equipos

de comunicaciones electrónicas que puedan obstaculizar la puesta en el mercado de dichos equipos y su libre circulación en los Estados miembros y entre estos últimos.

2. Cuando las disposiciones de la presente Directiva sólo puedan aplicarse mediante la implantación de características técnicas específicas en las redes de comunicaciones electrónicas, los Estados miembros informarán a la Comisión de conformidad con el procedimiento establecido en la

Directiva 98/34/CE del Parlamento Europeo y del Consejo, de 22 de junio de 1998, por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas y de las reglas relativas a los servicios de la sociedad de la información (9).

3. Cuando proceda, se podrán adoptar medidas para garantizar que los equipos terminales estén fabricados de manera compatible con el derecho de los usuarios de proteger y controlar el uso de sus datos personales, de conformidad con la Directiva 1999/5/CE y la Decisión 87/95/CEE del

Consejo, de 22 de diciembre de 1986, relativa a la normalización en el campo de la tecnología de la información y de las telecomunicaciones (10).

Artículo 15

Aplicación de determinadas disposiciones de la Directiva 95/46/CE

1. Los Estados miembros podrán adoptar medidas legales para limitar el alcance de los derechos y las obligaciones que se establecen en los artículos 5 y 6, en los apartados 1 a 4 del artículo 8 y en el artículo 9 de la presente Directiva, cuando tal limitación constituya una medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y

persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas a que se hace referencia en el apartado 1 del artículo 13 de la Directiva 95/46/CE. Para ello, los Estados miembros podrán adoptar, entre otras, medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado justificado por los motivos establecidos en el presente apartado. Todas las medidas contempladas en el presente apartado deberán ser conformes con los principios generales del Derecho comunitario, incluidos los mencionados en los apartados 1 y 2 del artículo 6 del Tratado de la Unión Europea.

2. Las disposiciones del capítulo III sobre recursos judiciales, responsabilidad y sanciones de la

Directiva 95/46/CE se aplicarán a las disposiciones nacionales adoptadas con arreglo a la presente

Directiva y a los derechos individuales derivados de la misma.

3. El Grupo de protección de las personas en lo que respecta al tratamiento de datos personales, creado por el artículo 29 de la Directiva 95/46/CE, ejercerá también las funciones especificadas en el artículo 30 de dicha Directiva por lo que se refiere a los asuntos objeto de la presente Directiva, a saber, la protección de los derechos y las libertades fundamentales y de los intereses legítimos en el sector de las comunicaciones electrónicas.

Artículo 16

Disposiciones transitorias

1. El artículo 12 no se aplicará a las ediciones de guías ya producidas o puestas en el mercado en forma impresa o electrónica no conectada antes de que entren en vigor las disposiciones nacionales adoptadas en virtud de la presente Directiva.

2. Cuando los datos personales de los abonados a la telefonía vocal pública de tipo fijo o móvil se hayan incluido en una guía de abonados pública de conformidad con las disposiciones de la

Directiva 95/46/CE y del artículo 11 de la Directiva 97/66/CE antes de que las disposiciones nacionales adoptadas en cumplimiento de la presente Directiva entren en vigor, los datos personales de dichos abonados podrán seguir incluidos en dicha guía pública, en su versión impresa o electrónica, incluidas las versiones con funciones de búsqueda retrospectiva, a menos que los abonados indiquen lo contrario, tras haber recibido información completa sobre los fines y opciones con arreglo al artículo 12 de la presente Directiva.

Artículo 17

Incorporación al Derecho nacional

1. Los Estados miembros pondrán en vigor antes del 31 de octubre de 2003 las disposiciones necesarias para dar cumplimiento a lo establecido en la presente Directiva. Informarán inmediatamente de ello a la Comisión.

Cuando los Estados miembros adopten dichas disposiciones, éstas harán referencia a la presente

Directiva o irán acompañadas de dicha referencia en su publicación oficial. Los Estados miembros establecerán las modalidades de la mencionada referencia.

2. Los Estados miembros comunicarán a la Comisión el texto de las disposiciones de Derecho interno que adopten en el ámbito regulado por la presente Directiva, así como cualquier modificación ulterior de las mismas.

Artículo 18

Revisión

La Comisión presentará al Parlamento Europeo y al Consejo, a más tardar tres años después de la fecha contemplada en el apartado 1 del artículo 17, un informe sobre la aplicación de la presente

Directiva y su impacto en los operadores económicos y los consumidores, con especial atención a las disposiciones sobre comunicaciones no solicitadas y teniendo en cuenta la situación internacional. Para ello, la Comisión podrá recabar información de los Estados miembros, quienes deberán facilitarla sin retrasos indebidos. Cuando proceda, la Comisión presentará propuestas para modificar la presente Directiva teniendo en cuenta los resultados del informe mencionado, los cambios que hayan podido tener lugar en el sector y cualquier otra propuesta que juzgue necesaria para mejorar la eficacia de la presente Directiva.

Artículo 19

Derogación

Se deroga la Directiva 97/66/CE con efecto a partir de la fecha contemplada en el apartado 1 del artículo 17.

Las referencias a la Directiva derogada se entenderán hechas a la presente Directiva.

Artículo 20

Entrada en vigor

La presente Directiva entrará en vigor el día de su publicación en el Diario Oficial de las Comunidades Europeas.

Artículo 21

Destinatarios

Los destinatarios de la presente Directiva serán los Estados miembros.

Hecho en Bruselas, el 12 de julio de 2002.

Por el Parlamento Europeo

El Presidente

P. Cox

Por el Consejo

El Presidente

T. Pedersen

(1) DO C 365 E de 19.12.2000, p. 223.

(2) DO C 123 de 25.4.2001, p. 53.

(3) Dictamen del Parlamento Europeo de 13 de noviembre de 2001 (no publicado aún en el Diario

Oficial), Posición común del Consejo de 28 de enero de 2002 (DO C 113 E de 14.5.2002, p. 39) y

Decisión del Parlamento Europeo de 30 de mayo de 2002 (no publicada aún en el Diario oficial).

Decisión del Consejo de 25 de junio de 2002.

(4) DO L 281 de 23.11.1995, p. 31.

(5) DO L 24 de 30.1.1998, p. 1.

(6) DO L 178 de 17.7.2000, p. 1.

(7) DO L 91 de 7.4.1999, p. 10.

(8) DO L 108 de 24.4.2002, p. 33.

(9) DO L 204 de 21.7.1998, p. 37; Directiva modificada por la Directiva 98/48/CE (DO L 217 de

5.8.1998, p. 18).

(10) DO L 36 de 7.2.1987, p. 31; Decisión cuya última modificación la constituye el Acta de adhesión de 1994.