



**Consejo Económico  
y Social**

Distr.  
GENERAL

E/CN.4/1997/67  
12 de diciembre de 1996

ESPAÑOL  
Original: ARABE/ESPAÑOL  
FRANCES/INGLES

COMISION DE DERECHOS HUMANOS  
53° período de sesiones  
Tema 12 del programa provisional

LOS DERECHOS HUMANOS Y EL PROGRESO CIENTIFICO Y TECNOLOGICO

Cuestión de la aplicación de los principios rectores de la  
reclamación de los ficheros computadorizados de datos  
personales: informe del Secretario General preparado en  
virtud de la decisión 1995/114 de la Comisión

INDICE

	<u>Página</u>
INTRODUCCION . . . . .	2
I. APLICACION DE LOS PRINCIPIOS RECTORES EN EL SISTEMA DE LAS NACIONES UNIDAS . . . . .	3
II. INFORMACION RECIBIDA DE LOS ESTADOS . . . . .	7
Argentina . . . . .	7
Austria . . . . .	9
Croacia . . . . .	10
Estonia . . . . .	10
Alemania . . . . .	11
Jamahiriya Arabe Libia . . . . .	11
Luxemburgo . . . . .	13
Mauricio . . . . .	13
México . . . . .	13
Filipinas . . . . .	16
San Marino . . . . .	17
Suecia . . . . .	19
Reino Unido de Gran Bretaña e Irlanda del Norte . . . . .	20
Uruguay . . . . .	22

#### INTRODUCCION

1. En su decisión 1995/114, de 8 de marzo de 1995, la Comisión de Derechos Humanos, refiriéndose a los principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales (E/CN.4/1990/72), aprobados por la Asamblea General en su resolución 45/95, de 14 de diciembre de 1990, y tomando nota del informe del Secretario General presentado de conformidad con la decisión 1993/113 de la Comisión (E/CN.4/1995/75), decidió lo siguiente:

- a) Pedir a los Estados y a las organizaciones intergubernamentales, regionales y no gubernamentales que cooperen plenamente con el Secretario General proporcionándole todas las informaciones pertinentes relativas a la aplicación de los principios rectores;
- b) Pedir al Secretario General que continúe velando por la aplicación de los principios rectores en el seno del sistema de las Naciones Unidas;
- c) Pedir al Secretario General que informe a la Comisión en su 53º período de sesiones acerca de:
  - i) la aplicación de los principios rectores en el seno del sistema de las Naciones Unidas;
  - ii) las informaciones recibidas de los Estados y de las organizaciones intergubernamentales, regionales y no gubernamentales acerca de la aplicación de los principios rectores en los planos nacional y regional.

2. Con arreglo a esa decisión, el 6 de junio de 1996 el Secretario General transmitió solicitudes a los órganos, organismos, comisiones regionales, organismos especializados y organizaciones afines de las Naciones Unidas para que facilitasen información sobre la aplicación de los principios rectores dentro de las secciones correspondientes del sistema de las Naciones Unidas.

3. Con la misma fecha se transmitieron asimismo solicitudes a los Estados y a organizaciones intergubernamentales y no gubernamentales para que facilitasen información sobre la aplicación de los principios rectores en los niveles regional y nacional.

4. Al 10 de diciembre de 1996, se habían recibido respuestas de los siguientes órganos, organismos y organismos especializados de las Naciones Unidas: División de Prevención del Delito y Justicia Penal, Departamento de Asuntos Humanitarios, Comisión Económica para Europa, Comisión Económica para América Latina y el Caribe, Programa de las Naciones Unidas para el Medio Ambiente, Fondo de Población de las Naciones Unidas, Programa Mundial de Alimentos, Organismo Internacional de Energía Atómica, Organización Internacional del Trabajo, Fondo Monetario Internacional, Unión Internacional de Telecomunicaciones y Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura.

5. Han presentado información los Gobiernos de los siguientes países: Alemania, Argentina, Austria, Croacia, Estonia, Filipinas, Jamahiriya Arabe Libia, Luxemburgo, Mauricio, México, Reino Unido de Gran Bretaña e Irlanda del Norte, San Marino, Suecia y Uruguay.
6. Se recibió una respuesta de una organización intergubernamental: la Organización de Estados Americanos indicó que no estaba en condiciones de facilitar la información solicitada.
7. No se recibió ninguna respuesta de organizaciones no gubernamentales.
8. El presente informe contiene un resumen de las respuestas recibidas. Las respuestas que se reciban ulteriormente se publicarán como adición al presente documento.

#### I. APLICACION DE LOS PRINCIPIOS RECTORES EN EL SISTEMA DE LAS NACIONES UNIDAS

9. De los 33 órganos, organismos, comisiones regionales, organismos especializados y organizaciones conexas de las Naciones Unidas a las que se dirigió la solicitud, sólo han respondido 12.
10. El Departamento de Asuntos Humanitarios, la Comisión Económica para América Latina y el Caribe y la Unión Internacional de Telecomunicaciones afirmaron que no tenían información pertinente que transmitir ni observaciones que formular en relación con la cuestión.
11. La Comisión Económica para Europa afirmó que en ella no había actividad alguna a la que pudieran aplicarse las decisiones de la Comisión de Derechos Humanos en esta esfera, pues los archivos estadísticos de la Comisión eran anónimos o constaban de datos agregados.
12. El Programa de las Naciones Unidas para el Medio Ambiente indicó que su práctica era conforme a las disposiciones contenidas en los principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales.
13. El Organismo Internacional de Energía Atómica afirmó que las disposiciones contenidas en la sección 8 de su Manual Administrativo que trata de la protección de la información confidencial sobre el personal, se ajustaban a los principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales aprobados por la Asamblea General.
14. El Fondo Monetario Internacional (FMI) indicó también que los procedimientos relativos al acceso a los ficheros de datos personales en el FMI parecían ajustarse a los principios rectores.
15. La Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura confirmó que estaba aplicando los principios rectores en el mantenimiento de ficheros de datos personales.

16. El Fondo de Población de las Naciones Unidas (FNUAP) indicó que todas las cuestiones de personal del FNUAP eran administradas por el PNUD y por lo tanto seguían los principios rectores de las Naciones Unidas y el PNUD, que reflejaban los principios esbozados en el documento E/CN.4/1990/72 y la resolución 45/95 de la Asamblea General.

17. El Programa Mundial de Alimentos (PMA) presentó la siguiente declaración:

"El mantenimiento de los ficheros computadorizados de datos personales relativos al personal empleado directamente por el PMA corre a cargo de la Organización de las Naciones Unidas para la Agricultura y la Alimentación (FAO), con sede también en Roma, con la que compartimos un sistema computadorizado de datos sobre el personal (PERSYS). La FAO administra este sistema y es responsable del mismo. El personal del Servicio de Recursos Humanos del PMA tiene acceso limitado a los ficheros computadorizados correspondientes al personal del PMA.

A nuestro entender, el FAO/Persys se ajusta a todos los principios rectores expuestos en el documento E/CN.4/1990/72, de 20 de febrero de 1990."

18. La División de Prevención del Delito y Justicia Penal (Oficina de las Naciones Unidas en Viena) presentó la información siguiente:

"1. En sus actividades, la División a menudo se remite a los principios rectores. Valga como ejemplo su inclusión en las siguientes publicaciones de venta:

- a) Guía para la computadorización de los sistemas de información en la esfera de la justicia penal (ST/ESA/STAT/SER.F/58, publicación de las Naciones Unidas, N° de venta S.92.XVII.6, pág. 177), preparada conjuntamente por la División de Estadística en la sede y nuestra División;
- b) Manual de las Naciones Unidas sobre prevención y control de delitos informáticos (Revista internacional de política criminal, Nos. 43 y 44, 1994, ST/ESA/SER.M/43-44, publicación de las Naciones Unidas, N° de venta S.94.IV.5, párr. 138).

2. También se hicieron alusiones a los principios rectores en los documentos de trabajo preparados por la División para el Octavo y el Noveno Congresos de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente, celebrados en 1990 y 1995, respectivamente. En particular, figuran en los documentos siguientes:

- a) A/CONF.144/14 ("Computadorización de la administración de justicia penal"), párr. 12;
- b) A/CONF.169/6 ("Sistemas de justicia y de policía: gestión y perfeccionamiento de la policía y otros órganos encargados de

hacer cumplir la ley, del ministerio público, de los tribunales y de los establecimientos penitenciarios, y función de los abogados"), párr. 89.

3. En sus actividades de capacitación de profesionales de la justicia penal, que se realizan particularmente en los países en desarrollo, los expertos, a petición de la División y el propio personal de ésta, informan a esos profesionales sobre el papel de la confidencialidad en el tratamiento de ficheros manuales y computadorizados de sospechosos y convictos, de acuerdo con los principios rectores. Recientemente la División examinó cuestiones relativas a la protección de la intimidad en el curso interregional de capacitación sobre la red computadorizada de información de las Naciones Unidas sobre delincuencia y justicia y los datos destinados a los países en desarrollo y procedentes de éstos, organizado bajo los auspicios de las Naciones Unidas por el Gobierno de la República de Corea (Seúl, 9 a 13 de septiembre de 1996).

4. Por último, en diversas consultas oficiosas con especialistas en la cuestión del delito informático y desde la perspectiva de la División, ésta sostuvo la opinión de que en el nivel de la administración interna de justicia penal, los principios rectores pueden ser útiles si se pueden aplicar a las dos tendencias universales actuales:

- a) mayor peligro de delincuencia organizada y actos de terrorismo;
- b) un progreso muy dinámico en la esfera de las nuevas tecnologías de tratamiento de la información.

5. Esas dos tendencias guardan relación directa con las actividades de los sistemas de justicia penal e influyen en el papel de los órganos encargados de aplicar la ley (principios 1 a 4, en los que se subraya la licitud y la lealtad en el acopio de datos), con el posible menoscabo de la protección de la intimidad (principio 6, relativo a la facultad de hacer excepciones).

6. Para reforzar la licitud y la lealtad en el acopio de datos y velar por la aplicación de los principios rectores en todos los países, tal vez convendría estudiar la posibilidad de revisar las tendencias en al menos dos esferas:

- a) si después de 1990 (año de aprobación de los principios rectores) los países han promulgado legislación relativa a la protección de datos;
- b) si existe una práctica de informar al público sobre las bases de datos electrónicas de justicia penal que se crean y se mantienen (sistemas avanzados de reconocimiento visual/circuito cerrado de televisión, reconocimiento computadorizado de rostros, bases de datos nacionales de ADN con los rasgos genéticos identificativos de presuntos delincuentes, sistemas

inteligentes de rastreo de vehículos en carretera, tarjetas inteligentes de identificación y de otro tipo que facilitan diversas transacciones personales)."

19. La Organización Internacional del Trabajo (OIT) presentó la información siguiente:

"En lo que se refiere a la aplicación de los principios rectores en la Oficina Internacional del Trabajo, ésta aún no ha establecido archivos computadorizados de datos personales. Esos archivos aún existen en papel y se manipulan manualmente. No obstante, la Oficina está introduciendo un sistema de información sobre el personal (PERSIS) que consta de distintos bancos de datos que están computadorizados. El sistema PERSIS sigue el modelo del Sistema integrado de información de gestión (SIIG) elaborado por la Secretaría de las Naciones Unidas en Nueva York, y se da por supuesto que el SIIG fue elaborado de conformidad con los principios rectores.

Las prácticas de la OIT se ajustan completamente a los siguientes principios rectores:

Principio de la licitud y lealtad: se cumple;

Principio de exactitud: actividad continua de limpieza y actualización de la base de datos;

Principio de finalidad: todos los datos del SIIG guardan relación directa con las necesidades de administración del personal y la nómina, y no se incluyen datos innecesarios;

Principio de acceso de la persona interesada: se cumple;

Principio de no discriminación: se cumple;

Facultad de establecer excepciones: se cumple;

Principio de seguridad: el servidor que contiene la base de datos está sumamente protegido dentro de la red de la OIT y la Organización acaba de instalar un sistema de protección muy estricto contra el acceso sin autorización a sus ficheros;

Control y sanciones: se cumple;

Flujo de datos a través de las fronteras: se cumple;

Campo de aplicación: se cumple."

20. La OIT también se refirió a una Reunión de Expertos sobre la protección de la vida privada de los trabajadores, prevista del 1º al 7 de octubre de 1996 en Ginebra. Estaba previsto que en esa reunión se debatiera un proyecto de repertorio de recomendaciones prácticas sobre la protección de

los datos personales de los trabajadores y otras posibles medidas de la OIT. El proyecto se refiere a cualquier uso de datos personales, inclusive el acopio, el almacenamiento y la transmisión.

## II. INFORMACION RECIBIDA DE LOS ESTADOS

### Argentina

[Original: español]  
[22 de agosto de 1996]

1. A partir de la reforma constitucional que tuvo lugar en agosto de 1994, la Carta Magna incluye, en su artículo 43, párrafo 3º, la acción de amparo en relación con la toma de conocimiento por parte de cualquier persona, sobre datos referidos a ella, que consten en registros o bancos de datos públicos o privados, destinados a proveer informes, y en caso de falsedad de los mismos o cualquier forma de discriminación que de ellos se desprenda, para exigir su supresión, rectificación, confidencialidad o actualización, así como también para conocer la finalidad para la cual han sido recabados.

2. La norma constitucional mencionada responde en forma positiva a los principios rectores aprobados por la Asamblea General de las Naciones Unidas en su resolución 45/95 del 14 de diciembre de 1990 y a la decisión 1995/114 aprobada por la Comisión de Derechos Humanos el 8 de marzo de 1995. Entre los principios tomados como base para la norma constitucional, es importante destacar el de finalidad (expresado en el párrafo 3º); el de acceso de la persona interesada (4º); el de no discriminación (5º); el de establecimiento de controles (8º); y el referido al campo de aplicación en registros públicos y privados (10º).

3. En lo que respecta a la actividad legislativa en esta materia, se han presentado al Congreso Nacional 18 proyectos de ley, de los cuales, a la fecha, sólo uno ha recibido media sanción, por la Cámara de Diputados del Congreso de la Nación en la sesión del 5 de junio de 1996.

4. Dicho proyecto recoge los principios rectores de manera total, estableciendo excepciones a su aplicación de conformidad con las directrices fijadas en su párrafo 6º. Por otra parte, establece de manera clara las definiciones a los conceptos tratados, para evitar discrepancias conceptuales que perjudiquen su plena aplicación y efectividad.

5. En cuanto a la autoridad de aplicación, el artículo 5 del proyecto crea, en el ámbito del Congreso Nacional, una Comisión Bicameral de Seguimiento de Protección de Datos, a los fines de posibilitar la salvaguarda y protección de los derechos tutelados por dicha ley.

6. Merece comentario el artículo 11 del proyecto de que se trata, que establece que determinados datos personales deberán estar especialmente protegidos: i) ideología, raza, religión, hábitos personales y comportamiento sexual; ii) estado de salud (a este respecto, el artículo 12

establece la excepción tendiente a suministrar la información pertinente a centros sanitarios y profesionales sobre personas que a ellos consulten o reciban tratamientos), situación patrimonial y obligaciones tributarias, salvo razones de interés general y por disposición legal o consentimiento del interesado; iii) datos relativos a procesos penales o infracciones administrativas, los cuales sólo podrán ser incluidos en registros o bancos de datos pertenecientes a las administraciones públicas competentes, siempre a través de sus respectivas normas reguladoras.

7. El proyecto dispone que los datos de carácter personal sólo podrán ser cedidos con el previo consentimiento por escrito del interesado -que podrá ser siempre revocado-, estableciendo a su vez, la sanción de nulidad de la cesión si no se desprende de ella con claridad la finalidad de la misma, (art. 15). El consentimiento del interesado no será requerido en los casos específicamente previstos por el proyecto y que atienden a razones de interés público como la eficaz administración de justicia y la salud pública general.

8. La transmisión de datos al extranjero, organismos internacionales o supranacionales, deberá gozar de la misma protección que los datos de carácter personal en el ámbito de la República.

9. Los titulares de la información que se encuentran en los ficheros gozan de los siguientes derechos: i) impugnar los actos administrativos o decisiones privadas que tengan por único fundamento la valoración que de su persona se haga a partir del tratamiento de datos de carácter personal; ii) conocer la existencia de los registros o bancos de datos, su finalidad e identidad del responsable; iii) solicitar y obtener la información personal que figura en dichos registros o bancos de datos sin la exigencia de contraprestación alguna; iv) rectificar, eliminar y conservar los datos de carácter personal.

10. En relación con la tutela de los derechos, el proyecto prevé acción sumaria para establecer responsabilidad por daños o lesiones a los bienes o derechos del interesado causados como consecuencia de la información archivada y que deberá establecer una reparación bajo la forma de indemnización. La acción prevista se efectuará bajo el procedimiento sumario y no obstará a la interposición de la acción de amparo, prevista constitucionalmente y en consonancia con la Ley N° 16986, para la aplicación de la cual el Código Civil y Procesal de la Nación prevé en su artículo 321 la vía sumarísima para su tramitación.

11. Por su parte, el proyecto establece, para las personas responsables de los registros o bancos de datos -sin perjuicio de las responsabilidades emergentes de los daños y perjuicios ocasionados al afectado y de las sanciones penales a que hubieran dado lugar los delitos cometidos- las sanciones de apercibimiento, suspensión, multa, eliminación o clausura de los registros o bancos de datos, por parte del Defensor del Pueblo, quien, de acuerdo con la reglamentación a dictar por la Comisión Bicameral creada por la propia ley, será el órgano de aplicación.



12. De acuerdo al último artículo del proyecto que se comenta, se invita a las provincias a crear sus registros de bancos de datos provinciales y a establecer sus órganos de aplicación; sin perjuicio de ello, el proyecto dispone que la ausencia de reglamentación procesal en la materia no obstará a la tramitación de la acción sumarísima prevista en el artículo 43 de la Constitución Nacional.

13. Lo informado en párrafos precedentes representa en somera síntesis los avances que la República Argentina ha efectuado en la materia. Sin perjuicio de ello, se adjunta copia completa del proyecto de ley que se comenta\*.

#### Austria

[Original: inglés]  
[11 de septiembre de 1996]

1. La Ley austríaca de protección de datos, publicada en el Boletín legislativo federal (Datenschutzgesetz) N° 565/1978 abarca todos los principios contenidos en los principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales de las Naciones Unidas. En particular, los conceptos de finalidad (principio 3), de licitud y lealtad (principio 1) y de facultad de establecer excepciones (principio 6) constituyen la base de la protección de datos en Austria, como puede verse en la sección 1 del Boletín.

2. El principio 5 está comprendido en el artículo 6 del Convenio para la protección de las personas en relación al tratamiento automatizado de los datos de carácter personal, del Consejo de Europa, que fue ratificado por Austria en 1988 ( Boletín legislativo federal N° 317/1988), y es aplicado por las autoridades competentes desde entonces.

3. Con arreglo a la directiva 46/95/EC de la Unión Europea, la liberalización del flujo de datos a través de las fronteras (principio 9) en relación con otros Estados miembros de la Unión Europea comenzará a aplicarse próximamente.

4. Se adjuntó una copia de la traducción no oficial de la Ley austríaca de protección de datos\*.

---

\* Puede consultarse en los archivos de la Secretaría.

Croacia

[Original: inglés]  
[4 de septiembre de 1996]

1. El Gobierno de la República de Croacia, por conducto de sus órganos competentes, ha examinado minuciosamente los principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales aprobados por la Asamblea General en su resolución 45/95, a fin de aplicar sus disposiciones a escala nacional tanto mediante la legislación como en la práctica.
2. En la actualidad no existe ningún texto legal amplio relativo a la reglamentación de los ficheros computadorizados de datos personales. No obstante, esa reglamentación figura en distintos textos legales en relación con esferas particulares de la vida pública en las que se precisa la protección de datos personales, particularmente en cuestiones internas, de ciudadanía y de estado civil, de atención médica y, en cierta medida, de la ejecución de sanciones penales. Además, algunos aspectos de los ficheros computadorizados de datos personales están regulados por los reglamentos internos de los respectivos órganos gubernamentales y públicos que se ocupan de las cuestiones antes mencionadas.
3. Actualmente está en marcha la redacción de un texto legal completo sobre la reglamentación de los archivos de datos personales, que está previsto someter al examen parlamentario en el curso del otoño de 1996.
4. En el proceso de preparación de ese texto se han tomado como modelo varios instrumentos internacionales de protección de datos, en particular el Convenio para la protección de las personas con relación al tratamiento automatizado de los datos de carácter personal, del Consejo de Europa, los principios rectores de las Naciones Unidas antes mencionados y la más reciente directiva de la Unión Europea al respecto, publicada en 1996. Además se ha tenido en cuenta la legislación recientemente adoptada por varios países europeos.
5. Una vez aprobado, ese texto legal contribuirá sin duda a reforzar la protección y la unificación de las normas de uso de ficheros computadorizados de datos personales.

Estonia

[Original: inglés]  
[10 de septiembre de 1996]

Las autoridades competentes de Estonia consideran que los principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales de las Naciones Unidas son plenamente razonables y aplicables.

Alemania

[Original: inglés]  
[12 de septiembre de 1996]

1. En virtud de la Directiva 95/46 del Parlamento Europeo y del Consejo de Europa, de 24 de octubre de 1995, que se refiere a la protección de datos, los Estados miembros de la Unión Europea tienen en general que adaptar su legislación nacional en materia de protección de datos. Las disposiciones de la Directiva deben aplicarse antes del 23 de octubre de 1998. No obstante, la mayoría de los requisitos que se establecen en la Directiva ya están previstos en la legislación alemana en materia de protección de datos. Actualmente se están introduciendo las siguientes novedades en relación con algunos de los principios rectores de las Naciones Unidas sobre la protección de datos, respecto de la situación expuesta en el documento E/CN.4/1990/72.

Principio 4

2. La protección de datos se hará más transparente para el ciudadano. Ello se conseguirá, entre otras cosas, haciendo extensiva al sector público la obligación de informar a la persona a la que se refieren los datos sobre el almacenamiento o la comunicación de esos datos, introduciendo en el sector privado la obligación general de informar a la persona a la que conciernen los datos sobre la recogida de sus datos y aumentando ligeramente el derecho de acceso de las personas a los datos que les conciernen.

Principio 9

3. En el proceso de adaptación de la legislación en materia de protección de datos a la correspondiente Directiva de la Unión Europea, será necesario introducir una disposición que condicione la comunicación de datos a terceros países a la existencia en ellos de un nivel suficiente de protección de datos. Además, debe introducirse una lista amplia de excepciones a ese principio con el fin de evitar que el comercio con terceros países se vea obstaculizado. También, es preciso crear normas legales que impidan a los usuarios de los datos trasladarse a Estados no pertenecientes a la Unión Europea cuyo nivel de protección de datos sea inferior, haciendo que las disposiciones nacionales aprobadas para poner en vigor la Directiva de la Unión Europea se apliquen también en esos países si los medios de tratamiento de los datos, como los terminales o los cuestionarios, se encuentran en el territorio de un Estado miembro de la Unión Europea.

Jamahiriyá Árabe Libia

[Original: árabe]  
[2 de octubre de 1996]

1. Habiendo estudiado el proyecto de principios rectores sobre la reglamentación de ficheros computadorizados de datos personales al que se hizo referencia en la resolución 44/132 de la Asamblea General y en los que se destaca la necesidad de respetar los derechos humanos y libertades

fundamentales del individuo, la Jamahiriya Arabe Libia Popular y Socialista, afirmando su apoyo a esos principios de acuerdo con su política sostenida de defensa de la libertad y protección de los derechos de la persona dondequiera que se encuentre, y de conformidad con su legislación basada en los preceptos del Corán, en el que se consagra a la persona como delegado de Dios en la Tierra y, en particular, basándose en el Gran Documento Verde sobre los Derechos Humanos, ha recopilado sus convicciones sobre esa cuestión en la Ley de información N° 4, de 1990, que se refiere al sistema nacional de datos y documentación, y en cuyo artículo 6 se tratan los datos personales de modo plenamente conforme con los principios rectores de las Naciones Unidas.

Artículo 6 de la Ley de información

2. Está prohibido utilizar cualquier medio de presión o engaño para acopiar información o datos personales en el marco del sistema nacional de información. La persona interesada tiene derecho a conocer esa información y esos datos y a suprimir o rectificar cualquier cosa que, en su opinión, difiera de la verdad antes de que se documente.

3. El uso de esos datos o información se limita a los fines de estudios económicos y sociales. Ningún tercero, ni siquiera si se trata de una autoridad pública, tiene acceso a ellos y no está permitido difundirlos de modo que se indique la identidad de las personas a que se refieren, ni pueden utilizarse con ningún otro fin ni aceptarse como prueba en ningún proceso jurídico en violación de lo estipulado anteriormente.

4. Cabe señalar que este artículo de la ley libia se atiene a los siguientes principios:

1. Licitud y lealtad en el acopio de datos personales.
2. Verificación de la fiabilidad y la exactitud de los datos personales.
3. Finalidad del acopio de los datos.
4. Acceso de la persona interesada a los ficheros que contienen sus datos personales.
5. No discriminación, que el artículo dispone implícitamente al prohibir la difusión o el uso de la información con fines distintos de los que permite la ley y de modo que indique o revele la identidad de las personas interesadas.

5. Los otros principios rectores en relación con la seguridad, el control y las sanciones están comprendidos en los artículos 7, 8 y 9 de la Ley de información de Libia.

6. Así pues, la Jamahiriya ha adoptado los principios rectores, que a su juicio constituyen las garantías mínimas que deben ofrecerse a fin de proteger los derechos humanos fundamentales.

Luxemburgo

[Original: francés]  
[22 de agosto de 1996]

1. La Ley enmendada de 31 de marzo de 1979 por la que se regula la utilización de datos nominativos sometidos a tratamiento informático se ajusta a los principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales (E/CN.4/1990/72) aprobados por la Asamblea General en su resolución 45/95, de 14 de diciembre de 1990, salvo en lo que respecta a los principios 8 (control y sanciones) y 9 (flujo de datos a través de las fronteras), cuyas disposiciones no están expresamente previstas en nuestra legislación.

2. Esos principios quedarán recogidos en una nueva ley de Luxemburgo en materia de protección de las personas en relación con el tratamiento de los datos personales que les incumben, ley que trasladará al derecho nacional las disposiciones de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas con relación al tratamiento de los datos de carácter personal y la libre circulación de esos datos; la transposición de la Directiva a la legislación nacional tendrá lugar en un plazo de tres años a partir de la aprobación de la Directiva.

Mauricio

[Original: inglés]  
[10 de septiembre de 1996]

El Gobierno de Mauricio presentará próximamente un proyecto de ley sobre tecnología de la información (disposiciones diversas), que, entre otras cosas, se ocupa de los delitos en la esfera de la protección y la seguridad de los datos y el uso indebido de computadoras.

México

[Original: español]  
[21 de octubre de 1996]

Principio de la licitud y lealtad

1. En lo que corresponde a este principio, el Registro Nacional de Población e Identificación Personal se encuentra regulado por la Ley general de población y sus funciones son, conforme lo establece el artículo 87 de esa ley, inscribir a los mexicanos mediante el Registro Nacional de Ciudadanos, el Registro Nacional de Menores y el Padrón de los Mexicanos residentes en el Extranjero y a los extranjeros a través del Catálogo de los Extranjeros residentes en la República Mexicana.

2. En la actualidad, sólo se está trabajando en la integración del Registro de Menores de Edad, cuya información se obtiene de las actas de nacimiento que han remitido los registros civiles de la República a partir del año 1982, conforme lo señala el artículo 89 de la mencionada ley.

3. Los registros civiles están regulados por las leyes emitidas por los congresos locales, en las que se establece la manera como deberán realizarse las inscripciones respectivas para cumplir con el principio de legalidad y también determinan las disposiciones necesarias para preservar el principio de licitud y lealtad.

#### Principio de exactitud

4. En el Registro Nacional de Población e Identificación Personal se tiene la obligación de verificar la exactitud y la pertinencia de los datos que se registran, realizando una validación de campos para evitar errores de digitación o se consideran campos obligatorios para evitar omisión de información importante.

#### Principio de finalidad

5. La mencionada ley cumple con este principio, ya que aunque únicamente se cuenta ahora con el Registro de Menores de Edad, la propia ley establece en su artículo 86 que el Registro Nacional de Población e Identificación Personal tiene como finalidad registrar a cada una de las personas que integran la población del país con los datos que permitan certificar o acreditar fehacientemente su identidad. Todo ello, para posteriormente emitir la cédula de identidad ciudadana, que será el documento oficial de identificación como prueba plena sobre los datos de identidad que contiene en relación con su titular.

6. Al ser el acta de nacimiento o la carta de naturalización, como certificado de nacionalidad, el requisito indispensable para llevar a cabo la inscripción de las personas, las leyes que regulan el Registro Civil establecen que éste debe ser público, de tal modo que toda persona pueda solicitar un testimonio de las actas del Registro Civil.

7. Sin embargo, en el caso de la información del Registro Nacional de Población e Identificación Personal, se estima que sólo el interesado o la autoridad judicial pueden tener acceso a dicha información. En el caso del interesado, la misma ley prevé para los menores de edad, la expedición de un documento de identificación y para los mayores de edad la expedición de la cédula de identidad ciudadana.

8. En cuanto a la conservación de los datos personales, ésta debe ser permanente, ya que incluso debe inscribirse el acta de defunción de las personas, lo que lleva a otra finalidad del propio registro, señalada en el artículo 112 de la ley, de proporcionar al Instituto Federal Electoral la información del Registro Nacional de Ciudadanos que sea necesaria para la integración de los instrumentos electorales.

Principio de acceso de la persona interesada

9. El párrafo segundo de la fracción I del artículo 36 de la Constitución Política de los Estados Unidos Mexicanos dispone que el Registro Nacional de Ciudadanos y la expedición de la cédula de identidad ciudadana son servicios de interés público y, por tanto, responsabilidad que corresponde al Estado y a los ciudadanos.

10. La Ley general de población establece la expedición de la cédula de identidad ciudadana y del documento de identificación a los mexicanos menores de 18 años. Para el efecto, los interesados tienen acceso a esta información con lo que se evitarán los registros ilícitos, injustificados o inexactos. Sin embargo, la citada ley no contempla el recurso para la rectificación de los mismos.

Principio de no discriminación

11. La información que obtiene el Registro Nacional de Población e Identificación Personal, a través de las actas del Registro Civil y las leyes que regulan dicha institución prevén de manera categórica el registro de datos que puedan originar una discriminación ilícita o arbitraria, de tal modo que no es factible que información que no esté señalada en dichas actas se pueda asentar en la base de datos.

Facultad de establecer excepciones

12. La publicidad de la información que contiene la base de datos del Registro Nacional de Población e Identificación Personal está prevista en el artículo 112 de la Ley general de población, que establece que la Secretaría de Gobernación proporcionará al Instituto Federal Electoral la información del Registro Nacional de Ciudadanos necesaria para integrar los instrumentos electorales.

Principio de seguridad

13. Para proteger los ficheros contra riesgos naturales, su destrucción por siniestro u otros, señalados en el punto 7 de los Principios Rectores sobre la Utilización de Ficheros Computarizados de Datos Personales, el Registro Nacional de Población e Identificación Personal respalda la información de su base de datos y la envía a una caja de seguridad fuera de sus instalaciones.

Control y sanciones

14. La Ley general de población en su artículo 113 establece las sanciones que las autoridades de la propia Secretaría de Gobernación, dependencia gubernamental encargada de la base de datos, según el sistema jurídico interno, podrán aplicar a los empleados que incurran en distintas violaciones a las disposiciones establecidas, tales como proporcionar información acerca de asuntos de carácter confidencial sin estar autorizados, entorpecer el

trámite normal de los asuntos por dolo o por grave negligencia, intervenir en la gestión de asuntos en materia de la ley o patrocinen o aconsejen la manera de evadir disposiciones y trámites por sí o por intermediarios.

Flujo de datos a través de las fronteras

15. El Registro Nacional de Población e Identificación Personal únicamente deberá obtener información de los mexicanos radicados en el extranjero. Sin embargo, tal información se obtendrá a través de la Secretaría de Relaciones Exteriores conforme lo señala el artículo 96 de la Ley general de población.

Filipinas

[Original: inglés]  
[15 de noviembre de 1996]

El Gobierno de Filipinas presentó los siguientes documentos, facilitados por la Comisión de Administración Pública de Filipinas:

- i) Normas de aplicación, de fecha 21 de abril de 1989, de la Ley N° 6713 de la República, de 20 de febrero de 1989, tituladas "Código de conducta y normas éticas para funcionarios y empleados públicos";
- ii) Resolución de la Comisión de Administración Pública N° 92-1908, de 25 de noviembre de 1992, titulada "Aclaración sobre la Ley de transparencia con arreglo a la Constitución de 1987 y la Ley de la República N° 6713"; y
- iii) Memorando de la Comisión de Administración Pública N° 73, serie de 1993.

La información contenida en esos documentos completa el informe del Gobierno de Filipinas sobre su aplicación de los principios rectores, presentado el 22 de septiembre de 1994 (véase E/CN.4/1995/75)\*.

---

\* Puede consultarse en los archivos de la Secretaría.



San Marino

[Original: inglés/italiano]  
[5 y 11 de septiembre de 1996]

1. En la República de San Marino, la legislación relativa al almacenamiento en computadoras de datos confidenciales está constituida por la Ley N° 70, de 23 de mayo de 1995 (Enmienda de la Ley N° 27 de 1° de marzo de 1983, que regula el acopio computadorizado de datos personales), y la Ley N° 71, de 23 de mayo de 1995 (Reglamentación del acopio de datos estadísticos y la competencia pública en el tratamiento de los datos), que se refiere más específicamente al tratamiento de datos en la administración pública.

2. No obstante, ya se habían hecho intentos de regular la cuestión; en particular, la Ley N° 70 de 1995 revocó y sustituyó por completo la Ley N° 27 de 1° de marzo de 1983, con la excepción, no obstante, de una serie de decretos de la Regencia que se aprobaron para aplicar la Ley N° 27/83:

Decreto N° 7 de 13 de marzo de 1984, "Establecimiento de un banco de datos estatal según dispone el artículo 5 de la Ley N° 27 de 1° de marzo de 1983";

Decreto N° 7 de 3 de junio de 1986, "Integración al Decreto N° 7 de 13 de marzo de 1984, por el que se establece un banco de datos estatal";

Decreto N° 140 de 26 de noviembre de 1987, "Procedimientos para el establecimiento de bancos de datos privados".

3. En el párrafo II del artículo 20 de la Ley N° 27/83 se afirma claramente que esos decretos siguen en vigor y son compatibles con la nueva reglamentación.

4. La Ley N° 70/95 desempeña un papel mucho más importante en relación con la cuestión de que se trata. Esa ley introdujo en el ordenamiento jurídico de San Marino una serie de principios generales de protección de los archivos de datos personales. Tras un examen minucioso, se declaró que esos principios se ajustaban perfectamente a los afirmados por la Comisión de Derechos Humanos, que establecen una norma a la que deben amoldarse todas las reglamentaciones nacionales.

5. El ordenamiento jurídico de San Marino afirma el principio de la licitud y lealtad prohibiendo claramente en el párrafo I del artículo 7 de la Ley N° 70/95 el acopio de datos personales y confidenciales por medios fraudulentos, ilícitos o desleales.

6. Los encargados del establecimiento y el mantenimiento de bancos de datos tienen la obligación expresa de aplicar los principios de exactitud, pertinencia y cabalidad, como estipula claramente el artículo 14 de la Ley N° 70/95, que contiene la obligación de rectificar, actualizar e integrar

los datos de oficio siempre que se detecte información inexacta o incompleta. El artículo 14 prevé también que toda rectificación, integración o actualización se notifique a las personas interesadas de modo gratuito.

7. En lo que se refiere a las razones que llevan al establecimiento de un sistema de archivo computadorizado, la legislación vigente no define los objetivos concretos que deben alcanzarse. Cabe deducir éstos del procedimiento que debe seguirse para crear un banco de datos, que exige la autorización previa tanto del Congreso Estatal (el Gobierno) como del Garante de la protección de los datos confidenciales y personales (art. 15). Así pues, todo objetivo concreto que motive la creación de un banco de datos es autorizado en última instancia conjuntamente por esos órganos. Además, toda persona cuyos datos personales vayan a integrarse en un banco computadorizado debe ser debidamente informada de los objetivos previstos (art. 8). Es cierto que debe especificarse mejor este principio.

8. Por el contrario, el sistema legal de San Marino protege con gran eficacia el derecho de acceso a ficheros y archivos y datos confidenciales: cualquier individuo tiene derecho tanto a preguntar si sus datos personales han sido acopiados o procesados (art. 10) como a obtener copia de los mismos (art. 11), y a exigir que todo dato inexacto, anticuado, incompleto o ambiguo, o cuyo acopio, tratamiento, transmisión o mantenimiento esté prohibido, sea rectificado, integrado, aclarado, actualizado o suprimido (art. 12).

9. En cualquier caso, de plantearse dudas sobre la veracidad y la conformidad de los datos acopiados y tratados, puede hacerse una reclamación por escrito al Garante, que está obligado a responder en un plazo de 60 días a partir de la recepción tras haber examinado si es necesaria una investigación administrativa o la intervención de la magistratura (art. 13); la decisión del Garante puede ser objeto de recurso.

10. La Ley Nº 70/95 sanciona plenamente el principio de no discriminación, que autoriza el acopio de información especial sólo a condición de que las personas interesadas den su consentimiento, pues en el caso de información relativa a ideas o actividades políticas, sindicales o religiosas, ello podría dar lugar a discriminación ilícita o arbitraria. El acopio de información de carácter sumamente personal está prohibido en todos los casos (art. 7).

11. El principio de seguridad, que prevé medidas apropiadas para prevenir la destrucción potencial de archivos o ficheros e impedir el acceso no autorizado, queda recogido en términos generales en el párrafo 4 del artículo IV. Ese artículo dispone que el personal del banco de datos debe observar rigurosamente el principio del secreto profesional y prevé medidas precautorias para impedir que la información sea alterada, falsificada o revelada a personal no autorizado.

12. El control de la observancia efectiva de los principios incumbe al Garante de la protección de datos confidenciales y personales, que es la autoridad competente para examinar toda denuncia o petición relativa a la

aplicación de la ley antes mencionada, y decide en los casos en que se ha violado la confidencialidad de los datos personales. No obstante, siempre puede apelarse a una instancia de orden superior, sea ordinaria o administrativa. Las otras funciones del Garante están también definidas en la ley (arts. 15 y 16). La forma en que se ha concebido este órgano responde plenamente a la necesidad de garantizar la imparcialidad e independencia del personal que se ocupa de la computadorización de datos confidenciales. La función de Garante es desempeñada por un juez del Tribunal Administrativo.

13. A fin de velar por la máxima protección de los datos confidenciales y por una aplicación más eficaz de las leyes pertinentes, la infracción de ciertas normas está castigada con penas o sanciones administrativas (arts. 17 y 18).

14. La difusión de datos confidenciales sobre personas de San Marino que son transferidos fuera de las fronteras de la República está condicionada a la autorización previa y motivada del Garante, que habrá de verificar si el país al que se transmite la información confidencial garantiza el mismo nivel de protección de datos personales que el que establece la legislación de San Marino.

15. La Ley N° 70/95 tiene un margen de aplicación amplio y generalizado, pues rige, sin distinción, para todo sistema de archivo o banco de datos computadorizado, sea privado o público, o propiedad de una persona física o jurídica (art. 1).

16. En conclusión, la legislación de la República de San Marino en materia de protección de datos confidenciales y personales se ajusta en esencia a los principios afirmados por la Comisión de Derechos Humanos.

#### Suecia

[Original: inglés]

[26 de agosto de 1996]

1. En agosto de 1994, Suecia presentó un informe sobre esta cuestión (véase E/CN.4/1995/75) que sigue vigente con algunas modificaciones. Como se mencionaba en ese informe, el Gobierno presentó un proyecto de ley al Parlamento el 14 de abril de 1994 con ciertas enmiendas a la Ley de datos de 1973. Esas enmiendas entraron en vigor el 1° de enero de 1995. En el informe de 1994 se describen esas enmiendas.

2. Se ha producido, no obstante, un cambio en las enmiendas respecto de la información que contiene el informe: no todas las apelaciones contra las decisiones del Organismo de Protección de Datos tienen que ser necesariamente tramitadas por un tribunal de justicia. Si el demandante es una autoridad pública dependiente del Gobierno, la instancia de apelación sigue siendo el Gobierno.

3. Hoy en día, la principal cuestión legislativa en relación con la protección de los datos se refiere a la nueva Directiva de la Unión Europea sobre la protección de las personas en relación con el tratamiento de datos

personales y la libre circulación de esos datos (Directiva 95/46/EC). Los Estados miembros disponen de un plazo de tres años, a partir de la fecha de adopción, para transponer la directiva a la legislación nacional. La directiva fue adoptada el 24 de octubre de 1995.

4. El Gobierno ha creado una comisión parlamentaria especial encargada de redactar legislación totalmente nueva en materia de protección de datos dentro del marco de la directiva de la Unión Europea. Una de las instrucciones del Gobierno a la Comisión es que la ley se aplique a los datos personales con independencia del tipo de técnica que se utilice. La Comisión ultimaré sus tareas antes de finales de marzo de 1997.

Reino Unido de Gran Bretaña e Irlanda del Norte

[Original: inglés]  
[30 de septiembre de 1996]

1. La Ley del Reino Unido sobre protección de los datos computadorizados tiene presentes los principios rectores establecidos por las Naciones Unidas. La Ley de protección de los datos computadorizados de 1984 otorga derechos a las personas respecto de las cuales existe información sujeta a tratamiento automatizado (esto es, mediante computadora). La persona puede obtener acceso a la información de que se disponga sobre ella, objetar su exactitud y, en algunos casos, exigir indemnización. Los depositarios de información personal computadorizada deben registrarse ante el Secretario de Protección de los Datos Computadorizados (Data Protection Registrar) y acatar los principios establecidos que rigen el modo en que obtienen, registran y utilizan dichos datos.

2. Los aspectos principales de la legislación son los siguientes:

- i) La ley se aplica a todos los datos de carácter personal computadorizados o contenidos en un formato que permita su tratamiento automatizado, excepto los que se procesan en casa con fines domésticos y los que manejan las empresas a efectos de pagos, administración de pensiones, contabilidad, compras o ventas (exceptuados los que se destinan a registros de personal o a fines de comercialización). Otras excepciones son los casos en que los miembros de clubes reconocidos utilizan los datos informatizados únicamente para distribuir artículos o información a las personas a las que conciernen los datos; los casos en que la ley obliga al usuario a hacer públicos los datos (por ejemplo, los del censo electoral); y aquéllos en que los datos se conservan por razones de seguridad nacional (según lo establezcan los ministerios pertinentes).
- ii) Todos los usuarios de datos a quienes no se apliquen las excepciones a la ley deben registrar lo siguiente: información sobre el tipo de datos que conservan; la finalidad a la que los destinan; las fuentes de los datos; las personas a las que éstos puedan revelarse y los países extranjeros a los que puedan transferirse.

- iii) Los usuarios deben acatar los principios sobre protección de los datos computadorizados. Dichos principios estipulan que los datos de carácter personal deben recogerse y elaborarse de manera leal y lícita; deben conservarse únicamente para los fines lícitos que se hayan indicado en el registro de la secretaría; y han de utilizarse exclusivamente para dichos fines, así como revelarse únicamente a las personas que se indiquen en el registro. Los datos deben ser justificados, pertinentes y ajustados a la finalidad para la que se los conserva; han de ser exactos y destinarse a la finalidad registrada y deberán protegerse con medidas de seguridad apropiadas.
- iv) Para asegurar el cumplimiento de los principios el Secretario podrá enviar tres tipos de notificación: una notificación de incumplimiento en que se indiquen las medidas que se adoptarán; una notificación de anulación de la inscripción, en parte o en su totalidad (la conservación de datos sin estar registrado oficialmente en la secretaría constituye delito); y una notificación de prohibición de transferencia por la cual se impide transmitir los datos a otro país.
- v) Las personas a las que conciernen los datos (personas naturales y no organizaciones) podrán recurrir a los tribunales en demanda de indemnización por los daños resultantes de la pérdida, la destrucción y la divulgación no autorizada de datos de carácter personal, o por lo daños que hayan sido consecuencia de la inexactitud de los datos. La persona a la que concierne la información podrá asimismo presentar una queja ante el Secretario o recurrir a los tribunales para obtener la rectificación o la supresión de los datos. Podrá asimismo obtener de todo usuario de los datos, mediante solicitud escrita y previo pago de un derecho, copia de la información personal que se conserve sobre ella (excepto en el caso de que esto pueda obstaculizar la prevención o la detección de un delito). En el caso de que no se le otorgue acceso a dicha información en un plazo de 40 días, podrá quejarse ante el Secretario o solicitar una orden judicial a los tribunales.
- vi) En caso de que la persona a la que conciernen los datos considere que se ha violado uno de los principios o alguna disposición de la ley, podrá quejarse ante el Secretario, el cual deberá examinar la queja, siempre que ésta sea fundamentada y se haya presentado sin retraso indebido. El Secretario podrá adoptar un fallo oficioso, presentar una demanda judicial o enviar una notificación al usuario de los datos.
- vii) Todo usuario de los datos podrá revelar información sobre una persona, siempre que se haya inscrito debidamente a su destinatario en el registro de la secretaría, o que se prevea una exención a las disposiciones que prohíben divulgarla (por ejemplo, en los casos en que la ley exija su divulgación o en que ésta se efectúe con el consentimiento de la persona a la que concierne).

- viii) El Secretario rinde cuentas directamente al Parlamento. Lleva el Registro de los usuarios de datos computadorizados y de sus oficinas, lo mantiene a disposición del público y da a conocer información sobre la ley y su aplicación. El Secretario promueve además el respeto de los principios y, cuando procede, alienta la elaboración de códigos de conducta. Examina las quejas respecto de violaciones de los principios o de la ley y, en caso necesario, entabla demandas judiciales o envía notificaciones.
- ix) Existe un Tribunal de Protección de los Datos Computadorizados ante el cual los usuarios de los datos o las oficinas de informática pueden apelar de las decisiones del Secretario en virtud de las cuales éste rechace solicitudes de inscripción, envíe notificaciones de incumplimiento, invalide las inscripciones o envíe notificaciones de prohibición de transferencia. El Tribunal podrá revocar las decisiones del Secretario. Las apelaciones basadas en cuestiones jurídicas podrán presentarse ante el Tribunal Supremo.

3. El 3 de febrero de 1995 se enmendó la ley a fin de constituir en delito el que una persona obtenga información personal si sabe o tiene motivos razonables para creer que la difusión de esa información infringe la Ley de protección de datos; y constituir en delito distinto del anterior el que esa persona venda o ponga a la venta los datos que se ha procurado de esa manera. Esa disposición refuerza la protección de la seguridad de los datos personales prevista en la Ley de 1984 y se introdujo en respuesta a las inquietudes expresadas acerca de las actividades de empresas de investigación que ponían a la venta información personal confidencial (inclusive de orden financiero).

#### Uruguay

[Original: español]  
[11 de junio de 1996]

1. El Estado uruguayo no ha desarrollado hasta el presente una legislación penal especial para la regulación del "delito informático". Sin perjuicio de ello, la doctrina nacional considera que los principios rectores que deben regir la utilización de ficheros personales computarizados se hallan reconocidos y protegidos por la legislación actualmente vigente.

2. En el derecho uruguayo, debemos partir del marco constitucional. Así, corresponde resaltar:

Artículo 7, que establece que los habitantes de la República tienen el derecho a ser protegidos en el goce de -entre otros- su honor, trabajo y propiedad. Nadie puede ser privado de estos derechos sino conforme a las leyes que se establecieron por razones de interés general;

Artículo 19, que dispone que ningún habitante será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe;

Artículo 32, que establece que la propiedad es un derecho inviolable, pero sujeto a lo que dispongan las leyes por razones de interés general.

Nadie podrá ser privado de su derecho de propiedad sino en los casos de necesidad o utilidad públicas establecidos por una ley y recibiendo siempre del Tesoro Nacional una justa y previa compensación;

Artículo 33, que preceptúa que el trabajo intelectual, el derecho del autor, del inventor, serán reconocidos y protegidos por la ley;

Artículo 36, que establece que toda persona puede dedicarse al trabajo, industria, comercio, profesión o cualquier otra actividad lícita; salvo las limitaciones de interés general que establezcan las leyes.

3. Cabe señalar, que además de las citadas normas específicas, el artículo 72 dispone textualmente:

"La enumeración de derechos, deberes y garantías hecha en la Constitución, no excluye los otros que son inherentes a la personalidad humana o se deriven de la forma republicana de gobierno."

4. Asimismo, el artículo 332 establece que:

"Los preceptos de la presente Constitución que reconocen derechos a los individuos, así como los que atribuyen facultades e imponen deberes a las autoridades públicas, no dejarán de aplicarse por falta de la reglamentación respectiva, sino que ésta será suplida, recurriendo a los fundamentos de leyes análogas, a los principios generales de derecho y a las doctrinas generalmente admitidas."

5. Las normas referenciadas dan un marco conceptual firme en la protección de los derechos que se busca tutelar <sup>1</sup>.

6. Cabe señalar, no obstante, que la carencia de normas jurídicas concretas que regulen un tema preciso referido con las bases de datos, podría ser cubierta por la acción de amparo, según lo dispuesto por la Ley N° 16011 de 19 de diciembre de 1988. En efecto, el artículo 10 dispone que:

"Cualquier persona física o jurídica, pública o privada, podrá deducir la acción de amparo contra todo acto, omisión o hecho de las autoridades estatales o paraestatales, así como de particulares que, en forma actual o inminente, a su juicio, lesione, restrinja, altere o amenace, con ilegitimidad manifiesta, cualquiera de sus derechos y libertades reconocidos expresa o implícitamente por la Constitución (art. 72), con excepción de los casos en que proceda la interposición del recurso de "hábeas corpus"." <sup>2</sup>

---

<sup>1</sup>Dr. Mario Barreto Gugelheim, "Protección jurídica de la base de datos", en La Justicia Uruguaya, tomo 108, 1994, págs. 41 a 50.

<sup>2</sup>N. Bergstein, "Derecho penal e informática" en La Justicia Uruguaya, tomo 111, 1995, pág. 43 y ss.

7. En función de la referida ley, podría comparecer el creador intelectual de una base de datos, deduciendo la acción de amparo, contra todo aquel que lesione, altere o amenace el derecho consagrado constitucionalmente en el artículo 33 de la Constitución, o sea su trabajo intelectual. O, podría el inversor ampararse en la mencionada acción para defender su derecho de propiedad (arts. 7, 32 y 36 de la Carta). O, podría el habitante común y corriente, defender su derecho a la intimidad -reconocido implícitamente por el artículo 72 de la Constitución- haciendo cesar la omisión o hecho de las autoridades o de los particulares que a su juicio, lesione, restrinja, altere, o amenace la divulgación, mal uso de destino distinto que se pueda dar a sus datos personales 1/.

8. En las hipótesis de incorporación dolosa a los ficheros de informaciones inexactas sobre personas, las conductas pueden ser consideradas a la luz de lo dispuesto en el artículo 240 del Código Penal uruguayo. Dicha norma dispone:

"El que hiciere un documento privado falso, o alterare uno verdadero, será castigado, cuando hiciere uso de él, con 12 meses de prisión a 5 años de penitenciaría."

9. En aquellos casos en que la falsificación ideológica tengan como sujeto activo a un funcionario público es de eventual aplicación el artículo 238 del Código Penal que dispone:

"El funcionario público que, en el ejercicio de sus funciones diere fe de la ocurrencia de hechos imaginarios, o de hechos reales pero alterando las circunstancias, o con omisión o modificación de las declaraciones prestadas con ese motivo o mediante supresión de tales declaraciones, será castigado con dos a ocho años de penitenciaría."

10. Con relación al debido respeto del principio de finalidad, la revelación de datos personales, sin justa razón, está penalizado a través de los artículos 301 y 302 del Código Penal, que establecen:

"Artículo 301. El que, sin justa causa, revelare el contenido de los documentos que se mencionan en el artículo precedente (públicos o privados), que hubieren llegado a su conocimiento por los medios en él establecidos o en otra forma delictuosa, será castigado con tres meses de prisión a tres años de penitenciaría."

Artículo 302. El que, sin justa causa, revelare secretos que hubieran llegado a su conocimiento, en virtud de su profesión, empleo o comisión, será castigado, cuando el hecho causare perjuicio, con multa de 100 a 2.000 pesos."

-----