NACIONES UNIDAS **E**

Consejo Económico y Social

Distr.
GENERAL

E/CN.4/1995/75
23 de diciembre de 1994

ESPAÑOL
Original: ESPAÑOL/FRANCES/INGLES

COMISION DE DERECHOS HUMANOS
51º período de sesiones
Tema 14 del programa provisional

LOS DERECHOS HUMANOS Y EL PROGRESO CIENTIFICO Y TECNOLOGICO

Medidas adoptadas en relación con los Principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales

Informe del Secretario General preparado de conformidad con la decisión 1993/113 de la Comisión

INDICE

INDICE (continuación)

INTRODUCCION

1. En su decisión 1993/113, de 10 de marzo de 1993, 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, decidió, pedir al Secretario General que informara a la Comisión en su 51º período de sesiones acerca de:

a) la aplicación de los Principios rectores en el seno del sistema de las Naciones Unidas;

b) 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 regional y nacional.

2. De conformidad con esa decisión, el 4 de mayo de 1994 el Secretario General envió a los órganos y organismos especializados de las Naciones Unidas peticiones de información sobre la aplicación de los Principios rectores en las secciones apropiadas del sistema de las Naciones Unidas.

3. En la misma fecha se enviaron solicitudes de información a los Estados, organizaciones intergubernamentales y organizaciones no gubernamentales acerca de la aplicación de los Principios rectores en los planos regional y nacional.

4. Al 1º de diciembre de 1994 se habían recibido respuestas de los siguientes órganos y organismos especializados de las Naciones Unidas: Departamento de Coordinación de Políticas y Desarrollo Sostenible, Fondo de Población de las Naciones Unidas, Universidad de las Naciones Unidas, Corte Internacional de Justicia, Programa Mundial de Alimentos, Organización Internacional del Trabajo, Organización de las Naciones Unidas para la Agricultura y la Alimentación, Organización Mundial de la Salud, Organización Marítima Internacional y Organismo Internacional de Energía Atómica.

5. Han presentado información los Gobiernos de los siguientes países: Alemania, Arabia Saudita, Argentina, Croacia, España, Filipinas, Luxemburgo, Malta, Noruega, Reino Unido de Gran Bretaña e Irlanda del Norte, República Centroafricana, Suecia y Yugoslavia.

6. Además, se recibieron respuestas de las siguientes organizaciones intergubernamentales: Comisión Africana de Derechos Humanos y de los Pueblos, Consejo de Europa e Interpol.

7. No se recibieron respuestas de organizaciones no gubernamentales.

8. El presente informe contiene un resumen de las respuestas sustantivas recibidas. Las respuestas que se reciban posteriormente se publicarán en una adición a este documento.

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

9. De un total de 62 órganos, comisiones regionales, organismos especializados y organizaciones conexas de las Naciones Unidas a los que se enviaron solicitudes, sólo 10 han respondido.

10. El Departamento de Coordinación de Políticas y Desarrollo Sostenible y la Universidad de las Naciones Unidas declararon que no tenían información alguna que presentar sobre la aplicación de los Principios rectores relativos a los ficheros computadorizados de datos personales.

11. La Corte Internacional de Justicia respondió que no podía dar información al respecto porque aún no trabajaba con ficheros computadorizados de datos.

12. La Organización Marítima Internacional (OMI) declaró que suscribía los Principios rectores y tomaría disposiciones para que se aplicaran cuando emprendiera la computadorización de los ficheros de datos personales con fines internos.

13. El Organismo Internacional de Energía Atómica declaró que su Reglamento del Personal y su Estatuto del Personal, así como las políticas y procedimientos aplicables en materia de reunión, mantenimiento y protección de los datos personales manuales y computadorizados se ajustaban a los Principios rectores enunciados en el documento E/CN.4/1990/72.

14. También el Fondo de Población de las Naciones Unidas señaló que se ajustaba a todas las garantías estipuladas en los Principios rectores.

15. La Organización de las Naciones Unidas para la Agricultura y la Alimentación y el Programa Mundial de Alimentos respondieron que el sistema de ficheros computadorizados de datos personales de la FAO se utilizaba principalmente a los efectos de la nómina de sueldos, es decir, para posibilitar la atribución autómatica de las prestaciones relacionadas con la nómina de sueldos. Sólo contenía datos sobre el personal referentes a la nacionalidad, el sexo, la fecha de nacimiento y el estado civil y no incluían datos sobre la raza, la religión, el grupo étnico, etc. Los ficheros se utilizaban exclusivamente con fines internos. Los datos personales no podían comunicarse a terceros sino con el consentimiento del funcionario interesado. Se había establecido un subsistema de seguridad para proteger los ficheros del acceso no autorizado y el abuso. Se declaraba que la FAO aplicaba los principales principios enunciados en la parte A del documento E/CN.4/1990/72.

16. La Organización Internacional del Trabajo (OIT) declaró que su Departamento de Personal conocía la existencia de los Principios rectores de las Naciones Unidas para la reglamentación de los ficheros computadorizados de datos personales desde hacía al menos dos años. Cuando la OIT había decidido utilizar el Sistema integrado de información de gestión (SIIG) de las Naciones Unidas como base para su nuevo Sistema de Información sobre

Personal y Nómina de Sueldos (PERSIS), había investigado los Principios rectores, encontrándolos detallados en el Conditions of Work Digest de la OIT, volumen 10, Nº 2 de 1991.

17. La OIT había sido invitada a participar en octubre de 1993 en una reunión patrocinada por el Consejo de Europa sobre el tema de la protección de los datos personales. La reunión se había centrado en la manera en que las organizaciones internacionales abordaban esa cuestión. Todas las organizaciones que habían participado habían dado a conocer su situación en la materia y sus problemas, lo cual había constituido un segundo estímulo para adelantar en la cuestión.

18. El Departamento de Personal había examinado los Principios rectores y los apoyaba en su totalidad. Sin embargo, el Principio Nº 9 no era aplicable a la OIT .

19. Como su nuevo sistema de personal se basaba en el SIIG, la OIT esperaba que los Principios rectores de la Naciones Unidas ya se hubieran aplicado en el momento de construir el sistema. De su propio examen de los tipos de datos que la OIT mantendría en su versión del SIIG (PERSIS), resultaba con certeza que no se estaban almacenando datos sin cumplir con los Principios rectores.

20. Los problemas de la OIT se plantean en lo que se refiere a la exactitud -especialmente al requisito de que los datos sean completos, dado que es muy costoso revisar continuamente los datos para cerciorarse de que se introduce la nueva información a medida que se dispone de ella. La OIT tiene intención de redactar un "documento circular". Ese documento se enviaría a todos los funcionarios y contendría una lista de los datos importantes que se mantienen sobre ellos. Se les pediría que los verificaran y actualizaran y devolvieran después la lista al Departamento de Personal para su procesamiento. De ese modo se contribuía a cumplir los Principios rectores Nos. 2 y 4.

21. En relación con los ficheros de datos manuales, la OIT también está de acuerdo en que los Principios rectores son aceptables. Antes, la OIT tenía un sistema de dos ficheros de datos personales manuales (A y B). El funcionario no tenía acceso a su fichero B. Esto se está cambiando. No se crean nuevos ficheros B y los viejos están siendo procesados y pronto estarán disponibles para que el funcionario interesado pueda acceder a ellos.

22. Hasta la fecha, no hay en la OIT una persona a la que se haya designado como autoridad encargada de controlar el respeto de esos principios rectores. Si bien la OIT ha elaborado algunos convenios y recomendaciones sobre el tema de los datos personales, aún no ha aprobado su propio conjunto de principios rectores para reglamentar la gestión de los datos personales en el seno de su Organización.

23. Se añadía que el Servicio de Condiciones de Trabajo y Prestaciones Sociales de la OIT había producido otros dos volúmenes del Conditions of Work Digest, que también abordaban aspectos del tratamiento de los ficheros computadorizados de datos.

24. La Organización Mundial de la Salud (OMS) presentó la siguiente información:

Presupuesto y finanzas

25. Todos los ficheros de datos personales en esta esfera son básicamente confidenciales. El Sistema de Información y Finanzas de la OMS funciona sobre la base de "la necesidad de saber".

Gestión del sistema de información

26. La División encargada en la OMS es la División de Gestión del Sistema de Información. Esta División desarrolla algunas aplicaciones de la elaboración electrónica de datos. Sin embargo, desarrolla sistemas de información comunes o institucionales, que son los sistemas destinados a todos los programas y divisiones de la OMS, diferentes de los sistemas únicos utilizados sólo por un elemento de la organización. A este respecto, no hay sistemas de información comunes que contengan ficheros de datos personales distintos de los que figuran en el componente Personal del Sistema de Apoyo Informativo en Administración y Finanzas (AFI) de la División de Presupuesto y Finanzas, y nuestra interpretación de los referidos Principios rectores es que esos datos no se consideran datos personales per se.

27. La División de Gestión del Sistema de Información presta asistencia a los programas y divisiones en la búsqueda de consultores para desarrollar los sistemas únicos que puedan necesitar. No nos consta que los programas y divisiones dispongan de sistemas únicos que contengan datos personales distintos de los incluidos en el mencionado componente Personal.

Personal

28. Los ficheros de datos personales que mantiene la División de Personal se utilizan de conformidad con los Principios rectores a que se hace referencia en el documento de las Naciones Unidas E/CN.4/1990/72.

II. INFORMACION RECIBIDA DE LOS ESTADOS

A. Argentina

[Original: español]
[12 de octubre de 1994]

29. La Convención Nacional Constituyente, que el 25 de mayo de 1994 diera comienzo a sus tareas de reforma de la Constitución Nacional, adoptó un texto el 22 de agosto que entró en vigor el 24 de agosto de 1994. En virtud de las reformas introducidas al texto constitucional, se ha incorporado un nuevo capítulo a la primera parte de la Constitución Nacional denominado "Nuevos derechos y garantías". En este contexto, el artículo 43 consagra a nivel constitucional la acción de amparo, ya vigente a nivel legislativo. El tercer párrafo de la norma mencionada dispone:

"Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística."

De esta forma el hábeas data resulta habilitado expresamente por una norma constitucional.

B. República Centroafricana

[Original: francés]
[13 de julio de 1994]

30. El Gobierno de la República Centroafricana, por su parte, está decidido a poner todas los medios para asegurar el respeto de los Principios rectores en cuestión integrándolos en su legislación y reglamentación nacionales en la materia. En este sentido, todas las administraciones de la República Centroafricana han recibido copia del documento E/CN.4/1990/72 relativo a esos Principios rectores a fin de que puedan tenerlos en cuenta.

C. Croacia

[Original: inglés]
[1º de septiembre de 1994]

31. En la República de Croacia, los datos personales relativos al estado civil (registros de nacimientos, matrimonios y defunciones, registros de ciudadanía y listas del censo electoral) en la mayoría de los lugares están computadorizados; sin embargo, en algunos lugares esos registros todavía son manuales.

32. Corresponde al Ministerio de Administración supervisar los órganos de la administración pública que mantienen los registros estatales de las fichas del censo electoral y los registros de nacimientos, matrimonios y defunciones. Las listas del censo electoral son registros estatales de los ciudadanos con derecho de voto. Los registros de los nacimientos, matrimonios y defunciones comprenden los datos estipulados por la ley para cada uno de esos acontecimientos.

33. Los datos del registro de la ciudadanía (registros de ciudadanía) son mantenidos por órganos de la administración pública -oficinas de administración general-, cuya supervisión incumbe al Ministerio de Administración; sin embargo, la aplicación de las disposiciones sobre la ciudadanía y los registros de ciudadanía cae bajo la jurisdicción del Ministerio del Interior.

34. El Ministerio de Defensa mantiene los registros de los conscriptos de conformidad con la Ley de defensa. La República de Croacia está computadorizando todo el sistema de datos sobre los conscriptos.

35. En la República de Croacia los registros estatales de los derechos electorales y datos personales de los ciudadanos (nacimiento, matrimonio, defunción) no están conectados con un sistema central de computadora. Esos datos sólo se han computadorizado parcialmente en los órganos de la administración pública directamente encargados de mantenerlos; hasta el presente no están conectados entre sí dentro del territorio de la República de Croacia. Su conexión a un sistema central aún tiene que hacerse y dependerá de los fondos disponibles.

36. Los datos personales relativos a los derechos electorales, los nacimientos, matrimonios y defunciones se recopilan, elaboran y utilizan de acuerdo con los Principios rectores para la reglamentación de los ficheros computadorizados de datos personales (E/CN.4/1990/72). La reglamentación de la República de Croacia sobre los procedimientos para mantener registros comprende los siguientes principios rectores:

a) La ley estipula cuáles son los datos que deben recogerse, así como la manera en que han de elaborarse y los fines con que se utilizan (principio de la licitud y lealtad).

b) Una ley separada establece que incumbe a los órganos de la administración pública controlar la exactitud y pertinencia de los datos (principio de exactitud).

c) La ley determina la utilización de los datos registrados estableciendo la finalidad del fichero y las circunstancias en que puede utilizarse. Por ejemplo, la inscripción de una persona en los registros estatales le otorga el derecho a acceder a documentos mediante los cuales pueden probarse acontecimientos como el nacimiento, el matrimonio o las defunciones. Los registros estatales expiden varias clases de documentos (transcripciones, partidas de nacimiento, certificados) mediante los cuales pueden comprobarse los datos personales, según la necesidad y la solicitud hecha (principio de finalidad).

d) Los datos sobre los derechos electorales son accesibles al público durante las elecciones, mientras que los datos personales (nacimiento, matrimonio, defunción) gozan de una protección especial tanto para el acceso a los registros estatales como para la recepción de documentos públicos. Se expiden documentos públicos cuando quien los solicita es una persona que tiene un interés legal en esos documentos, mientras que a los registros estatales pueden acceder las personas a las que conciernen esos datos, los miembros de su familia inmediata y los padres adoptivos o tutores, y sólo si tienen un interés legalmente estipulado, también otras personas (principio de acceso de la persona interesada).

e) Esos registros no contienen datos sobre el origen racial o religioso, el color, la vida sexual, las opiniones políticas, las convicciones religiosas, filosóficas o de otro tipo ni sobre la

participación en una asociación o la aplicación a un sindicato, de manera que no pueden dar origen a ningún tipo de discriminación por los mencionados criterios (principio de no discriminación).

f) La ley no prevé la posibilidad de utilizar los datos para necesidades excepcionales que puedan violar los principios enunciados en los apartados a) a e) supra.

37. Existen disposiciones especiales sobre la seguridad de los datos. Las listas del censo electoral deben conservarse cinco años después de haber sido confirmadas (son confirmadas inmediatamente antes de las elecciones), mientras que los registros de los nacimientos, matrimonios y defunciones se conservan permanentemente.

38. Los datos computadorizados están protegidos de la destrucción y los daños por un proyecto especial para copiarlos y conservarlos en un lugar seguro.

39. Desafortunadamente, a pesar de todas las medidas de seguridad, la República de Croacia no tiene acceso a los registros existentes en los territorios temporalmente ocupados. Se ignora si se han destruido datos personales de los ciudadanos.

40. Las medidas de seguridad del sistema de proceso electrónico de datos para impedir el uso no autorizado de datos personales son las siguientes: un código especial de programa para cada trabajo; puestos de toma de datos para un solo trabajo (sólo pueden acceder a los datos las personas autorizadas); a cada programa sólo se le asigna la estructura de datos correspondiente. Sin embargo, la República de Croacia todavía carece de una reglamentación jurídica sobre la seguridad de los sistemas de información, tanto por lo que se refiere a las medidas de protección de los programas como a las de protección del material. Las medidas de protección de los programas de los sistemas de información requieren programas especiales de protección de datos que garanticen la integridad total de un banco de datos y puedan entrar en funcionamiento inmediatamente en caso de avería del sistema por cualquier razón.

41. El Ministerio de Administración controla la aplicación de la ley relativa a los registros mencionados, es decir, registros de nacimientos, matrimonios y defunciones y listas del censo electoral, mientras que el Ministerio del Interior controla la aplicación de la Ley sustantiva sobre el registro de la ciudadanía.

42. La futura ley de protección de los datos personales está en curso de elaboración y se aprobará a fines de 1994. Establecerá un mecanismo de protección jurídica de todos los grupos estructurados de datos personales (no sólo los computadorizados).

43. La ley propuesta se basa en los principios enunciados en las orientaciones sobre la protección de la vida privada y las corrientes transfronterizas de datos personales de la Organización de Cooperación y Desarrollo Económicos (París, 1980) y el Convenio para la protección de las

personas con relación al tratamiento automatizado de los datos de carácter personal (Consejo de Europa, Estrasburgo, 1981). Como esos principios también forman parte de los Principios rectores para la reglamentación de los ficheros computadorizados de datos personales, la ley propuesta ya contiene los principios enunciados en los párrafos 1 a 9 de los Principios rectores.

44. El objetivo principal de esta ley es estipular la protección jurídica de los datos personales (de los ciudadanos a que se refieren los datos) y, a este respecto, establecer derechos, principios, procedimientos y condiciones para impedir la injerencia no autorizada, irregular e innecesaria (excesiva) en la intimidad de una persona (vida privada) en todas las actividades consistentes en reunir, procesar, almacenar y utilizar datos personales en el ámbito de la vida pública y privada.

D. Alemania

[Original: inglés]
[9 de agosto de 1994]

45. Como muchos otros Estados europeos, la República Federal de Alemania y sus länder federales han promulgado leyes de protección de datos para sus ámbitos de competencia. En 1970, el land federal de Hesse fue la primera entidad en todo el mundo en aprobar una ley de protección de datos; la primera ley federal de protección de datos (Bundesdatenschutzgesetz, BDSG) se promulgó en 1977. En todos los länder hay leyes de protección de datos, algunas que ya son de la segunda o tercera generación. La Ley federal de protección de datos también fue modificada totalmente en 1990.

46. Debido a la división de responsabilidades establecida por la Ley fundamental (Grundgesetz), la Ley federal de protección de datos regula la protección de datos en los órganos federales públicos, así como en los órganos privados, mientras que las leyes de protección de datos de los länder contienen disposiciones que rigen la protección de datos en los órganos públicos del respectivo land. Algunas leyes sectoriales, como el Código de Ley Social, también contienen disposiciones sectoriales en materia de protección de datos.

47. Además, la protección de los datos personales está consagrada en la Constitución de Alemania. El Tribunal Constitucional Federal (Bundesverfassungsgericht), en su decisión sobre la Ley del censo (Volkszählungsgesetz), de 15 de diciembre de 1983, reconoció que los derechos generales de libertad enunciados en el párrafo 1 del artículo 2 de la Ley fundamental, conjuntamente con el párrafo 1 del artículo 1 de la Ley fundamental, incluían el "derecho del individuo a determinar la utilización y divulgación de los datos sobre su persona". Sólo se admiten limitaciones a este derecho en la medida en que prime el interés público y las limitaciones se basen en una ley claramente definida que respete el principio del carácter razonable de la decisión.

48. Podría decirse que la legislación alemana en materia de protección de datos se ha anticipado a los Principios rectores de las Naciones Unidas. Por lo tanto, no ha habido realmente necesidad de promulgarlos en una ley nacional.

49. Las siguientes declaraciones, que se refieren a los Principios rectores de las Naciones Unidas, se basan en la Ley federal de protección de datos. No obstante, las leyes de protección de datos de los länder contienen disposiciones similares.

a) Principio 1 - La Ley federal de protección de datos prohíbe el uso de datos personales a menos que una disposición legal disponga lo contrario o que el sujeto a que se refieren los datos haya dado su consentimiento (apartado 1 del artículo 4).

b) Principio 2 - Toda persona encargada de controlar ficheros tiene la obligación de asegurar la protección de los datos personales adoptando medidas técnicas y de organización (artículo 9 de la Ley federal de protección de datos).

c) Principio 3 - El Tribunal Constitucional Federal, en la mencionada "decisión sobre el censo", ya ha establecido los principios de especificación de la finalidad y utilización con la finalidad especificada. Estos principios se han puesto en práctica en el artículo 14 de la Ley federal de protección de datos, por no nombrar sino una entre otras disposiciones, que contiene una enumeración exhaustiva de los hechos que permiten que, por razones importantes, los datos se utilicen con fines distintos de los especificados (por ejemplo, para un enjuiciamiento criminal, para evitar un peligro).

d) Principio 4 - La Ley federal de protección de datos garantiza el derecho de la persona interesada a acceder a sus datos personales (arts. 19 y 34), así como los derechos de rectificación, supresión y bloqueo (arts. 20 y 35). Con arreglo al artículo 6 de esta Ley, éstos son algunos de los derechos obligatorios de la persona a que se refieren los datos (es decir, derechos que no pueden ser excluidos ni restringidos, incluso con el consentimiento de la persona interesada) (art. 6).

e) Principio 5 - La protección especial de los datos de carácter confidencial se regula predominantemente en leyes sectoriales.

f) Principio 6 - Los criterios enunciados en este principio reflejan bastante fielmente las leyes y la Constitución de Alemania. El derecho del individuo a determinar la utilización que ha de darse a sus datos personales debe compararse constantemente con otros valores protegidos por la Constitución, y a veces valores de jerarquía superior o de igual jerarquía pesarán más que ese derecho.

g) Principio 7 - La Ley federal de protección de datos en su artículo 9 exige que todas las personas encargadas de controlar ficheros tomen medidas técnicas y de organización con el fin de garantizar la integridad de los datos personales. Se anexa a esa disposición una lista de diez puntos que contiene instrucciones precisas.

h) Principio 8 - En los órganos públicos de la Federación y de los länder, la vigilancia del cumplimiento de las disposiciones en materia de protección de datos incumbe al Comisionado federal para la protección de datos y a los comisionados para la protección de datos de los länder. Estos son independientes en el ejercicio de sus funciones y sólo están sujetos a la ley y los estatutos, como los jueces. En el caso de los órganos privados, es decir, principalmente las empresas privadas, las funciones de control incumben a las autoridades de supervisión del Land que están obligadas por instrucciones y a una parte de la estructura administrativa jerárquica. Sin embargo, dichas autoridades son independientes del órgano que es vigilado, como lo estipula el principio 8. En la medida en que la legislación penal general (por ejemplo los artículos 201 y ss. del Código Penal) no se aplica cuando se infringen disposiciones en materia de protección de datos, la Ley federal de protección de datos (arts. 43 y 44) y las leyes de protección de datos de los länder dan a determinados casos carácter de delitos penales o administrativos.

i) Principio 9 - La República Federal apoya y aplica el principio de "garantías comparables" cuando se comunican datos a través de las fronteras. Al interpretar las disposiciones jurídicas pertinentes, el nivel de protección brindado por el país receptor es un factor que debe considerarse al estimar los intereses de la persona a que se refieren los datos.

j) Principio 10 - La Ley federal de protección de datos abarca los ficheros de datos automatizados y manuales y, en la esfera pública, también los registros, es decir, todo documento que tenga fines oficiales. Sin embargo, la Ley federal no se aplica a las personas jurídicas. No obstante, la protección de los datos relativos a las personas jurídicas, que son casi exclusivamente empresas, deriva de la libertad de comercio consagrada en el artículo 12 de la Ley fundamental. En Alemania, la protección de esos datos se inscribe en el marco del derecho comercial en sentido amplio, y no en el de la legislación en materia de protección de datos.

E. Luxemburgo

[Original: francés]
[16 de septiembre de 1994]

50. Desde 1979 Luxemburgo dispone de una ley que reglamenta la utilización de los datos nominativos en el tratamiento informático, modificada posteriormente 1/, que responde a los "Principios rectores para 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.

51. En virtud de la Ley de 19 de noviembre de 1987, Luxemburgo aprobó el Convenio (del Consejo de Europa) para la protección de las personas con relación al tratamiento automatizado de los datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981 (STE 108), único instrumento jurídico internacional obligatorio existente hasta la fecha.

F. Malta

[Original: inglés]
[3 de octubre de 1994]

52. El Gobierno de Malta declaró que todos los puntos abarcados en los Principios rectores (E/CN.4/1990/72) se abordaban en el proyecto de ley amplio que estaba siendo examinado por el Gabinete antes de ser propuesto a la aprobación de la Cámara de Representantes de Malta. Se preveía que esa Ley, conocida como la Ley de prácticas de información, se promulgaría a mediados de 1995.

G. Noruega

[Original inglés]
[23 de agosto de 1994]

53. El Gobierno de Noruega citó en su respuesta la Ley de registro de datos personales, de 9 de junio de 1978 1/, y las Disposiciones reglamentarias promulgadas en cumplimiento de esta Ley el 21 de diciembre de 1978, con las enmiendas introducidas el 10 de marzo de 1981 1/, en que se trataban los Principios rectores enunciados en el documento E/CN.4/1990/72, a saber:

a) el principio 1 quedaba abarcado en la Ley de registro de datos personales, así como mediante la labor del Cuerpo de Inspección de Datos establecido en virtud de dicha Ley;

b) el principio 2 quedaba abarcado en el artículo 8 de la Ley;

1/ Puede consultarse en los archivos de la Secretaría.

c) el principio 3 quedaba abarcado en el párrafo 1 del artículo 11 de la Ley, mediante la labor del Cuerpo de Inspección de Datos y en el párrafo 2 de los artículos 1 y 2 de las Disposiciones reglamentarias promulgadas en virtud de la Ley;

d) el principio 4 quedaba abarcado en el artículo 7 de la Ley;

e) el principio 5 quedaba abarcado en el párrafo 2 del artículo 6 de la Ley;

f) el principio 6 quedaba abarcado en los artículos 9 y 6 de la Ley;

g) el principio 7 quedaba abarcado en los artículos 8 b) y 11 de la Ley, por medio de la labor del Cuerpo de Inspección de Datos;

h) el principio 8 quedaba abarcado en los artículos 2, 5 y 38 de la Ley;

i) el principio 9 quedaba abarcado en el artículo 36 de la Ley y en el capítulo 8 de las Disposiciones reglamentarias;

j) el principio 10 quedaba abarcado en los artículos 1 y 9 de la Ley.

H. Filipinas

[Original: inglés]
[22 de septiembre de 1994]

54. El Gobierno de Filipinas comunicó que había instituido ciertas normas o garantías, como lo demostraban varias leyes y casos de jurisprudencia, que incluían lo siguiente:

a) Disposiciones legislativas

i) La Constitución de Filipinas, en el párrafo 1 de la sección 3 de su artículo III dispone que "será inviolable el secreto de la comunicación y de la correspondencia salvo en virtud de auto legal de un tribunal".

ii) La Ley de la República Nº 4200, conocida como la Ley "que prohíbe las interceptaciones de las comunicaciones", prohíbe y penaliza el uso de dispositivos electrónicos para escuchar comunicaciones con el fin de obtener información sobre una determinada persona.

iii) El Código Civil de Filipinas, en su artículo 32, penaliza a todo funcionario o empleado público y a todo particular que directa o indirectamente obstruya o viole el carácter privado de las comunicaciones y la correspondencia.

iv) Las circulares Nos. 78 y 196 (de la Presidencia) promulgan normas sobre la seguridad de los asuntos reservados en las oficinas públicas, prohibiendo la divulgación de los informes que consten en documentos gubernamentales y exigiendo al organismo gubernamental que inscriba en los documentos reservados la palabra "confidencial" y la siguiente advertencia:

> "La divulgación no autorizada de la información que consta en los documentos adjuntos, aunque no ponga en peligro la seguridad nacional, sería perjudicial para el interés o el prestigio de la nación o cualquier actividad gubernamental o causaría embarazo administrativo o una lesión no justificada a un individuo o aprovecharía a una nación extranjera."

v) El Código Penal Revisado, en su artículo 228, penaliza a todo funcionario público que, sin la debida autoridad, abra o permita que se abran papeles, documentos u objetos cerrados confiados a su custodia. En el artículo 229, el Código sanciona a todo funcionario público que revele cualquier secreto de que tenga conocimiento por razón de su empleo oficial o entregue ilegalmente papeles que tenga a su cargo. El artículo 230 del mismo Código sanciona a todo funcionario público que revele los secretos de un particular de que tenga conocimiento por razón de sus funciones.

b) Jurisprudencia filipina

i) En el caso Valmonte c. Belmonte, Jr. (170 SCRA 256), la Corte Suprema de Filipinas decidió, el 13 de febrero de 1989, que "no puede haber duda alguna de que el derecho a la no injerencia en la vida privada está protegido por la Constitución";

ii) En el caso Orfe c. Mutuc (130 Phil 415, 1968 y 22 SCRA 424), que sentó jurisprudencia, la Corte Suprema de Filipinas, hablando por intermedio del entonces magistrado Juez Fernando, declaró:

> "El derecho a la no injerencia en la vida privada como tal se reconoce independientemente de su identificación con la libertad; en sí mismo merece plena protección de la Constitución. Las palabras del profesor Emerson son particularmente apropiadas: "El concepto de gobierno limitado siempre ha incluido la idea de que los poderes públicos se acaban ante ciertas intrusiones en la vida personal del ciudadano. Efectivamente, esta es una de las distinciones básicas entre gobierno absoluto y gobierno limitado. El control extremo y omnipresente del individuo, en todos los aspectos de su vida, es la característica del Estado absoluto. En cambio, un régimen de gobierno limitado salvaguarda el sector privado, que pertenece al individuo, distinguiéndolo firmemente del sector público, que el Estado puede controlar. La protección de este sector privado -la protección, en otras palabras, de la dignidad e integridad del individuo- se ha

> hecho cada vez más importante con el desarrollo de la sociedad moderna. Todas las fuerzas de la era tecnológica -la industrialización, la urbanización y la organización- intervienen para reducir el ámbito de la vida privada y facilitan la intrusión en él. En términos modernos, la capacidad de mantener y apoyar ese enclave de vida privada es lo que denota la diferencia entre una sociedad democrática y una sociedad totalitaria."

55. Filipinas considera que lo anteriormente expuesto (disposiciones jurídicas y jurisprudencia filipinas) representa garantías suficientes para reforzar el derecho de la persona a la protección de su vida privada. Estas son normas esenciales para reforzar el derecho a la libre determinación, que se prevé en las disposiciones de los Principios rectores de las Naciones Unidas para la reglamentación de los ficheros computadorizados de datos personales. Los Principios rectores, si se adoptan estrictamente como medio para alcanzar los fines de las leyes y jurisprudencia mencionadas, fomentarán y reforzarán la integridad de los derechos básicos de los filipinos cuando éstos se comuniquen con la entera comunidad humana.

56. Por lo tanto, Filipinas no halla razón alguna para no apoyar la versión revisada de los Principios rectores de las Naciones Unidas para la reglamentación de los ficheros computadorizados de datos personales. Por esta razón y conforme a estas consideraciones, la Comisión Filipina de Derechos Humanos ha aprobado los Principios rectores para la utilización y gestión de los ficheros computadorizados de datos personales 1/.

I. Arabia Saudita

[Original: inglés]
[30 de mayo de 1994]

57. El Gobierno de Arabia Saudita presentó las siguientes observaciones:

> "Los "ficheros computadorizados de datos personales" sobre los ciudadanos son de propiedad del Estado. Por consiguiente, los "Principios rectores" en esta materia no son aplicables a Arabia Saudita."

J. España

[Original: español]
[15 de julio de 1994]

58. El Gobierno de España presentó copias de las siguientes leyes:

a) Ley Orgánica Nº 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (B.O.E. 31 de octubre de 1992) 1/;

b) Real Decreto Nº 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos 1/;

c) Real Decreto Nº 1332/1994, de 20 de junio, por el que se desarrolla determinados aspectos de la Ley Orgánica Nº 5/1992, de 29 de octubre, de regulación de tratamiento automatizado de los datos de carácter personal 1/.

K. Suecia

[Original: inglés]
[25 de agosto de 1994]

59. El Gobierno declaró que Suecia tenía una larga tradición de protección de la vida privada con respecto a los ficheros de datos computadorizados. La Ley de protección de los datos computadorizados que promulgó Suecia en 1973 fue la primera legislación nacional de este tipo en el mundo (se adjuntó copia de su texto, con las modificaciones que entraron en vigor el 1º de julio de 1992) 1/. En 1982 Suecia fue el primer país que ratificó el Convenio del Consejo de Europa para la Protección de las Personas con relación al Tratamiento Automatizado de los Datos de Carácter Personal (ETS 108).

60. La Ley de 1973 reglamenta la utilización de los ficheros de datos personales. Los "ficheros de datos personales" son los expedientes, las listas y otros registros en que se utiliza el tratamiento automatizado de datos y que contienen datos personales sobre una persona física identificable. La Ley no abarca los ficheros manuales.

61. La ley estipula que debe haber una autoridad responsable de todos los ficheros automatizados que contengan datos personales. Esta será la persona natural, el organismo o la persona jurídica encargados de las decisiones relativas a la información que figura en el fichero que podrán, cuando proceda, modificarlo o presentar su contenido de manera inteligible.

62. Conforme a las disposiciones de la Ley de protección de datos computadorizados de 1973, toda persona que desee crear un fichero automatizado de datos personales está obligada a notificar al Organismo de Protección de Datos Computadorizados de Suecia (Datainspektionen) y a solicitar una licencia. Esta licencia otorga al controlador del expediente el derecho a crear y manejar una cantidad ilimitada de ficheros relacionados con la autorización concreta que haya obtenido.

63. Además del requisito de licencia, la Ley de 1973 contiene disposiciones relativas a ciertos ficheros de datos personales delicados, para mantener los cuales se requiere un permiso especial del Organismo. Entre las categorías especiales de datos personales, para las cuales se prevén garantías extraordinarias, figuran los datos relacionados con condenas judiciales o detenciones basadas en decisiones administrativas, los relativos a la salud o la vida sexual, y los que revelen el origen racial, las opiniones políticas y las convicciones religiosas o de otro tipo. Se necesita igualmente

autorización para mantener ficheros cuyo contenido suponga juicios sobre las personas. Se requiere asimismo permiso para crear expedientes con información sobre personas que no tengan una relación concreta con el controlador. En caso de que exista esta relación concreta entre el controlador del expediente y la persona registrada, dichos ficheros estarán exentos del requisito de autorización. Entre estos expedientes privilegiados figuran los que contienen información sobre clientes, miembros de organizaciones, etc., o empleados. Se requiere, por último, permiso del Organismo para la cotejación de ficheros, esto es, la transferencia de datos de un expediente a otro y el tratamiento simultáneo de varios archivos con datos personales.

64. El Organismo de Protección de los Datos Computadorizados concederá la autorización únicamente cuando considere que el tratamiento automatizado del fichero que contiene datos personales no supondrá una violación indebida del derecho de la persona registrada a la protección de su vida privada.

65. Para transferir un expediente a otro país se requiere también el permiso del Organismo, excepto en el caso de que dicha transferencia se efectúe hacia un país que haya firmado el Convenio del Consejo de Europa para la Protección de las Personas con relación al Tratamiento Automatizado de los Datos de carácter personal de 1981. Dicha autorización se concederá únicamente cuando el Organismo considere que la transferencia no constituye una violación del derecho de la persona registrada a la protección de su vida privada.

66. Hay asimismo algunas disposiciones de carácter general sobre el almacenamiento en archivos de los ficheros que contienen datos personales.

67. El Organismo de Protección de los Datos Computadorizados supervisa a los controladores de los ficheros, así como la aplicación general de la Ley.

68. En caso de que en el tratamiento automatizado de los datos de carácter personal se haya violado el derecho a la protección de la vida privada, o de que se prevea que así ocurrirá, el Organismo podrá fijar condiciones específicas para dicho tratamiento; cuando no sea posible examinar de ninguna otra manera el contenido del expediente, el Organismo prohibirá el tratamiento del expediente al controlador, o revocará la autorización en caso de que ya la haya concedido.

69. Las decisiones del Organismo de Protección de los Datos Computadorizados están sujetas a revisión por el Gobierno.

70. En 1993, una comisión presentó una propuesta relativa a una nueva Ley de protección de los datos computadorizados. Dada la incertidumbre respecto del alcance de las medidas futuras de protección de los datos en Europa, por el momento el Gobierno ha decidido no proponer la promulgación de una nueva Ley.

71. En tanto, el 14 de abril de 1994 el Gobierno presentó al Parlamento un proyecto de enmienda de la Ley de protección de los datos computadorizados de 1973, a fin de simplificar la normativa de las autorizaciones especiales y

aumentar las facultades de supervisión del Organismo de Protección de los Datos Computadorizados. El proyecto contiene, entre otras cosas, la propuesta de que en lo sucesivo la instancia de apelación de las decisiones del Organismo de Protección de los Datos sean los tribunales y no, como hasta ahora, el Gobierno. Se ha propuesto que las modificaciones a la Ley de protección de los datos entren en vigor el 1º de enero de 1995.

L. Reino Unido de Gran Bretaña e Irlanda del Norte

[Original: inglés]
[15 de septiembre de 1994]

72. El Gobierno ha manifestado que 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.

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

a) 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 objeto de los datos; los casos en que la ley obliga al usuario a hacer públicos los datos (por ejemplo, los del Registro electoral); y aquéllos en que los datos se conservan por razones de seguridad nacional (según lo establezcan los ministerios pertinentes).

b) 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 de ultramar a los que puedan transferirse.

c) 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; que deben conservarse únicamente para los fines lícitos que

se hayan indicado en el registro de la secretaría; y que 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 precisos, y en caso necesario se deberá actualizarlos; no se podrá conservarlos por un período que exceda el tiempo necesario para alcanzar la finalidad con que se han registrado; y deberán protegerse con medidas de seguridad apropiadas.

d) 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 constituyen delito); y una notificación de prohibición de transferencia por la cual se impide transmitir los datos a un país de ultramar.

e) 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.

f) 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.

g) 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.

h) 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.

i) 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.

74. Se adjuntaron copias de algunos principios rectores elaborados por el Secretario de Protección de los Datos Computadorizados, en los que se explica en mayor detalle la Ley de 1984 1/.

M. Yugoslavia

[Original: inglés]
[14 de noviembre de 1994]

75. El Gobierno de la República Federativa de Yugoslavia presentó la siguiente información.

76. En su octava sesión, celebrada el 2 de octubre de 1990, los dos Consejos de la Asamblea Federativa adoptaron la Ley sobre ratificación del Convenio para la Protección de las Personas con relación al Tratamiento Automatizado de los Datos de Carácter Personal. De este modo, la República Federativa de Yugoslavia contrajo la obligación de reglamentar en su legislación interna la protección de los datos de carácter personal que se conserven en ficheros computadorizados.

77. Basándose en el párrafo 4 del artículo 33 de la Constitución de la República Federativa de Yugoslavia, conforme al cual la legislación federal reglamenta el acopio, el tratamiento, la utilización y la protección de los datos de carácter personal, el Ministerio Federal de Derechos Humanos y de las Minorías y el Instituto Federal de Informática prepararon un proyecto de ley sobre la protección de los datos computadorizados de carácter personal, que fue aprobado el 21 de abril de 1994 por los órganos del Gobierno Federativo en su 164ª reunión. Sus disposiciones son compatibles con las del Convenio señalado. El proyecto de ley se ha presentado para su examen a la Asamblea Federativa.

78. El proyecto de ley sobre la protección de los datos computadorizados de carácter personal incorpora todos los principios rectores, excepto los que se refieren a los ficheros de las organizaciones internacionales gubernamentales que contienen datos personales.

Se enumeran a continuación los principios rectores y los artículos del proyecto de ley que los incorporan:

a) Principio de la licitud y lealtad; artículos 1 y 2 del proyecto de ley;

b) Principio de exactitud; artículo 12 del proyecto de ley;

c) Principio de finalidad; artículo 2 del proyecto de ley;

d) Principio de acceso de la persona interesada; artículos 11 y 12 del proyecto de ley;

e) Principio de no discriminación; artículo 20 del proyecto de ley;

f) Facultad de establecer excepciones; artículo 13 del proyecto de ley;

g) Principio de seguridad; artículo 8 del proyecto de ley;

h) Control y sanciones; artículos 21 a 25 y 27 del proyecto de ley;

i) Flujo de datos a través de las fronteras; artículo 26 del proyecto de ley.

III. INFORMACION PRESENTADA POR ORGANIZACIONES INTERGUBERNAMENTALES

A. Consejo de Europa

[Original: inglés]
[12 de agosto de 1994]

79. La Comisión Europea de Derechos Humanos del Consejo de Europa señaló que, de conformidad con el artículo 8 del Convenio Europeo de Derechos Humanos, había recibido la solicitud de ocuparse de la utilización de ficheros de datos personales por diferentes autoridades nacionales. Sin embargo, había muy pocas decisiones relativas a ficheros de datos computadorizados. Se adjuntó la decisión Nº 10473/83 de la Comisión, de fecha 11 de diciembre de 1985 (Tom Lundvall c. Suecia) 1/.

B. Interpol

[Original: francés]
[9 de agosto de 1994]

80. La Organización Internacional de Policía Criminal (Interpol) presentó la siguiente información.

OBSERVANCIA POR LA OIPC/INTERPOL DE LOS PRINCIPIOS RECTORES SOBRE LA UTILIZACION DE FICHEROS COMPUTADORIZADOS DE DATOS PERSONALES

Introducción

El principio de la protección de los datos que conserva la Secretaría General de la OIPC/Interpol se refleja en un tratado (el Acuerdo relativo a la Sede y el Canje de Notas de 1982) entre el Gobierno de la República Francesa y la Organización, así como en un reglamento interno, el Reglamento relativo a la cooperación policial internacional y al control interno de los ficheros de la OIPC/Interpol. Se adjunta el texto de estos tres instrumentos jurídicos, así como el del Reglamento de la Organización 1/, que constituyen el marco jurídico para la aplicación de los principios rectores enunciados en el documento E/CN.4/1990/72, que se han integrado en el régimen jurídico de la Organización.

1. Excepción a la legislación nacional del país sede

El Acuerdo relativo a la Sede, de 1982, que entró en vigor el 14 de febrero de 1984, declara inviolables la sede, los archivos y la correspondencia de la Organización (arts. 4, 7 y 9). Dispone asimismo que "los ficheros (de la Interpol) están sujetos al control interno de la Organización, conforme a las normas generales establecidas en virtud del canje de notas con el Gobierno de la República Francesa" (art. 8).

Este canje de notas somete los ficheros que conserva la Secretaría General de la OIPC/Interpol al control de una comisión independiente, cuya creación es de competencia de la Organización. Su composición, su funcionamiento y la normativa que rige los controles que debe efectuar están definidos con énfasis y claridad en las disposiciones del señalado canje de notas.

En consecuencia, los ficheros de la OIPC/Interpol están sujetos a las disposiciones del Acuerdo relativo a la Sede y exentos del control de la Comisión Nacional de Informática y Libertades Ciudadanas (Commission Nationale de l'Informatique et des Libertés (CNIL)), órgano francés encargado de velar por el respeto de la Ley de 1978 sobre la protección de los datos computadorizados en Francia.

2. Designación de la autoridad estatutariamente competente para velar por la correcta aplicación de los principios rectores

La Organización ha cumplido el compromiso que contrajo en el canje de notas, mediante la adopción del Reglamento relativo a la cooperación policial internacional y al control interno de los ficheros de la OIPC/Interpol. Dicho Reglamento, denominado en adelante Reglamento de cooperación, es la normativa conforme a la cual la Organización creó la Comisión de control interno de los ficheros de la OIPC/Interpol.

Este órgano fiscalizador es una dependencia subsidiaria de la Organización, que le ha dado el carácter de "autoridad estatutariamente competente para velar por la aplicación" de las normas adoptadas por la OIPC/Interpol en materia de protección de los datos personales.

La creación de esta Comisión, cuya composición y funcionamiento se describen en los artículos 15 y ss. del Reglamento de Cooperación, se atiene por tanto a las recomendaciones formuladas en el punto B del documento E/CN.4/1990/72, con respecto a las organizaciones internacionales.

Cabe señalar que el magistrado Sr. Louis Joinet, Relator Especial de la Comisión de Derechos Humanos de las Naciones Unidas, que era Consejero Técnico del Gabinete del Primer Ministro francés en el período en que la OIPC/Interpol y Francia negociaron el Acuerdo relativo a la Sede, señaló que este órgano podía servir como modelo para las instituciones de control de los ficheros de numerosas organizaciones internacionales que tienen su sede en Francia.

3. Contenido de los principios rectores adoptados por la OIPC/Interpol

La OIPC/Interpol ha incorporado del siguiente modo en su régimen jurídico interno "los Principios rectores sobre la utilización de los ficheros de las organizaciones internacionales gubernamentales que contienen datos personales".

Principio de la licitud y la lealtad (Nº 1)

Este Principio está consagrado en el Reglamento de la OIPC/Interpol, especialmente en el artículo 2, que enuncia las tareas principales de la Organización, delimita su ámbito de competencia y hace alusión expresa al espíritu de la Declaración Universal de Derechos Humanos y al respeto de las leyes de los Estados que se relacionan con la Interpol a través de las Oficinas Centrales Nacionales que forman parte de sus instituciones nacionales.

De conformidad con este principio, el apartado 2) del artículo 1 del Reglamento de Cooperación precisa que su finalidad es "proteger contra toda utilización impropia las informaciones policiales procesadas y comunicadas dentro del sistema de cooperación policial internacional establecido por la OIPC/Interpol, a fin de prevenir, especialmente, todo atentado contra los derechos de las personas".

El respeto del principio de la licitud supone, a la vez, el de las dos normas jurídicas fundamentales del sistema de la Interpol. Estas figuran en el apartado 3) del artículo 5 y en el apartado 3) del artículo 3 del Reglamento de Cooperación.

El apartado 3) del artículo 5 de dicho Reglamento dispone que "la Secretaría General es únicamente depositaria de las informaciones policiales que le comunican las autoridades policiales nacionales. Se desprende de esta disposición que las autoridades policiales nacionales (que son la fuente principal de información de la Interpol) deben verificar que al comunicar la información que deseen transmitir a la Organización lo hacen de manera legítima y legal.

Una vez comunicada la información al Secretario General, su tratamiento, su registro y su comunicación quedan sujetos a las normas propias de la Organización. El apartado 3) del artículo 3 del Reglamento de Cooperación dispone que "el procesamiento de informaciones policiales por la Secretaría General... no está sujeto a ninguna legislación nacional. Se efectúa conforme a las disposiciones del presente Reglamento y a las de los acuerdos concertados con el Estado sede".

Principio de exactitud (Nº 2)

Varias disposiciones del Reglamento de Cooperación consagran este Principio como obligación de la Secretaría General de la Organización y del país de origen de la información que se comunique a la Secretaría General. Se trata del apartado 2) del artículo 5, el apartado 2) del artículo 6, el apartado 3) del artículo 6, el apartado 5) del artículo 7 y el apartado 4) del artículo 9 del Reglamento de Cooperación.

La obligación de mantener información exacta supone no sólo la de actualizarla sino también la de depurarla. El apartado 5) del artículo 5 del Reglamento de Cooperación dispone que "la destrucción por la Secretaría General de informaciones policiales consideradas obsoletas con arreglo a ciertos criterios generales se determinará mediante un reglamento particular aprobado por la Asamblea General". Este Reglamento se adoptó en 1987.

Principio de finalidad (Nº 3)

De conformidad con el apartado 4) del artículo 3 del Reglamento de Cooperación, "el tratamiento de informaciones policiales por la Secretaría General se efectúa con objeto de prevenir y reprimir las infracciones penales de derecho común en el sentido del párrafo b) del artículo 2 del Estatuto, y que no sean objeto del artículo 3 del Estatuto, así como a efectos de las investigaciones relativas a ellas, de la búsqueda de personas desaparecidas y de la identificación de cadáveres".

Este Principio está consagrado también en el párrafo b) del artículo 22 del Reglamento de Cooperación, que asigna a la Comisión de Control Interno de los Ficheros la responsabilidad de velar por que la información que conserve la Secretaría General sea registrada y procesada con finalidades determinadas.

Los datos de carácter personal que recoge y procesa la Secretaría General se utilizan, en consecuencia, con fines policiales. Por esta razón y conforme al Principio Nº 6 que prevé la facultad de establecer excepciones, la Organización ha establecido una excepción a la norma que dispone que la información debe ser objeto de una medida de publicidad o ponerse en conocimiento de la persona interesada antes de que sea utilizada o comunicada a las autoridades policiales.

Principio de acceso de la persona interesada (Nº 4)

Este Principio está consagrado en el artículo 23 del Reglamento de Cooperación, que prevé la posibilidad de que la persona eventualmente interesada solicite a la Comisión de Control que verifique la información que le concierne. Una vez efectuada esta verificación, la Comisión lo notificará de inmediato al solicitante, sin revelar el contenido de la información que se conserva. Se trata, pues, de un derecho de acceso indirecto de las personas a los ficheros policiales de la Organización.

Este carácter indirecto del acceso a los ficheros policiales se justifica por la diferencia de finalidad entre un fichero nacional y un fichero internacional de policía administrado por la Organización depositaria de la información que se le facilita. No corresponde a la Organización determinar si la divulgación de una información policial puede atentar contra el orden público de un Estado miembro o contra la colaboración entre dos o más Estados miembros.

Gracias a este sistema establecido por la Organización numerosas personas que no gozan del derecho de acceso, siquiera indirecto, a los ficheros policiales de su país pueden ejercerlo en el plano internacional.

Principio de no discriminación (Nº 5)

A reserva de la necesidad de identificar a personas buscadas en el marco de pesquisas internacionales y de describir los hechos constitutivos de infracciones penales de derecho común, este Principio está consagrado en el artículo 3 del Estatuto de la Organización, que prohíbe a ésta intervenir en cuestiones de carácter político, militar, religioso o racial.

Facultad de derogación (Nº 6)

Las normas adoptadas por la Organización en materia de protección de los datos corresponden a los Principios que figuran en el documento E/CN.4/1990/72 de las Naciones Unidas, a reserva de las excepciones o adaptaciones justificadas por la naturaleza concreta de las actividades de la OIPC/Interpol, adaptaciones que son autorizadas por el punto B) y por el

Principio Nº 6 del punto A) del documento señalado, que prevén "la facultad de establecer excepciones" a algunos principios para proteger la seguridad, el orden público y los derechos y libertades de los demás.

Por otra parte, la Organización cumple una misión humanitaria al encargarse de la búsqueda de personas desaparecidas y de la identificación de cadáveres. La labor de la Organización en esta esfera no es sino la extensión al plano internacional de la misión humanitaria de cada policía nacional.

Por último, conforme a los apartados 3) y 4) del artículo 3 del Reglamento de Cooperación, todos los datos policiales podrán utilizarse también para la gestión interna, así como para la investigación y la divulgación científicas y para cualquier otra finalidad legítima, con la condición de que se lo haga de manera que resulte imposible identificar a las personas eventualmente interesadas.

Principio de seguridad (Nº 7)

El apartado 2) del artículo 1 (mencionado supra) del Reglamento de Cooperación, que prohíbe toda utilización impropia de información policial, y el artículo 4 del mismo Reglamento, consagran este principio de seguridad. El artículo 4 del Reglamento de Cooperación dispone que "la Secretaría General toma las medidas necesarias para salvaguardar el carácter reservado y garantizar la seguridad de la información policial, así como para impedir que ésta sea procesada o comunicada de manera ilícita o impropia". Este artículo dispone asimismo que "el personal de la Secretaría General está obligado a respetar el secreto profesional". Los miembros de la Comisión de Control también están sujetos a dicha obligación, de conformidad con el artículo 19 del Reglamento.

Además, la Secretaría General ha elaborado complejos mecanismos de protección de los datos computadorizados y procedimientos administrativos rigurosos, a fin de impedir toda alteración o acceso no autorizado.

Control y sanciones (Nº 8)

Conforme al artículo 22 del Reglamento de Cooperación, la responsabilidad principal de la Comisión de control interno de los ficheros de la OIPC/Interpol es velar por que la información de carácter personal contenida en los ficheros de la Interpol sea recogida, procesada y conservada con arreglo a los principios que se enuncian en el presente documento.

Para ejercer sus funciones de control general la Comisión dispone de acceso directo a todos los ficheros de la Organización y tiene el derecho de efectuar investigaciones, que puede invocar ante la Secretaría General. Además, podrá consultar al Comité Ejecutivo de la Organización y a las

autoridades policiales del país de origen de la información sujeta a su verificación. En el cumplimiento de su misión de control general, la Comisión examina expedientes policiales que selecciona al azar para efectuar las verificaciones, a las que puede proceder por petición de un particular o de oficio.

Conforme al apartado 3) del artículo 24 del Reglamento de Cooperación la Comisión podrá solicitar que se modifique o se destruya la información que conserva la Secretaría General. El resultado de sus labores de fiscalización y de sus investigaciones se notifica al Comité Ejecutivo de la Organización, para que los órganos competentes introduzcan las modificaciones necesarias, con arreglo al artículo 25 del Reglamento de Cooperación.

Flujo de datos a través de las fronteras (Nº 9)

La circulación de información entre la Secretaría General y las autoridades policiales de los Estados miembros o las demás entidades habilitadas se rige por los Principios que se enuncian supra y por diversas disposiciones concretas del Reglamento de Cooperación (arts. 5, 7, 8 y 9), que establecen condiciones estrictas para la comunicación de información policial a las autoridades pertinentes o a otras entidades nacionales o internacionales.

Campo de aplicación (Nº 10)

La Secretaría General de la Organización mantiene dos clases de ficheros sobre personas: los ficheros policiales y los administrativos.

Los principios que se exponen supra se aplican a los ficheros policiales manuales o automatizados (Criminal Information System).

Los ficheros administrativos comprenden los que corresponden al personal de la Organización y a las personas que tienen contacto oficial con ella. Estos expedientes no están sujetos a las mismas normas jurídicas que rigen para los ficheros policiales. No obstante, con respecto a ellos la Organización observa igualmente los Principios rectores que se enuncian en el documento E/CN.4/1990/72, sin perjuicio de que pueda adaptarlos para atender al buen funcionamiento de la Organización y al cumplimiento de la labor de verificación que realiza la Comisión de Control Interno de los Ficheros de la OIPC/Interpol.

En resumen, las informaciones que conserva la Secretaría General sobre el personal, los subcontratistas y los visitantes de la Organización se recogen de manera lícita, a través de declaraciones de los propios interesados u obteniéndose de fuentes públicas (registros civiles o comerciales, autoridades nacionales, órganos internacionales, etc.), teniendo presente la

actualización que efectúan los interesados o los servicios competentes de la Secretaría General, y previa verificación de su exactitud. Estos ficheros administrativos se destinan a fines de gestión, contabilidad, seguridad social, administración y a toda otra finalidad compatible con los objetivos de la Organización que se enuncian en su Estatuto y en sus reglamentos internos.

El Estatuto y el Reglamento del personal incorporan los principios de la función pública internacional, adaptando algunos de los que figuran en el documento E/CN.4/1990/72. Dichas normativas autorizan al personal a tener acceso directo a su fichero. Los datos relativos al personal son confidenciales y se utilizan únicamente a efectos de gestión y de administración. Está prohibido todo acceso a ellos sin autorización o que no se justifique por las necesidades del servicio. La violación de estos principios puede dar lugar a procedimientos disciplinarios, sometidos al control del Tribunal Administrativo de la OIT.

Anexo

PRINCIPIOS RECTORES SOBRE LA UTILIZACION DE FICHEROS COMPUTADORIZADOS DE DATOS PERSONALES

Las modalidades de aplicación de los reglamentos relativos a los ficheros computadorizados de datos personales se dejan a la libre iniciativa de cada Estado con sujeción a las siguientes orientaciones:

A. Principios relativos a las garantías mínimas que deberían preverse en la legislación nacional

1. Principio de la licitud y lealtad

Las informaciones relativas a las personas no se deberían recoger ni elaborar con procedimientos desleales o ilícitos, ni utilizarse con fines contrarios a los propósitos y principios de la Carta de las Naciones Unidas.

2. Principio de exactitud

Las personas encargadas de la creación de un fichero o de su funcionamiento deberían tener la obligación de verificar la exactitud y pertinencia de los datos registrados y cerciorarse de que siguen siendo lo más completos posibles a fin de evitar los errores por omisión y de que se actualicen, periódicamente o cuando se utilicen las informaciones contenidas en un expediente, mientras se estén procesando.

3. Principio de finalidad

La finalidad de un fichero y su utilizacion en función de esta finalidad deberían especificarse y justificarse y, en el momento de su creación, ser objeto de una medida de publicidad o ponerse en conocimiento de la persona interesada a fin de que ulteriormente sea posible asegurarse de que:

a) todos los datos personales reunidos y registrados siguen siendo pertinentes a la finalidad perseguida;

b) ninguno de esos datos personales es utilizado o revelado sin el consentimiento de la persona interesada, con un propósito incompatible con el que se haya especificado;

c) el período de conservación de los datos personales no excede del necesario para alcanzar la finalidad con que se han registrado.

4. Principio de acceso de la persona interesada

Toda persona que demuestre su identidad tiene derecho a saber si se está procesando información que le concierne, a conseguir una comunicación intelegible de ella sin demoras o gastos excesivos, a obtener las rectificaciones o supresiones adecuadas cuando los registros sean ilícitos, injustificados o inexactos y, cuando esta información sea comunicada, a

conocer los destinatarios. Debería preverse una vía de recurso, en su caso, ante la autoridad encargada del control de conformidad con el principio 8 infra. En caso de rectificación, el costo debería sufragarlo el responsable del fichero. Es conveniente que las disposiciones de este principio se apliquen a todas las personas, cualquiera que sea su nacionalidad o su residencia.

5. Principio de no discriminación

A reserva de las excepciones previstas con criterio limitativo en el Principio 6, no deberían registrarse datos que puedan originar una discriminación ilícita o arbitraria, en particular información sobre el origen racial o étnico, color, vida sexual, opiniones políticas, convicciones religiosas, filosóficas o de otro tipo o sobre, la participación en una asociación o la afiliación a un sindicato.

6. Facultad de establecer excepciones

Sólo pueden autorizarse excepciones a los Principios 1 a 4 si son necesarias para proteger la seguridad nacional, el orden público, la salud o la moral pública y, en particular, los derechos y libertades de los demás, especialmente de personas perseguidas (cláusula humanitaria), a reserva de que estas excepciones se hayan previsto expresamente por la ley o por una reglamentación equivalente, adoptada de conformidad con el sistema jurídico nacional, en que se definan expresamente los límites y se establezcan las garantías apropiadas.

Las excepciones al Principio 5, relativo a la prohibición de discriminación, deberían estar sujetas a las mismas garantías que las previstas para las excepciones a los Principios 1 a 4 y sólo podrían autorizarse dentro de los límites previstos por la Carta Internacional de Derechos Humanos y demás instrumentos pertinentes en materia de protección de los derechos y de lucha contra la discriminación.

7. Principio de seguridad

Se deberían adoptar medidas apropiadas para proteger los ficheros contra los riesgos naturales, como la pérdida accidental o la destrucción por siniestro, y contra los riesgos humanos, como el acceso sin autorización, la utilización encubierta de datos o la contaminación por virus informático.

8. Control y sanciones

Cada legislación debería designar a la autoridad que, de conformidad con el sistema jurídico interno, se encarga de controlar el respeto de los Principios anteriormente enunciados. Dicha autoridad debería ofrecer garantías de imparcialidad, de independencia con respecto a las personas u organismos responsables del procesamiento de los datos o de su aplicación, y de competencia técnica. En caso de violación de las disposiciones de la

legislación interna promulgada en virtud de los Principios anteriormente enunciados, deberían preverse sanciones penales y de otro tipo así como recursos individuales apropiados.

9. Flujo de datos a través de las fronteras

Cuando la legislación de dos o más países afectados por un flujo de datos a través de sus fronteras ofrezca garantías comparables de protección de la vida privada, la información debe poder circular tan libremente como en el interior de cada uno de los territorios respectivos. Cuando no haya garantías comparables, no se podrán imponer limitaciones injustificadas a dicha circulación, y sólo en la medida en que así lo exija la protección de la vida privada.

10. Campo de aplicación

Los presentes Principios deberían aplicarse en primer lugar a todos los ficheros computadorizados, tanto públicos como privados y, por extensión facultativa y a reserva de las adaptaciones pertinentes, a los ficheros manuales. Podrían tomarse disposiciones particulares, igualmente facultativas, para extender la aplicación total o parcial de estos Principios a los ficheros de las personas jurídicas, en particular cuando contengan en parte información sobre personas físicas.

B. Aplicación de los Principios rectores a los ficheros de las organizaciones internacionales gubernamentales que contienen datos personales

Los presentes Principios rectores deberían ser aplicables a los ficheros de las organizaciones internacionales gubernamentales de datos personales, a reserva de las adaptaciones necesarias para tener en cuenta las posibles diferencias que puedan existir entre los ficheros con fines internos, como los relativos a la gestión del personal, y los ficheros con fines externos relativos a terceras personas relacionadas con la organización.

Cada organización debería designar a la autoridad que estatutariamente es competente para velar por la correcta aplicación de estos Principios rectores.

Cláusula humanitaria: debería preverse de manera específica una excepción a estos Principios cuando el fichero tenga por finalidad proteger los derechos humanos y las libertades fundamentales de la persona de que se trate, o prestar asistencia humanitaria.

La legislación nacional debería contener una excepción análoga para las organizaciones internacionales gubernamentales en cuyo convenio sobre la sede no se hubiera excluido la aplicación de dicha legislación nacional, así como para las organizaciones internacionales no gubernamentales a que sea aplicable dicha legislación.
