
Principios rectores para la reglamentación de los ficheros computadorizados de datos personales, A.G. res. 44/132, 44 U.N. GAOR Supp. (No. 49) p. 211, ONU Doc. A/44/49 (1989).

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 posible 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 utilización 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 inteligible 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 humanos 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.