La Confidencialitat i el Secret Professional

Document elaborat per la Comissió de Confidencialitat i Secret Professional

COL·LEGI OFICIAL
DE DIPLOMATS
EN TREBALL SOCIAL I
ASSISTENTS SOCIALS
DE CATALUNYA

LA CONFIDENCIALITAT I EL SECRET PROFESSIONAL
COMPONENTS DE LA COMISSIÓ I COL·LABORADORS

Aquest document ha estat treballat i elaborat per:

Esther Mallans Riera (Col. N. 9), Montserrat Colomer Salmons (Col. N. 66), Maria Llucià Figueres (Col. M. 361), Pilar Porcel Omar (Col. N. 383), Anna Martínez Martín (Col. N. 575); Mei Cerdà Herrero (Col. N. 1748), Àgata Gelpí Lluch (Col. 1769) i Maria del Mar Peña Ocaña (Col. N. 1891).
També s'ha comptat amb la col·laboració de Soledat Colomé Coca, assessora jurídica de l'Àrea de Política Social de l'Ajuntament de l'Hospitalet de Llobregat, Rosa Barenys Martorell (Col. N. 324) en aportació de documents legislatius i Rosa Ma. Casas Terés (Col. 2796) en el suport administratiu.

TREBALL IMPRÈS EL MAIG DEL 2000

Edita: Col·legi Oficial de Diplomats en Treball Social i Assistents Socials de Catalunya
C/ Portaferrissa, 18 1r 1a
08002- Barcelona
Telèfon: 93 318 55 93

Producció: CatPress, serveis de comunicació
Ctra. de Cardona, 2 2n 2a
08240- Manresa
Telèfon 93 872 14 22

Índex

1. Presentació

El mes d'octubre de 1997 es va realitzar a Barcelona la I Jornada de SSAP amb el títol "Dilemes ètics en la nostra pràctica: entre el control i la inserció", organitzada pels Col.legis de Psicòlegs, Educadors i Educadores Socials i Diplomats en Treball Social i Assistents Socials de Catalunya.

La Jornada fou un èxit de participació, de debat, de reflexió, i a l'hora de la cloenda vaig anunciar la creació d'una Comissió que estudiés la confidencialitat i el secret professional, els seus límits i la legislació vigent al respecte, i que aportés una valoració i unes recomanacions tant per als professionals com per a les administracions, entitats, associacions i empreses que treballem.

Des del Col·legiu vàrem convidar a formar part d'aquesta Comissió treballadors socials de reconegut prestigi dins la professió i interessats en la recerca d'aquesta temàtica. Així mateix vam sol·licitar la incorporació d'un membre del Consell d'Ètica del Col.legi.

Hem de dir que les nostres companyes han fet un treball magnífic, que ara us presentem, fruit d'un treball rigorós, científic i constant de dos anys.

Vull, en nom de la Junta i en el propi, agrair l'esforç i la dedicació d'aquest equip, dedicació compartida moltes vegades amb altres responsabilitats professionals i col·legials. Però, sobretot, vull agrair la seva generositat envers la professió i, concretament, envers el Col.legi.

Moltes gràcies!

M. Carme Alòs i Pintó
Presidenta

Barcelona, maig 2000

2. Objectius

L'activitat professional quotidiana ha portat, des de sempre, el treballador social a ser coneixedor d'intimitats personals, familiars i de situacions de vida de les persones per a les quals treballa: els clients. El període de canvi que es viu a la societat, la tècnica que tenim a l'abast a finals del segle XX, la quantitat de professionals diversos que poden intervenir en situacions complexes, la mecanització dels processos, la dispersió de recursos i el tractament automatitzat (informàtic) de les dades de caràcter personal, etc., fan que, per garantir el dret constitucional a la intimitat, el respecte i la no-discriminació a la persona, haguem de revisar conceptes tan assumits com la confidencialitat i el secret professional.

Per l'essència mateixa de la nostra professió, a través de les entrevistes, les activitats grupals i comunitàries, els treballadors socials, mitjançant el procés de comunicació i interacció directa amb el client, som dipositaris de molta informació de caràcter personal i familiar. La major part d'aquesta informació és imprescindible que es guardi en el expedients personals individuals/familiars i, per tant, cal garantir-ne la guarda i custòdia, el respecte i la no-divulgació.

La pràctica diària, la poca claredat i abstracció de les lleis, i l'absència de regularització jurídica concreta, ens porten a reflexionar, racionalment i metòdicament, sobre les decisions i actuacions en el camp del Treball Social, per tal de tenir en compte els límits, el marc legal i aquells aspectes que poden comprometre els drets dels usuaris/clients en la nostra intervenció.

Els professionals hem de disposar de mecanisme de tot tipus-legals, tècnics i recomanacions ètiques- que en permetin mantenir l'equilibri entre els drets del client, la professionalitat del tècnic i els seus deures, el respecte de l'empresari, i l'aplicació i la utilització de tots els elements i mitjans que la vida moderna en posa a l'abast.

Amb data de 16 de març de 1998, el Col·legi Oficial de Diplomats en Treball Social i Assistents Socials de Catalunya crea una comissió d'estudi de la legislació respecte als temes de la Confidencialitat i el Secret Professional en l¡àmbit del Treball Social. Aquesta comissió, que neix motivada per algunes de les conclusions de les Primeres Jornades de Serveis Socials respecte a la mancança legal i documental en temes relacionats amb el secret professional, la confidencialitat, l'ètica, etc., es planteja com a primer objectiu fer una recerca, prospecció i selecció documental en relació a aquests temes. Com a objectiu segon es planteja la reflexió conjunta en relació a la realitat actual i els seus efectes en la pràctica professional. I l'assoliment d'ambdós objectius ens porta a l'emissió d'unes recomanacions adreçades tant al conjunt de professionals com al propi Col.legi.

3. Conceptualització

Respecte al principi de **Confidencialitat**, la Federació Internacional de Treballadors Socials va establir, en Assemblea General l'any 1994, els principis ètics professionals entre els quals figura l'apartat destinat a "Criteris del Treball Social en relació als clients". En aquest apartat figura el principi següent:

"Salvaguardar el derecho del cliente/usuario a una relación de confianza, intimidad y confidencialidad, así como al uso responsable de la información o datos que sólo debe realizarse en función de un servicio profesional, manteniendo al cliente informado de su necesidad y utilización. No se divulgará información sin el conocimiento y consentimiento previo del cliente o usuario, excepto si éste no es responsable o se puede perjudicar gravemente a otras personas. El cliente tiene acceso a los expedientes de trabajo social que le conciernen"

Jurídicament, el principi de Confidencialitat apareix a la Llei Orgànica 5/1992 de 29 d'octubre de "Regulación del tratamiento automatizado de los datos de caràcter personal". Estableix que queden excloses de tota utilització, sense consentiment previ de la persona afectada, totes les dades que afectin la seva ideologia, les creences religioses, la raça, la salut o la vida sexual.

Així, el principi de Confidencialitat s'estén al desenvolupament normal de les tasques i funcions professionals que en cada cas són necessàries per assolir els objectius del Treball Social.

El principi del **Secret professional** es deriva també de la mateixa font jurídica que el principi de la confidencialitat. El secret professional es configura com un dret i un deure dels treballadors socials en l'exercici de la seva professió. Aquest principi no impedeix les coordinacions, comunicacions i col·laboracions interprofessionals que es produeixin en el desenvolupament normal

de l'exercici professional, sempre i quan l'usuari n'estigui informat i hagi autoritzat el professional que les seves dades personals referides a ideologia, creences religioses, raça, salut o vida sexual, siguin conegudes per uns altres professionals.
L'Usuari (entès com a persona que utilitza els serveis assistencials) o el Client (en referència a aquest terme cal dir que existeixen connotacions d'elecció) obté la condició legal d'interessat segons la llei 30/1992 de Règim Jurídic de les Administracions Públiques i del Procediment Administratiu Comú, en formular una demanda als serveis- de Treball Social- ja que aquesta demanda donarà lloc a l'inici d'un procediment on constataran dades de caràcter personal i íntim (sempre i quan es tracti de serveis prestats a l'administració).

Així, l'usuari/client, en ostentar la condició d'interessat en un procediment administratiu, és titular d'uns drets i d'unes obligacions. La condició d'interessat és personal, podrà ser exercida personalment o, en el seu defecte, per aquella persona que jurídicament tingui la representació legal (en casos de menors o incapacitats).

L'evolució de la societat obliga, cada vegada més, a incorporar **noves tecnologies**, com és el cas de la informàtica, en els expedients dels usuaris, com a suport automatitzat. Però aquest suport automatitzat comporta alguns riscos segona la seva forma d'utilització. A tal efecte:
La Llei 5/1992 de 19 d'octubre de "Regulació del tractament automatitzat de les dades de caràcter personal" i el reial Decret 1332/1994 que desenvolupa la llei, preveuen la protecció de les dades personals i defineixen conceptes.

L'art. 3 de la llei defineix:

a) **Dades de caràcter personal:** qualsevol informació referent a persones físiques identificades o identificables.
b) **Fitxer automatitzat:** conjunt organitzat de dades de caràcter personal que sigui objecte d'un tractament automatitzat, sigui quina sigui la forma o modalitat de la seva creació, emmagatzematge, organització i accés.
c) **Tractament de les dades:** operacions i procediments tècnics, de caràcter automatitzat o no, que permetin la recollida, gravació, conservació, elaboració, modificació, bloqueig i cancel·lació, així com les cessions de dades que resultin de comunicacions, consultes, interconnexions i transferències.
d) **Responsable del fitxer:** persona física, de naturalesa pública o privada, o òrgan administratiu, que decideixi sobre la finalitat, contingut i ús de les dades.
e) **Afectat:** persona física titular de les dades que siguin objecte de tractament a les quals es refereixi l'apartat c) del present article.
f) **Procediment de dissociació:** tractament de dades personals de manera que la informació obtinguda no pugui associar-se a una persona determinada o determinable.

Per a la protecció de dades: caldrà el consentiment de l'afectat el tractament automatitzat de les dades de caràcter personal (art. 6 de la llei), a excepció dels supòsits que la llei contempli.
La seguretat de les dades: recau en el responsable del fitxer. Aquest ha d'adoptar les mesures de caire tècnic i organitzatiu necessàries que garanteixin la seguretat de les dades de caràcter personal i evitin la seva alteració, pèrdua, tractament o accés no autoritzat, tenint en compte l'estat de la tecnologia, la naturalesa de les dades emmagatzemades i els riscos a que estan exposades, tant si provenen de l'acció humana com del medi físic o natural.
No s'enregistraran dades de caràcter personal en fitxers automatitzats que no reuneixin les condicions que es determinin per via reglamentària respecte a la seva integritat i seguretat i a les dels centres de tractament, local, equips, sistemes i programes.
La Llei també inclou el **dret de les persones d'accés a la informació** sobre les seves dades de caràcter personal incloses en els fitxers automatitzats, i també es preveu el dret a la rectificació i/o cancel·lació.
La informació podrà consistir en la mera consulta dels fitxers mitjançant la seva visualització, o en la comunicació de les dades pertinents per escrit, còpia, telecòpia o fotocòpia, certificada o no, en forma llegible i intel·ligible, sense utilitzar claus o codis convencionals que requereixin l'ús de dispositius mecànics específics.
El dret d'accés al qual es refereix aquest article només podrà ser exercitat a intervals no inferiors a dotze mesos, llevat que l'afectat acrediti un interès legítim a l'efecte.

4. Suport legislatiu

La tasca diària del treball social comporta aspectes relacionats amb el món del Dret i les seves garanties.
Hem de donar garanties de custòdia de la informació aportada pels clients respecte a dades referides a la seva intimitat (informació escrita i/o verbal).

La legislació vigent en matèria del respecte a la persona i les seves circumstàncies, de la seva intimitat, del seu honor i de la seva pròpia imatge, és la següent:

El dret a la intimitat és un dret constitucionals (Consitución Española de 1978, arts. 18, 20 i 105) que estem obligats a complir i a garantir.

- Art. 18.1 "Se garantiza el derecho al honor, o a la intimidad personal y familiar y a la propia imagen". Art. 18.4 "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".
- Art. 20.1 d)"Se reconocen y protegen los derechos a comunicar o recibir libremente información veraz por cualquier medio de difusión. La ley regulará el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de estas libertades".
- Art. 105 b) "La ley regulará el acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas".

Garanties Constitucionals:

Ley Orgánica 1/1982, de 5 de mayo, derecho al honor, a la intimidad personal y familiar a la propia imagen (art. 7.4)

Ley Orgánica 5/1992, de 29 de octubre, por la cual se regula el tratamiento automatizado de los datos de carácter personal (en particular arts. 9 y 10) desarrollada por el Real Decreto 1332/1994, de 20 de junio (adjuntem el text de la Llei i el Reial Decret a l'annex d'aquest document)

Ley 30/1995 de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo común.
Codi Penal: Llei Orgànica 10/1995 de 23 de noviembre

Títol X: "Delitos contra la intimidad, el derecho a la propia imagen, la inviolabilidad del domicilio". Capítulo I: "Del descubrimiento y revelación de los secretos" (arts. 197-201; 278-280)

Codis Deontològics dels Col.legis Professionals

Molts Col.legis professionals tenen algun capítol del seu Codi Deontològic que fa referència al secret professional.

Ens plau fer esment del codi del Col.legi de Metges que recentment s'ha actualitzat per tal d'introduir-hi modificacions que regulin aspectes de les noves tècniques professionals, les modernes tecnologies aplicades, el treball en equips no solament multidisciplinars sinó també multicèntrics, etc., que posen en risc el respecte a la intimitat del pacient.

5. Qüestions més habituals derivades de la pràctica diària del Treball Social

La pràctica del Treball Social comporta la recaptació d'informació íntima i personal de l'usuari/client, i el seu registre en expedients per tal de tenir elements que ens permetin orientar i/o prioritzar el recurs més idoni en cada situació. El registre de la informació comporta per al professional un seguir de dilemes ètics derivats d'una insuficiència de criteris. Davant d'aquesta complexa i compromesa situació, ens hem formulat les següents qüestions respecte a la informació: què registrem, on ho registrem, per què ho fem, qui pot tenir accés als nostres registres, quina informació demanem, qui és el propietari d'aquesta informació, quin ús es por fer de la informació rebuda, com la traspassem, qui ens la pot demanar i quina informació estem obligats a donar.

1. **Què registrem o hauríem de registrar?** Només aquelles dades imprescindibles que ens permetin identificar, situar i abordar el client i la seva problemàtica i els mecanismes d'intervenció, i aquelles que ens facilitin el seguiment de cas, si cal.
2. **On registrem?** En els expedients personals, en els informes a tercers, quan aquests són necessaris i en la documentació de sol·licitud de recurs quan la intervenció professional ho requereixi. Cal garantir que aquesta documentació quedi absolutament guardada, lluny de l'abast de terceres persones.
3. **Per què registrem?** Per tenir constància de cada situació concreta amb les especificitats de cada cas, cosa que ens ha de permetre marcar objectius d'intervenció i fer-ne el seguiment.
4. **Qui pot tenir accés als nostres registres?** Només aquelles persones que nosaltres, en l'exercici responsable de la nostra professió, creguem convenients. I altres membres de l'equip multidisciplinar que intervinguin en el mateix cas.
5. **Quina informació demanem o hem de demanar?** Només aquella que clarifica la situació específica que presenta el client i que ens permet orientar-la adequadament.
6. **Qui és el propietari d'aquesta informació?** Només el client. Això obliga el professional a notificar-la quan se'n faci ús, especificant perquè i l'abast d'aquesta utilització.
7. **Quin ús es fa d'aquesta informació?** Només aquell que és absolutament indispensable per aconseguir l'objectiu de la demanda i/o per a l'anàlisis de la situació.
8. **Com es traspassa aquesta informació?** Per escrit, amb el màxim d'objectivitat possible i només al professional o institució que pot ajudar a resoldre la situació/problema que presenta el client. I caldrà informar el client d'aquest traspàs d'informació
9. **Qui ens pot demanar informació?** Els nostres superiors- i en aquest cas podem donar aquella informació que mantingui en l'anonimat els nostres clients- o aquelles institucions que pel fet de ser dispensadores d'algun recurs específic, ens ho exigeixin reglamentàriament. També els jutges en exercici de la seva professió.
10. **Quina mena d'informació estem obligats a donar?** El mínim imprescindible que cada situació reclami, assegurant-nos que tenim autorització de l'interessat. Mai no donarem informació sense que l'usuari ho sàpiga, a excepció d'aquelles situacions que impliquin un risc per a tercers.

Totes aquestes situacions i qüestions que semblen de fàcil resposta són complexes i polèmiques d'interpretar en situacions específiques i concretes.

Allò que ha de quedar clar per part de tots- professionals, institucions, càrrecs de comandament, polítics, etc.- és que necessitem algun tipus d'informació però que aquesta només s'ha d'utilitzar en funció d'objectius professionals i amb permís de l'interessat.

És fonamental en la pràctica del Treball Social tenir en compte que:

- Sempre hi ha d'haver un objectiu professional que justifiqui una informació.
- El client haurà d'autoritzar el treballador social.

6. Elements del procés de comunicació i interacció entre client i treballador social

En matèria de Treball Social, rebre, analitzar i utilitzar la informació rebuda no és cosa de dos elements sinó que, en aquest procés, hi intervenen molts més protagonistes: els clients, els professionals, el procediment informàtics, terceres persones o institucions, l'empresa que ha contractat el professional....

Farem un breu repàs de cada un d'aquests elements:

a) Els usuaris/clients

Poden donar-se dues circumstàncies: que acudeixi voluntàriament a demanar un servei, recurs, prestació, o simplement informació o orientació; o que hagi estat citat pel professional. En ambdues situacions serà imprescindible obtenir algun tipus d'informació.

La primera responsabilitat del professional és situar el client davant l'encàrrec, ja sigui a demanar pròpia o bé per intervenció del professional, de tal manera que sigui capaç de comprendre el perquè de les preguntes i les dades que se li demanen, quin ús

se'n farà, i si es buscarà informació complementària. També cal que sàpiga si s'implicarà en aquest procés la resta del grup familiar al qual pertany, o altres circumstàncies que puguin sorgir durant el procés de la intervenció professional.

El client ha de saber amb claredat l'objectiu i el marc de la intervenció professional, ha de tenir la certesa que la discreció serà absolutament respectada i que se'l consultarà sempre que s'hagi de transmetre una informació que li pertany.

En aquesta concreció de la intervenció professional s'ha d'aconseguir un clima de diàleg i confiança mútua que faci possible la resolució de problemes, però no més.

Avui és freqüent que a la taula del treballador social hi hagi ordinador. Si el client té dubtes de les dades que dóna i de la seva destinació, se li ha d'aclarir de manera senzilla i entenedora, respectant que no vulgui facilitar alguna dada. En aquest cas, si la resposta fos imprescindible per aconseguir l'objectiu assistencial (si no ho és, no cal ni demanar-lo), també se li ha de fer saber per tal que conegui les conseqüències de la seva negativa.

b) Els professionals

Quan s'està davant d'un client, el respecte a la persona és indispensable. S'ha d'aconseguir crear un clima de tranquil·litat i confiança imprescindible en qualsevol relació interpersonal. Si hi ha presència d'altres professionals de l'equip, el client ha de saber qui són, per què són allà, quin paper juguen en la seva problemàtica. A partir d'aquí cal que el professional seleccioni la informació a obtenir i com fer-ho, explicant sempre la conseqüència de la mateixa.

Quan s'ha de fer un informe per a una altre institució, cal comunicar-ho al client explicant-li els motius i, sempre que sigui possible, se li llegirà el contingut de l'informe i es demanarà el seu consentiment. Si per raons alienes (incapacitats de qualsevol tipus) aquest consentiment no es pot obtenir, es podrà demanar la intervenció de la família. Si realment no hi ha ningú que pugui autoritzar aquesta activitat, serà responsabilitat del treballador social actuar en conseqüència.

Actualment, la tecnologia ens permet traspassar informació de manera fàcil (fax, correu electrònic, xarxa informàtica, etc.) però amb l'inconvenient que de vegades no sabem on va a parar, qui la recull, quin ús se'n fa. Hem de prendre certes precaucions en la forma de traspassar informació per tal d'assegurar que el fax el rep només la persona a qui va dirigit, que l'ordinador només l'utilitzen les persones compromeses amb el secret professional del servei, etc.

Quan l'informe conté el diagnòstic de la situació, cal que el client sàpiga com i per què s'ha arribat a aquestes conclusions, per què emetem l'informe, a qui va dirigit, i quin resultats se'n trauran. Però també hem d'estar disposats a treballar conjuntament amb el client per modificar aquelles problemàtiques o situació social anòmala.

c) Terceres persones, altres institucions

El tema de la confidencialitat i el respecte a les persones, famílies o grups és punyent i s'ha de tenir molta cura per tal que no s'escapi del control professional ni dintre ni fora del servei. Aquesta vigilància es va tornant més feble quan la informació va destinada a tercers, ja siguin persones o institucions, malgrat que la responsabilitat legal serà de la persona/institució que rep la informació.

Podem transferir informació sempre que tinguem el permís i consentiment de l'interessat, a excepció d'aquelles situacions que impliquin risc a tercers: menors, incapacitats.... Cal actuar amb prudència suficient per tal de transferir només aquella informació estrictament imprescindible i sense opcions ni comentaris personals, és a dir, el més objectivament possible.

d) L'empresa contractant del treballador social

Quan parlem d'empresa contractant no fem cap diferència entre l'Administració i l'empresa privada, ja sigui mercantil, sense afany de lucre, fundació o societat anònima, perquè les mesures, les dificultats i els riscos són els mateixos i l'obligació de mantenir la confidencialitat i el secret professional, també.

Les empreses, moltes vegades, obliden que cal facilitar la tasca dels professionals, tant en el sentit de preservar la intimitat en la seva relació amb el client com en la responsabilitat de la guarda de les dades recollides a través de les entrevistes o d'altres canals, i es creuen amb el dret de demanar informació no necessària.

Si diem que per obtenir una bona intervenció professional cal establir un cert nivell de confiança entre el client i el treballador social, també és cert que per obtenir resultats positius, la millora de les situacions individuals i col·lectives, és imprescindible un

clima de respecte i confiança entre el professional i la seva empresa representada pel cap de servei, el gerent o el regidor corresponent.

e) El procés informàtic

Cada vegada més, el suport informàtic i altres tècniques de comunicació, són a l'abast dels treballadors socials, la qual cosa facilita la intervenció professional des de la vessant individual a les tasques de planificació.

Si bé la informatització ens facilita el treball, també por comportar riscos. Cal garantir la seguretat de la no-violació de les dades arxivades i impedir-hi l'accés a tota persona aliena a la intervenció professional.

Si la seguretat dels fitxers ha d'estar garantida, no cal dir també que s'ha d'assegurar la transferència de la informació per vies mecàniques (fax, correu electrònic, etc.). De vegades encarreguem a tercers aquesta feina sense tenir en compte que el seu contingut és matèria reservada perquè inclou dades personals garantides per la confidencialitat.

En el traspàs d'una informació de professionals a professional, s'ha de tenir en compte que entremig hi pot haver altres estaments de professionals que poden ser molt respectuosos amb el contingut de la documentació que manipulen, però que poden donar inseguretat al client en perjudici del clima de confiança necessari per a una bona intervenció professional.

No cal dir que el responsable de la guarda de tota aquesta informació està obligat pel Secret Professional, fins i tot després de finalitzar les seves relacions tant amb el client com amb l'empresa. No oblidem que molts expedients reculen dades referides a comportament personal, salut, creences, a històries de vida, que si no estan ben guardades no podem garantir la confidencialitat ni vetllar pel seu bon ús, amb la conseqüent violació d'un dret constitucional: el dret a la intimitat.

Dins d'aquest marc conceptual, és molt interessant l'acord pres pel Ple de l'Ajuntament de l'Hospitalet de Llobregat el dia 5 de març de 1999 (B.O.P. 29-4-99)

7. Situacions que dificulten la garantia de confidencialitat i secret professional

En la pràctica professional, el treballador social ha d'evitar obstacles i situacions que dificultin la garantia del dret de l'usuari a la confidencialitat i al secret professional.

a) Referent a la infraestructura dels serveis:

El treballador social ha de vetllar per la correcta adequació de les infraestructures. Caldrà evitar:

- Els despatxos oberts, que no estan insonoritzats, ubicats en llocs concorreguts, compartits per altres serveis i professionals al mateix temps, amb manca d'infraestructura mínima per evitar la interrupció de les entrevistes (contestador automàtic, informador/a)...
- La poca protecció dels expedients per manca d'arxius adequadament protegits i per manca de legislació respecte a la guarda i custòdia de la documentació generada pels serveis de Treball Social.
- L'indiscriminat accés als arxius informàtics quan s'utilitzen les noves tecnologies: fax, ordinador, etc., com a canal de transmissió.

b) Referent a la pràctica professional:

El treballador social ha d'aconseguir:

- Gestionar adequadament el propi temps de dedicació professional. La sobrecàrrega de treball dificulta en ocasions la tasca d'arxivar i protegir adequadament la informació.
- Recollir únicament les dades de l'usuari estrictament necessàries.
- Emetre informes amb rigor professional, on solament constin aquelles dades de l'usuari estrictament necessàries i indicadors que justifiquin l'objecte de l'informe.
- Vetllar per la protecció dels expedients, Quan el treballador social treballa en més d'un centre, caldrà evitar endur-se expedients d'un lloc a un altre, i en el supòsit que sigui necessari fer-ho cal protegir la informació en els desplaçaments.
- Vetllar per la discreció d'alumnes de pràctiques, personal voluntari o altres.
- Garantir la confidencialitat quan es traspassa la informació continguda en expedients a un altre professional, ja sigui per canvi de professionals o per un altre tipus de causa.

c) Referent a la sol·licitud de recursos

El treballador social generalment no disposa de potestat resolutòria per concedir o denegar el recurs sol·licitat. Així doncs, quan sol·licita un recurs a la pròpia institució per a la qual treballa:

- Intentarà mantenir en l'anonimat del demandant, és a dir, protegirà el seu dret a la confidencialitat, ja que moltes vegades, sobretot en col·lectius petits, aquella sol·licitud passa a ser de domini públic amb els comentaris conseqüents.
- Quan el recurs se sol·licita a una entitat aliena, l'anonimat és impossible de mantenir però el treballador social haurà de buscar els mecanismes adients per a la protecció de les dades.
- Cal tenir present que existeixen circumstàncies en les quals el professionals no pot controlar l'ús que es fa de la informació continguda en informes que ell ha emès. Més d'un professional s'haurà trobat davant de possibles processos judicials on els informes del treballador social van i vénen dels advocats als procuradors, dels jutges a la part contrària, etc., amb una lleugeresa i frivolitat que pot tenir conseqüències molt negatives per a tothom, primer per a l'interessat però també per al conjunt dels treballadors socials que tenen una imatge d'irresponsables.
- Per evitar situacions desagradables, el professional haurà d'ésser discret i en els informes únicament exposarà dades i indicadors estrictament necessaris.

d) Referent a l'organigrama de la institució

El professional vetllarà perquè no es produeixi intromissió del poder polític i perquè aquest garanteixi també els drets que té l'usuari.

El treballador social, si cal, justificarà la seva feina, davant la institució, amb documents tècnics i objectius on solament constin les dades mínimes imprescindibles de l'usuari/client.

8. Conclusions

- EL SECRET PROFESSIONAL es configura com un dret i un deure dels treballadors socials en l'exercici de la seva professió
- EL DRET DE LES PERSONES A L'ACCÉS A LA INFORMACIÓ sobre les seves dades de caràcter personal està regulat per la legislació vigent, i és d'obligat compliment.
- SEMPRE HI HA D'HAVER UN OBJECTIU PROFESSIONAL que justifiqui demanar una informació
- En la pràctica professional s'ha d'evitar els obstacles i situacions que dificultin la GARANTIA DE L'USUARI/CLIENT A LA CONFIDENCIALITAT I AL SECRET PROFESSIONAL.
- L'emissió d'informes s'haurà de posar en CONEIXEMENT DEL CLIENT i, sempre que sigui possible, aconseguir el seu vistiplau respecte del seu contingut.
- Existeix un BUIT DE REGULACIÓ LEGAL del secret professional, lligada a la regulació de l'exercici de la professió; no solament regulació corporativa, sinó amb l'existència d'una llei general. També cal una regulació del Secret Professional en la qual es contempli l'àmbit de l'exercici lliure de la professió i l'exercici per compte aliè.

9. Recomanacions

a) Recomanacions per als professional

1. Davant la informació registrada, hem de tenir molt present: quina informació demanem; on la registrem; qui pot tenir-hi accés, qui és el propietari de la mateixa; qui ús se'n pot fer; com la traspassem; i quina informació estem obligats a donar.
2. En els informes emesos solament hi ha de constar aquelles dades personals estrictament necessàries, així com indicadors que justifiquin l'objecte de l'informe.
3. En la determinació i/o assignació de recursos (o mesures) que afectin directament l'usuari/client es tindrà cura que no es produeixi cap intromissió (ni de l'estament polític, administratiu, ni d'altres estaments). I en el cas d'actuacions conjuntes també es vetllarà per garantir el dret a la confidencialitat de l'usuari/client.
4. En els serveis o centres s'ha de determinar responsables dels diferents aparells i noves tecnologies que transmetin informació (fax, ordinador).
5. Els serveis o centres han de disposar d'un espai físic suficient i adequat que permeti el correcte arxiu sistemàtic dels expedients i que disposi d'un sistema de seguretat que impedeixi l'accés a persones no autoritzades.

b) Recomanacions per al Col.legi Professional

1. El Col.legi Professional ha de proporcionar les eines i el suport tècnic necessari per tal que els treballadors socials puguin desenvolupar les tasques i funcions inherents i necessàries per a la consecució dels objectius de la professió, mantenint el màxim respecte a la dignitat de les persones (usuari/client) i garantir el dret a la intimitat de les mateixes. Per dur a terme aquesta tasca col·legial, cal que la Junta de Govern garanteixi la realització de les següents funcions:
    - Seguiment del compliment de les recomanacions emeses en el present document.
    - Emetre informes tècnics davant situacions de dubte o conflicte a demanda dels serveis, centres i/o professionals.
    - Assessorament tècnic i consultiu
    - Emissió de peritatges tècnics
    - Proposar millores continuades en l¡àmbit de l'administració, serveis, mitjans de comunicació i professionals.

Considerem que aquestes funcions haurien d'anar a càrrec d'un tècnic responsable vinculat a la Junta de Govern i a la Comissió d'Ètica.

2. Per adequar el Codi d'Ètica a la situació actual del treball professional, cal fer-ne una revisió general i la modificació d'alguns aspectes.
3. És necessari que el Col.legi adopti les mesures pertinents i faci les gestions indispensables en les instàncies oficials per tal que es regulin legalment els temes fonamentals derivats del desenvolupament de la professió del Treball Social: el secret professional, la confidencialitat...

10. Bibliografia

Suport legislatiu

- La Constitución Española del 1978
- Llei Orgànica 1/1982 de 5 de maig
- Llei Orgànica 5/1992 de 29 d'octubre. Informàtica. Regulació del tractament informatitzat en les dades de caràcter personal
- Decret 1332/1994, de 20 de juny, que desenvolupa determinats aspectes d'aquesta llei
- Llei Orgànica 10/1995 de 23 de novembre, del Codi Penal
- Llei 30/1992 de 26 de novembre de regim jurídic de les administracions públiques i de procediment administratiu comú
- Llei 2/1994 de 24 de març, de bases de delegació en el govern per a adequació de les lleis de Catalunya a la Llei de règim jurídic de les administracions públiques i el procediment administratiu comú (Presidència de la Generalitat)
- Decret legislatiu 5/1994 de 13 de juliol pel qual s'adequa la Llei 26/1985 de 26 de desembre, de serveis socials a la Llei 30/1992, de 26 de novembre, de règim jurídic de les administracions públiques i del procediment administratiu comú (departament de Benestar Social)
- Decret 145/1994 de 30 de maig, pel qual es porta a terme l'adequació dels procediments del departament de Benestar Social a la Llei 30/1992 de 26 de novembre de règim jurídic les administracions públiques i del procediment administratiu comú (Departament de Benestar Social)

Codis deontològics

- Col.legi Oficial de Diplomats en Treball Social i Assistents Social de Catalunya.
- Col.legi Oficial de Diplomats en Treball Social de Burgos
- Consell de Col.legi de Metges de Catalunya

Altres documents

- Sol·licitud d'informació per part dels òrgans de l'Administració de Justícia o per part d'altres administracions públiques. Fitxes d'informació jurídica, número 1. Ajuntament de l'Hospitalet de Llobregat
- Informe: Protecció del dret a la intimitat. Confidencialitat de les dades de caràcter personal. Ajuntament de l'Hospitalet de Llobregat.
- Fitxes d'informació jurídica. Número 2. Ajuntament de l'Hospitalet de Llobregat

- Dades automatitzades. Ajuntament de l'Hospitalet de Llobregat
- Accés dels clients als arxius dels serveis socials. Document elaborat el 1997 en una trobada organitzada pel departament de Salut i Seguretat Social de Londres i el Centre Europeu per a la investigació i formació en el benestar social de Viena
- Recomanacions sobre la confidencialitat en la Corporació Sanitària Parc Taulí. Sabadell.

ANNEX 1

Llei Orgànica 5/1992 de 29 d'octubre de 1992

INFORMÀTICA. Regulació del tractament automatitzat de les dades de caràcter personal.

Don Juan Carlos I,
Rey de España.

A todos los que la presente vieren y entendieren, sabed:
Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley Orgánica:

EXPOSICIÓN DE MOTIVOS:

1. La Constitución española, en su artículo 18.4, emplaza al legislador a limitar el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el legítimo ejercicio de sus derechos. La aún reciente aprobación de nuestra Constitución y, por tanto, su moderno carácter, le permitió expresamente la articulación de garantías contra la posible utilización torticera de ese fenómeno de la contemporaneidad que es la informática.

El progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la privacidad, en efecto, a una amenaza potencial antes desconocida. Nótese que se habla de la privacidad y no de la intimidad: aquélla es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona -el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo-, la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado.

Y si la intimidad, en sentido estricto, está suficientemente protegida por las previsiones de los tres primeros párrafos del artículo 18 de la Constitución y por las leyes que los desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo.

Ello es así porque, hasta el presente, las fronteras de la privacidad estaban defendidas por el tiempo y el espacio. El primero procuraba, con su transcurso, que se evanescieran los recuerdos de las actividades ajenas, impidiendo, así, la configuración de una historia lineal e ininterrumpida de la persona; el segundo, con la distancia que imponía, hasta hace poco difícilmente superable, impedía que tuviésemos conocimiento de los hechos que, protagonizados por los demás, hubieran tenido lugar lejos de donde nos hallábamos. El tiempo y el espacio operaban, así, como salvaguarda de la privacidad de la persona.

Uno y otro límite han desaparecido hoy: las modernas técnicas de comunicación permiten salvar sin dificultades el espacio, y la informática posibilita almacenar todos los datos que se obtienen a través de las comunicaciones y acceder a ellos en apenas segundos, por distante que fuera el lugar donde transcurrieron los hechos, o remotos que fueran éstos.

Los más diversos datos -sobre la infancia, sobre la vida académica, profesional o laboral, sobre los hábitos de vida y consumo, sobre el uso del denominado *dinero plástico*, sobre las relaciones personales o, incluso, sobre las creencias religiosas e ideologías, por poner solo algunos ejemplos- relativos a las personas podrían ser, así, compilados y obtenidos sin dificultad. Ello permitiría a quien dispusiese de ellos acceder a un conocimiento cabal de actitudes, hechos o pautas de comportamiento que, sin duda, pertenecen a la esfera privada de las personas; a aquélla a la que sólo deben tener acceso el individuo y, quizás, quienes le son más próximos, o aquellos a los que él autorice. Aún más: el conocimiento ordenado de esos datos puede dibujar un determinado perfil de la persona, o configurar una determinada reputación o fama que es, en definitiva, expresión del honor; y este perfil, sin duda, puede resultar luego valorado, favorable o desfavorablemente, para las más diversas actividades públicas o privadas, como pueden ser la obtención de un empleo, la concesión de un préstamo o la admisión en determinados colectivos.

Se hace preciso, pues, delimitar una nueva frontera de la intimidad y del honor una frontera que sustituyendo los límites antes definidos por el tiempo y el espacio, los proteja frente a la utilización mecanizada, ordenada y discriminada de los datos a ellos referentes; una frontera, en suma, que garantice que un elemento objetivamente provechoso para la Humanidad no redunde en perjuicio para las personas. La fijación de esa nueva frontera es el objetivo de la previsión contenida en el artículo 18.4 de la Constitución, y al cumplimiento de ese objetivo responde la presente Ley.

2. Partiendo de que su finalidad es hacer frente a los riesgos que para los derechos de la personalidad puede suponer el acopio y tratamiento de datos por medios informáticos, la Ley se nuclea en torno a los que convencionalmente se denominan *ficheros de datos*: Es la existencia de estos ficheros y la utilización que de ellos podría hacerse la que justifica la necesidad de la nueva frontera de la intimidad y del honor.

A tal efecto, la Ley introduce el concepto de tratamiento de datos, concibiendo los ficheros desde una perspectiva dinámica; dicho en otros términos, no los entiende sólo como un mero depósito de datos, sino también, y sobre todo,

como una globalidad de procesos o aplicaciones informáticas que se llevan a cabo con los datos almacenados y que son susceptibles, si llegasen a conectarse entre sí, de configurar el perfil personal al que antes se hizo referencia.

La Ley está animada por la idea de implantar mecanismos cautelares que prevengan las violaciones de la privacidad que pudieran resultar del tratamiento de la información. A tal efecto se estructura en una parte general y otra especial.

La primera atiende a recoger los principios en los que ha cristalizado una *opinio iuris*, generada a lo largo de dos décadas, y define derechos y garantías encaminados a asegurar la observancia de tales principios generales. Alimentan esta parte general, pues, preceptos delimitadores del ámbito de aplicación de la Ley, principios reguladores de la recogida, registro y uso de datos personales y, sobre todo, garantías de la persona.

El ámbito de aplicación se define por exclusión, quedando fuera de él, por ejemplo, los datos anónimos, que constituyen información de dominio público o recogen información, con la finalidad, precisamente, de darla a conocer al público en general -como pueden ser los Registros de la Propiedad o Mercantiles-, así como, por último, los de uso estrictamente personal. De otro lado, parece conveniente la permanencia de las regulaciones especiales que contienen ya suficientes normas de protección y que se refieren a ámbitos que revisten tal singularidad en cuanto a sus funciones y sus mecanismos de puesta al día y rectificación que aconsejan el mantenimiento de su régimen específico.

Así ocurre, por ejemplo, con las regulaciones de los ficheros electorales, del Registro Civil o del Registro Central de Penados y Rebeldes; así acontece, también, con los ficheros regulados por la Ley 12/1989, de 12 de mayo, sobre Función Estadística Pública, si bien que, en este último caso, con sujeción a la Agencia de Protección de Datos. En fin, quedan también fuera del ámbito de la norma aquellos datos que, en virtud de intereses públicos prevalentes, no deben estar sometidos a su régimen cautelar.

Los principios generales, por su parte, definen las pautas a las que debe atenerse la recogida de datos de carácter personal, pautas encaminadas a garantizar tanto la veracidad de la información contenida en los datos almacenados cuanto la congruencia y la racionalidad de la utilización de los datos. Este principio, verdaderamente cardinal, de la congruencia y la racionalidad, garantiza que los datos no puedan ser usados sino cuando lo justifique la finalidad para la que han sido recabados; su observancia es, por ello, capital para evitar la difusión incontrolada de la información que, siguiendo el mandato constitucional, se pretende limitar.

Por su parte, el principio de consentimiento, o de autodeterminación, otorga a la persona la posibilidad de determinar el nivel de protección de los datos a ella referentes. Su base está constituida por la exigencia del consentimiento consciente e informado del afectado para que la recogida de datos sea lícita; sus contornos, por otro lado, se refuerzan singularmente en los denominados *datos sensibles*, como pueden ser, de una parte, la ideología o creencias religiosas -cuya privacidad está expresamente garantizada por la Constitución en su artículo 16.2- y, de otra parte, la raza, la salud y la vida sexual. La protección reforzada de estos datos viene determinada porque los primeros de entre los datos mencionados sólo serán disponibles con el consentimiento expreso y por escrito del afectado, y los segundos sólo serán susceptibles de recopilación mediando dicho consentimiento o una habilitación legal expresa, habilitación que, según exigencia de la propia Ley Orgánica, ha de fundarse en razones de interés general; en todo caso, se establece la prohibición de los ficheros creados con la exclusiva finalidad de almacenar datos personales que expresen las mencionadas características. En este punto, y de acuerdo con lo dispuesto en el artículo 10 de la Constitución, se atienden las exigencias y previsiones que para estos datos se contienen en el Convenio Europeo para la protección de las personas con respecto al tratamiento automatizado de datos con carácter personal, de 1981, ratificado por España.

Para la adecuada configuración, que esta Ley se propone, de la nueva garantía de la intimidad y del honor resulta esencial la correcta regulación de la cesión de los datos almacenados. Es, en efecto, el cruce de los datos almacenados en diversas instancias o ficheros el que puede arrojar el repetidamente aludido perfil personal, cuya obtención transgrediría los límites de la privacidad. Para prevenir estos perturbadores efectos, la Ley completa el principio del consentimiento, exigiendo que, al procederse a la recogida de los datos, el afectado sea debidamente informado del uso que se les puede dar, al objeto de que el consentimiento se preste con conocimiento cabal de su exacto alcance. Sólo las previsiones del Convenio Europeo para la protección de los Derechos Fundamentales de la Persona -artículo 8.2- y del Convenio 108 del Consejo de Europa -artículo 9.2-, que se fundamentan en exigencias lógicas en toda sociedad democrática, constituyen excepciones a esta regla.

3. Las garantías de la persona son los nutrientes nucleares de la parte general, y se configuran jurídicamente como derechos subjetivos encaminados a hacer operativos los principios genéricos. Son, en efecto, los derechos de autodeterminación, de amparo, de rectificación y de cancelación los que otorgan virtualidad normativa y eficacia jurídica a los principios consagrados en la parte general, principios que, sin los derechos subjetivos ahora aludidos, no rebasarían un contenido meramente programático.

En concreto, los derechos de acceso a los datos, de rectificación y de cancelación, se constituyen como piezas centrales del sistema cautelar o preventivo instaurado por la Ley. El primero de ellos ha cobrado en nuestro país, incluso, plasmación constitucional en lo que se refiere a los datos que obran en poder de las Administraciones Públicas (artículo 105.b). En consonancia con ello queda recogido en la Ley en términos rotundos, no previéndose más excepciones que las derivadas de la puesta en peligro de bienes jurídicos en lo relativo al acceso a los datos policiales y a los precisos para asegurar el cumplimiento de las obligaciones tributarias en lo referente a los datos de este carácter, excepciones ambas que pueden entenderse expresamente recogidas en el propio precepto constitucional antes citado, así como en el Convenio Europeo para la protección de los Derechos Fundamentales.

4. Para la articulación de los extremos concretos que han de regir los ficheros de datos, la parte especial de la Ley comienza distinguiendo, en su Título Cuarto, entre los distintos tipos de ficheros, según sea su titularidad pública o privada. Con la pretensión de evitar una perniciosa burocratización, la Ley ha desechado el establecimiento de supuestos como la autorización previa o la inscripción constitutiva en un registro.

Simultáneamente, ha establecido regímenes diferenciados para los ficheros en razón de su titularidad, toda vez que, con toda evidencia, resulta más problemático el control de los de titularidad privada que el de aquéllos de titularidad pública. En efecto, en lo relativo a estos últimos, no basta la mera voluntad del responsable del fichero sino que es precisa norma habilitante, naturalmente pública y sometida al control jurisdiccional, para crearlos y explotarlos, siendo en estos supuestos el informe previo del órgano de tutela el cauce idóneo para controlar la adecuación de la explotación a las exigencias legales y recomendar, en su caso, las medidas pertinentes.

Otras disposiciones de la parte especial que procede destacar son las atinentes a la transmisión internacional de los datos. En este punto, la Ley traspone la norma del artículo 12 del Convenio 108 del Consejo de Europa, apuntando así una solución para lo que ha dado en llamarse flujo transfronterizo de datos. La protección de la integridad de la información personal se concilia, de esta suerte, con el libre flujo de los datos, que constituye una auténtica necesidad de la vida actual de la que las transferencias bancarias, las reservas de pasajes aéreos o el auxilio judicial internacional pueden ser simples botones de muestra. Se ha optado por exigir que el país de destino cuente en su ordenamiento con un sistema de protección equivalente al español, si bien permitiendo la autorización de la Agencia cuando tal sistema no exista pero se ofrezcan garantías suficientes. Con ello no sólo se cumple con una exigencia lógica, la de evitar un fallo que pueda producirse en el sistema de protección a través del flujo a países que no cuentan con garantías adecuadas, sino también con las previsiones de instrumentos internacionales como los Acuerdos de Schengen o las futuras normas comunitarias.

5. Para asegurar la máxima eficacia de sus disposiciones, la Ley encomienda el control de su aplicación a un órgano independiente, al que atribuye el estatuto de Ente público en los términos del artículo 6.5 de la Ley General Presupuestaria. A tal efecto la Ley configura un órgano especializado, denominado Agencia de Protección de Datos, a cuyo frente sitúa un Director.

La Agencia se caracteriza por la absoluta independencia de su Director en el ejercicio de sus funciones, independencia que trae causa, en primer lugar, de un expreso imperativo legal, pero que se garantiza, en todo caso, mediante el establecimiento de un mandato fijo que sólo puede ser acortado por un *numerus clausus* de causas de cese.

La Agencia dispondrá, además, de un órgano de apoyo definido por los caracteres de colegiación y representatividad, en el que obtendrán presencia las Cámaras que representan a la soberanía nacional, las Administraciones Públicas en cuanto titulares de ficheros objeto de la presente Ley, el sector privado, las organizaciones de usuarios y consumidores y otras personas relacionadas con las diversas funciones que cumplen los archivos informatizados.

6. El inevitable desfase que las normas de derecho positivo ofrecen respecto de las transformaciones sociales es, si cabe, más acusado en este terreno, cuya evolución tecnológica es especialmente, dinámica. Ello hace aconsejable, a la hora de normar estos campos, acudir a mecanismos jurídicos dotados de menor nivel de vinculación, susceptibles de una elaboración o modificación más rápida de lo habitual y caracterizados por que es la voluntaria aceptación de sus destinatarios la que les otorga eficacia normativa. En esta línea la Ley recoge normas de autorregulación, compatibles con las recomendaciones de la Agencia, que evitan los inconvenientes derivados de la especial rigidez de la Ley Orgánica que, por su propia naturaleza, es inidónea para un acentuado casuísmo.

La propia experiencia de lo ocurrido con el Convenio del Consejo de Europa, que ha tenido que ser objeto de múltiples modificaciones al socaire de las distintas innovaciones tecnológicas, de las sucesivas y diferentes aplicaciones -estadística, Seguridad Social, relaciones de empleo, datos policiales, publicidad directa o tarjetas de crédito, entre otras- o de la ampliación de los campos de utilización -servicio telefónico o correo electrónico- aconseja recurrir a las citadas normas de autorregulación.

De ahí que la Ley acuda a ellas para aplicar las previsiones legales a los distintos sectores de actividad. Tales normas serán elaboradas por iniciativa de las asociaciones y organizaciones pertinentes y serán aprobadas, sin valor reglamentario, por la Agencia, siendo precisamente la iniciativa y participación de las entidades afectadas la garantía de la virtualidad de las normas.

7. La Ley no consagra nuevos tipos delictivos, ni define supuestos de responsabilidad penal para la eventualidad de su incumplimiento. Ello obedece a que se entiende que la sede lógica para tales menesteres no es esta Ley, sino sólo el Código Penal.

Sí se atribuye, sin embargo, a la Administración la potestad sancionadora que es lógico correlato de su función de inspección del uso de los ficheros, similar a las demás inspecciones administrativas, y que se configura de distinta forma según se proyecte sobre la utilización indebida de los ficheros públicos, en cuyo caso procederá la oportuna responsabilidad disciplinaria, o sobre los privados, para cuyo supuesto se prevén sanciones pecuniarias.

De acuerdo con la práctica usual, la Ley se limita a tipificar, de conformidad con lo requerido por la jurisprudencia constitucional y ordinaria, unos supuestos genéricos de responsabilidad administrativa, recogiendo una gradación de

infracciones que sigue la habitual distinción entre leves, graves y muy graves, y que toma como criterio básico el de los bienes jurídicos emanados.

Las sanciones, a su vez, difieren según que los ficheros indebidamente utilizados sean públicos o privados: en el primer caso, procederá la responsabilidad disciplinaria, sin perjuicio de la intervención del Defensor del Pueblo; para el segundo, se prevén sanciones pecuniarias; en todo caso, se articula la posibilidad en los supuestos, constitutivos de infracción muy grave, de cesión ilícita de datos o de cualquier otro atentado contra los derechos de los afectados que revista gravedad, de inmovilizar los ficheros.

8. Finalmente, la Ley estipula un período transitorio que se justifica por la necesidad de ajustar la utilización de los ficheros existentes a las disposiciones legales.

Pasado este período transitorio, y una vez en vigor la Ley, podrá muy bien decirse, una vez más, que el desarrollo legislativo de un precepto constitucional se traduce en una protección reforzada de los derechos fundamentales del ciudadano. En este caso, al desarrollar legislativamente el mandato constitucional de limitar el uso de la informática, se está estableciendo un nuevo y más consistente derecho a la privacidad de las personas.

TÍTULO I.
DISPOSICIONES GENERALES

Artículo 1. Objeto.
La presente Ley Orgánica, en desarrollo de lo previsto en el apartado 4 del artículo 18 de la Constitución, tiene por objeto limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos.

Artículo 2. Ámbito de aplicación.
1. La presente Ley será de aplicación a los datos de carácter personal que figuren en ficheros automatizados de los sectores público y privado y a toda modalidad de uso posterior, incluso no automatizado, de datos de carácter personal registrados en soporte físico susceptible de tratamiento automatizado.

2. El régimen de protección de los datos de carácter personal que se establece en la presente Ley no será de aplicación:

a. A los ficheros automatizados de titularidad pública cuyo objeto, legalmente establecido, sea el almacenamiento de datos para su publicidad con carácter general.
b. A los ficheros mantenidos por personas físicas con fines exclusivamente personales.
c. A los ficheros de información tecnológica o comercial que reproduzcan datos ya publicados en boletines, diarios o repertorios oficiales.
d. A los ficheros de informática jurídica accesibles al público en la medida en que se limiten a reproducir disposiciones o resoluciones judiciales publicadas en periódicos o repertorios oficiales.
e. A los ficheros mantenidos por los partidos políticos, sindicatos e Iglesias, confesiones y comunidades religiosas en cuanto los datos se refieran a sus asociados o miembros y ex miembros, sin perjuicio de la cesión de los datos que queda sometida a lo dispuesto en el artículo 11 de esta Ley, salvo que resultara de aplicación el artículo 7 por tratarse de los datos personales en él contenidos.

3. Se regirán por sus disposiciones específicas:

a. Los ficheros regulados por la legislación de régimen electoral.
b. Los sometidos a la normativa sobre protección de materias clasificadas.
c. Los derivados del Registro Civil y del Registro Central de Penados y Rebeldes.
d. Los que sirvan a fines exclusivamente estadísticos y estén amparados por la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, sin perjuicio de lo dispuesto en el artículo 36.
e. Los ficheros automatizados cuyo objeto sea el almacenamiento de los datos contenidos en los informes personales regulados en el artículo 68 de la Ley 17/1989, de 19 de julio, Reguladora del Régimen del Personal Militar Profesional.

Artículo 3. Definiciones.
A los efectos de la presente Ley se entenderá por:

a. Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables.
b. Fichero automatizado: Todo conjunto organizado de datos de carácter personal que sean objeto de un tratamiento automatizado, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
c. Tratamiento de datos: Operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
d. Responsable del fichero: Persona física, jurídica de naturaleza pública o privada y órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento.
e. Afectado: Persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.
f. Procedimiento de disociación: Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona determinada o determinable

TÍTULO II.
PRINCIPIOS DE LA PROTECCIÓN DE DATOS

Artículo 4. Calidad de los datos.
1. Sólo se podrán recoger datos de carácter personal para su tratamiento automatizado, así como someterlos a dicho tratamiento, cuando tales datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades legítimas para las que se hayan obtenido.
En su clasificación sólo podrán utilizarse criterios que no se presten a prácticas ilícitas.

2. Los datos de carácter personal objeto de tratamiento automatizado no podrán usarse para finalidades distintas de aquellas para las que los datos hubieran sido recogidos.

3. Dichos datos serán exactos y puestos al día de forma que respondan con veracidad a la situación real del afectado.

4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 15.

5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados y registrados.

No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos sus valores históricos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.

6. Serán almacenados de forma que permitan el ejercicio del derecho de acceso por parte del afectado.

7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

Artículo 5. Derecho de información en la recogida de datos.
1. Los afectados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a. De la existencia de un fichero automatizado de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
b. Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
c. De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
d. De la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación.
e. De la identidad y dirección del responsable del fichero.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.

3. No será necesaria la información a que se refiere el apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

Artículo 6. Consentimiento del afectado.
1. El tratamiento automatizado de los datos de carácter personal requerirá el consentimiento del afectado, salvo que la Ley disponga otra cosa.

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias, ni cuando se refieran a personas vinculadas por una relación negocial, una relación laboral, una relación administrativa o un contrato y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.

3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuya efectos retroactivos.

Artículo 7. Datos especialmente protegidos.
1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.

Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.

2. Sólo con consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento automatizado los datos de carácter personal que revelen la ideología, religión y creencias.

3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados automatizadamente y cedidos cuando por razones de interés general así lo disponga una Ley o el afectado consienta expresamente.

4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, religión, creencias, origen racial o vida sexual.

5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros automatizados de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

Artículo 8. Datos relativos a la salud.
Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento automatizado de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en los artículos 8, 10, 23 y 61 de la Ley 14/1986, de 25 de abril, General de Sanidad ; 85.5, 96 y 98 de la Ley 25/1990, de 20 de diciembre, del Medicamento; artículos 2, 3 y 4 de la Ley Orgánica 3/1986, de 14 de abril, de medidas especiales en materia de Salud Pública, y demás Leyes sanitarias.

Artículo 9. Seguridad de los datos.
1. El responsable del fichero deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros automatizados que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros automatizados y las personas que intervengan en el tratamiento automatizado de los datos a que se refiere el artículo 7 de esta Ley.

Artículo 10. Deber de secreto.
El responsable del fichero automatizado y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero automatizado o, en su caso, con el responsable del mismo.

Artículo 11. Cesión de datos.
1. Los datos de carácter personal objeto del tratamiento automatizado sólo podrán ser cedidos para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del afectado.

2. El consentimiento exigido en el apartado anterior no será preciso:

a. Cuando una Ley prevea otra cosa.
b. Cuando se trate de datos recogidos de fuentes accesibles al público.
c. Cuando el establecimiento del fichero automatizado responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho fichero con ficheros de terceros. En este caso la cesión sólo será legítima en cuanto se limite a la finalidad que la justifique.
d. Cuando la cesión que deba efectuarse tenga por destinatario el Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales, en el ejercicio de las funciones que tienen atribuidas.
e. Cuando la cesión se produzca entre las Administraciones Públicas en los supuestos previstos en el artículo 19.
f. Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero automatizado o para realizar los estudios epidemiológicos en los términos establecidos en el artículo 8 de la Ley 14/1986, de 25 de abril, General de Sanidad.

3. Será nulo el consentimiento cuando no recaiga sobre un cesionario determinado o determinable, o si no constase con claridad la finalidad de la cesión que se consiente.

4. El consentimiento para la cesión de datos de carácter personal tiene también un carácter de revocable.

5. El cesionario de los datos de carácter personal se obliga, por el solo hecho de la cesión, a la observancia de las disposiciones de la presente Ley.

6. Si la cesión se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

TÍTULO III.
DERECHOS DE LAS PERSONAS

Artículo 12. Impugnación de valoraciones basadas exclusivamente en datos automatizados.
El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento cuyo único fundamento sea un tratamiento automatizado de datos de carácter personal que ofrezca una definición de sus características o personalidad.

Artículo 13. Derecho de información.
Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de ficheros automatizados de datos de carácter personal, sus finalidades y la identidad del responsable del fichero. El Registro General será de consulta pública y gratuita.

Artículo 14. Derecho de acceso.
1. El afectado tendrá derecho a solicitar y obtener información de sus datos de carácter personal incluidos en los ficheros automatizados.

2. La información podrá consistir en la mera consulta de los ficheros por medio de su visualización, o en la comunicación de los datos pertinentes mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos convencionales que requieran el uso de dispositivos mecánicos específicos.

3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que al afectado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes.

Artículo 15. Derecho de rectificación y cancelación.
1. Por vía reglamentaria se establecerá el plazo en que el responsable del fichero tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del afectado.

2. Los datos de carácter personal que resulten inexactos o incompletos serán rectificados y cancelados en su caso.

3. Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá notificar la rectificación o cancelación efectuada al cesionario.

4. La cancelación no procederá cuando pudiese causar un perjuicio a intereses legítimos del afectado o de terceros o cuando existiese una obligación de conservar los datos.

5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del fichero y el afectado.

Artículo 16. Procedimiento de acceso.
1. El procedimiento para ejercitar el derecho de acceso, así como el de rectificación y cancelación será establecido reglamentariamente.

2. No se exigirá contraprestación alguna por la rectificación o cancelación de los datos de carácter personal inexactos.

Artículo 17. Tutela de los derechos y derecho de indemnización.
1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los afectados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine.

2. Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo.

3. Los afectados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable del fichero, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.

4. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas.

5. En el caso de los ficheros de titularidad privada la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

TÍTULO IV.
DISPOSICIONES SECTORIALES
CAPÍTULO I.
FICHEROS DE TITULARIDAD PÚBLICA

Artículo 18. Creación, modificación o supresión.
1. La creación, modificación o supresión de los ficheros automatizados de las Administraciones Públicas sólo podrán hacerse por medio de disposición general publicada en el *Boletín Oficial del Estado* o diario oficial correspondiente.

2. Las disposiciones de creación o de modificación de los ficheros deberán indicar:

a. La finalidad del fichero y los usos previstos para el mismo.
b. Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.
c. El procedimiento de recogida de los datos de carácter personal.
d. La estructura básica del fichero automatizado y la descripción de los tipos de datos de carácter personal incluidos en el mismo.
e. Las cesiones de datos de carácter personal que, en su caso, se prevean.
f. Los órganos de la Administración responsables del fichero automatizado.
g. Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación y cancelación.

3. En las disposiciones que se dicten para la supresión de los ficheros automatizados se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción.

Artículo 19. Cesión de datos entre Administraciones Públicas.
1. Los datos de carácter personal recogidos o elaborados por las Administraciones Públicas para el desempeño de sus atribuciones no serán cedidos a otras Administraciones Públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la cesión hubiese sido prevista por las disposiciones de creación del fichero o por disposición posterior de igual o superior rango que regule su uso.

2. Podrán, en todo caso, ser objeto de cesión los datos de carácter personal que una Administración Pública obtenga o elabore con destino a otra.

3. No obstante lo establecido en el artículo 11.2.b) la cesión de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una Ley prevea otra cosa.

Artículo 20. Ficheros de las Fuerzas y Cuerpos de Seguridad.
1. Los ficheros automatizados creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley.

2. La recogida y tratamiento automatizado para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas, están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías, en función de su grado de fiabilidad.

3. La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta.

4. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

A estos efectos se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

Artículo 21. Excepciones a los derechos de acceso, rectificación y cancelación.

1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior podrán denegar el acceso, la rectificación o la cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

2. Los responsables de los ficheros de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

3. El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores, podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del Organismo competente de cada Comunidad Autónoma en el caso de ficheros automatizados mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones Tributarias Autonómicas, quien deberá asegurarse de la procedencia o improcedencia de la denegación.

Artículo 22. Otras excepciones a los derechos de los afectados.

1. Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones Públicas o cuando afecte a la Defensa Nacional, a la Seguridad pública o a la persecución de infracciones penales o administrativas.

2. Lo dispuesto en el artículo 14 y en el apartado 1 del artículo 15 no será de aplicación si, ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante razones de interés público o ante intereses de terceros más dignos de protección. Si el órgano administrativo responsable del fichero automatizado invocase lo dispuesto en este apartado, dictará resolución motivada e instruirá al afectado del derecho que le asiste a poner la negativa en conocimiento del Director de la Agencia de Protección de Datos o, en su caso, del órgano equivalente de las Comunidades Autónomas.

CAPÍTULO II.
FICHEROS DE TITULARIDAD PRIVADA

Artículo 23. Creación.
Podrán crearse ficheros automatizados de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que esta Ley establece para la protección de las personas.

Artículo 24. Notificación e inscripción registral.
1. Toda persona o entidad que proceda a la creación de ficheros automatizados de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos.

2. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad y las cesiones de datos de carácter personal que se prevean realizar.

3. Deberán comunicarse a la Agencia de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación.

4. El Registro General de Protección de Datos inscribirá el fichero automatizado si la notificación se ajusta a los requisitos exigibles.

En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación.

5. Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos.

Artículo 25. Comunicación de la cesión de datos.
1. El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando asimismo la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario.

2. La obligación establecida en el apartado anterior no existirá en el supuesto previsto en los apartados 2, letras c), d) y e), y 6 del artículo 11 ni cuando la cesión venga impuesta por Ley.

Artículo 26. Datos sobre abonados a servicios de telecomunicación.
Los números de los teléfonos y demás servicios de telecomunicación, junto con otros datos complementarios, podrán figurar en los repertorios de abonados de acceso al público, pero el afectado podrá exigir su exclusión.

Artículo 27. Prestación de servicios de tratamiento automatizado de datos de carácter personal.
1. Quienes, por cuenta de terceros, presten servicios de tratamiento automatizado de datos de carácter personal no podrán aplicar o utilizar los obtenidos con fin distinto al que figure en el contrato de servicios, ni cederlos, ni siquiera para su conservación, a otras personas.

2. Una vez cumplida la prestación contractual, los datos de carácter personal tratados deberán ser destruidos, salvo que medie autorización expresa de aquél por cuenta de quien se prestan tales servicios, porque razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se podrán almacenar con las debidas condiciones de seguridad por un período de cinco años.

Artículo 28. Prestación de servicios de información sobre solvencia patrimonial y crédito.
1. Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito sólo podrán tratar automatizadamente datos de carácter personal obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el afectado o con su consentimiento. Podrán tratarse, igualmente, datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés.

En estos casos se notificará a los afectados respecto de los que hayan registrado datos de carácter personal en ficheros automatizados, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos y se les informará de su derecho a recabar información de la totalidad de ellos, en los términos establecidos por la presente Ley.

2. Cuando el afectado lo solicite, el responsable del fichero le comunicará los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y dirección del cesionario.

3. Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los afectados y que no se refieran, cuando sean adversos, a más de seis años.

Artículo 29. Ficheros con fines de publicidad.
1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad o venta directa y otras actividades análogas, utilizarán listas tratadas automáticamente de nombres y direcciones u otros datos personales, cuando los mismos figuren en documentos accesibles al público o cuando hayan sido facilitados por los propios afectados u obtenidos con su consentimiento.

2. Los afectados tendrán derecho a conocer el origen de sus datos de carácter personal, así como a ser dados de baja de forma inmediata del fichero automatizado, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.

Artículo 30. Ficheros relativos a encuestas o investigaciones.
1. Sólo se utilizarán de forma automatizada datos de carácter personal en las encuestas de opinión, trabajos de prospección de mercados, investigación científica o médica y actividades análogas, si el afectado hubiera prestado libremente su consentimiento a tal efecto.

2. Los datos de carácter personal tratados automáticamente con ocasión de tales actividades no podrán ser utilizados con finalidad distinta ni cedidos de forma que puedan ser puestos en relación con una persona concreta.

Artículo 31. Códigos tipo.
1. Mediante acuerdos sectoriales o decisiones de empresa, los responsables de ficheros de titularidad privada podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto de los principios y disposiciones de la presente Ley y sus normas de desarrollo.

Los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación.

En el supuesto de que tales reglas o estándares no se incorporaran directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél.

2. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos, que podrá denegar la inscripción cuando considere que no se ajustan a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el Director de la Agencia de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas.

TÍTULO V.
MOVIMIENTO INTERNACIONAL DE DATOS

Artículo 32. Norma general.

No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento automatizado o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.

Artículo 33. Excepciones.
Lo dispuesto en el artículo anterior no será de aplicación:

a. Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de Tratados o Convenios en los que sea parte España.
b. Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.
c. Cuando la misma tenga por objeto el intercambio de datos de carácter médico entre facultativos o instituciones sanitarias y así lo exija el tratamiento del afectado, o la investigación epidemiológica de enfermedades o brotes epidémicos.
d. Cuando se refiera a transferencias dinerarias conforme a su legislación específica.

TÍTULO VI.
AGENCIA DE PROTECCIÓN DE DATOS

Artículo 34. Naturaleza y régimen jurídico.
1. Se crea la Agencia de Protección de Datos.

2. La Agencia de Protección de Datos es un Ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio que será aprobado por el Gobierno, así como por aquellas disposiciones que le sean aplicables en virtud del artículo 6.5 de la Ley General Presupuestaria.

3. En el ejercicio de sus funciones públicas, y en defecto de lo que dispongan la presente Ley y sus disposiciones de desarrollo, la Agencia de Protección de Datos actuará de conformidad con la Ley de Procedimiento Administrativo. En sus adquisiciones patrimoniales y contratación estará sujeta al Derecho privado.

4. Los puestos de trabajo de los órganos y servicios que integren la Agencia de Protección de Datos serán desempeñados por funcionarios de las Administraciones Públicas y por personal contratado al efecto, según la naturaleza de las funciones asignadas a cada puesto de trabajo. Este personal está obligado a guardar secreto de los datos de carácter personal de que conozca en el desarrollo de su función.

5. La Agencia de Protección de Datos contará, para el cumplimiento de sus fines, con los siguientes bienes y medios económicos:

a. Las asignaciones que se establezcan anualmente con cargo a los Presupuestos Generales del Estado.
b. Los bienes y valores que constituyan su patrimonio, así como los productos y rentas del mismo.
c. Cualesquiera otros que legalmente puedan serle atribuidos.

6. La Agencia de Protección de Datos elaborará y aprobará con carácter anual el correspondiente anteproyecto de presupuesto y lo remitirá al Gobierno para que sea integrado, con la debida independencia, en los Presupuestos Generales del Estado.

Artículo 35. El Director.
1. El Director de la Agencia de Protección de Datos dirige la Agencia y ostenta su representación. Será nombrado, de entre quienes componen el Consejo Consultivo, mediante Real Decreto, por un período de cuatro años.

2. Ejercerá sus funciones con plena independencia y objetividad y no estará sujeto a instrucción alguna en el desempeño de aquéllas.

3. El Director de la Agencia de Protección de Datos sólo cesará antes de la expiración del período a que se refiere el apartado 1 a petición propia o por separación acordada por el Gobierno, previa instrucción de expediente, en el que necesariamente serán oídos los restantes miembros del Consejo Consultivo, por incumplimiento grave de sus obligaciones, incapacidad sobrevenida para el ejercicio de su función, incompatibilidad o condena por delito doloso.

4. El Director de la Agencia de Protección de Datos tendrá la consideración de Alto Cargo.

Artículo 36. Funciones.

Son funciones de la Agencia de Protección de Datos:

a. Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación y cancelación de datos.
b. Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias.
c. Dictar, en su caso y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos automatizados a los principios de la presente Ley.
d. Atender las peticiones y reclamaciones formuladas por las personas afectadas.
e. Proporcionar información a las personas acerca de sus derechos en materia de tratamiento automatizado de los datos de carácter personal.
f. Ordenar la cesación de los tratamientos de datos de carácter personal y la cancelación de los ficheros, cuando no se ajusten a las disposiciones de la presente Ley.
g. Ejercer la potestad sancionadora en los términos previstos por el Título VII de la presente Ley.
h. Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley.
i. Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.
j. Velar por la publicidad de la existencia de los ficheros automatizados de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.
k. Redactar una memoria anual y remitirla al Ministerio de Justicia.
l. Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.
m. Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 45.
n. Cuantas otras le sean atribuidas por normas legales o reglamentarias.

Artículo 37. Consejo Consultivo.

El Director de la Agencia de Protección de Datos estará asesorado por un Consejo Consultivo compuesto por los siguientes miembros:

- Un Diputado, propuesto por el Congreso de los Diputados.
- Un Senador, propuesto por la correspondiente Cámara.
- Un representante de la Administración Central, designado por el Gobierno.
- Un representante de la Administración Local, propuesto por la Federación Española de Municipios y Provincias.
- Un miembro de la Real Academia de la Historia, propuesto por la misma.
- Un experto en la materia, propuesto por el Consejo Superior de Universidades.
- Un representante de los usuarios y consumidores, seleccionado del modo que se prevea reglamentariamente.
- Un representante de las Comunidades Autónomas, cuya propuesta se realizará a través del procedimiento que se establezca en las disposiciones de desarrollo de esta Ley.
- Un representante del sector de ficheros privados, para cuya propuesta se seguirá el procedimiento que se regule reglamentariamente.
- El funcionamiento del Consejo Consultivo se regirá por las normas reglamentarias que al efecto se establezcan.

Artículo 38. El Registro General de Protección de Datos.
1. Se crea el Registro General de Protección de Datos como órgano integrado en la Agencia de Protección de Datos.

2. Serán objeto de inscripción en el Registro General de Protección de Datos:

a. Los ficheros automatizados de que sean titulares las Administraciones Públicas.
b. Los ficheros automatizados de titularidad privada.
c. Las autorizaciones a que se refiere la presente Ley.
d. Los códigos tipo a que se refiere el artículo 31 de la presente Ley.
e. Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación y cancelación.

3. Por vía reglamentaria se regulará el procedimiento de inscripción de los ficheros, tanto de titularidad pública como de titularidad privada, en el Registro General de Protección de Datos, el contenido de la inscripción, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes y demás extremos pertinentes.

Artículo 39. Potestad de inspección.
1. La Agencia de Protección de Datos podrá inspeccionar los ficheros a que hace referencia la presente Ley recabando cuantas informaciones precise para el cumplimiento de sus cometidos.

A tal efecto, podrá solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos accediendo a los locales donde se hallen instalados.

2. Los funcionarios que ejerzan la inspección a que se refiere el apartado anterior, tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

Estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.

Artículo 40. Órganos correspondientes de las Comunidades Autónomas.
1. Las funciones de la Agencia de Protección de Datos reguladas en el artículo 36, a excepción de las mencionadas en los apartados j), k) y l) y en los apartados f) y g) en lo que se refiere a las transferencias internacionales de datos, así como en los artículos 45 y 48, en relación con sus específicas competencias, serán ejercidas, cuando afecten a ficheros automatizados de datos de carácter personal creados o gestionados por las Comunidades Autónomas, por los órganos correspondientes de cada Comunidad, a los que se garantizará plena independencia y objetividad en el ejercicio de su cometido.

2. Las Comunidades Autónomas podrán crear y mantener sus propios registros de ficheros públicos para el ejercicio de las competencias que se les reconoce sobre los mismos, respecto de los archivos informatizados de datos personales cuyos titulares sean los órganos de las respectivas Comunidades Autónomas o de sus Territorios Históricos.

3. El Director de la Agencia de Protección de Datos podrá convocar regularmente a los órganos correspondientes de las Comunidades Autónomas a efectos de cooperación institucional y coordinación de criterios o procedimientos de actuación. El Director de la Agencia de Protección de Datos y los órganos correspondientes de las Comunidades Autónomas podrán solicitarse mutuamente la información necesaria para el cumplimiento de sus funciones.

Artículo 41. Ficheros de las Comunidades Autónomas en materias de su exclusiva competencia.
1. Cuando el Director de la Agencia de Protección de Datos constate que el mantenimiento o uso de un determinado fichero automatizado de las Comunidades Autónomas contraviene algún precepto de esta Ley en materia de su exclusiva competencia, podrá requerir a la Administración correspondiente para que adopte las medidas correctoras que determine en el plazo que expresamente se fije en el requerimiento.

2. Si la Administración Pública correspondiente no cumpliera el requerimiento formulado, el Director de la Agencia de Protección de Datos podrá impugnar la resolución adoptada por aquella Administración.

TÍTULO VII.
INFRACCIONES Y SANCIONES

Artículo 42. Responsables.
1. Los responsables de los ficheros estarán sujetos al régimen sancionador establecido en la presente Ley.

2. Cuando se trate de ficheros de los que sean responsables las Administraciones Públicas se estará, en cuanto al procedimiento y a las sanciones, a lo dispuesto en el artículo 45, apartado 2.

Artículo 43. Tipos de infracciones.
1. Las infracciones se calificarán como leves, graves o muy graves.

2. Son infracciones leves:

a. No proceder, de oficio o a solicitud de las personas o instituciones legalmente habilitadas para ello, a la rectificación o cancelación de los errores, lagunas o inexactitudes de carácter formal de los ficheros.
b. No cumplir las instrucciones dictadas por el Director de la Agencia de Protección de Datos, o no proporcionar la información que éste solicite en relación a aspectos no sustantivos de la protección de datos.
c. No conservar actualizados los datos de carácter personal que se mantengan en ficheros automatizados.
d. Cualquiera otra que afecte a cuestiones meramente formales o documentales y que no constituya infracción grave o muy grave.

3. Son infracciones graves:

a. Proceder a la creación de ficheros automatizados de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el *Boletín Oficial del Estado* o diario oficial correspondiente.
b. Proceder a la creación de ficheros automatizados de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.

c. Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible, o sin proporcionarles la información que señala el artículo 5 de la presente Ley.
d. Tratar de forma automatizada los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidas en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.
e. El impedimento o la obstaculización del ejercicio del derecho de acceso y la negativa a facilitar la información que sea solicitada.
f. Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara.
g. La vulneración del deber de guardar secreto, cuando no constituya infracción muy grave.
h. Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria, se determinen.
i. No remitir a la Agencia de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos.
j. La obstrucción al ejercicio de la función inspectora.

4. Son infracciones muy graves:

a. La recogida de datos en forma engañosa y fraudulenta.
b. La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.
c. Recabar y tratar de forma automatizada los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado; recabar y tratar de forma automatizada los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una Ley o el afectado no haya consentido expresamente o violentar la prohibición contenida en el apartado 4 del artículo 7.
d. No cesar en el uso ilegítimo de los tratamientos automatizados de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia de Protección de Datos o por las personas titulares del derecho de acceso.
e. La transferencia, temporal o definitiva, de datos de carácter personal que hayan sido objeto de tratamiento automatizado o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos.
f. Tratar de forma automatizada los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.
g. La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7.

Artículo 44. Tipos de sanciones.

1. Las infracciones leves serán sancionadas con multa de 100.000 a 10.000.000 de pesetas.

2. Las infracciones graves serán sancionadas con multa de 10.000.001 pesetas a 50.000.000 de pesetas.

3. Las infracciones muy graves serán sancionadas con multa de 50.000.001 pesetas a 100.000.000 de pesetas.

4. La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad y a la reincidencia.

5. El Gobierno actualizará periódicamente la cuantía de las sanciones de acuerdo con las variaciones que experimenten los índices de precios.

Artículo 45. Infracciones de las Administraciones Públicas.
1. Cuando las infracciones a que se refiere el artículo 43 fuesen cometidas en ficheros de los que sean responsables las Administraciones Públicas, el Director de la Agencia de Protección de Datos dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.

2. El Director de la Agencia podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones Públicas.

3. Se deberán comunicar a la Agencia las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

4. El Director de la Agencia comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores.

Artículo 46. Prescripción.
1. Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves al año.

2. El plazo de prescripción comenzará a contarse desde el día en que la infracción se hubiera cometido.

3. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reanudándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causa no imputable al presunto infractor.

4. Las sanciones impuestas por faltas muy graves prescribirán a los tres años, las impuestas por faltas graves a los dos años y las impuestas por faltas leves al año.

5. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquél en que adquiera firmeza la resolución por la que se impone la sanción.

6. La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

Artículo 47. Procedimiento sancionador.
1. Por vía reglamentaria se establecerá el procedimiento a seguir para la determinación de las infracciones y la imposición de las sanciones a que hace referencia el presente Título.

2. Contra las resoluciones de la Agencia de Protección de Datos, u órgano correspondiente de la Comunidad Autónoma, procederá recurso contencioso-administrativo.

Artículo 48. Potestad de inmovilización de ficheros.
En los supuestos, constitutivos de infracción muy grave, de utilización o cesión ilícita de los datos de carácter personal en que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el Director de la Agencia de Protección de Datos podrá, además de ejercer la potestad sancionadora, requerir a los responsables de ficheros automatizados de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos. Si el requerimiento fuera desatendido la Agencia de Protección de Datos podrá, mediante resolución motivada, inmovilizar tales ficheros automatizados a los solos efectos de restaurar los derechos de las personas afectadas.

DISPOSICIÓN ADICIONAL PRIMERA. Exclusión de la aplicación de los Títulos VI y VII.
Lo dispuesto en los Títulos VI y VII no es de aplicación a los ficheros automatizados de los que sean titulares las Cortes Generales, el Defensor del Pueblo, el Tribunal de Cuentas, el Consejo General del Poder Judicial y el Tribunal Constitucional.

DISPOSICIÓN ADICIONAL SEGUNDA. Ficheros existentes con anterioridad a la entrada en vigor de la Ley.

1. Dentro del año siguiente a la entrada en vigor de la presente Ley Orgánica deberán ser comunicados a la Agencia de Protección de Datos los ficheros y tratamientos automatizados de datos de carácter personal existentes con anterioridad y comprendidos dentro de su ámbito de aplicación.

2. Dentro del año siguiente a la entrada en vigor de la presente Ley Orgánica, las Administraciones Públicas responsables de ficheros automatizados ya existentes deberán adoptar una disposición de regulación del fichero o adaptar la que existiera.

Estos plazos se prorrogaron por seis meses, por Real Decreto-Ley 20/1993, de 22 de diciembre.

DISPOSICIÓN ADICIONAL TERCERA. Competencias del Defensor del Pueblo.
Lo dispuesto en la presente Ley Orgánica se entiende sin perjuicio de las competencias del Defensor del Pueblo y de los órganos análogos de las Comunidades Autónomas.

DISPOSICIÓN TRANSITORIA ÚNICA. Adaptaciones complejas a lo establecido en la Ley.
Cuando la adaptación de los ficheros automatizados a los principios y derechos establecidos en la presente Ley requiera la adopción de medidas técnicas complejas o el tratamiento de un gran volumen de datos, tales adaptaciones y tratamientos deberán realizarse en el plazo de un año desde la entrada en vigor de la Ley, sin perjuicio del cumplimiento, en todo lo demás, de las disposiciones de la misma.

DISPOSICIÓN DEROGATORIA ÚNICA. Derogación de la disposición transitoria primera de la Ley Orgánica 1/1982.
Queda derogada la disposición transitoria primera de la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al honor, a la intimidad personal y familiar y a la propia imagen.

DISPOSICIÓN FINAL PRIMERA. Habilitación de desarrollo reglamentario.
El Gobierno dictará las disposiciones necesarias para la aplicación y desarrollo de la presente Ley, y para regular la estructura orgánica de la Agencia de Protección de Datos.

DISPOSICIÓN FINAL SEGUNDA. Extensión de la aplicación de la Ley a ficheros convencionales.
El Gobierno, previo informe del Director de la Agencia de Protección de Datos, podrá extender la aplicación de la presente Ley, con las modificaciones y adaptaciones que fuesen necesarias, a los ficheros que contengan datos almacenados en forma convencional y que no hayan sido sometidos todavía o no estén destinados a ser sometidos a tratamiento automatizado.

DISPOSICIÓN FINAL TERCERA. Preceptos con carácter de Ley ordinaria.
Los artículos 18, 19, 23, 26, 27, 28, 29, 30, 31, los Títulos VI y VII, las disposiciones adicionales primera y segunda y la disposición final primera tienen carácter de Ley ordinaria.

DISPOSICIÓN FINAL CUARTA. Entrada en vigor.
La presente Ley Orgánica entrará en vigor a los tres meses de su publicación en el *Boletín Oficial del Estado*.

Por tanto, mando a todos los españoles, particulares y autoridades que guarden y hagan guardar esta Ley Orgánica.

Madrid, 29 de octubre de 1992.

ANNEX 2

Reial Decret 1332/1994, de 20 de juny de 1994

INFORMÀTICA. Desenvolupament determinats aspectes de la Llei Orgànica 5/1992

Real Decreto 1332/94 de 20 de junio, por el que se desarrollan algunos preceptos de la Ley Orgánica.

MINISTERIO DE JUSTICIA E INTERIOR

REAL DECRETO 1332/1994, de 20 de junio, por el que se desarrolla determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.

La Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, habilita al Gobierno, en su disposición final primera, para dictar las disposiciones necesarias para la aplicación y desarrollo de la referida Ley, a la par que contiene en diferentes preceptos unos concretos mandatos al Gobierno para que por vía reglamentaria regule determinados aspectos, en su mayoría de orden procedimental, referentes al ejercicio de los derechos de acceso, rectificación y cancelación, a la forma de reclamar ante la Agencia de Protección de Datos por actuaciones contrarias a la
Ley, a la notificación e inscripción de los ficheros automatizados de datos y al procedimiento para la determinación de las infracciones y la imposición de las sanciones.

En uso de dicha habilitación, y cumplimentando el mandato conferido en los artículos 15.1, 16.1, 17.1, 24.2, 38.3, y 47.1 de la citada Ley Orgánica, se dicta la presente disposición.
En su virtud, a propuesta del Ministro de Justicia e Interior, con la aprobación del Ministro para las Administraciones Públicas, previo informe de la Agencia de Protección de Datos, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 17 de junio de 1994,

DISPONGO:

CAPITULO I

Disposiciones Generales

Artículo 1. Definiciones.

A efectos de lo dispuesto en el presente Real Decreto se entenderá por:

Bloqueo de datos: la identificación y reserva de datos con el fin de impedir su tratamiento.
Cesión de datos: toda obtención de datos resultante de la consulta de un fichero, su interconexión con otros ficheros y la comunicación de datos realizada por una persona distinta de la afectada.
Datos accesibles al público: los datos que se encuentran a disposición del público en general, no impedida por cualquier norma limitativa, y están recogidos en medios tales como censos, anuarios, bases de datos públicas, repertorios de jurisprudencia, archivos de prensa, repertorios telefónicos o análogos, así como los datos publicados en forma de listas de personas pertenecientes a grupos profesionales que contengan únicamente los nombres, títulos, profesión, actividad, grados académicos, dirección e indicación de su
pertenencia al grupo.
Datos de carácter personal: toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable.

Identificación del afectado: cualquier elemento que permita determinar directa o indirectamente la identidad física, fisiológica, psíquica, económica, cultural o social de la persona física afectada.

Transferencia de datos: el transporte de datos entre sistemas informáticos por cualquier medio de transmisión, así como el transporte de soportes de datos por correo o por cualquier otro medio convencional.

Artículo 2. Regímenes especiales.

De conformidad con lo dispuesto en el artículo 2.3 de la Ley Orgánica 5/1992 se regirán por las disposiciones que, en materia de protección de datos, contienen las leyes y reglamentos respectivos, los ficheros siguientes:

El censo electoral, el fichero de electores y ficheros complementarios, regulados por la legislación de régimen electoral.
Los ficheros automatizados creados con fines exclusivamente estadísticos y amparados en cuanto a protección de datos por la normativa reguladora de la función estadística pública, sin perjuicio de lo prevenido en el artículo 36, m) de la Ley Orgánica 5/1992.
Los ficheros automatizados de estado civil, amparados por la Ley del Registro Civil y su Reglamento.
Los ficheros automatizados de antecedentes penales.
Los ficheros automatizados creados o gestionados al amparo de la normativa sobre protección de materias clasificadas.
Los ficheros automatizados cuyo objeto sea el almacenamiento de los datos contenidos en los informes personales regulados en el artículo 68 de la Ley 17/1989, de 19 de julio, reguladora del Régimen del personal militar profesional.
La remisión al Derecho nacional, contenida en los Títulos IV y VI del Convenio de 19 de junio de 1990, de aplicación del Acuerdo de Schengen de 14 de junio de 1985, así como cualquier otra remisión hecha a disposiciones nacionales de protección de datos personales contenida en convenios internacionales, se entenderá referida a la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, y a las disposiciones reglamentarias de desarrollo.

CAPITULO II

Transferencia internacional de datos

Artículo 3. Régimen de las transferencias.

Si la transferencia de los datos de carácter personal tuviera como destinatario un país que no proporciona un nivel de protección equiparable al que presta la Ley Orgánica 5/1992, el Director de la Agencia de Protección de Datos autorizará la transferencia de los mismos, siempre que el cedente de los datos acredite haber cumplido lo dispuesto en los preceptos de la referida Ley y otorgue las garantías que al efecto le sean exigidas. A tal fin, la autorización deberá ser sometida al cumplimiento de las condiciones o cargas

modales que se consideren necesarias para que de la transferencia no se deriven perjuicios a los derechos de los afectados y se respeten los principios contenidos en el Título II de la Ley Orgánica 5/1992.

En caso de incumplimiento de los términos de la autorización el cedente y el cesionario de los datos responderán solidariamente a efectos de lo previsto en el artículo 17.3 de la Ley Orgánica 5/1992.

Artículo 4. Excepciones.

Se exceptúan, en todo caso, de la autorización previa del Director de la Agencia de Protección de Datos las transferencias de datos de carácter personal que resulten de la aplicación de tratados o convenios de los que sea parte España y, en particular:
Las transmisiones de datos registrados en ficheros creados por las Fuerzas y Cuerpos de Seguridad en función de una investigación concreta, hechas por conducto Interpola u otras vías previstas en convenios en los que España sea parte, cuando las necesidades de la investigación en curso exijan la transmisión a servicios policiales de otros Estados.
Las transmisiones de datos registrados en la parte nacional española del Sistema de Información Schengen, con destino a la unidad de apoyo del sistema, a los solos efectos de una investigación policial en curso que requiera la utilización de datos del sistema.
Las transmisiones de datos previstas en el sistema de intercambios de información contemplado en el Título VI del Tratado de la Unión Europea.

Las transmisiones de los datos registrados en los ficheros creados por las Administraciones tributarias, en favor de los demás Estados miembros de la Unión Europea o en favor de otros Estados terceros, en virtud de lo dispuesto en los convenios internacionales de asistencia mutua en materia tributaria.

Se exceptúan, asimismo, de la autorización previa del Director de la Agencia de Protección de Datos, cualquiera que sea el Estado destinatario de los datos, las transmisiones de datos que se efectúen para cumplimentar exhortas, cartas órdenes, comisiones rotatorias u otras peticiones de auxilio judicial internacional, y los demás supuestos previstos en el artículo 33 de la Ley Orgánica 5/1992.

CAPITULO III

Notificación e inscripción de ficheros

Artículo 5. Notificación de ficheros de titularidad pública.

Todo fichero de datos de carácter personal, de titularidad pública, será notificado a la Agencia de Protección de Datos por el órgano competente de la Administración responsable del fichero para su inscripción en el Registro General de Protección de Datos, mediante el traslado, a través del modelo normalizado que al efecto elabore la Agencia, de una copia de la disposición de creación del fichero.

Artículo 6. Notificación de ficheros de titularidad privada.

La persona o entidad que pretenda crear un fichero de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos mediante escrito o soporte informático en modelo normalizado que al efecto elabore la Agencia, en el que se especificarán los siguientes extremos:
Nombre, denominación o razón social, documento nacional de identidad o código de identificación fiscal, dirección y actividad u objeto social del responsable del fichero.
Ubicación del fichero.
Identificación de los datos que se pretendan tratar, individualizando los supuestos de datos especialmente protegidos.
Dirección de la oficina o dependencia en la cual puedan ejercerse los derechos de acceso, rectificación y cancelación.
Origen o procedencia de los datos.
Finalidad del fichero.
Cesiones de datos previstas.
Transferencias temporales o definitivas que se prevean realizar a otros países, con expresión de los mismos.
Destinatarios o usuarios previstos para las cesiones o transferencias.
Sistemas de tratamiento automatizado que se vayan a utilizar.
Medidas de seguridad.

Artículo 7. Inscripción de los ficheros.

Los ficheros de titularidad pública serán inscritos de oficio por la Agencia de Protección de Datos, una vez haya recibido la copia de la disposición de creación del fichero.
El Director de la Agencia de Protección de Datos, a propuesta del Registro General de Protección de Datos, acordará la inscripción de los ficheros de titularidad privada si la notificación contuviera la información preceptiva y se cumplen las restantes exigencias legales, requiriendo, en caso contrario, al responsable del fichero para que la complete o subsane en el plazo de diez días, con indicación de que, si así no lo hiciera, se le tendrá por desistido de su petición, archivándose sin más trámite.

La inscripción contendrá, en el supuesto de ficheros de titularidad pública, las indicaciones previstas en el artículo 18.2 de la Ley Orgánica 5/1992, con especificación de la disposición general de creación y del diario oficial de su publicación, y, en el supuesto de ficheros de titularidad privada, los extremos relacionados en el artículo 6 del presente Real Decreto, con excepción de las medidas de seguridad.

La inscripción será notificada al responsable del fichero por el Registro General de Protección de Datos.

Artículo 8. Modificación y cancelación de la inscripción.

La modificación o, en su caso, cancelación de la inscripción de los ficheros de titularidad pública se producirá de oficio por la Agencia de Protección de Datos, previo traslado por el órgano de la Administración responsable del fichero de una copia de la disposición general que modifique o suprima aquél.

Cuando se trata de ficheros de titularidad privada, cualquier modificación posterior en el contenido de los extremos a que se refiere el artículo 6 del presente Real Decreto se comunicará, a efectos de inscripción, en su caso, a la Agencia de Protección de Datos dentro del mes siguiente a la fecha en que aquélla se hubiera producido. En igual plazo se comunicará la decisión de supresión del fichero a efectos de la cancelación del correspondiente asiento de inscripción.

Artículo 9. Inscripción y publicidad de los códigos tipo.

Los códigos tipo se depositarán, para su inscripción, en el Registro General de Protección de Datos.

El Director de la Agencia de Protección de Datos podrá denegar la inscripción si el código tipo no se ajusta a las disposiciones de la Ley Orgánica 5/1992 y del presente Real Decreto, sin perjuicio de requerir a los solicitantes para que subsanen las deficiencias.
Los particulares podrán obtener copias de los códigos tipo depositados e inscritos en el Registro General de Protección de Datos.

En caso de incumplimiento de las normas contenidas en los códigos tipo se estará a lo dispuesto al efecto en los acuerdos o decisiones que los formulen.

Artículo 10. Recursos.

Contra las resoluciones del Director de la Agencia de Protección de Da tos relativas a la inscripción o, en su caso, a la modificación o cancelación de la inscripción de un fichero o código tipo, procederá el recurso contencioso-administrativo.

CAPITULO IV

Ejercicio y tutela de los derechos del afectado

Artículo 11. Carácter personal de los derechos.

Los derechos de acceso a los ficheros automatizados, así como los de rectificación y cancelación de datos son personalísimos y serán ejercidos por el afectado frente al responsable del fichero, sin otras limitaciones que las que prevén la Ley Orgánica 5/1992 y el presente Real Decreto.

Podrá, no obstante, actuar el representante legal del afectado cuando éste se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de los mismos.

Artículo 12. Derecho de acceso.

El derecho de acceso se ejercerá mediante petición o solicitud dirigida al responsable del fichero, formulada por cualquier medio que garantice la identificación del afectado y en la que conste el fichero o ficheros a consultar.

El afectado podrá optar por uno o varios de los siguientes sistemas de consulta del fichero, siempre que la configuración e implantación material del fichero lo permita:
Visualización en pantalla.
Escrito, copia o fotocopia remitida por correo.
Telecopia.
Cualquier otro procedimiento que sea adecuado a la configuración e implantación material del fichero, ofrecido por el responsable del mismo.

El responsable del fichero resolverá entre la petición de acceso en el plazo máximo de un mes, a contar de la recepción de la solicitud. Transcurrido este plazo sin que de forma expresa se responda a la petición de acceso, éste podrá entenderse desestimada a los efectos de la interposición de la reclamación prevista en el artículo 17.1 de la Ley Orgánica 5/1992.
Si la resolución fuera estimatoria, el acceso se hará efectivo en el plazo de los diez días siguientes a la notificación de aquélla.

Artículo 13. Contenido de la información.

La información, cualquiera que sea el soporte en que fuere facilitada, se dará en forma legible e inteligible, previa transcripción en claro de los datos del fichero, en su caso.
La información comprenderá los datos de base del afectado y los resultantes de cualquier elaboración o proceso informático, así como el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos.

Artículo 14. Denegación del acceso.

Se denegará el acceso a los datos de carácter personal registrados en ficheros de titularidad pública cuando se dé alguno de los supuestos contemplados en los artículos 14.3, 21.1 y 2 y 22.2 de la Ley Orgánica 5/1992.
Tratándose de datos de carácter personal registrados en ficheros de titularidad privada, únicamente se denegará el acceso cuando la solicitud sea formulada por persona distinta del afectado.

Artículo 15. Derecho de rectificación o cancelación.

Cuando el acceso a los ficheros revelare que los datos del afectado son inexactos o incompletos, inadecuados o excesivos, podrá éste solicitar del responsable del fichero la rectificación o, en su caso, cancelación de los mismos.

No obstante, cuando se trate de datos que reflejen hechos constatados en un procedimiento administrativo, aquéllos se considerarán exactos siempre que coincidan con éste.
La rectificación o cancelación se hará efectiva por el responsable del fichero dentro de los cinco días siguientes al de la recepción de la solicitud. En idéntico plazo se efectuará la notificación a que se refiere el artículo 15.3 de la Ley Orgánica 5/1992.

En el supuesto de que el responsable del fichero considere que no procede acceder a lo solicitado por el afectado, se lo comunicará motivadamente y dentro del plazo señalado en el apartado anterior, a fin de que por éste se pueda hacer uso de la reclamación prevista en el artículo 17.1 de la Ley Orgánica 5/1992.
Transcurrido el plazo previsto en el apartado 2 sin que de forma expresa se responda a la solicitud de rectificación o cancelación, ésta podrá entenderse desestimada a los efectos de la interposición de la reclamación que corresponda.

Artículo 16. Bloqueo de los datos.

En los casos en que, siendo procedente la cancelación de los datos, no sea posible su extinción física, tanto por razones técnicas como por causa del procedimiento o soporte utilizado, el responsable del fichero procederá al bloqueo de los datos, con el fin de impedir su ulterior proceso o utilización.

Se exceptúa, no obstante, el supuesto de que se demuestre que los datos han sido recogidos o registrados por medios fraudulentos, desleales o ilícitos, en cuyo caso la cancelación de los mismos comportará siempre la destrucción del soporte en el que aquéllos figuren.
Contra la resolución por la que el responsable del fichero acuerde el bloqueo de los datos procederá reclamación ante el Director de la Agencia de Protección de Datos.

Artículo 17. Tutela de los derechos.

Las reclamaciones de los afectados ante la Agencia de Protección de Datos, a que se refiere el artículo 17.1 de la Ley Orgánica 5/1992, se sustanciarán en la forma prevista en el presente artículo.

El procedimiento se iniciará a instancia del afectado o afectados, expresando con claridad el contenido de su reclamación y de los preceptos de la Ley Orgánica 5/1992 que se consideran vulnerados.

Recibida la reclamación en la Agencia de Protección de Datos, se dará traslado de la misma al responsable del fichero, para que, en el plazo de quince días, formule las alegaciones que estime pertinentes.

Recibidas las alegaciones o transcurrido el plazo previsto en el apartado anterior, la Agencia de Protección de Datos, previos los informes, pruebas y otros actos de instrucción pertinentes, incluida la audiencia del afectado y nuevamente del responsable del fichero, resolverá sobre la reclamación formulada, dando traslado de la misma a los interesados.
Contra la resolución del Director procederá recurso contencioso-administrativo.

CAPITULO V

Procedimiento sancionador

Artículo 18. Iniciación e instrucción.

El procedimiento sancionador previsto en el artículo 47 de la Ley Orgánica 5/1992, se iniciará siempre de oficio, bien por propia iniciativa o en virtud de denuncia de un afectado o afectados, por acuerdo del Director de la Agencia de Protección de Datos, en el cual se designará instructor y, en su caso, secretario, con expresa indicación del régimen de recusación de los mismos.
En el referido acuerdo se identificará a la persona o personas presuntamente responsables y se concretarán los hechos imputados, con expresión de la infracción presuntamente cometida y de la sanción o sanciones que pudieran imponerse, así como de las medidas provisionales que, en su caso, se adopten.

El acuerdo de incoación del expediente se notificará al presunto responsable y en el mismo se informará a éste de su derecho a formular alegaciones y utilizar los medios de defensa procedentes y que la autoridad competente para imponer, en su caso, la sanción es el Director de la Agencia de Protección de Datos, con cita expresa del presente artículo y del artículo 36, g) en relación con el artículo 35, ambos de la Ley Orgánica 5/1992.

Dentro de los quince días siguientes a la notificación del acuerdo de incoación, el instructor ordenará, de oficio, la práctica de cuantas pruebas y actos de instrucción sean adecuados para esclarecer los hechos y determinar las responsabilidades susceptibles de sanción.
En idéntico plazo, el presunto responsable podrá formular las alegaciones y proponer las pruebas que considere convenientes.

Transcurrido el plazo previsto en el apartado anterior, el instructor acordará la práctica de las pruebas que estime pertinentes, a cuyo efecto concederá un plazo de treinta días, transcurrido el cual el expediente se pondrá de manifiesto al presunto responsable para que, en el plazo de quince días, formule alegaciones y aporte cuantos documentos estime de interés.

Artículo 19. Resolución.

Cumplimentados los trámites previstos en el artículo anterior, el instructor formulará propuesta de resolución motivada en la cual se fijarán de modo claro y preciso los hechos, se razonará, en su caso, la denegación y de la práctica probatoria propuesta por el presunto responsable, se valorarán jurídicamente aquéllos a fin de determinar la infracción cometida y se señalará la sanción a imponer, determinando su cuantía con arreglo a los criterios establecidos en el artículo 44.4 de la Ley Orgánica 5/1992, o bien, se propondrá la declaración de no existencia de responsabilidad.

La propuesta de resolución se notificará al presunto responsable para que, en el plazo de quince días, pueda formular nuevas alegaciones si lo considera oportuno.

Notificada la propuesta de resolución o expirado el plazo de alegaciones previsto en el apartado anterior, el instructor elevará el expediente completo al Director de la Agencia de Protección de Datos.

El Director podrá, antes de dictar resolución, ordenar al instructor la práctica de cuantas actuaciones considere necesarias, lo que se llevará a efecto en un plazo máximo de quince días.

La resolución, que se dictará dentro de los diez días siguientes, determinará con la necesaria precisión los hechos imputados, la infracción cometida, con expresión del precepto que la tipifique, el responsable de la misma y la sanción impuesta; o bien, la declaración de no existencia de responsabilidad. Contendrá, asimismo, la declaración pertinente en orden a las medidas provisionales adoptadas durante la tramitación del procedimiento.
La resolución se notificará al responsable con expresión de su derecho a interponer recurso contencioso-administrativo, el plazo de interposición, y el órgano ante el cual deba ser presentado.

Si el procedimiento se hubiera iniciado como consecuencia de denuncia de un afectado, la resolución deberá ser notificada al firmante de la misma.

Disposición adicional primera. Comunicación de ficheros preexistentes.
Los ficheros automatizados de datos de carácter personal que se hubiesen creado con posterioridad a la entrada en vigor de la Ley Orgánica 5/1992 y antes de la vigencia del presente Real Decreto se deberán comunicar a la Agencia de Protección de Datos antes del 31 de julio de 1994.

Disposición adicional segunda. Ficheros de las Comunidades Autónomas.
Corresponde a las Comunidades Autónomas, respecto de sus propios ficheros, la regulación del ejercicio y tutela de los derechos del afectado y del procedimiento sancionador en los términos y con los límites establecidos en la Ley Orgánica 5/1992 y de acuerdo con las normas del procedimiento administrador común.

Disposición adicional tercera. Ficheros de las Administraciones Tributarias.
Los ficheros creados por las Administraciones Tributarias para la gestión de los tributos que se les encomienden, se regirán por las disposiciones del presente Real Decreto y por las demás disposiciones reglamentarias que, en desarrollo y con sujeción a lo dispuesto en la Ley Orgánica 5/1992, específicamente se aprueben para los mismos.

Disposición final primera. Lista de países con equiparable protección.
Se faculta al Ministro de Justicia e Interior para que, previo informe del Director de la Agencia de Protección de Datos, apruebe la relación de países que, a efectos de lo dispuesto en el artículo 32 de la Ley Orgánica 5/1992, se entiende que proporcionan un nivel de protección equiparable al de dicha Ley.

Disposición final segunda. Entrada en vigor.
El presente Real Decreto entrará en vigor el día siguiente al de su publicación en el "Boletín Oficial del Estado".

Dado en Madrid a 20 de junio de 1994.
JUAN CARLOS R.
El Ministro de Justicia e Interior,
JUAN ALBERTO BELLOCH JULBE