ISRAEL: PROTECTION OF PRIVACY LAW 5741-1981

CHAPTER ONE: INFRINGEMENT OF PRIVACY

1. Prohibition of infringement of privacy

No person shall infringe the privacy of another without his consent.

2. What is infringement of privacy

Any of the following constitutes an infringement of privacy:

(1) Spying on or trailing a person in a manner likely to harass him, or any other harassment;
(2) listening in prohibited under any Law;
(3) photographing a person while he is in a private domain;
(4) publishing a person's photograph under circumstances, in which the publication is likely to humiliate him or to bring him into contempt;
(5) copying or using, without permission from the addressee or the writer, the contents of a letter or of any other writing not intended for publication, unless the writing is of historical value or fifteen years have passed since the time when it was written;
(6) using a person's name, appellation, picture or voice for profit;
(7) infringing an obligation of secrecy laid down by law in respect of a person's private affairs;
(8) infringing an obligation of secrecy laid down by explicit or implicit agreement in respect of a person's private affairs;
(9) using, or passing on to another, information on a person's private affairs, otherwise than for the purpose for which it was given;
(10) publishing or passing on anything that was obtained by way of an infringement of privacy under paragraphs (1) to (7) or (9);
(11) publishing any matter that relates to a person's intimate life, state of health or conduct in the private domain.

3. Definition of terms

In this Law

"person" does not - for purposes of sections 2,7,13,14 and 25 - include a body corporate;
"consent" - explicit or implied consent;
"holder, in connection with database" - a person, who has a database in his permanent possession and who is entitled to use it;
"publication" has the meaning it has in the Defamation (Prohibition) Law, 5725-1965
"photography" includes filming;
"use" includes disclosure, transfer and delivery.

4. Infringement of privacy - a civil wrong

An infringement of privacy is a civil wrong, and the provisions of the Civil Wrongs Ordinance (New Version) shall apply to it, subject to the provisions of this Ordinance.

5. Infringement of privacy - an offense

If a person willfully infringes the privacy of another in any of the ways stated in section 2 (1), (3) to (7) and (9) to (11), then he is liable to five years imprisonment.

6. Trifling act

No right to bring a civil or criminal action under this Law shall accrue through an infringement that has no real significance.

CHAPTER TWO: PROTCTION OF PRIVACY IN DATA BASE

7. Definition

In this Chapter and in Chapter Four -

"data security" - protection of the integrity of data, or protection of the data against exposure, use or copying, all when done without due permission;
"data base" - a collection of data, kept by magnetic or optical means and intended for computer processing, exclusive of -

(1) a collection for personal use other than for business purposes; or
(2) a collection that includes only names, addresses and ways of communicating, which by itself does not create any characterization that infringes on the privacy of the people whose names are included in it, or condition that neither the owner of the collection, nor a body corporate under his control owns an additional collection,

"information" - data on the personality, personal status, intimate affairs, state of health, economic position, vocational qualifications, opinions and beliefs of a person,
"sensitive information" -

(1) data on a person's personality, private family relations, state of health, economic condition, opinions and faith,
(2) information which the Minister of Justice - by order with approval by the Knesset Constitution, Law and Justice Committee - designated as sensitive information.

"data base manager" - the active manager of the body, which owns or holds a data base, or a person authorized for this person by the aforesaid manager;
"Registrar" - a person qualified to be appointed Magistrates Court judge, whom the Government appointed by, notice in Reshumot, to keep the "Register of Data Bases" (hereafter: Register) as said in section 12;

"integrity of information" - the identity of data in the data base to the source from which they were derived, without having been changed, delivered or destroyed with due permission.

Article One: Data Bases

8. Registration and use of data base

(a) No person shall manage or possess a data base that the must be registered under this section, unless one of the following holds true:

(1) the data base was registered in the Register;
(2) an application for registration of the data base was submitted and the provisions of section 10 (b1) are complied with,
(3) the data base must be registered under subsection (e) and the Registrar's instructions included permission to operate and keep the data until it is registered.

(b) No person shall use information in a data that must be registered under this section, except for the purposes for which the data base was set up.
(c) The obligation of registration in the Register falls on the owner of the data base, and the owner of the data base must register it if one of the following applies,

(1) the data base includes information about more than 10,000 persons;
(2) the data base includes sensitive information;
(3) the data base includes information about persons and the information was not provided to the data base by them, on their behalf or with their consent;
(4) the data base belongs to a public body, within its definition in section 23;
(5) the data base is used for direct mail, as said in section 17c.

(d) The provision of subsection (c) shall not apply to a data base which only includes information made public by lawful authority, or which was opened to public inspection by lawful authority.
(e) The Registrar may, for special reasons which shall be recorded, order hat the obligation to register be in effect for data bases that are exempt of the obligation to register under subsection (c) and (d); a said order shall be served on the owner of the data base, and in it the registrar shall spell out directions for the operation and maintenance of the data base until its registration; the owner of the data base may appeal against a decision of the Registrar under this subsection before the District Court within 30 days after he was served notice of the Registrar's decision.

9. Application for registration

(a) An application for registration of a data base shall be submitted to the Registrar.
(b) An application for registration of a base shall specify -

(1) the identities of the owner of the data base, of the person who holds possession of the data base, and their addresses in Israel;
(2) the purposes of setting up the data and the purposes for which the information is

intended;
(3) the types of information to be included in the data base;
(4) particulars on the transfer abroad of information;
(5) particulars on the constant receipt of information from a public body, as defined in section 23, the name of the public body that provides the information provided, exclusive of particulars delivered by consent of the persons who are subjects of the information.

(c) The Minster may-by regulations - prescribe further particulars to be stated in the application for registration.
(d) The owner or possessor of a data base shall notify the Registrar of every change in any of the particulars specified in subsection (b) or prescribed under subsection (c), and of the discontinuation of the operation of the data base.

10. Power of Registrar

(a) When an application for registration of a data base has been submitted -

(1) the Registrar shall register it in the Register within 90 days after the application was submitted to him, unless he has reasonable grounds to assume that the data base is used or is liable to be used for illegal activities or as a cover for them, or that the information included in it was obtained, accrued or was collected in violation of this Law or in violation of the provisions of any enactment.
(2) The Registrar may register a purpose different from that specified in the application, register a number of purposes for a data base, of order that several applications be submitted instead of the application that was submitted, all if he concludes that doing so is appropriate to the actual activity of the data base,
(3) The Registrar shall refuse to register a data base under paragraph (1) or use his powers under paragraph (2) only after he gave the applicant an opportunity to state his case.

(b) The owner of a data base may appeal before the District Court against a decision by the Registrar under subsection (a), within 30 days after he was served notice of the decision.
(b1) If the Registrar did not register the data base within 90 days after the day on which the application was submitted and if he did not inform the applicant of his refusal to register, or of a delay in the registration for special reasons which shall be specified in his notice - then the applicant may operate or keep the data base, even if it is not registered.
(b2) If the Registrar informed the applicant of his refusal to register the data base, or of a delay as said in subsection (b1), then the applicant must not operate or keep the data base, except when the Court has decided otherwise.
(b3) The Registrar shall strike the registration of a data base from the Register, if the owner of the data base informed him that the information in that data base has been deleted and if he supported his notice by affidavit; if the data base was kept by a person different from the owner of the data base, then the notice shall also be supported by an affidavit of the person who kept it.
(c) The Registrar shall supervise compliance with the provisions of this Law and of the regulations thereunder.
(d) The Minister of Justice shall, by order with approval by the Knesset Constitution, Law and

Justice Committee, set up a unit for the supervision of data base, for their registration and for the security of the information in them: the size of the unit shall be according to the needs of supervision.
(e) The Registrar shall head the supervision unit and he shall appoint inspectors to carry out the supervision under this Law, only persons with suitable professional training in computers, information security and the use of authorities under this Law shall be appointed inspectors, if the Israel Police expressed no objection to their appointment for reasons of public security.
(f) In order to perform his duties, an inspector may -

(1) require any concerned person to deliver to him information and documents related to a data base,
(2) to enter any place in respect of which it is reasonable to assume that a data base is operated there, to conduct a search there and to seize any object, if he satisfied that it is necessary to do, so in order to assure implementation of this Law and to prevent violation of its provisions: the provisions of the Criminal Procedure Ordinance (Arrest and Searches) (New Version) 5792-1969 shall apply to any object seized under this section: arrangements for entry into a military installation or into an military installation or into an installation of a security authority, within its meaning in section 19(c), shall be prescribed by the Minister of Justice, in consultation with the Minister in charge of the security authority, as the case may be; in this paragraph: "object" includes computer material and output, within their definitions in the Computers Law 5755-1995:
(3) notwithstanding the provisions of paragraph (2), he shall enter a said place that is used only for residential purposes only under an order from a Magistrates Court judge.

Note: The designation of both the preceding and the following subsections as "(f)" is the result of an apparent eitor in the Hebrew original of Amendment No. 4 - Tr.
(f) If the possessor or the owner of a data base infringes any provision of this Law or of regulations thereunder, or if he fails to comply with a request made to him by the Registrar, then the Registrar may apply to the District Court fir an order that cancels the registration of the data in the Register or suspends it for a period prescribed by the Court.
(g) The Registrar and any person who acts on his behalf shall be treated as State employees.

10A. Privacy protection report

The Privacy Protection Council shall submit to the Knesset Constitution, Law and Justice Committee, not later than April 1 of each year, a report prepared by the Registrar about enforcement and supervision activities during the year that preceded the submission of the report, together with the Council's comments.

11. Notice to accompany request for information

Any request to a person for information, with the intention to keep and use it in a data base, shall be accompanied by a notice that indicates -

(1) whether that person is under a legal obligation to deliver that information, or whether its delivery depends on his volition and consent;

(2) the purpose for which the information is requested;
(3) to whom the information is to be delivered and for what purpose.

12. Register of data bases

(a) The Registrar shall keep a Register of data bases, which shall be open for inspection by the public.
(b) The Register shall include the registration particulars stated in section 9.
(c) Notwithstanding the provisions of subsections (a) and (b), the particulars said in section 9 (b) (3), (4) and (5) shall not be open to inspection by the public for data bases of security authorities.

13. Right to inspect information

(a) Every person is entitled to inspect - in person, through a representative authorized by him in writing, or through his guardian - any information about him which is kept in a data base.
(b) The owner of a data base shall, at the request of a person said in subsection (a) (hereafter: applicant), make it possible to inspect the information in the Hebrew, Arabic or English language.
(c) The owner of a data base may refrain from delivering to the applicant information that relates to his state of physical or mental health, if he believes that the information may cause severe harm to the applicant's physical or mental health or endanger his life; in such a case the owner of the data base shall deliver the information to a physician or psychologist on the applicant behalf.
(c1) The provisions of this section shall not obligate the owner of a data base to deliver information in violation of its privileged status, as prescribed under any enactment, unless the applicant's is the person for whose benefit the privilege is intended.
(d) The manner and conditions in which the right to inspect information can be exercised, and payment therefor shall be prescribed by regulations.
(e) The provisions of this section and of section 13A shall not apply -

(1) to the data of a security authority, within its meaning in section 19 (c);
(1a) to the data base of the Prisons Service;
(2) to the data base of a tax authority, within its meaning in the Tax Law Amendment (Exchange of Information Between Tax Authorities) Law 5727 - 1967;
(3) when the security or the foreign relations of the State or the provisions of any enactment require that information about any person not be disclosed to him;
(4) to the data base of any body, in resect of which the Minister of Justice determined in consultation with the Minister of Defense or the Minister of Foreign Affairs, as the case may be, and with approval by the Knesset Defense and Foreign Affairs Committee - that it includes information which the State's defense or foreign affairs require that it not be disclosed (hereafter' secret information), however, any person who requests to examine the information about himself stored in that data base shall be entitled to examine the information that is not secret information;
(5) to a data base about investigation and law enforcement by an authority lawfully authorized to investigate an offense, so determined by the Minister of Justice by order with approval of the Knesset Constitution, Law and Justice Committee.

13A. Inspection of material not of the owner of a data base

Without derogating from the provisions of section 13-

(1) if the owner of a data base keeps it with another (in this section- possessor) - then he shall refer the applicant to the possessor, stating his address, and he shall instruct the possessor in writing that ha make the inspection possible;
(2) if the applicant first applied to the possessor, then the possessor shall inform him whether he holds information about him, and also of the name and address of the owner of the data base.

14 .Amendment of information

(a) If, on inspecting information about himself, a person finds that it is not correct, not complete, not clear or not up to date, he may request the owner of the base or - if that owner is foreign resident - its possessor to amend or delete the information.
(b) If the owner of a data base agrees to a request under subsection (a), he shall make the necessary changes in the information and he shall communicate it to every person who received the information from him within a period prescribed by regulations.
(c) If the owner of a data base refuses to comply with a request under subsection (a), he shall give notice to that effect - in the form and manner prescribed by regulations - to the person who made the request.
(d) The possessor must correct information, if the owner of the data base agreed to the requested correction, or if a Court ordered the correction to be made.

15. Appeal to Court

A person who requested information may - in the form and manner prescribed by regulations - appeal to a Magistrates' Court against a refusal by the owner of a data base to enable him to make inspection under section 13 or section 13A, and against a notice of refusal under section 14(c).

16. Secrecy

No person shall disclose any information obtained by him by virtue of his functions as an employee, manager or possessor of a data base, save for the purpose of performing his work or of implementing this Law or under a Court order in connection with a legal proceeding; if a request has been made before a proceeding was instituted, it shall be heard in a Magistrates' Court; if a person violates the provisions of this section, he shall be liable to five years imprisonment.

17. Penalty

The owner of a data base, the possessor of a data base and the manager of a data base are each individually responsible for the protection of the information in the data base.

17A. Possessor of data bases of different owners

(a) A possessor of data bases of different owners shall make sure that only persons explicitly authorized therefor in a written agreement between him and the owner of that data base be allowed access to each data base.
(b) A possessors of at least five data bases that require registration under section 8, shall annually deliver to the Registrar a list of data bases in his possession, standing the names of the owners of the data bases, an affidavit that the persons authorized to have access to each data base have been designated in agreements between him and the owners, and the name of the person in charge of security said in section 17B.

17B. Security officer

(a) The bodies specified below must appoint suitable trained persons to be in charge of information security (hereafter: security officer):

(1) a person who holds five data bases that require registration under section 8;
(2) a public body, as defined in section 23;
(3) banks, insurance companies and companies engaged in ranking or evaluating credit ratings.

(b) Without derogating from the provisions of section 17, the security officer shall be responsible for the security of information in data bases kept by the bodies said in subsection (a).
(c) A person found guilty of an heinous offense or of an offense against the provisions of this Law shall not be appointed security officer.

Article Two: Direct Mail

17C Definitions

In this Article -

"direct mail" - an individual approach to persons, based on their belonging to a population group determined by one or more characteristics of persons whose names are included in a data base;
"approach" - includes in writing, in print, by telephone, by facsimile, by computerized means and by some other means;
"direct mail services" - the provision of direct mail services to others by way of transferring lists, adhesive labels or data by any means whatsoever.

17D. Direct mail

No person shall operate or hold a data base used for direct mail services, unless he is registered in the Register, and unless one of his registered purposes is direct mail services.

17E. Stating source of information

No person shall operate or hold a data base used for direct mail services, unless he has a record stating the source from which he obtained every collection of data used for purposes of the data base and the date of its receipt, as well as the purpose to whom he gave any said collection of data.

17F. Deletion of information from data base used for direct mail

(a) Every direct mail approach shall include, clearly and prominently -

(1) a statement that it is a direct mail approach, also stating the registration number in the data base Register of the data base used for the direct mail services;
(2) notice that the recipient of the approach has the right to be deleted from the data base as said in subsection (b), and also whom to address for that purpose;
(3) the identity and address of the data base that includes the information according to which the approach was made, and the sources from which the owner of the data base received that information.

(b) Every person is entitled to demand - in writing - from the owner of a data base used for direct mail that information related to him be deleted from the data base.
(c) Every person is entitled to demand - in writing - from the owner of a data base used for direct mail or from the owner of a data base which includes information on the basis of which the approach was made, that information related to him not be given to any person, to a category of persons or to certain persons, either for a limited period of time o permanently.
(d) When a person has informed an owner of a data base of his demand said in subsections (b) or (c), then the owner of the data base shall act in accordance with the demand and shall inform that person, in writing, that he has done so.
(e) If the owner of a data did not give notice as said in subsection (d) within 30 days after he received the demand, then the person to whom the information relates may apply to a Magistrates Court in the manner set by regulations that it order the owner of the data base to act as aforesaid.
(f) The rights under this section of a deceased person included in a data base shall also be held by his spouse, his child and his parent.

17G. Applicability to items of knowledge

The provisions of this Article shall apply to items of knowledge that relates to a person's private affairs, even if they do not constitute information, to the same extent that they apply to information.

17H. Not applicable to public body

This Article shall not apply a public body, within its meaning in section 23(1), when it performs its tasks under an enactment.

17I. Saving of enactments

The provisions of this Article are intended to add to the provisions of any enactment.

CHAPTER THREE: DEFENSES

18. Defenses

In any criminal or civil proceeding for infringement of privacy, it shall be a good defense if one of the following is the case: (1) the infringement was committed by way of a publication protected under section 13 of the Defamation (Protection) Law 5725-1965 ;
(2) the defendant or accused committed the infringement in good faith in any of the following circumstances;

(a) he did not know and need not have known that an infringement of privacy might occur;
(b) the infringement was committed under circumstances, under which the infringer was under a legal, moral, social or professional obligation to commit it;
(c) the infringement was committed in defense of a legitimate personal interest of the infringer;

(d) the infringement was committed in the lawful pursuit of the infringer's occupation and in the ordinary course of his work, as long as it was not committed by way of publication;
(e) the infringement was committed by way of taking a photograph in the public domain, or of publishing a photograph taken there, and the injured party appears in it coincidentally;
(f) the infringement was committed by way of a publication protected under paragraphs (4) to (11) of section 15 of the Defamation (Prohibition) Law 5725 - 1965;
(3) the infringement involved a public interest that justified it under the circumstances of the case, on condition that - if the infringement was committed by way of publication - the publication was not untruthful.

19. Exemption

(a) No person shall bear responsibility under this Law for an act which he is empowered to do by Law.
(b) A security authority or a person employed by it or acting on its behalf shall bear no responsibility under this Law for an infringement reasonably committed within the scope of their functions and for the purpose of their performance.
(c) For purpose of this section, "security authority" - any of the following:

(1) the Israel Police;
(2) the Intelligence Branch of the General Staff of the Israel Defense Forces, and the Military Police;
(3) the General Security Services;
(4) the Institute for Intelligence and Special Assignments.

20. Onus of proof

(a) If an accused or defendant proves that he committed an infringement of privacy under any of the circumstances said in section 18(2) and that it did not exceed the limits reasonable under those circumstances, he shall be presumed to have committed it in good faith.
(b) The accused or defendant shall be presumed not to have committed the infringement of privacy in good faith, if - in committing it - he knowingly exceeded what was reasonably necessary for purposes of the matters protected by section 18(12).
(c) If an accused person or defendant pleads a defense under section 18(2)(d), he shall be presumed not to have infringed privacy in good faith if he infringed it in violation of the rules or principles of professional ethics that apply to him by Law or which are accepted by the members of the profession to which he belongs.

21. Rebuttal of defense pleas

If an accused or defendant produces evidence or testifies in person to prove one of the defense pleas provided by this Law, the prosecutor or plaintiff may produce rebutting evidence; this provision shall not derogate from the Court's power under any Law to permit the production of evidence by the parties.

22. Mitigating circumstances

In passing sentence or awarding compensation, the Court may also take the following into account in favor of the accused or defendant;
(1) that the infringement of privacy was merely a repetition of something said before and that he mentioned the source on which he relied;
(2) that he did not intend to commit an infringement;
(3) if the infringement was committed by way of publication - that ha has apologized and has taken steps to discontinue the sale or distribution of copies of the publication that contains the infringement, provided the apology was published in the same place and in the same dimensions and manner in which the infringing matter had been published, and that it was unqualified.

CHAPTER FOUR: DELIVERY OF INFORMATION BY PUBLIC BODIES

23. Definitions

In this Chapter -
"public body" -

(1) a Government department and other State institution, a local authority and any other body that performs lawful public functions;
(2) a body designated by the Minister of Justice, by order with approval by the Knesset Constitution, Law and Judiciary Committee, provided the order specifies the categories of information and of items which the body is entitled to deliver and to receive.
(3) Repealed

23A. Applicability to information

The provisions of this Chapter shall apply even to those items about a person's private affairs which do not constitute information, just as they apply to information.

23B. Must not deliver information

(a) A public body must not deliver information, unless it is information that has been published under lawful authority, or unless it has been made available for public inspection under lawful authority, or unless the person to whom the information refers agreed to its delivery.
(b) The provisions of this section shall not prevent a security authority, as defined in section 19, from accepting or delivering information in the performance of its function, as long as the acceptance or delivery was not forbidden by legislation.

23C. Limitation on prohibition

Notwithstanding the provisions of section 23B, delivery of information shall be permitted - if it is not prohibited by legislation or by professional ethics -
(1) between public bodies, when one of the following holds true:

> (a) delivery of the information is part of the authority or of the functions of whoever delivers the information and it is required in order to implement legislation or for a purpose within the authority or the function of whoever delivers or receives the information;
> (b) the information is delivered to a public body which is entitled to demand the information lawfully from any other source;

(2) from a public body to a Government department or to another State institution, or between aforesaid departments or institutions, if delivery of the information is required for the implementation of any legislation or for a purpose within the authority or within the scope of activity of whoever delivers or receives the information;
however, information provided on condition that it not be delivered to others shall not be delivered as
aforesaid.

23D. Obligations of public body

(a) If a public body regularly delivers information in accordance with section 23C, then it shall specify that fact on all its lawful requests for information.
(b) If a public body delivers information in accordance with section 23C, then it shall keep a record of the information delivered.
(c) If a public body regularly receives information in accordance with section 23C and stores that information in a data base, then it shall so inform the Registrar, and that information shall be included in the list of data bases under section 12.
(d) If a public body received information in accordance with section 23C, then it shall use it only within the framework of its authority and functions.

(e) In connection with the obligation, under any Law, to maintain confidentiality, information delivered to a public body under this Law shall be treated like any information obtained by that body from any other source, and all the rules applicable to the body that delivered the information shall also apply to the body that receives it.

23E. Surplus information

(a) If information which may be delivered under sections 23B or 23C is located in a single file, together with other information (hereafter: surplus information), then the body that delivers the information may deliver the requested information to the recipient body together with the surplus information.

(b) The delivery of surplus information under subsection (a) shall be conditional upon the establishment of procedures that will prevent any use at all being made of the surplus information received; the said procedures shall be prescribed by regulations and - as long as they have not been prescribed by regulations - the body that requests the aforesaid information shall specify procedures in writing and it shall deliver a copy of them to the body that delivers information, on its request.

23F. Permitted delivery does not infringe privacy

A delivery of information, which is permitted under this Law, shall not constitute an infringement of privacy, and the provisions of sections 2 and 8 shall not apply to it.

23G. Regulations on delivery of information

The Minister of Justice may, with approval by the Knesset Constitution, Law and Justice Committee, make regulations on ways of the delivery of information by public bodies.

23H. Repealed

CHAPTER FIVE: MISCELLANEOUS

24. The State

This Law shall apply to the State.

25. Death of injured party

(a) If a person, whose privacy was infringed, dies within six months after the infringement without having filed an action or complaint in respect thereof, then his spouse, child or parent, or - if he left no spouse, child or parent - his brother or sister may file an action or complaint in respect of that infringement within six months after his death.
(b) If a person, who filed an action or complaint in respect of an infringement of privacy, dies before the proceeding is concluded, then his spouse, child or parent or - if he left no spouse, child

or parent - his brother or sister may, within six months after his death, notify the Court that they wish to proceed with the action or complaint, and upon that notification they shall take the place of the plaintiff or complainant.

26. Prescription

The period of prescription of civil actions under this Law is two years.

27. Applicability of certain provisions of the Defamation (Prohibition) Law

The provisions of sections 21,23 and 24 of the Defamation (Prohibition) Law 5725 - 1965, shall apply, mutatis mutandis, to legal proceeding for infringement of privacy.

28. Evidence of a person's bad reputation, character or past

In a criminal or civil proceeding for infringement of privacy, no evidence shall be produced, and no witness shall be examined on the bad reputation or on the character, past, activities or options of the injured party.

29. Additional orders

(a) In a criminal or civil proceeding for infringement of privacy, the Court may order, in addition to any penalty and other relief -

> (1) that distribution of copies of the infringing matter be prohibited or that they be confiscated; a confiscation order under this paragraph is effective against any person who has such material in his possession for sale, distribution or storage, also if he is not a party to the proceeding; if the Court ordered confiscation, then it shall direct how to dispose of the confiscated copies;
> (2) that all or part of the judgment be published; publication shall be at the expense of the accused or defendant, in a place, of a size and at the manner prescribed by the Court;
> (3) that the infringing matter be surrendered to the injured party;
> (4) that the unlawfully received information be deleted, or that use of the said information - or of the surplus information, as defined in section 23E - is prohibited, or it may make any other in respect of the information.

(b) The provisions of this section shall not prevent keeping a copy of a publication in public libraries. archives and the like - unless the Court imposes a restriction also on that by a confiscation order under subsection (a) (1) - and they shall not prevent an individual keeping a copy of a publication.

30. Responsibility for publication in newspaper

(a) If an infringement of privacy is published in a newspaper, within its meaning in the Press Ordinance (hereafter: newspaper), then the criminal and civil responsibility for the infringement shall be borne by the person who brought the material to the newspaper and thereby caused its

publication, by the editor of the newspaper and by the person who actually decided on the publication of the infringement in the newspaper, and civil responsibility shall also be borne by the publisher of the newspaper.
(b) In a criminal case under this section, it shall be a good defense for the editor of the newspaper that he took reasonable steps to prevent the publication of the infringement or that he did no know of the publication.
(c) In this section, "editor" of a newspaper includes an acting editor within the scope of the powers or functions of the body that transmits or receives the information.

31. Responsibility of printer and distributor

If an infringement of privacy was published in print, except in a newspaper published under a valid license at intervals of not less than forty days, then criminal and civil responsibility for the infringement shall also be borne by the possessor of the printing press, within its meaning in the Press Ordinance, on which the infringement was printed, and by the person who sells or otherwise distributes the publication; however, they shall not bear responsibility unless they knew or ought to have known that the publication contained and infringement of privacy.

31 A. Penalties in due diligence offenses

(a) If a person does one of the following, then he is liable to one year imprisonment:
(1) he operates, keeps or uses a data base in violation of section 8;
(2) he delivers false particulars in an application for the registration of a data base, an required in section 9:
(3) he does not deliver particulars or delivers false particulars in a notice attached to a request for information under section 11;
(4) he does not comply with the provisions of sections 13 and 13A, concerning the right to inspect information kept in a data base, or he does not correct a data base according to the provisions of section 14:
(5) he grants access to a data base in violation of the provisions of section 17 A (a). or does not deliverdocuments or an affidavit in accordance with the provisions of section 17 A (b) to the Registrar;
(6) does not appoint a security officer for the protection of information under section 17B.
(7) operates or keeps a data base used for direct mail services in violation of the provisions of sections 17D to 17F;
(8) delivers information in violation of sections 23B to 23E.
(b) An offense under this section does not require that criminal intent or negligence be proven.

31B. Civil wrong

An act or omission in violation of the provisions of Chapters Two or Four, or in violation of regulations made under this Law, shall constitute a civil wrong under the Civil Wrongs Ordinance (New Version).

32. Material inadmissible as evidence

Material obtained by the commission of an infringement of privacy shall not be used as evidence in Court without the consent of the injured party, unless the Court, for reasons which shall be recorded, permits it to be so used, or if the infringer, who is a party to the proceeding, has a defense or enjoys exemption under this Law.

33. Amendment of Civil wrongs Ordinance

Section 34A of the Civil Wrongs Ordinance (New Version) is hereby repealed.

34. Amendment of Criminal Procedure Law

In the Schedule to the Criminal Procedure Law 5725-1965, the following paragraph shall be added after paragraph (12):
"(13) offenses under the Protection of Privacy Law 5741-1981."

35. Saving of Laws

The provisions of this Law shall not derogate from the provisions of any other Law.

36. Implementation and regulations

The Minister of Justice is charged with the implementation of this Law and be may, with approval by the Knesset Constitution, Law and Justice Committee, make regulations on any matter that relates to its implementation and, inter alia, on -
(1) conditions for keeping and safeguarding information in data bases;
(2) conditions for transmitting information to or from data bases outside the boundaries of the State;
(3) rules of conduct and ethics for owners, possessors and operators of data bases;
(4) provisions on the deletion of information when a data base ceases to function.

36A. Fees

(a) The Minister may, with approval by the Knesset Constitution, Law and Justice Committee, set fees for registration and inspection under this Law.
(b) The fees collected under this section shall b allocated to the Registrar and to the supervision unit for their activities under this Law.

37. Effect

Chapter Two shall go into effect six months after the date of publication of this Law.