

**On Information, on Privacy, and on Protecting Information and
Privacy – the State of Affairs of Legal Protections in the Digital Era
in Israel**

By: Guy Kedem, Advocate

(i) Introduction – Protection of Privacy and Databases in the Digital World

In December 1890, Warren and Brandeis published their article: The Right to Privacy¹ which evolved into one of the most influential articles in the American law and laid the foundation for the modern western outlook of the right to privacy: the right to be let alone. Approximately 120 years have since transpired, and this definition remains unabated in vigour.

At the time that I approached writing this article which you are presently reading, I remembered a lecture of the Chief of the Israeli Law, Information and Technology Authority in the Ministry of Justice that I attended a number of years ago. At that lecture it was demonstrated how each of us “leave tracks” in the virtual world, in Cyberspace, and how upon the press of a button the same details of information that none of us would have been interested in revealing to the public can be exposed.

Thus, with a click of a button you can reveal where each of us surfed on the internet, what each of us searched by Search Engine, which undergarments we sought, the type of monetary investments we were interested in, that we were interested in the recommended methods of activity for an individual on the brink of bankruptcy, the fact that we sought recommendations for marriage counselors or private investigators that will follow our spouses, and such other private information that a reasonable person is in no hurry to expose before the entire world.

In the digital world of the end of the 20th and beginning of the 21st centuries, where the social networks and search engines allow everybody to know everything about

everyone, the laws of protection of privacy are receiving redoubled force, and Warren and Brandeis' "right to be let alone" is receiving double importance.

The accumulation of millions of details of information in countless databases, and the ability to perform hybridization between these databases in order to create an individual profile on each one of us, brought different countries, and amongst them also the State of Israel, to institute, from a legal and constitutional perspective, the protection of privacy, and as a derivative of this, the protection of databases.

In Israel, from a legal and constitutional perspective, there is a balancing between the basic obligation of Israel as a democratic state to protect the privacy of an individual and the privacy of his/her personality on the one hand; and on the other hand, to promise a free flow of information that is a guarantee to a pluralistic society and to an open market of ideas and opinions.

Naturally, a proper survey of the protection that the Israeli law grants to information and to databases cannot be conducted without discussing the protection granted in the law to privacy. Information and Privacy are in fact sides to the same coin, and it is not in vain that they have been settled together in the framework of one law – the Protection of Privacy Law, 5741 - 1981 (hereinafter – “**the Law**”; “**the Protection of Privacy Law**”).

In this article, I request to present, in a nutshell, the topic of protection of information and of privacy in the State of Israel, with an emphasis on legal protection in the digital era.

(ii) **The Protection of Privacy Law, 5741 - 1981**

The Protection of Privacy Law is the foremost legislation that sets forth the issue of the right to privacy in Israel as well as the issue of activating and maintaining databases that include private information and also sensitive information, while taking into account the right to privacy.

The Law defines what will be considered an offense of privacy, and even sets forth different situations that the offense will be permitted (subject to the existence of a variety of limiting conditions). Section 1 of the Law establishes the leading principle whereby, “a person shall not abuse the privacy of another without his consent”. The Israeli legislator elected to refrain from providing a concise and exact definition of the term “privacy”, and rather, defined in Section 2 of the Law, what are the forbidden ways to abuse privacy:

- Spying or tracking a person which is likely to bother him/her or bother another person.
- Wiretapping which is forbidden by law.
- Photographing an individual in private domain.
- Publishing photographs of an individual in public in circumstances that the publication is likely to humiliate or scorn him/her.
- Copying the content of a letter or other writing that is not intended for publication, or use of the contents without the permission of the addressee or writer, so long that the writing is not of historical value and fifteen years from the time of the writing has not yet elapsed.
- Use of the name of a person, his nickname, his picture or his voice for the purpose of profit.
- A breach of an obligation to secrecy prescribed by law regarding the private matters of a person.
- A breach of an obligation to secrecy regarding the private matters of a person, that was set forth explicitly or implicitly in an agreement.
- Use of the knowledge of the private matters of a person or transmitting them to another, which are not for the purpose for which they were provided.
- Publication or transmission of something that was presented in a way of abuse of privacy.
- Publication of a matter concerning privacy of the personal life of a person, or of their medical condition, or their behavior in the private domain.

(iii) **The Privacy as One of the Foundation Stones of Human Rights and the Democracy in the State of Israel**

The right to privacy is one of the key rights amongst the rights granted to individuals in Israel, and is recognized as one of the freedoms that designs the character of the regime in Israel as a democratic regime². The right to privacy is intended to provide the individual with a "personal territory" in which he establishes the ways of his conduct without the intervention of society. In this "territory" the person is being "let alone". The roots of the Israeli right to privacy are deeply embedded in the traditions of the Jewish nation, and demonstrates the values of Israel as a Jewish and democratic State as one³.

In Biblical Law, there were those that requested to see this already in the words of Bilaam, who about Israel said, "how goodly are your tents, O Jacob your dwelling places, O Israel!" (Numbers Chapter 24, verse 5), and the intention was that there would not be openings of the doors and windows of the people of Israel from directions of one facing the other⁴.

The right to privacy was recognized by the Israeli common law as a human right, and was anchored in 1981 in the Protection of Privacy Law, and in the beginning of the nineties, officially obtained constitutional status.

Already at the time of the establishment of the State of Israel, the right to privacy played a major role in the informal civil rights charter in Israel, but was significantly strengthened at the time it was formally anchored as a constitutional right in 1992, with the enactment of the Basic Law: Human Dignity and Liberty⁵. Section 7 of the Basic Law grants legality to the right of an individual to privacy and intimacy and sets forth:

- All persons have the right to privacy and to intimacy.
- There shall be no entry into the private premises of a person who has not consented thereto.

- No search shall be conducted on the private premises of a person, nor in the body or personal effects.
- There shall be no violation of the confidentiality of conversation, or of the writings or records of a person.

While referring to the right to privacy as a right of constitutional status, which the government has to honor and the courts have to guarantee its existence, the High Court of Justice ruled:

“The right to privacy is a fundamental right in Israel. It is anchored in Section 7 of the Basic Law: Human Dignity and Liberty. An affront to privacy by the authorities of the state is permissible only by a law that is befitting the values of the State of Israel, enacted for a proper purpose, and to an extent no greater than is required... Section 11 of the Basic Law, which imposes on the authorities of the state the obligation to honor the rights anchored in it, even obligates the court to provide precise interpretation to laws that harm the privacy...”⁶.

On the aspects of the framework of the right to privacy in Section 7(a) of the Basic Law: Human Dignity and Liberty it was determined:

“...there are two aspects to the right to privacy mentioned in Section 7(a) of the Basic Law: Human Dignity and Liberty. One aspect, the roots of which can be found in Human Dignity, is “the right of a person to conduct a way of life that he desires in the seclusion of his house, without disturbance from outside”... This statement should not be limited to the physical aspect of the house. It has to be understood in a more expansive manner, metaphorically, in the spirit of the expression that Warren Brandeis coined it “the right to be let alone”... The other aspect involves the concern due to the excess power of the state, that it would amass in its hands extensive

information relating to citizens and residents and would make detrimental use of that information.”⁷.

(iv) **Protection of Privacy in Databases**

In 1996, the Protection of Privacy Law was amended, and two important chapters were added which set forth the protection on databases as well as the different aspects that relate to databases for the purpose of Direct Mailing. The Law defines “**Database**” as a collection of informational details, which is stored magnetically or optically and is intended for computerized processing, except:

- Collection for personal use that is not for business purposes. Or –
- A collection that includes only name, address, and contact details, which in itself does not create a characterization that violates the privacy of the persons whose names are included, and this is so long as the owner of the collection or a corporation in his control does not have an additional collection.

“**Information**” is defined by the Law as details on the personality of a person, his personal status, the privacy of his personality (such as sexual habits), health condition, economic status, professional training, opinions and belief.

“**Sensitive Information**” is defined as details on the personality of a person, the privacy of his personality (such as sexual habits), health condition, economic status, opinions and faith, and all information that the Minister of Justice determined in an order that it is Sensitive Information.

In the matter of **Tsadok Matityahu v. The State of Israel**, the District Court in Tel Aviv deliberated the issue of the appropriate interpretation of the phrase “Information”, which appears in the Law. The court embraced an expansive interpretation to the phrase "Information", and determined:

“The expression Information is to be interpreted on the background of the statutory purpose of the Protection of Privacy Law generally, and especially on the chapter regarding protection of privacy in databases. According to this goal, one should not hold the view that the interpretation has to be performed in a narrow manner, because a narrow interpretation will bring an excessive affront to the privacy of a person, and it was not for this that the legislator intended.”⁸.

The Law establishes an obligation to register certain databases with the “Registrar of Databases”. The Registrar is a division of the Israeli Ministry of Justice and is entrusted on behalf of the State with safeguarding the privacy of individuals from the risks associated with maintaining databases. The Registrar can enact enforcement and/or preventive measures, by its initiative and by response to requests of the public, in order to ensure the optimum protection of the privacy in the databases.

Which databases require registration with the Registrar of Databases? – The Law requires registration of databases where one of the following exist:

- The database contains Informational details regarding more than 10,000 people. .
- There is Sensitive Information in the database as defined above.
- The database contains Information about people that did not provide the Information and did not provide their consent to their inclusion in the database.
- The database is of a public entity (governmental entities, local authorities and other public entities).
- The database is used for Direct Mailing.

“Direct Mailing” is defined by the Law as a personal approach to a person, on the basis of him belonging to a population group determined in accordance with one or more characterizations of persons whose names are included in the database.

When the above conditions which require registration exist in a database, one may not hold or manage the database without registering it. Of course, the registration needs to be updated for every change in the details contained in the database.

It is important to state that the Law imposes the responsibility to secure the information on each one of the owners of the database, the holders of the database, as well as the manager of the database.

(v) **Databases for the Purpose of Direct Mailing**

As mentioned, the Law defines “Direct Mailing” as a personal approach to a person, based on his belonging to a population group, determined in accordance with one or more characterizations of persons whose names are included in the database. ”**Approach**” – includes written, printed, telephone, fax, computerized manner and other means.

The Law explicitly determines that a person will not manage and will not maintain a database that serves Direct Mailing purposes unless he is registered in the database ledger, and one of his registered purposes is mailing services. Also determined is that a person will not manage and will not maintain a database for Direct Mailing services unless he possesses a registration which states the source from which he obtained the collection of details which are used for purposes of the database, the time they were received, and also to whom the entire collection of details was transmitted to.

Additionally, the Law sets forth that all approaches by Direct Mailing shall include in a clear and prominent manner a marking that the approach is via Direct Mailing, and there shall also appear a notice of the right of the recipient to be erased from the database, the details of the database should be indicated, and there should also be a detailing of the source from which the database information was obtained.

The purpose of the requirement for providing the above details is to provide the recipient (and if deceased and he is registered in the database – to his spouse, children,

parents or siblings) the right to request his erasure from the database so that he will not be bothered in the future, and the Law even sets forth the technical procedure to delete information from a database which serves for Direct Mailing.

With regards to this it should be noted that the Protection of Privacy Law does not forbid sending Direct Mailing in itself, and this is forbidden (excluding a small number of exceptions) in the framework of Amendment no. 40 to the Communications Law (Telecommunications and Broadcasting), 5742 - 1982 that went into effect at the end of 2008, and imposes prohibitions and limitations on sending “junk mail” (SPAM). Amendment no. 40 to the Communications Law does not apply to written direct mailings. Likewise, the Communications Law permits sending advertising materials by fax, without receiving prior written agreement, on the condition that it is a onetime approach to a business, and that it includes an offer to consent to receive promotional materials from the sender by fax⁹.

(vi) **Perusal of Databases**

In parallel to the right not to be included in a database, the Law grants the right to peruse databases and demand an amendment of the information or deletion of such. Every person is entitled to peruse the information about him that is held in the database, and every database owner has to permit a perusal of this sort. An individual who perused the information about him and discovered that it is incorrect, incomplete, unclear or outdated, can request that it be corrected or deleted.

Nevertheless, the owner of the database is permitted not to provide the requester with information that relates to his medical or mental condition if in his opinion the information will cause severe damage to the physical or mental health of the requester or endanger his life. In such a situation the database owner will provide the information to a doctor or psychologist on behalf of the requester.

Additionally, a database owner is not obligated to provide information contrary to any legal privilege (unless the privilege is intended for the benefit of the requester).

Similarly, various restrictions apply (and their application is subject to judicial review) concerning perusals of the databases of the security agencies and police, the Tax Authority, or when the security of the state, its foreign relations or statutory instructions require not revealing information to an individual about him.

The right to peruse the databases of public authorities is also set forth in the instructions of the Freedom of Information Act 5758 – 1998. The Freedom of Information Act establishes in Section 1 the principle that stands at the basis of the legislation, and it is that every Israeli citizen or resident of the State of Israel has the right to obtain information from public authorities in accordance with the instructions of the Freedom of Information Act. The Freedom of Information Act sets forth the manner for submitting requests to public authorities for the purpose of perusing the information in its possession, the manner of handling the requests, and it even sets forth the obligation to appoint in each authority, from amongst the employees of the authority, an appointee to be in charge of setting up the information available to the public domain, on handling requests to receive information and on applying instructions of the Freedom of Information Act.

It is important to elucidate that within the Freedom of Information Act there are a number of exceptions, relating to perusal of information where there is a likelihood that a disclosure of such would harm the security of the state, its foreign relations or the security or well being of an individual; information that a disclosure of such would be a violation of privacy, as defined in the Protection of Privacy Law, unless the disclosure is permitted by law; and the like.

(vii) **Transferring Information to Databases outside of the Boundaries of the State of Israel**

The Protection of Privacy Law does not make a distinction between information that was collected by people out of Israel to information on people in Israel. However, limitations apply on registered databases with all connected to transferring information out of the boundaries of Israel and this is by virtue of the force of the

Protection of Privacy Regulations (Transfer of Information to Databases Outside of the State's Boundaries) 5761- 2001 (hereinafter – the “**Regulations**”).

The Regulations establish that a person shall not transfer information and shall not permit the transfer of information from a database in Israel out of its boundaries, unless the laws of the state to which the information is transferred guarantee a level of protection on the information which is not less than the level of protection of information set forth in the Israeli law, and so long that the foreign country establishes the following principles:

- Information will be collected and processed in a legal and fair manner.
- Information will be held, will serve and will be delivered only for the purpose for which it was received.
- Information that is stored will be exact and updated.
- The right of perusal and correction is granted to whom the information is about.
- There exists an obligation to adopt suitable safety measures to protect the information in the databases.

However, despite the above said, the owner of a database can transfer information or permit the transfer of information from his database in Israel out of its boundaries, if one of the following is fulfilled:

- The person that the information relates to agrees to the transfer.
- The consent of the person that the information relates to cannot be received and the transfer is necessary in order to protect his health or the well being of his body.
- The information is transferred to a corporation controlled by the owner of the database from which the information was transferred, and he guaranteed the protection of privacy after such transfer.
- The information was transferred to one who had contracted with the owner of the database from whom the information was transferred to fulfill the

conditions for maintaining information and the use of it which apply to a database in Israel, mutatis mutandis.

- The information was lawfully published to the public or was lawfully made available to the review of the public.
- Transferring the information is mandated by the Israeli law.
- The information is transferred to a database in a country that is:
 - o A party to the Counsel of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.
 - o The recipient of the information is from a country that is a member of the European Union, according to the same acceptance criteria.
 - o A country that the Registrar of Databases proclaimed that there exists within it an authority that is responsible for the protection of privacy, after it came to a cooperation agreement with the same authority.

(viii) **Illustration – Interesting Court Cases which were Adjudicated in the Israeli Courts**

Nearing conclusion, we shall present two interesting court cases that were adjudicated in Israel on the topic of the Protection of Privacy Law.

The first is the case of **Registrar of Databases v. Ventura**¹⁰ which was deliberated in the Supreme Court. There, the court adjudicated the refusal of the Registrar of Databases to register a database that's purpose was to distribute lists of issuers of checks that were dishonored. The Supreme Court determined that distribution of the information that the respondents wanted to register was an invasion of the privacy of a person. It was determined, that even though the Protection of Privacy Law allows compromising the privacy of a person if he consents, whether explicitly or implicitly, the fact that a person issues a check does not mean by itself that he agrees to provide his details as appearing on the check to just anyone.

The second court case was deliberated in the District Court in Tel Aviv, and a judgment was recently issued. In the case of **Liran v. Pelephone et al.**¹¹ the plaintiff

demanded the deletion of the list of calls carried out from his cellular telephone from the databases of two cellular companies.

The court, in its decision describes that in the framework of the ongoing activity of each of the defendants, the cellular companies, a list of details of calls carried out by the customers is maintained, and in this list, the dialed number is recorded, as is the length of the call, and the time that each call was carried out. Records of the calls are maintained by the companies in computerized databases for several years. The plaintiff claimed that the records of the calls are required by the defendants only for the purpose of billing the client for services received, and upon the fulfillment of payment, their interest with this information is concluded. Likewise the plaintiff claimed that the essence of saving the information when there is no use for the purpose for which it was provided to the defendants is an affront to the privacy of the client, since the information can leak to third parties who will negatively exploit it.

The defendants counterclaimed that the databases are an important layer in their business activities, and the information accumulated in them serves for many additional purposes beyond the charging of the client, for example, settling of accounts with third parties, internal control, and reporting to the Tax Authority and the Ministry of Communications.

The court rejected the claim to issue a mandatory injunction to the cellular companies to delete the list of calls the plaintiff made from their databases. The court determined that there is no dispute on the importance of the right to privacy, and that the managing of a database inherently includes the risk that private information may leak. Despite this, protection of privacy is not the be-all and end-all, since the legislator recognized the possibility of maintaining a database and the advantage in maintaining information and safeguarding sensitive information, and this is subject to supervision of the manner of use and protection of the information. The court determined that the defendants carried out the supervision in accordance with that which is required.

(ix) **The Remedies Available by Virtue of the Law to those Injured**

To conclude we shall describe the remedies available to one who was harmed from a breach of the Law and the legal exposure to someone who breached the Law.

One who breached the provisions of the Protection of Privacy Law inter alia by not maintaining a database in accordance with the provisions of the Law, is exposed to civil and criminal sanctions as one. The Law even allows the injured to claim statutory damages up to a sum of NIS 50,000, and when it is proved that the invasion of privacy was done with intent to harm, up to a sum of NIS 100,000.

Likewise, in addition to any punishment or other relief the court is entitled to, in a criminal or civil trial for breach of a provision the Law, the court may order the prohibition of distributing copies of the materials that harm the privacy or ban it; the publication of the court judgment, in all or part (on account of the accused or defendant); require the delivery of the breaching material to the injured; demand the destruction of information which was unlawfully received or to forbid of such use; and so forth.

It shall also be stated that the Law sets forth liability for offensive publications in a newspaper which violate privacy, and imposes criminal liability for injury to a person that brought the matter to the newspaper and caused it to be published, to the editor of the newspaper and to the one who actually decides to publish the offense in the newspaper. The publisher of the newspaper will also bear civil liability. Court rulings have expanded this liability also to additional methods of communication.

(x) **Conclusion**

The right to privacy is a relatively new right in Western law, and oceans of ink have been spilled trying to explain its meaning, contents and scope. In this regard the State of Israel is not different from the other Western countries,

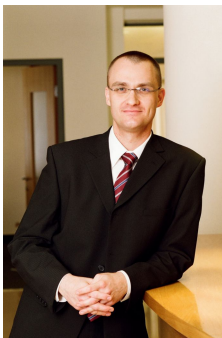
In this article, we saw, that due to the centrality of the right to privacy as a foundation stone in the Israeli democracy, the terms “privacy” and “violation of privacy” are wide and are intended to apply to a variety of circumstances and activities.

We surveyed the constitutional, the legal, the judicial and the regulatory protections that secure the right of privacy in the State of Israel and the protection granted to databases as a direct derivative of the right to privacy.

We have learned, that the regulatory and other obligations imposed on the bearer or on the operator of a database influenced by the information in the database, and from the question of if and until how much the holding of that same information and the use of it are subject to the limitations derived from the obligation to protect the privacy of other people.

Therefore, it is only natural that with the passing of time the laws also change, and with the development of technology the terminology changes as well. Therefore, while taking into consideration the civil and criminal sanctions imposed on one who breaches the provisions of the laws which regulate the protection of privacy and the registration of databases, it is highly recommended to consult with an expert in the field of privacy and database protection in order to appropriately calculate one's steps.

* * *



Advocate Guy Kedem is a partner at Gideon Koren & Co., Law Offices and Notary (www.gkl.co.il). Advocate Kedem specializes in Intellectual Property, Protection of Privacy and Databases, and in Cyberspace law.

This article is for informational purposes only, and should not be viewed as any form of legal advice or a legal opinion. For questions and comments relating to the article, you are invited to contact Advocate Guy Kedem by email: main-rg@gkl.co.il

¹ *Harvard Law Review*, Vol. IV, December 15, 1890, No. 5.

² *Bagatz* 6650/04 *Plonit v. The Netanya Region Rabbinical Court* 2006(2) TAK-EL 1736 (2006).

³ *Ibid.*

⁴ *CrimComp (Jerusalem Peace Court)* 102/05 *Bank HaMizrahi HaMeuhad Ltd. v. Shaul Shauli* 2005(3) TAK-SHAL 1397 (2005).

⁵ Israel has an unwritten constitution, in the form of Basic Laws.

⁶ *CrimApp* 537/95 *Ganimat v. The State of Israel* 49(3) P.D. 355, 375 (1995).

⁷ *Bagatz* 8070/98 *The Association For Civil Rights In Israel v. The Ministry of Interior* 16 Dinim Elyon 799 (2004).

⁸ *CivilApp (Tel Aviv District Court)* 71165/99 *Tsadok Matityahu v. The State of Israel* (Published in <http://www.nevo.co.il>) (2000).

⁹ Sending written mailings and also advertising by fax to businesses, was permitted due to the fierce lobbying of small and medium business owners that claimed that the aforesaid advertising methods are the less expensive and more efficient means to advertise themselves (as opposed to expensive advertising on billboards, commercial television and the like).

¹⁰ *CivilApp* 439/88 *Registrar of Databases v. Ventura* 48(3) P.D. 808 (1994).

¹¹ *Civil Case (Tel Aviv District Court)* 1994/06 *Liran v. Pelephone Communications Ltd. et al.* 2010(4) TAK-MEH 13911 (2010).