UIC John Marshall Journal of Information Technology & Privacy Law

Volume 14
Issue 3 *Journal of Computer & Information Law - Spring 1996*

Article 2

Spring 1996

Computer Legislation: Israel's New Codified Approach, 14 J. Marshall J. Computer & Info. L. 461 (1996)

Miguel Deutch

COMPUTER LEGISLATION: ISRAEL'S NEW CODIFIED APPROACH

by DR. MIGUEL DEUTCH†

I. INTRODUCTION

Statutory regulation of computers, particularly in the field of criminal law, has become widespread over the last years.[1] Different countries have adopted various legislative models in terms of both the scope and the technique employed. Israel recently established its statutory regulation of this area with the enactment of the Computer Law.[2]

Efforts to draft a computer law began in Israel about twelve years ago, culminating in a Draft Bill.[3] Israel has since witnessed significant changes in the status and the social function of computers, as well as long debate regarding the appropriate character of computer legislation and its content. Those opposed to creating a special body of law for computers argued it would lead to the "demonization" of computers.[4] Others saw the need to supply the public and the courts with a guide through

† Senior Lecturer, Faculty of Law, Tel Aviv University. The author prepared the Draft Bill of 1990 and took an active part in the preparation of the current legislation.

1. *See* Ulrich Sieber, General Report on Computer Crime: The Emergence of Criminal Information Law, International Academy of Comparative Law, 13th International Congress (Montreal, August 19-24, 1990) (surveying the current legislation in different countries concerning criminal law and the rules of evidence). Two important laws were enacted after this Congress: The Computer Misuse Act, 1990 (Eng.) and the revision of 18 U.S.C. § 1030 (1994). *See generally* Martin Wasik, *The Computer Misuse Act*, 1990 CRIM. L. REV. 767.

2. The Computer Law (5755-1995), 1534 LAWS OF THE STATE OF ISRAEL 366.

3. The Computer Draft Bill (5747-1987)(originally titled Offenses, Protection of Software and Rules of Evidence); *see* Moshe Shalgi, *Computer-Ware: Protection and Evidence, An Israeli Draft Bill*, 9 COMPUTER/L.J. 299 (1989) (outlining the draft bill); *see also* Yoram Bar Sela, *Computer Legislation in Israel: A Proposal Being Developed by the Ministry of Justice*, 21 ISR. L. REV. 58 (1986) (describing the preparation of the Draft Bill); *see generally Symposium*, The Computer and the Law, 21 ISR. L. REV. 1 (1986).

4. *See* Eliezer Lederman, *Improper Computer-Assisted Activity and Criminal Law in Israel*, 13 TEL AVIV U. L. REV. 499 (1988) (Hebrew). The controversy over whether special arrangements in the realm of computers are at all required is worldwide. *See* COLIN TAPPER, COMPUTER LAW 270-271 (4th ed., 1988).

this evolving technology. The purpose of this article is to evaluate the Israeli model adopted in the Computer Law in light of its original aims and the legislative process.

II. THE STRUCTURE OF THE COMPUTER LAW

The Israeli legislature chose a codified approach to the regulation of computers. The codified character of the legislation is expressed in two structural elements. First, the legal fields influenced by computers are grouped under a common legislative umbrella, as opposed to spreading the rules among the various areas. Second, computers and computerized materials are singled out as unique legal objects.

A. THE SCOPE OF LEGISLATION: A COMPREHENSIVE FRAMEWORK

The Computer Law deals with almost every legal field affected by the development of computers—criminal law, torts, evidence, search and seizure—within one comprehensive framework.[5] The advantage of this inclusive arrangement is that it prevents disparity between different branches of the law. The comprehensive approach provides a statutory basis for an entirely new branch of law. Yet, as detailed below, this new branch is organically integrated with the more traditional ones.

From a comparative perspective, the concept of a separate and comprehensive computer law is quite exceptional. During the drafting stage, one proposal was to amend various existing laws instead of creating a new legislative layer. The approach favoring the amendment of separate laws may result in a certain measure of incoherence. On the other hand, if a sharp disconnection is established between the special arrangements in the computer law and those prescribed by the general existing laws, it may result in the creation of contradictory provisions and legal confusion.[6]

On these grounds, Israel adopted a mixed approach. On one hand, the Computer Law places all the computerized information under one "umbrella," by this creating a uniform substantial and definitional

5. However, the Computer Law does not deal with the important issue of copyright protection. In 1988, an amendment was introduced into the 1924 Israeli Copyright Ordinance, protecting computer programs as literary works. The Copyright Ordinance § 2a, 1924 LAWS OF THE STATE OF ISRAEL 171. Nevertheless, substantive questions have remained open, such as the right to produce backup copies of computer programs, the authorship of computer generated works, and the duration of copyright protection for a computer program. On the other hand, these issues are addressed by the English Copyright, Designs and Patent Act, 1988. Legislation on this subject has not yet been completed in Israel as a public committee is now considering a general reform of Israeli law regarding intellectual property.

6. *See generally* TAPPER, *supra* note 4, at IV-XV for a discussion of the preferability of an approach integrating computer law existing laws; *see also* Lederman, *supra* note 4.

framework applicable to all computer operations. Thus, for example, the definitions of technological concepts such as "computer," "program," and "information" apply to all legal fields.[7] On the other hand, the Computer Law, in certain cases, planted its arrangement into the prevailing law in the subject area.[8] This allows continued reliance on the existing concepts in force within such an established field.

As an example of the codified approach, the Draft Bill of 1990 suggested that in order for harm to computerized information to be considered criminal, it must be performed "without lawful authorization." The initial formulation defined an act as tortious when it takes place "without lawful consent." No justification could be adduced for this distinction and therefore a third formulation, "unlawfully," was included in the final version. This ability to consider the total picture is one of the important advantages of a comprehensive codified approach to computer law.

B. Isolating Computers and Computerized Information

One question that emerged at the drafting stage was whether the arrangements in the Computer Law should be strictly confined to the field of computers or rather be extended to other similar technologies. For instance, one may wonder whether it is justified to consider disruptions to computer systems as a criminal offense, when the legal system provides no special protection to other centralized systems which bear a special social importance such as, power stations and railways.

The Israeli Computer Law acknowledges that computers play a unique role in social and economic life. Some of the arrangements specified in this law could extend to additional objects, but the law generally preferred to limit its scope to codification of computer laws. Nevertheless, two examples reveal the legislature's attempt to harmonize computers with other areas. First, the Computer Law changes rules concerning the admissibility of evidence, and applies these new rules of admissibility not only to computer print-outs, but to all business documents. Second, the Computer Law's regulation of torts refrains from

7. The Computer Law (5755-1995) § 1, 1534 Laws of the State of Israel 366.

8. In the law of search, for instance, the Computer Law amends the Criminal Procedure Ordinance (Arrest and Search) [New Version] (5729-1969), 2 Laws of the State of Israel (New Version) 284, by integrating the search of computerized material within the existing arrangements of this Ordinance. An indirect amendment was also in the Evidence Ordinance [New Version] (5731-1971), 18 Laws of the State of Israel (New Version) 421. In the area of torts, an intermediary approach was adopted. Although the existing Civil Wrongs Ordinance [New Version] was not amended, it was prescribed that a breach of a duty according to the Computer Law constitutes a new tort, and the general provisions of the Civil Wrongs Ordinance [New Version] such as vicarious liability and immunity of minors, apply to it. Civil Wrongs Ordinance [New Version] (5728-1968), 10 Laws of the State of Israel [New Version] 266.

making electronic access to computerized material a tort, thus avoiding the creation of a special rule concerning privacy based only upon the device in which the information is stored.

A codified approach to computer law cannot ignore the broader legal system and must weave its way into the existing fabric. To overcome possible inconsistencies, the Computer Law only operates in when one of three situations arises. First, when a computerized object requires protection, these objects are too abstract for traditional laws to protect them. Second, when the existing laws protect a computerized object, this protection remains questionable and a clear-cut arrangement is required. Third, even when the existing law protects the object, this protection is inadequate concerning the objects quality or scope.

III. THE OBJECTS PROTECTED BY THE COMPUTER LAW

An introductory chapter in the Israeli Computer Law defines the objects protected by the law: computers, information and programs.[9] The question arises whether these items should be defined by law or by technology. The main concern is to refrain from fixing the legal meaning of these concepts in such a way that they conflict with an evolving technology. This concern is not removed by expecting future legislation to address new situations when they arise, as the legislative process lags so far behind technological progress.[10]

A. THE PROTECTION OF COMPUTERS

The Israeli Computer Law protects computers and computerized material against a series of acts, such as unlawful access, hindering or disrupting their use. Since the Computer Law also outlines new criminal offenses, the nature of the protected object must be considered carefully. Simple computers should not be entitled to special protection. The Computer Law follows other legal systems[11] and excludes calculators from its protection. During the preliminary discussions, the legislature considered the exclusion of another group of simple computers, such as those

9. Unlike the English Computer Misuse Act, which refrained from defining these objects, the English Act adopted the recommendations of the Law Commission Report No. 186, Computer Misuse, Cm. 819. *See* Wasik, *supra* note 1, at 768 n.7. The American Congress and some state legislatures have adopted definitions for computer components. *See* 18 U.S.C. § 1030(1) and FLA STAT. CH. 815.03 (1994); CAL. CRIMINAL CODE § 502(b)(5) (West 1988); *see also* Criminal Law Amendment Act, June 20, 1985, ch. C-19, § 301.2, 1985 CAN. STAT. 272; Sieber, *supra* note 1, at 22 n.71.

10. *See* R.W.M. DIAS, JURISPRUDENCE Ch. 15, at 307-08 (1985) (examining the relationship between the law, technology and society).

11. *See* 18 U.S.C. § 1030(e)(1) (1995) (excluding from the definition of computers "portable hand held calculator or other similar devices"); *see also* CAL. CRIMINAL CODE § 502(b)(5) (West 1995) (excluding "calculators which are not programmable").

used as computerized timing devices in washing machines or other appliances. These computerized devices lack the programmable dimension unique to computers and thus, are unworthy of special protection. However, it was ultimately decided to omit this specific exclusion, given the difficulties of drawing clear distinctions between simple and more sophisticated aiding devices, such as the computerized systems used to navigate airplanes.

As the exclusion was rejected, a great number of computers are protected under the Computer Law and therefore, the wide scope of the law's criminal provisions may seem unreasonable. However, further restrictions threaten to leave vital machines unprotected. Therefore, in cases where the computer is covered by the Computer Law, but it does not merit special protection, a *de minimis* concept applies under the general laws.[12]

During the drafting of the Computer Law, some argued that only computers and computerized material used by businesses and government warrant special protection. This approach was rejected, as most of computers presently in Israel are used for both business and personal needs, making this distinction impractical. It is also worth noting that the Computer Law does not protect communication systems connected to computers, but only the operation of computers. Therefore, only when harm to the communication systems disrupts the use of a computer does the law consider such activity to be an offense.

B. The Protection of Programs and Information—"Computerized Material"

Both computerized information and computer programs are defined by the Computer Law as "computerized material."[13] The Computer Law only protects information or programs conveyed in machine readable language. Interference at an earlier stage is not forbidden for two reasons. First, at a stage prior to its translation into machine readable language, the material has not yet reached a level of functional maturity to justify granting it special protection. Second, the concept of providing special legal protection to computerized information in the criminal realm draws support, inter alia, from the difficulties entailed in tracing electronic activities. This argument does not apply when the relevant information is not electronically conveyed. This highlights a worthy policy of the Com-

12. In Israeli tort law, the *de minimis* defense is established in the Civil Wrongs Ordinance [New Version] (5728-1968) § 4, 6 Laws of the State of Israel (New Version) 266. In criminal law, this defense appears in the Penal Law (5737-1977) § 34(17), 869 Laws of the State of Israel 226 (amended in 1994).

13. The Computer Law (5755-1995) § 1, 1534 Laws of the State of Israel 366 (defining the terms information and computers).

puter Law which is to reserve protection of an interest until that interest is suitably identified.

IV. COMPUTER CRIMES

A. INTRODUCTION

Computer crime refers to two types of offenses, those against computers and those where computer technology is vital to the performance of the crime (computer-assisted crimes). Traditional computer legislation deals with the second group,[14] and the first group, offenses against computers, is a later development. The perception of computer crime today is a broader one, which includes all "information crimes."[15] The Computer Law deals with both groups of offenses.

Until 1994, American federal statutes protected certain computers against unauthorized access, disruption of use, and damage to information.[16] The scope of federal offenses against computers was broadened significantly through the enactment of 18 U.S.C. § 1030(a)(5)(A) and 5(B).[17] In addition, this amendment also regulates civil liability.[18]

---

14. *See, e.g.*, Lisa Menelly, *Prosecuting Computer-Related Crime in the United States, Canada and England: New Laws for Old Offenses?*, 8 B. C. INT'L. & COMP. L. REV. 551 (1985).

15. *See* Sieber *supra* note 1, at 6-7.

16. 18 U.S.C. § 1030 (1988); *see* Joseph P. Daly, *The Computer Fraud & Abuse Act—A New Perspective: Let the Punishment Fit the Damage*, 12 J. MARSHALL J. COMPUTER & INFO. L. 445 (1993); Glenn D. Baker, *Trespasser will be Prosecuted: Computer Crime in the 1990's*, 12 COMPUTER L.J. 61 (1993); Darryl C. Wilson, *Viewing Computer Crime: Where Does the Systems Error Really Exist?*, 11 COMPUTER L.J. 265 (1991); Brenda Nelson, *Straining the Capacity of the Law: The Idea of Computer Crime in the Age of the Computer Worm*, 11 COMPUTER L.J. 299 (1991); Christopher D. Chen, *Computer Crime and the Computer Fraud and Abuse Act of 1986*, 10 COMPUTER L.J. 71 (1990).

17. *See* 18 U.S.C. § 1030(a)(5)(A) and 5(B) (1994) (broadening the scope of the protected objects). This section prohibits damage to information stored in all kinds of computers, as well as damage to the computer itself or to a computer system, network, data or program; and it protects not only the use of computer and information, but also of computer services, systems, network, data and program. *Id.* The *mens-rea* required by the amendment is intent to cause damage or "reckless disregard of a substantial and unjustifiable risk" that such damage will occur. In addition, the term "access" has been replaced in this context, by referring to "transmission" of a program, information, code or command to a computer or computer system." *Id.* Yet the amendment limits the prohibited activities to those performed through a computer used in interstate commerce or communications. *Id.*

18. 18 U.S.C. § 1030(g) (1988) (creating the tort of computer tampering). This section limits recovery to economic damages and creates a special statute of limitations of two years.

B. General Remarks

1. *The Required Mens Rea*

The computer offenses specified in the Computer Law do not mention any *mens rea* requirement, except for certain preparatory offenses. In Israeli criminal law, a statute that fails to mention a specific *mens rea* is viewed as requiring a mens-rea of recklessness.[19]

During the drafting process, the legislature considered whether mere negligence or other low level of *mens rea* should be required in more serious offenses, such as in the insertion of a computer virus. However, this option was rejected. Negligence offenses are quite rare in Israeli law,[20] and introducing a lower mental state would present unnecessary risks and lead to the "demonization" of computers in society. American law requires the highest level *mens rea* in computer crimes, such as "knowledge" or "specific intent." [21]

2. *Unlawful Activity*

Most of the activities listed in the Computer Law are routine and only become illegal if done without the consent of the authorized operator. Acts such as accessing a computer, or erasing information, are properly acceptable when authorized. In the field of computer activity, criminal offenses must be restricted to those actions performed without consent. However, the application of general legal principles will permit some actions to be taken even without consent. For instance, if employees responsible for maintaining a computer system go on strike, it probably would be unjust to label the resulting damage as a computer offense, as long as the strike itself is legal.[22] The Computer Law, therefore, describes as crimes only as acts performed "unlawfully." English[23] and American law,[24] however, define only those acts done "without authorization" as criminal.

Introducing this element into the definition of criminal activity places the burden of proving unlawfulness on the prosecution, as well as whether the owner of the computerized material did or did not agree to the defendant's activity.

---

19. Abu-Ravia v. Att'y. Gen., 17 P.D. 2913 (1963).

20. Yuval Levi & Eliezer Lederman, Principles of Criminal Responsibility 523-24 (1981) (Hebrew).

21. *See* 18 U.S.C. § 1030.

22. *See* The Computer Law (5755-1995), § 2, 1534 Laws of the State of Israel 366 (protecting the integrity of information).

23. The Computer Misuse Act, 1990 (Eng.).

24. *See* 18 U.S.C. § 1030.

3. *De Minimis Computer Offenses*

The difficulties of defining the objects protected by the Computer Law promotes a broad formulation of the offenses and as a result trivial acts may unjustifiably be perceived as offenses. These difficulties are overcome by resorting to the *de minimis* exception and through the exercise of discretion on the part of the prosecution.

4. *Expansion of Preparatory Offenses*

The Computer Law defines a considerable number of preparatory activities as offenses. This trend derives from the assumption that the completed criminal act is extremely hard to prove and therefore, the earlier stages of criminal activities should also be defined as offenses.

C. OFFENSES AGAINST COMPUTERS AND COMPUTERIZED MATERIAL

1. *Disrupting the use of Computers and Computerized Material*

Section 2(2) of the Computer Law makes the disruption of the use of computers or computerized material an offense. This provision highlights the computer's unique role in social and economic life. While Israeli law generally views trespassing as an interference with the possession of property, it does not prohibit the interference with the *use* of that property. The criminalization of disturbance in the Computer Law marks a departure from this rule and is a recognition of the special value attached to the free use of computers.

Regarding this offense, it is particularly important to consider the circumstances in which an omission will be seen as an offense, especially when disruptions are the result of strikes. Under the Israeli criminal law, an omission may constitute a crime if the omitting person is under a duty to act. During the discussions of early drafts of the Computer Law, it was suggested that a special proviso should address the issue of striking employees who are under a duty to maintain a computer system. However, this section was omitted. Whether the basic right to strike turns these interferences into lawful disruptions has yet to be decided.

2. *Damage to Computerized Material*

The Computer Law protects the integrity of information. Under Section 2(d), erasing, changing or misrepresenting information expressed in machine language is an offense. In other legal systems, the integrity of computer stored information is protected by statutory provisions dealing with offenses against property or by special legislation.[25] However, un-

25. Sieber, *supra* note 1, at 25-26.

like the terms of the Draft Bill,[26] the Computer Law does not protect the integrity of hardware because it would have created an unjustified overlap between the Computer Law and the general criminal laws protecting property.[27]

3. *Computer Viruses*

Aware of the threat of computer viruses pose to computerized material, the Computer Law includes a special provision in this regard.[28] Offenders are handled with particular severity.[29] First, the penalty for introducing or transferring a computer virus is heavier than for other damaging activities. Second, the Computer Law defines the preparatory stages of a viral attack as an offense, even if no damage results. This stage is defined rather broadly. It is forbidden to engage in the creation of a viral program intended to cause damage to computerized material or to computers.

However, the Computer Law does not turn someone in mere physical possession of a viral program into a criminal, even if he intends to use the program in the future. Although this seems to open a link in the chain of criminal liability, this skip is justified. A person receiving a program knowing that it contains a virus becomes an accomplice to the offense of transferring a viral program; and if that person proceeds to transfer this program or introduce it into a computer, he becomes a principal offender. The only situation left is where the holder intends to use the program in the future, but only decided to do so after receiving the program. As no act was performed by the holder simultaneous to the development of the appropriate *mens rea*, this situation could only constitute an offense of omission if the principal refrained from destroying the program. The Computer Law does not take the far-reaching step of ascribing criminal responsibility to a preparatory omission.[30]

---

26. The Computer Law Bill (5754-1994) §2, 2238 LAW BILLS OF THE STATE OF ISRAEL 478.

27. The Penal Law (5737-1977) § 452, 869 LAWS OF THE STATE OF ISRAEL 226 (prohibiting damage to property).

28. The Computer Law (5755-1995) §6, 1534 LAWS OF THE STATE OF ISRAEL 366.

29. *Id.* The maximum penalty for this offense is three years imprisonment, but may reach five years if the crime reaches more advanced stages, such as the actual transfer or introduction of a virus to another computer. *Id.*

30. For a discussion of computer viruses under American law, *see* Susan M. Mell, *Administrating the Antidote to Computer Viruses*, 19 RODGERS COMP. & TECH LAW J. 259 (1993); James Tramontana, Note, *Computer Viruses: Is there a Legal "Antibiotic,"* 16 RODGERS COMPUTER & TECH. LAW J. 253 (1990).

D. Computer-Assisted Crimes

The distinction between offenses against computers and offenses assisted by computers is not clear-cut. To some extent, offenses assisted by computers are also offenses against computers. For instance, unlawful access may be classified as an offense against computerized material.[31] At the same time, access is often an early stage on the way to another offense and in that sense, it is also an intermediary stage in an offense assisted by computers. Regardless, the following offenses in the Computer Law are traditionally defined as computer-assisted crimes.

1. *Unlawful Access to Computerized Material*

This is a principal offense in the category of computer-assisted crimes. Other legal systems also prohibit access to computerized material, even when lacking any intention to perform by this any other offense.[32]

Although the confidentiality of material stored in a computer might also serve as a basis for forbidding access, this is not the rationale of the Computer Law. First, the offense only deals with electronic access to the material stored in a computer and not the very unauthorized reading of the material presented on the screen.[33] Second, the Computer Law does not protect the privacy of information stored in the computer as a separate interest. Thus, accessing this material does not constitute a tort under the Computer Law.[34]

Objections were raised during drafting that the approach in the Computer Law creates interlacing layers of offenses because if a person engages in unlawful access, he becomes an offender on three counts: through simple access, through access with intent to commit another offense, and through the other offense itself. This objection, however, is unjustified. First, access with intent to commit another offense is not a distinct offense from access, but amounts only to aggravating circum-

---

31. The Computer Law (5755-1995) § 2, 1534 Laws of the State of Israel 366.

32. *See* the Computer Misuse Act (1990) (Eng.) (forbidding an electronic "knock on the door"). The Computer Misuse Act states that any person who "causes a computer to perform any function with intent to secure access to any program or data held in any computer" commits an offense. *Id.* In American law, the unauthorized access alone is not classified as an offense unless it is accompanied with an intent to commit another criminal act.

33. The Computer Law (5755-1995) § 4, 1534 Laws of the State of Israel 366 (stating that access alone is punishable by three years imprisonment). Access accompanied with the intention to commit an act which is considered an offense by another law is punishable by five years imprisonment. *Id.* § 5.

34. *See infra* note 53 and accompanying text.

stances.[35] Second, the Computer Law only inflicts more severe punishment on an offender whose intent was to commit an offense outside of those listed in the Computer Law, and this will not be always the case.

Two further remarks are in place here regarding the arrangements endorsed by the Computer Law on this issue. First, unlawful eavesdropping to communication between computers is not unlawful access to computerized material. Rather, this is defined as wiretapping and the ordinary criminal law applies here.[36] Second, the precise definition of the forbidden access is "access to computerized material stored in a computer." Thus, it includes situations in which a person is allowed access to a certain areas of a computer, and through some manner, gains access to a particular file that he was not authorized to enter.

2. *Computer Fraud*

Section 3 of the Computer Law deals with the classic core of computer-assisted offenses, the alteration of information for the purpose of obtaining advantage. Altering information is a *per se* offense of damaging the integrity of information.[37] Furthermore, it constitutes an offense of unlawful access.[38] Yet, when such act is accompanied with fraudulent intention, a special element of deterrence is required. This special deterrence is expressed in both the level of punishment in the Computer Law[39] and in the wide scope of the offense, including any acts which involve the preparation, use, transfer or storage of fraudulent material. The offense is committed even if the fraud miscarried and the offender fails to reap any benefits.

The definition of this offense solves difficulties that could arise within Israeli law and that have indeed emerged in English jurisprudence. Proprietary offenses such as obtaining things by deceit, forgery and theft[40] are not likely to apply to computer-assisted crimes. For instance, regarding deceit, the false assertion is performed in a computer-assisted crime toward a machine rather than a person.[41] As for theft, something that is "capable of being stolen" must be taken, but regarding

35. *See also* The Computer Misuse Act, § 2, 1990 (Eng.) (making criminal intent an aggravating factor).

36. The Computer Law (5755-1995) § 4, 1534 LAWS OF THE STATE OF ISRAEL 366.

37. *Id.* § 2.

38. *Id.* § 3. Israeli Law prescribes a more severe punishment when the offender intends by the access to commit another crime not listed in the Computer Law. However, destroying information is not an offence according to the general criminal law.

39. *Id.* § 3 (stating that the maximum penalty is five years imprisonment).

40. The Penal Law (5737-1977) §§ 383, 415, 418, 869 LAWS OF THE STATE OF ISRAEL 226.

41. *See* Lederman, *supra* note 4, at 529 for a description of the Israeli law. *See* TAPPER, *supra* note 4, at 283-85 for a description of the English law.

electronic activities performed through computers, no taking occurs because the original information remains with person who entered it into to machine.[42] In forgery, the crime must involve a "document" and despite a broad interpretation, Israeli case-law is still unclear about the status of electronic signals as documents.[43]

E. Duty to Report

Following the Draft Bill of 1987, it was suggested that a failure of a director to report to authorities a computer crime against a public institution be labeled a criminal offense. This provision was omitted from the final version of the Computer Law. Israeli law does not impose a general obligation to report offenses committed in the past except in extreme cases, such as those involving minors or the disabled.[44] Despite the importance of the computer, defining this failure as a crime would be another source of "demonization" for computers and distort the proportions between computer crimes and others.

V. TORTS

A. Identification of the Interests Deserving Special Protection

Computerized activities raise a series of questions in the field of torts. For instance, questions arise concerning civil liability for computer-assisted fraud and concerning liability for negligence in the preparation of software or hardware.[45] Damages caused by using computers or computerized material can be addressed through the Israeli law of torts and they require no legislative reform. Because the tort of negligence is flexible and in a constant state of development,[46] it can easily be applied to these situations. Presently, the elements of negligence are open and retain their flexibility while listing specific provisions in this context might limit the creation of new computer-assisted torts.

Thus, the Computer Law focuses on the protection of two interests which are unprotected in the general law of torts. First, it protects the integrity of information. Erasing or altering computerized material stored in machine readable language constitutes a tort.[47] Second, the

42. *See* Lederman, *supra* note 4, at 522-27 for a discussion of this difficulty.

43. *See* Lederman, *supra* note 4, at 523-28. Lederman argues that despite the above mentioned difficulties, Israeli law can apply these traditional offenses to computers. *Id.*

44. The Penal Law (5737-1977) §§ 368A-E, 869 Laws of the State of Israel 226.

45. *See generally* Tapper, *supra* note 4, ch. 6.

46. *See* Daniel More, *The Civil Wrongs Ordinance in the Light of Forty Years of Case Law*, 39 Hapraklit 344, 366 (1990) (Hebrew).

47. The Computer Law (5755-1995) § 7(2), 1534 Laws of the State of Israel 366. For a discussion of civil liability and computer viruses in the United States, see Susan C. Lyman, *Civil Remedies for the Victims of Computer Viruses*, 11 Computer L.J. 607 (1992).

Computer Law protects the interest of use by defining the disruption of the use of computerized material or of the computer itself as a tort.[48]

The Israeli law of torts does not directly protect the right to use chattels, but only the possession of chattels. Similarly, Israeli law does not protect the integrity of abstract assets, but only that of tangible property. Yet, when there is an interference with the possession of tangible property, the interest of use is also disturbed and its damage can be a source of compensation under tort law.[49] Since information cannot be possessed, but only used, damage to information through electronic access is not actionable under Israeli tort law.

Yet, even when the possession of a tangible product containing information is disturbed, there are difficulties in awarding damages for the harm caused to the abstract interest. Because the interest protected by the tort of conversion concerns only the possession of the tangible object, it is questionable whether damages can be awarded for the "parasite" abstract interest.[50]

In English and in American law, the courts hesitate to protect abstract objects through proprietary torts, although the trend is to broaden the tort of conversion in this direction.[51] Both English and American law forbid the conversion of an abstract right when the right can be considered to be embodied in a concrete document which has been converted and evaluate compensation in such cases to include the value of the abstract object as well.

Negligence is constantly developing in Israel and may eventually protect these intangible interests without relying on the Computer Law. Two problems, however, make the protection of these interests less effective when based on this general legal instrument. First, a cause of action in negligence demands proof of damages. Such proof is difficult in terms of computerized material. Second, negligence demands the existence of fault, whereas proprietary torts under Israeli law impose absolute liability.

Israeli law provides protection to private information[52] and to commercial secrets.[53] The Computer Law does not independently protect the privacy of computerized information. Unauthorized access to com-

48. The Computer Law (5755-1995) § 7(1), 1534 LAWS OF THE STATE OF ISRAEL 366.

49. The Civil Wrongs Ordinance [New Version] (5728-1968) § 52, 10 LAWS OF THE STATE OF ISRAEL (NEW VERSION) 266.

50. *See* Gad Tedeschi, *Trade Secrets*, 35 HAPRAKLIT 5, 23-24 (1983) (Hebrew).

51. *See* PROSSER & KEATON, ON TORTS, 90-92 (5th ed., 1985) (discussing American law); JOHN G. FLEMMING, THE LAW OF TORTS, 54 n 27 (8th ed., 1992) (discussing English law).

52. *See* The Protection of Privacy Law (5741-1981) §§ 2(6)-2(9), 1011 LAWS OF THE STATE OF ISRAEL 128.

53. *See* Goodel v. Fenizia, 23(2) P.D. 434 (1965); Hahebra Lekbalim v. Kristianpoler Ltd., 29(a) P.D. 317 (1974) (protecting commercial secrecy through contract and confidence

puterized material without damage or disruption does not constitute a tort. Although the Computer Law does impose criminal liability for unlawful access *per se*,[54] this act is not defined as a tort in order to avoid different levels of civil liability between information stored in computer and that stored in more traditional forms. The legal protection of information should be a function of its content and not of the device within which it is embodied.

Why should not a similar consideration apply in the criminal field? Why is access to a computer, as such, perceived as a criminal offense in the Computer Law? The answer is that in the criminal field, the legal system seeks to deter access to computers in order to prevent additional computer offenses, and also because of the difficulty of proving that the offender succeeded in attaining results. The element of deterrence is not as intense in tort law[55] and therefore, there is no similarity between the criminal and civil arrangements.

B. The Nature of Protection

In Israel, proprietary torts are absolute in nature. Liability is not conditioned on proof of fault.[56] This view was adopted from English law,[57] and although this rule is the subject of strong criticism,[58] it is still the law in force. Should the protection of computerized material be patterned on the same model? If computerized material is deleted without fault, should responsibility for damages be imposed? The Computer Law chose an original solution, which differentiates between the two main remedies, injunction and damages. The remedy of injunction is granted unconditionally, without any proof of fault, and thus, in this respect, the legislature preserved the general frame of the Israeli law concerning proprietary wrongs. However, the Computer Law does not impose liability for damages unless the plaintiff can establish fault.[59] Freedom from liability in faultless situations reflects the understanding that sweeping responsibility is unjustified unless the right concerning information is classified as a right *in rem*. This question is hotly contested in the legal literature.[60] Furthermore, a single mistaken instruction in a program

---

law); *see also* Daniel Friedmann, The Law of Unjust Enrichment 306-12 (1982) (Hebrew).

54. The Computer Law (5755-1995), § 4, 1534 Laws of the State of Israel 366.

55. Flemming, *supra* note 51, at 7-8.

56. Oto-Bella v. Lucky Drive Ltd., 30(2) P.D. 207, 215 (1974).

57. *See* T. Weir, A Casebook on Tort 379 (4th ed., 1978); *see also*, Manfani and Co. Ltd. v. Midland Bank Ltd., 1 W.L.R. 956, 970-71 (1968) (Eng.).

58. D. Friedmann, Property Law and Fault 241 (1984) (Hebrew).

59. The Computer Law (5755-1995) § 9, 1534 Laws of the State of Israel 366.

60. *See* Arnold S. Weinrib, *Information and Property*, 38 U. Toronto L. Rev. 117 (1988).

may result in heavy damages to information and therefore extending liability in faultless situations is inappropriate. Rather than over extend liability, the Computer Law favored a more prudent approach.

VI. RULES OF EVIDENCE—ADMISSIBILITY OF COMPUTER PRINT-OUTS AND BUSINESS RECORDS

A. INTRODUCTION

In both the Anglo-American and the Israeli system, two fundamental obstacles hinder the admissibility of computer print-outs: the hearsay rule and the best evidence rule. As for the hearsay rule, computer print-outs are usually considered hearsay when they are used to prove the truth of the print-out's content. First, the person feeding material into a computer usually has no direct knowledge of truth of his information. Second, a print-out is the out of court statement of the person who made the entry and therefore, it is unacceptable as proof, unless an exception to the hearsay rule applies. Thus, according to the general rules of hearsay, print-outs are inadmissible even if submitted by the person who prepares them. A print-out is obviously inadmissible when the person testifying to its truth is not the one who prepared it.[61] Furthermore, according to the "best evidence" rule,[62] the print-out is only a copy of the original material that was entered into the computer.[63] Prior to the Computer Law, these legal doctrines precluded the admissibility of computerized material that should have been allowed on efficiency grounds.

The Israeli legislature was therefore motivated to bring about an essential change in the law. At the early stages, the initiative was limited to creating a new exception to the "best evidence" rule, namely, that when the basic material used to produce a print-out could be submitted as direct evidence, this rule would not preclude the presentation of a print-out based upon this material. This step would have been too cautious, however, as it would still preclude efficient submission of print-outs, considering that the basic material is often not based on direct knowledge. Thus, the legislature went a step further and prescribed that under certain conditions, a print-out is admissible as proof of its content even when the basic material could not be classified as direct evidence. This legislative move raised the question of whether there is a place for discrimination against non-computerized business records, since efficiency considerations apply to these records as well. Thus, the

61. *See* 2 MCCORMICK, ON EVIDENCE 294 (4th ed., 1992) (discussing American law on the admissibility of print-outs); *see also* CROSS, ON EVIDENCE 558-60 (Colin Tapper, ed., 7th ed., 1990).

62. ELIAHU HARNON, LAW OF EVIDENCE 146 (1970) (Hebrew).

63. Ofer Argov, *Admissibility of Computer Print-Outs*, 20 MISHPATIM 131, 162-63 (1990) (Hebrew); *see also* TAPPER, *supra* note 4, at 372.

Computer Law expanded its new admissibility rule to also include non-computerized records.

The Israeli legislature could rely on the Anglo-American experience. In England, print-outs are admissible in civil proceedings when they meet the condition of regularity; specifically, that the computer is used by the organization to process this type of information and that this information is supplied in the ordinary course of business. The proponent must also prove the proper operation of the computer at the relevant time.[64] However, English law does not require proof of direct knowledge on the part of the individual or the body holding the information.[65]

In the criminal field, submission of print-out has to meet the conditions of Section 69 of the Police and Criminal Evidence Act and of Section 24 of the Criminal Justice Act of 1988.[66] The Police and Criminal Evidence Act declares that if there is no reasonable grounds for believing that the print-out is inaccurate due to inappropriate use or malfunction, the print is admissible. The Criminal Justice Act requires proof that a business document be created or received by a person in the course of his business or profession and that the information was received from a person having personal knowledge about the underlying events. In appropriate cases, computer print-outs are admissible under the general hearsay exception dealing with a document prepared "under a duty."[67] In American federal law, admissibility of print-outs is covered by Section 803(6) of the Federal Rules of Evidence. This section states that business records are admissible if the recording takes place close to the event; the information is delivered by someone possessing personal knowledge of the facts; and the preparation and storage of these records is within the regular course of the business. However, Section 803(6) does not apply in circumstances pointing to lack of trustworthiness.[68]

B. Outline of Admissibility Under the Computer Law

The Computer Law states that records of a business or public body, computerized or not, are admissible as proof of the truth of their contents when the conditions outlined *infra* are met. This establishes a new exception to the hearsay rule and to the best evidence rule. The Computer Law does not detract from other exceptions to these rules. Furthermore, this exception is not meant to contravene other grounds of inadmissibility, such as irrelevance.

---

64. The Civil Evidence Act, 1968, § 5; *see also* Cross, *supra* note 61, at 558.

65. Tapper, *supra* note 4, at 385.

66. R. v. Minors, 2 All E.R. 208 (1989).

67. *Id.*

68. *See generally* 2 McCormick, *supra* note 61, at ch. 29.

The Computer Law does not distinguish between large and small businesses, nor does it distinguish between state controlled businesses, such as banks, and private concerns. Admissibility does not differ between civil and criminal proceedings and if the conditions are met, the records are admissible in both realms. Of course, documents prepared by the prosecution or other investigative bodies are excluded from serving as proof of the defendant's guilt. Admissibility under the Computer Law requires several elements. First, that the recording took place in the usual course of business. Second, the records must be prepared close to the subject events. Third, the record must be prepared in circumstances which give general credibility to the document. Fourth, there must be evidence that the computer was operated properly. Under the Computer Law, a print-out is regarded as an original document, rather than as a copy and thus the best evidence rule does not preclude its admissibility.

A prolonged controversy surrounded the ultimate formulation of this section, reflecting different views concerning the proper balance between efficiency and justice. Some of the critics see the conditions of admissibility as too lenient, while others claim with equal vehemence that the conditions are too rigid and hinder efficiency.

1. *Admissibility, Rather than Prima Facie Evidence*

Until the enactment of the Computer Law, Israeli banks benefitted from a special provision in the Evidence Ordinance (New Version) stating that bank documents were prima facie evidence.[69] This meant that bank records were not only admissible, but also granted significant weight. This advantage in terms of credibility was abolished by the Computer Law.[70] The present scheme addresses only admissibility and does not take a stand regarding the weight of the evidence.

Indeed, evidence which is admissible under the Computer Law may be insignificant in appropriate cases, because the Computer Law, as previously mentioned, does not take a stand regarding the weight of the evidence. Yet, in practice, once a document passes the admissibility test, it is not easily dismissed as lacking any value. Thus, one should not underestimate the practical consequences of the very admissibility of such records.

2. *Lack of Distinction Between Different Types of Businesses*

As noted, the Computer Law does not distinguish between records of

69. The Evidence Ordinance [New Version] (5731-1971) § 37, 18 LAWS OF THE STATE OF ISRAEL (NEW VERSION) 421.

70. The Computer Law (5755-1995) § 10(1), 1534 LAWS OF THE STATE OF ISRAEL 366.

large and small businesses, or between State controlled industries[71] and private concerns. These distinctions were considered inadvisable for two reasons. First, the scope or turnover of a business bears no relevance to the credibility of its documents. Nor does the existence of State control, as the State often lacks the appropriate instruments for examining the reliability of the organization's documents. Second, one of the conditions of admissibility is the need to prove that the circumstances which produced the record ensure credibility.[72] If the business does not enforce appropriate controlling procedures, the record will probably not meet this condition and thus, not be admissible.

3. *Foundational Procedures*

The Computer Law does not lay out a particular procedure for submitting records, nor does it determine who is the appropriate witness for laying foundation.[73] According to the Computer Law, the witness testifying to the truth of a record need not have direct knowledge of the underlying data. The main advantage to creating a special exception to the hearsay rule is that the person submitting the record need not be acquainted with it. Yet, he must provide evidence of the conditions of admissibility.

During the legislative process, it was suggested that the submission of a print-out be accompanied by an affidavit signed by the person in charge of the computerized processes. This person could be questioned, but only if so required by a court order. Although this suggestion generally follows the lines of current English law,[74] it was ultimately rejected. Unless the fulfillment of the preconditions becomes controversial, the preparation of such a document might inflict an unnecessary burden. On the other hand, denial of the absolute right to cross-examine the witness submitting the material is too harmful to the interests of the other party. The Computer Law refrained from prescribing any special provision on this issue, and thus the question of whether the preliminary conditions of admissibility have been met will be decided through ordinary testimony.

---

71. For the control of banks and insurance companies, *see* The Insurance Business (Control) Act (5741-1981), 1021 LAWS OF THE STATE OF ISRAEL 94; The Banking Ordinance, 1941 Official Gazette 1134, (E) 85.

72. The concept found in American law, FED. R. EVID. 803(6) (1995), was adopted in the Computer Law concerning this issue.

73. The American law prescribes that the person submitting the record must be a "custodian or other qualified witness." *Id.*

74. The Police & Criminal Evidence Act, 1984, § 69. According to part II, § 8, of Schedule 3, print-outs should be submitted through a document describing the way in which the print-out was produced, the devices used for this purpose and all other issues requiring proof. *Id.* Interrogation of the person submitting the document is left to the discretion of the Court. *Id.* part II, § 9.

4. *Lack of Organization Knowledge*

Unlike English and American approaches to the admissibility of computerized records, the Computer Law does not to require that the person preparing the record or any other person in the organization be personally acquainted with the facts. In other words, not only is there no requirement that the specific person preparing the record have personal knowledge of the events, but the entire the organization, as such, is exempt as well. Instead of such a requirement, a flexible demand for signs of credibility in the submitted record is established under the Computer Law. This demand looks, inter alia, to whether the organization has any direct knowledge of the facts, but without making this element a vital datum. Obviously, such a discretionary element diminishes legal certainty, but it empowers the courts with a powerful device for efficiently dispensing justice.

5. *Indirect Proof of Admissibility Conditions*

The Computer Law does not require proof of the specific circumstances under which the document was prepared, but only proof that such documents are generally drafted at the time of the event in a credible manner. A similar approach demanding only general proof concerning admissibility conditions is also applied by American law.[75] Nevertheless, direct proof is required of the fact that the specific record was produced in the regular course of business. Although this imposes a significant burden on admissibility, this demand seems unavoidable. The other conditions of admissibility become meaningless unless the typical procedures of the organization are linked to this particular document. However this burden is easily overcome through the use of circumstantial proof.

6. *The Search for Truth*

When the scope of admissibility for computerized evidence is broadened; concerns arise regarding the dangers of such admissibility to the process of finding the truth. Cross-examination of witnesses submitting the evidence will no longer yield results, as the witness is not required to have personal knowledge of the recorded facts. It is therefore necessary to provide the other party with appropriate means to refute the weight of the record. The Israeli law prescribes two such means.

First, Israeli law grants the right to full disclosure of documents available to the other party in the course of litigation.[76] Second, the

75. FED. R. EVID. 803(6).

76. The Criminal Procedure Law (5742-1982) § 24, 1043 LAWS OF THE STATE OF ISRAEL (CONSOLIDATED VERSION) 43; The Civil Procedure Regulations (5744-1984), § 112, 4685 REGULATIONS OF THE STATE OF ISRAEL 2220.

Computer Law contains a special rule concerning cross-examination. Usually, opponents will try to refute the truth of the computerized records by summoning witnesses. Often, the only witnesses with direct knowledge of the facts will be employed by the organization originally offering the record. Although a basic rule of procedure states that the party summoning a witness may not cross-examine him, the Computer Law allows the party who has summoned a witness connected to the organization submitting the document to cross-examine him.

These two techniques guarantee that the greater admissibility under the conditions of the Computer Law will not be overly harmful to the principle of justice. However, if the basic documents are unavailable, or the witness with personal knowledge of the data is unreachable, the courts may admit testimony that cannot be directly attacked, and may decide issues on flimsy evidence. Yet, it may reasonably be assumed that the courts will assign considerably low weight to such evidence, under the circumstances.

7. *Civil vis-a-vis Criminal Proceedings*

The new exceptions to the hearsay evidence rule and the best evidence rule in the Computer Law are, undoubtedly, a daring step forward in Israeli law. A great deal of apprehension surrounded the legislation regarding the admissibility of computerized evidence in criminal proceedings. The possibility that a defendant might be found guilty without any direct evidence seemed unacceptable to many, and the guarantees failed to allay these concerns. Nor did critics find comfort in the answer that only admissibility was being lowered and that indirect evidence still carried negligible weight. Critics felt that courts would nonetheless ascribe undue weight to such evidence in the absence of any rebuttal.

An attempt was made during the discussions to soften the impact of broadening the admissibility of business records. It was suggested that the Computer Law precludes conviction based solely on uncorroborated computerized evidence which would have been inadmissible prior to the Computer Law. However, this was rejected because it replaced one formal barrier, the conditions of admissibility, with another, the need for corroboration. Although the Computer Law made no distinction between civil and criminal proceedings, one proviso states that in criminal matters, any records produced by the prosecution or other investigative bodies in the course of preparing the criminal indictment are inadmissible as evidence of guilt.

VII. SEARCH AND SEIZURE

The Computer Law adapts the rules of search and seizure to computerized material as an abstract entity. Police and other investigative

bodies may need to engage in the search of computerized material to trace criminal activity. It is doubtful whether a search of this type could have been conducted before the legislation of the Computer Law, given the abstract nature of the object of the search. The Computer Law empowers these agencies with the authority to search computerized material. However, the Computer Law specifies two important reservations. First, computerized material may only be searched under court order, while searches concerning physical objects may sometimes be conducted without court order. Further, the court must explicitly specify the limits of such a search. Second, the search must be conducted by a person trained to work with computers to lessen or avoid potential damage to information from the search. These restrictions are based on the assumption that the search of computerized material may injure the privacy or damage the integrity of the information stored in the computer.

These elements create a balance between the practical need to search and the protection of the rights of the individual. Following the enactment of the Basic Human Dignity and Freedom Law,[77] this balance requires careful attention. Finally, the seizure of computers or computerized material is under judicial control, once the period of time exceeds forty-eight hours.

VIII. CONCLUSION

The anatomy of legislative process surrounding the Israeli Computer Law conveys the difficulties of the legal system in regulating technological developments. For no less than ten years, the legislature considered a long series of drafts before arriving at the present formulation. The final version contains very little material from the original Draft Bill, as if the legislature was waiting to gain a broader understanding of the impact of the computer in social and economic life. The attitude of reverence toward the computer at the beginning of the process has been replaced by more a realistic approach. Computers are now mundane possessions and the question has become whether the computer should be treated as legally different from other instruments at all. On the other hand, widespread familiarity with computers underlines the need for new laws to protect the unique aspects of computerization.

The legislature identified the most important issues: a need to protect the abstract interests embodied in computers and a need to enable the admissibility of computerized records. Additionally, a central contribution of the Computer Law is that as a by-product of the enhancement of the admissibility of computer print-outs, it catalyzed a change in the

77. The Basic Law: Human Dignity and Freedom (1992), 1391 LAWS OF THE STATE OF ISRAEL 150 (providing constitutional protection for, inter alia, the rights to privacy and property).

admissibility of all businesses and public body records. Undoubtedly, the information age will require additional structural developments and thus promote similar overdue modifications in other long-serving legal fields.