UIC John Marshall Journal of Information Technology & Privacy Law

Volume 9
Issue 3 *Computer/Law Journal - Summer 1989*

Article 2

Summer 1989

Computer-Ware: Protection and Evidence, An Israeli Draft Bill, 9 Computer L.J. 299 (1989)

Moshe Shalgi

COMPUTER-WARE: PROTECTION AND EVIDENCE, AN ISRAELI DRAFT BILL

By MOSHE SHALGI*

TABLE OF CONTENTS

I. INTRODUCTION

The massive computerization of the economy, administration, and other branches of social life in Israel began about a decade ago. With it came the need for legal protection of proprietary and other rights related to the spreading use of computers, a need that emerged in all of the technically developed parts of the world. Unlike legislatures elsewhere, the legislative machinery in Israel became aware of these needs before other circles, such as the academic, raised the issues involved. In 1983, the author was commissioned by the Fund for Advancement of Law, sponsored by the Ministry of Justice, to prepare a draft of a bill concerning the criminal aspects of the protection of hardware, software, and data. Subsequently, in 1984, the project was enlarged to include civil and evidentiary aspects. The preliminary draft was submitted to the Ministry of Justice in 1984. It was then examined by a committee composed of members of the staff of the Ministry of Justice, staff members of other governmental bodies, and legal advisers of firms in the

* Dr. Jur. M.A., Judge (ret.), District Court. (4 Joshaphat st., Jerusalem 93152, Israel).

computer business. The committee suggested several amendments, and this draft of the bill was accordingly revised by the author. In March 1987, the Deputy Attorney General for Legislation circulated a memorandum, regarding the legislative project, among the legal advisers of the Ministries, other governmental departments, the judiciary, the law faculties, and other interested parties. This memorandum pointed out and explained the proposed provision and included the revised draft of the bill (hereinafter "Draft Bill") itself.[1]

During the last decade, many jurisdictions have amended their laws in order to meet the new requirements posed by the developments in computerization. In most cases, the necessary amendments were made piecemeal, by each branch—criminal, copyright, evidence, etc.—of the law. The Draft Bill, on the other hand, attempted to deal comprehensively with all the aspects of the subject. From the point of view of giving proper legislative answers to social demands, there is no difference between these two methods. However, because the initiators of this bill intended to deal with the subject comprehensively, this resulted in a single piece of legislation, which seems more elegant.

This Article does not discuss the general problems of computers and the law, nor does it deal with questions that are of specific concern to the Israeli legal system. Instead, the purpose of this Article is to present the main premises and basic policies of the Draft Bill as one example of a legal solution to the goals of computer law.

II. DRAFT BILL: CHAPTER ONE

Chapter 1 of the Draft Bill defines key terms. The most important of which is the definition of "computer." Almost all computer laws include one or another definition of this term. The definition adopted in the Draft Bill[2] includes the essential features of computers and is based on a standard definition adopted by many states in the United States.[3] The nucleus of a computer is its arithmetic/logical faculty of processing, according to a program, data received or stored. Another essential feature is its ability to produce output in several forms. That their function is electronic and their manipulations are of electronic or magnetic

1. *See* Appendix *infra*, for text of Draft Bill.

2. *Id.* Draft Bill § 1.

3. *Cf.* S. Nycum, A. Snow & E. Bartlett, Computer Crime Legislation in the United States 20 (June 18, 1985) (prepared for the Harry Sacher Institute for legislative research and the International Symposium on Law and the Computer, Jerusalem, Israel, June 18, 1985). " 'Computer' means an electronic device which performs logic, arithmetic or memory functions by the manipulation of electronic or magnetic impulses and includes all input, output, processing, storage, software or communication facilities which are connected or related to such device in a system or network." In the United States, this definition is used in at least 13 states, among them Michigan, Wisconsin, Arizona, and Delaware. *Id.*

impulses is invariably true of computers, but this is not what differentiates them from many other machines. Thus, the Draft Bill's definition concentrates on what is necessary and sufficient for legal purposes. The second part of the standard definition is included summarily by the term "peripheral equipment." This enables the courts to include within the term "computer" all related devices—both those in use today and enumerated in the (standard) definition, and those that may come into use when new devices are invented and their use becomes widespread.

Because the term "program" has other connotations (both in English and in Hebrew), a definition of this term for the purposes of the law is indispensible. The Draft Bill's definition again includes what seems essential—that a program is a series of instructions for the operation of a computer. What has been added is an element peculiar to computer programs: a program may take several, completely different, forms of the same essence—in writing or in any other form, even not readable by man. This feature, as is well known, creates a major difficulty in applying traditional provisions of criminal law (theft, for instance), tort law, and copyright law to infringements related to programs. These laws are based on concepts of tangible objects and intellectual works reduced to forms accessible to the human senses of sight and hearing. The definition of "program" must, of course, include these forms as well as that of an "intangible object," the electronic form.

It is now generally accepted that material that is auxiliary to a program, such as documentation and specifications, ought to be protected in the same manner as the programs themselves. Although almost all of the Draft Bill's provisions apply equally to programs and to such related material,[4] it seemed advisable to provide different definitions for "program" and for "software" to obtain elegance of drafting. While the definition of "program" is descriptive of its essential features, the definition of "software"[5] is denotative. The definition of software also includes program specifications and auxiliary material. This is quite an open definition and allows the courts to widen it to include new forms of auxiliary materials that may be developed in the future.

Another important point is that the Draft Bill differentiates between "information" and "data." Information is data processed by the computer, and the two terms should not be confused. Input is always composed of data, but output may be made of data or of processed data. (Processed data can be defined as elements of data combined with elements of processing.) The aim of the Draft Bill is to make it clear that processed data is protected to the same extent as is a program.

4. *But cf.* Appendix *infra*, Draft Bill § 31(a)(3).
5. *Id.* Draft Bill § 1.

The definition of "thing" was also included[6] in order to enlarge the traditional definitions of the term in other laws because these traditional definitions do not cover software and data stored in an intangible form. Unless this element is included, for the purposes of the Draft Bill, the courts could interpret the term by analogy to exclude it. This term is used many times in the Draft Bill and it should be properly defined.

III. DRAFT BILL: CHAPTER TWO

Chapter 2 of the Draft Bill contains the criminal aspect of the provision, and it defines offenses so as to afford protection against computer abuses.

One major point ought to be mentioned first: the Draft Bill distinguishes between two forms of interests in computers—the proprietary interest on the one hand, and the public's interest in the proper and unimpaired function of computers on the other. The emphasis in the criminal provisions is on protecting the second interest rather than the first. The criminal provisions apply only to acts detrimental to hardware, software, data, or information that are used or are to be used for certain purposes, *i.e.*, by institutions or enterprises in the proper function of which there is a public interest.[7] When these are not used for such purposes, but rather for interests of a mere private character, the Draft Bill does not use criminal sanctions to protect them against malfeasors. The civil remedies enumerated elsewhere in the Draft Bill[8] seem to be more adequate in such cases and are not limited to specific categories of hardware, software, data, and information.

The reason for this distinction between the proprietary and public interests is linked to the severity of the Draft Bill's proposed criminal penalties. Compared with the standards of criminal punishment in the current Israeli penal law, the Draft Bill's are quite severe. As is well known, uncovering computer offenses is very often quite difficult—especially when, as in too many cases, the offenses are not even reported to the investigating authorities. In such cases, one means of securing effective deterrence, as the Draft Bill proposes, is severe punishment.[9]

---

6. *Id.*

7. *Id.* Draft Bill § 10.

8. *See id.* Draft Bill § 27.

9. Please note, however, that penalties prescribed by law in Israel are maximum penalties, except in very rare cases; the courts may award less severe punishment. Furthermore, since 1970, penal laws in Israel do not explicitly prescribe fines or other forms of punishment (*i.e.*, suspended sentences, public service, etc.), except when the penalty is solely a fine. General provisions of the Penal Code set forth a scale of maximum fines proportionate to the maximum imprisonment scale. Similarly, other general provisions provide for other forms of punishment.

Yet, such severe penalties are only justified when the interest protected is an important one. The proprietary interest is not deemed to be of such a character.

In accord with this policy of protecting the public interest, sections 2-4 define prohibitions that are of major public importance: disruption of a computer's operation, preclusion of computer services, and causing disrupted results of a computer's output. These are considered the most severe. The next three sections define offenses in terms more reminiscent of proprietary rights in software. What is actually protected is, again, the public's right to the proper functioning of computerized systems. Offenses under these sections are detrimental to both the public's interest in enjoying the unimpaired services of computers, and the owner's or holder's proprietary interests.

On the other hand, section 8 protects wholly proprietary rights. Because these offenses more characteristically involve software, the proprietary rights over software should be protected. Unlawfully obtaining programs is too common and too profitable a way to obtain another's property, like unjust enrichment, and it should be prohibited by law. In the author's opinion, this subject is included in the Draft Bill because traditional laws, such as theft, do not apply to programs in electronic form. It is also supposed that civil remedies, as provided for in Chapter 4 of the Draft Bill, do not suffice to prevent these profitable infringements, which are also difficult to trace. Therefore, penal sanctions are necessary.

The same attitude is taken in section 9. Inducing reliance on a false output is an offense similar to fraud. However, certain considerations justify its inclusion in the Draft Bill. Computer output enjoys a very high reputation for being correct and reliable. Drawing on this reputation, a false output is foreseeably detrimental to the innocent, and prior knowledge of it should be made an offense per se. Under the Israeli Penal Code, the traditional offense of fraud and similar offenses require that something is obtained through a fraudulent act.[10] This is not required under section 9; merely inducing reliance on an output that is knowingly false amounts to an offense.

Section 11 provides an excuse for the penitent who caused disrupted results by operating a computer under section 4. The purpose of this provision is to encourage an offender to try to prevent or to mitigate any damage that may result from his conduct before it occurs. Generally, post-offense conduct is taken into consideration to mitigate the sentence. Under the Draft Bill, conduct showing genuine repentance would not only amount to a defense against conviction, but to an

10. *See* §§ 414-15 of the Penal Law, 1977, Sefer Hahukim 1977, at 226 (Hebrew).

actual pardon by law.[11] The harm that the public suffers from disrupted results may be very serious, indeed, and such indulgence seems a price worth paying in order to prevent it.

Section 12 is in the same spirit as section 11 but for a different reason. Violations of legal provisions take innumerable forms, from the gravest to the most trivial. Yet convictions of criminal offenses carry a special stigma, in professional as well as public circles, often disproportionate to the actual nature of the offense. Section 12 empowers the court to refrain from convicting a culprit of an offense, under the Draft Bill, if it determines that the actual offense was not grave and was committed without malice. Abstention from conviction would not, however, preclude the court from convicting the defendant of another, less stigmatic, offense if the culprit's conduct amounted to one.

Another noteworthy provision concerns seizure of computers, and the media that store data, information, or software, by the authorities. Though the seizures themselves are in the public interest, they may also impede services to the public—a consequence the Draft Bill seeks to prevent. Section 13 suggests restricting the investigating authorities' powers to seize these objects. Unlike other objects that may constitute proof of an offense and may, under Israeli criminal procedure, be seized by the investigating authorities without a court order, these computers and media may not be seized without a court order. If such an order has been given ex parte, it is effective for only twenty-four hours.

Section 14 contains an uncommon provision: mandatory notification of an offense to the police. Under Israeli law, a person who knows that an offense has been committed is not obligated to report it to the authorities.[12] However, under the Draft Bill, a person in charge of an employee[13] who knows that the employee has committed an offense must report it unless his own superior is also aware of the offense. In the latter case, the superior has the duty to report the offense. Noncompliance with this duty is itself an offense punishable by one year's imprisonment.

The purpose of this provision is to minimize the well-known phenomenon, peculiar to computer offenses, that managers of business en-

11. *See* Appendix *infra*, Draft Bill § 11.

12. *But see* §§ 95, 262 of the Penal Law, 1977. Section 95 creates a duty to report when one knows of an intent to commit or knows of the committal of an offense against state security, foreign relations, or official secrets punishable under sections 97-121 of the law by imprisonment for fifteen years. This exception is an attempt to prevent the consequences that would result from the committal of such an offense. Section 262 creates, among other things, a duty to report when one knows of an intent to commit an offense punishable with imprisonment exceeding three years. This exception was created in an effort to prevent the committal of such an offense.

13. *See* Appendix *infra*, § 14(c).

terprises, and other institutions that value public confidence, are quite reluctant to publicize the fact that computer offenses have been committed within their businesses. They often prefer to tolerate the consequential losses rather than expose the incident to the public and experience the inevitable loss of reputation. It would be difficult to combat computer crimes if their victims, by keeping silent, became "accessories after the fact." As unpopular and exceptional as this provision may prove to be, its usefulness may be proven by its ability to abate computer crime.

Part B of Chapter 2 allows computer penetration for public security purposes. Unauthorized computer penetration or obtaining related software, data, or information may constitute an offense or a cause of action under the Draft Bill, the Privacy Protection Law,[14] or other laws. Nevertheless, state and public security demands may justify the violation of these protected rights, and may even sanction it. When state security demands it, the Prime Minister and the Minister of Defense are separately empowered to authorize a penetration as long as they are satisfied that the aim justifies taking this step.[15] If the purpose of the penetration is public security and is in the interest of preventing a crime or of apprehending offenders, the President of a District Court[16] may authorize the penetration.[17] There is no appeal or judicial supervision on the use of this power except to the extent that the President of the District Court may refuse to grant a permit.[18] The supervision, which is interministerial because the Minister of Justice also takes part, is only of political consequence.

Similar provisions are not novel in Israel. The Draft Bill follows almost exactly the same arrangements as those provided for in the Secret Eavesdropping Law.[19] As far as the author is aware, no one has expressed any dissatisfaction with the similar powers under this law.

IV. DRAFT BILL: CHAPTER THREE

The civil rights of a party wronged by the commission of a tortious act involving software, data, or information are dealt with more summarily in Chapter 3 of the Draft Bill.

Two actions are taken in the Draft Bill. First, as has already been mentioned, the present law of torts in Israel does not apply to intangi-

14. Privacy Protection Law, 1981.

15. *See* Appendix *infra*, Draft Bill § 16.

16. For the purposes of judicial jurisdiction, Israel is divided into five districts, and a district court has been established in each of these districts. In civil and criminal matters, its jurisdiction is both of first instance and appellate.

17. *See* Appendix *infra*, Draft Bill § 17.

18. *Id.* Draft Bill § 17(c).

19. Secret Eavesdropping Law, 1979, Sefer Hahukim 1979, at 110 (Hebrew).

ble property, such as electronically-stored material. Adapting the terms proposed in section 20 will overcome this difficulty. Consequently, insofar as conduct constitutes a wrong under existing provisions of tort law, it would be actionable, irrespective of the fact that the damaged object is intangible.

Second, section 19 declares every category of conduct prohibited under sections 2-9 a wrong. Even if the conduct is technically not a wrong under existing tort law it would become one, and a party wronged by criminal conduct would also be able to sue for a civil remedy.

Furthermore, the right of bringing a civil action is not limited to wrongful conduct with respect to computers, software, data, or information that serve public interests, but additionally applies to those serving purely private purposes.[20]

V. DRAFT BILL: CHAPTER FOUR

A third aspect of computer law concerns the rights of the software author. Chapter 4 of the Draft Bill is dedicated to this subject.

It is generally accepted that a proper way to protect the intellectual property rights of software authors is in a manner analogous to the copyright protection enjoyed by literary authors and artists. Consequently, many jurisdictions amended their national copyright laws to provide software authors with protection that is similar to that extended to authors of other creative works.

However, two major arguments have been raised in favor of a different approach. First, the interests of the author of software and data are, to a considerable extent, different from those of the artist or the literary author. This is easily shown by comparing two documents representative of the respective interests. First, under the Berne Convention for the Protection of Literary and Artistic Works,[21] the author of a work has the exclusive right to authorize the following: the reproduction of the work;[22] the translation of the work;[23] the broadcasting of the work;[24] the public recitation of the work;[25] the adaptation of the work;[26] the cinematographic adaptation and/or reproduction of the

20. *See* Appendix *infra*, Draft Bill § 21.

21. Berne Convention for the Protection of Literary and Artistic Works, Sept. 9, 1886, *revised at* Paris, July 24, 1971, *reprinted in* WORLD INTELLECTUAL PROPERTY ORGANIZATION (WIPO), GUIDE TO THE BERNE CONVENTION FOR THE PROTECTION OF LITERARY AND ARTISTIC WORKS (PARIS ACT, 1971) (1978) [hereinafter Berne Convention].

22. *Id.* art. 9.

23. *Id.* art. 8.

24. *Id.* art. 11*bis*.

25. *Id.* art. 11*ter*.

26. *Id.* art. 12.

work;[27] and the distribution and/or public performance of any derivative works resulting from the cinematographic adaptation or reproduction of the work.[28] A person choosing to reproduce, translate, broadcast, recite, adapt, etc., an author's work without the author's permission would be violating the literary author's rights. On the other hand, in 1978, the World Intellectual Property Organization (WIPO) recommended and adopted a Model Law which aims to protect the rights of software authors.[29] Section 5 of the Model Law prohibits the following acts, if done without the author's consent: disclosing software before it is made publicly accessible;[30] allowing or facilitating any person's access to any object storing or reproducing software, before the software is made accessible to the public;[31] copying software;[32] using a computer program or its description to produce similar programs or descriptions;[33] using a computer program;[34] offering or stocking computer programs for sales purposes;[35] and offering or stocking, for sales purposes, objects that are storing or reproducing the author's computer program.[36] A comparison of these two laws clearly shows that protecting software and data in a manner analogous to the protection of literary and artistic work is unsatisfactory and fails to protect major interests. For instance, an author of a literary work is mainly concerned that people read his work, irrespective of how many copies of his book have been distributed. His pecuniary interest, however, is in selling copies of his book; therefore, the law protects him by prohibiting its unauthorized reproduction. The main pecuniary value of a program lies in its use. What a program's author is primarily interested in is that people not *use* his creation without authorization, irrespective of how many copies of it have been produced. This explains why unauthorized use is included in WIPO's list in addition to copying. The two laws do have two prohibitions in common: copying (or reproducing) and adapting (including translating). Otherwise, the two laws' prohibitions, and the interests they protect, are different.

The second argument advocating a different approach for protecting software authors is that in order to meet their pressing needs,

27. *Id.* art. 14.

28. *Id.*

29. WIPO, MODEL PROVISIONS (1978), *reprinted in* WIPO, *Model Provisions on the Protection of Computer Software*, 14 COPYRIGHT: MONTHLY REVIEW OF THE WORLD INTELLECTUAL PROPERTY ORGANIZATION 6 (1978).

30. *Id.* § 5(i).

31. *Id.* § 5(ii).

32. *Id.* § 5(iii).

33. *Id.* § 5(iv)-(v).

34. *Id.* § 5(vi).

35. *Id.* § 5(vii).

36. *Id.* § 5(viii).

courts have made great efforts to stretch the meaning of key terms in copyright laws. This has occurred in order to include rights in electronically-stored software and to provide a legal umbrella where otherwise none would exist.[37] Thus, the courts consider a disk of metal that is populated with electric charges capable of producing required results according to certain arithmetic/logical formulas to be a "literary work" and, in jurisdictions that so require, a "writing."[38] Use of the program is usually considered a "translation" to allow it to be sanctioned by copyright laws.[39] The courts have gone too far in interpreting laws—beyond good reason and proper taste. The problem of protecting rights of authorship in software and data should be tackled and dealt with using concepts and terms appropriate to the subject—not by using those that are time-honored and useful in other fields.

The locus of the necessary provisions is of no consequence. They can be made as amendments to copyright laws or as independent pieces of legislation, so long as the proper concepts and terms are used and the proper provisions are made without resort to far-reaching attempts of interpretation. Because the Draft Bill contains provisions—with respect to computers, software, and data—pertaining to various branches of the law, it seems the proper place for regulation of the subject without resorting to the Copyright Act.[40]

This is version A's approach in the Draft Bill. This version has the support of many authorities and of the author. However, some circles in the Ministry of Justice support the more modest version B approach. This second approach follows some Anglo-Saxon and European countries.[41]

There is no need to go into details with respect to all of version A's provisions. Section 28, however, should be mentioned. This section

---

37. *Cf.* Shalgi, *Copyright in Software and Data*, 21 ISRAEL L. REV. 15, 17-18 (1986).

38. *Cf.* Apple Computer, Inc. v. Franklin Computer Corp., 714 F.2d 1240 (3d Cir. 1983), *cert. dismissed*, 464 U.S. 1033 (1984) (U.S.); Tandy Corp. v. Personal Micro Computers, Inc., 524 F. Supp. 171 (N.D. Cal. 1981) (U.S.); Space File Ltd. v. Smart Computing, 75 C.D.2d 281 (Can.).

The United Kingdom and Australia amended their respective laws to the same effect—*see* The Copyright (Computer Software) Amendment § 1(1) (U.K. 1985) *and* The Copyright Amendment Act § 3(f) (Aust. 1984). *See also* Apple Computer, Inc. v. New-Comb Technologies Ltd., A. (T.A.) 3021/84, 1987 Pesakim Mehozim 397 (Isr.) (Hebrew text).

39. *See* BRYAN NIBLETT, LEGAL PROTECTION OF COMPUTER PROGRAMS 51 (London, Eng. 1980).

40. The legal basis for copyright in Israel is the British Copyright Act, 1911 (2 Laws of Palestine, 412); *see also* Copyright Act, 1911 (Extension to Palestine Order), 1924 (*ibid.*). Although it was abolished in England in 1956, an amended version of the 1911 Act is still in force in Israel.

41. Computer Software Amendment Act of 1980, § 10, 17 U.S.C. § 101 (U.S. 1982); Copyright (Computer Software) Amendment Act (U.K. 1985); Copyright Amendment Act

mandates that any transfer of software enjoying protection under the Draft Bill must be accompanied by a certificate specifying the right protected and the time of its expiration. This is meant as a practical means of preventing unauthorized transactions of protected software.

Section 30 also deserves special attention. Because rights of authorship would not enjoy international protection under the Draft Bill as copyrights practically do, this section provides a technique for establishing international protection on the basis of reciprocal treaties. This is a similar technique to one used in copyright,[42] but while application of copyright law to works of foreign origin can be made, en block, to all the countries that are parties to the Berne and Geneva conventions,[43] in our case specific treaties must precede an order of application.

VI. DRAFT BILL: CHAPTER FIVE

The purpose of the provisions in Chapter 5 is to make computer output admissible as evidence without resorting to oral evidence as to the truth of its contents. Under common law best evidence and hearsay rules, which prevail in Israel, computer output is inadmissible as evidence in courts of law. The prevailing general practice of storing and manipulating documents, by computer, creates a pressing demand to rely on computer output to reflect information kept in, or deducible from, original documentation. The Draft Bill requires witness testimony to establish the credibility and authenticity of the process of obtaining the output. This is of formal character and does not go into the subject matter that is sought to be proven by the output.

Section 31 of the Draft Bill allows some presumptions concerning the credibility of output, if certain facts are established as to the propriety of the process of obtaining it. Section 32, however, dispenses with

---

(Aust. 1984); Amendment of 3.7.85 to the Copyright Law of 11.3.57 (Fr.); Law for Amendment of Rules in the field of Copyright Law, 24.6.85 (W. Ger.); Law No. 62 (Japan 1985).

See also Lawrence Perry, *The World Intellectual Property Organization Model Provisions*, in THE LEGAL PROTECTION OF COMPUTER SOFTWARE 174 (H. Brett & L. Perry eds. 1981). While this Article was in publication, the Israeli Legislature adopted, on July 27, 1988, of its own accord and without a proper proposal by the government or by a member of the Legislature, the provisions of version B. This is quite an unusual way of introducing new legislation in Israel. It seems that it was adopted as a result of pressure from business circles. However, it should not be considered a final legislative regulation of the subject, but rather a measure used because it was expedient.

42. *See* Copyright Ordinance § 6, 1924 (1 Laws of Palestine 389, *as amended in* 1953, Sefer Hahukim, 1953, at 38 (Hebrew) (the purpose of which is to meet the requirements of the Berne Convention for the Protection of Literary and Artistic works, 1886-1948, and the Universal Copyright Convention, Geneva, 1952).

43. For a list of the countries that have ratified the Berne Convention and the Universal Copyright Convention, *see* WIPO, *Treaties*, 25 COPYRIGHT: MONTHLY REVIEW OF THE WORLD INTELLECTUAL PROPERTY ORGANIZATION 7-13 (1989).

the proof required under section 31 with respect to output obtained by public institutions, or in the course of business.

Because these are prima facie presumptions, they are refutable by the opposing party. The party that offers the output is able to shift the burden of disproving the truth of its contents to the shoulders of the opponent because of the high credibility usually attached to computer output. If the opposing party is able to raise doubt as to this credibility, however, then that party may demand proof of the output's reliability.

VII. DRAFT BILL: CHAPTER SIX

Chapter 6 of the Draft Bill contains mainly transitory provisions to the effect that the criminal provisions of Chapter 2 shall not be retroactive and that, although civil protection under Chapter 3 shall be awarded to software that was created before the Law's enactment, preenactment infringements against software, data, and information shall not be actionable.

VIII. CONCLUSION

The author has tried to present an Israeli attempt at a legislative answer to pressing and just demands from flourishing industries and businesses. A legislative attempt on such a scale as the Draft Bill cannot be free of criticism. The subject is complicated, and the variety of solutions to the many problems are considerable, as a perusal of legislation around the world easily shows. This presentation is meant as another attempt to come to grips with the basic issues a computerized society poses to the legal order.

APPENDIX COMPUTER (OFFENSES, PROTECTION OF SOFTWARE, AND EVIDENCE) LAW, 5747-1987 DRAFT BILL[44]

CHAPTER 1: INTERPRETATION

1.*Definitions.*

"Computer"—A device for reception or storage of data and its arithmetic or logical processing, according to a program, and for output of data, results, orders of implementation or of operation, including peripheral equipment and communication systems connected thereto, and system of computers.

"Program"—A compilation of instructions for the operation of computers, whether registered in writing or otherwise, and whether preserved in electronic, electromagnetic, or some other form.

---

44. Translated by the Author.

"Software"—Program, program specifications, and auxiliary material for a program.

"Information"—Results of the processing of data put into the same computer.

"Thing"—Includes rights, benefits, software, and data in storage for use in a computer, and information.

"Act"—Includes omission.

CHAPTER 2: OFFENSES AND PENETRATION INTO COMPUTERS PART A: OFFENSES

2. *Disruption of Computer Operation.*

Whoever commits an act upon a computer, any of its parts, or a part designated for use in its operation without authority, knowing that the act may prevent its proper operation or cause disruption of its operation, is subject to imprisonment for seven years.

3. *Preclusion of Computer Services.*

(a) Whoever commits, without authority, any act from which the preclusion of computer services or their disruption may result, with intent to cause such results, is subject to imprisonment for seven years.

(b) The provisions of subsection (a) shall not apply to the abstention of an employee from his work due to a strike following a labor dispute.

4. *Causing Disrupted Results.*

(a) Whoever prepares any software or delivers it to another or operates a computer therewith, knowing that it will cause disrupted results with respect to the purpose of its operation, and having reasonable grounds to assume that another person will use the software in operating a computer or rely on an output of a computer operated thereby, is subject to imprisonment for seven years.

(b) Whoever supplies data, delivers it to another, or operates a computer with data or information, knowing that it will cause disrupted results with respect to the purpose of its use, while having reasonable grounds to presume that another person will use the data or information in operating a computer or rely on the output of a computer operated thereby, is subject to imprisonment for seven years.

5. *Use of Computer or Program to Obtain Some Thing.*

Whoever uses a computer or software, or causes them to be used, with the intent to obtain some thing, for himself or for another, unlaw-

fully, or who with intent prevents another from unlawfully possessing some thing, is subject to imprisonment for five years.

6. *Impairing Software, Data or Information with Intent to Obtain Some Thing.*

Whoever adds to, or detracts from, any software, data, or information that is, or may be, applied to a computer, without authorization and with intent to obtain some thing for himself or for another, or with intent to deny some thing from another person, is subject to imprisonment for five years.

7. *Deprivation of an Object that Contains Software with Intent to Obtain Some Thing.*

Whoever unlawfully deprives the lawful owner or possessor of an object containing software, data, or information that is, or may be, applied to a computer, with the intent of obtaining some thing for himself or for another, or with the intent to deprive another person of some thing, is subject to imprisonment for five years.

8. *Unlawful Obtaining of Software.*

Whoever unlawfully obtains software for himself or for another is subject to imprisonment for five years.

9. *Inducing Reliance on False Output.*

Whoever uses computer output to make representations to another person in connection with a transaction or submission of a professional opinion, knowing that the output is false, is subject to imprisonment for five years.

10. *Application.*

The provisions of this chapter shall only apply to computers, software data, or information, as the case may be, that are used or designated to be used by or for any of the following:

(1) The state or a corporation supplying service to the public;
(2) Business, industry, agriculture, health services, or for scientific purposes.

11. *Defense.*

It shall be a valid defense for a defendant charged under § 4 to prove that he made the falsity known to the other person, or made it possible for him to know it, before using the software, data, or information.

12. *Abstention from Conviction.*

The court may abstain from convicting a person of an offense under §§ 2-4, even if he is proven guilty, if it seems to the court that the injury is not grave and the offense has been committed without malice. Such abstention shall not prevent the defendant from being convicted of some other offense if that offense can be proven as a result of the same action.

13. *Restriction on Seizure.*

Notwithstanding any provision in any other law, no computer, or part of it, including any medium that stores data, information, or software, may be seized except by court order. Any order not given in the presence of the owner, or possessor thereof, shall be in force for twenty-four hours only and shall not be prolonged unless an opportunity has been given to the owner or the possessor to address the court. For counting purposes, Saturdays and holidays shall not be taken into account.

14. *Notification of Offense.*

(a) Any person in the civil service, or in a regulated corporation that supplies services to the public, who is in charge of another person and who has reasonable grounds to suspect that the other person has committed an offense under §§ 2-8 with respect to a computer in that institution or business, shall notify the police as promptly as possible. Whoever violates this provision shall be subject to imprisonment for one year.

(b) A person in charge shall be exempt from the duty under subsection (a) if he is under the supervision of another person and had reasonable grounds to assume that the suspicion and the reasons thereof were known to that person.

(c) For the purposes of this section, a "person in charge" means an employer or a person in charge of an employee on behalf of the employer, or the employer of a contractor with respect to the contractor or the contractor's employee.

PART B: PENETRATION INTO A COMPUTER FOR SPECIAL PURPOSES

15. *Definitions.*

In this part:

"Penetration into a computer" means obtaining software data and information stored therein and obtaining output from a computer.

"Minister" means the Prime Minister or the Minister of Defense.

"Security authority" means any of the following:

(1) Department of Intelligence in the General Staff of the Israel Defense Forces;

(2) The General Security Service.

An "authorized police officer" means a police officer of the rank of colonel, or of a higher rank, authorized by the Inspector General of Police.

16. *Penetration into a Computer for State Security Reasons.*

(a) A minister may permit, in writing, penetration into a computer if so requested by the head of a security authority, and if he is satisfied that it is required for reasons of state security.

(b) The identity of the possessor of the computer, and the place where the computer is located, insofar as they are known, and the means of penetration, shall be described in a permit under this section.

(c) The permit's period of validity shall be specified in it; this period shall not exceed three months from the date the permit was granted. The permit may be renewed from time to time.

(d) If the Minister of Defense grants or renews the permit, he shall promptly notify the Prime Minister; every three months each Minister shall inform the Minister of Justice of any permits granted by him under this section.

17. *Computer Penetration to Prevent Crime.*

(a) The President of a District Court, or in his absence, a Deputy President of a District Court, may grant an order authorizing the penetration of a computer, after reviewing an authorized police officer's petition, if he is convinced that it is required for prevention of offenses or for discovery of offenders.

(b) The hearing for the petition shall be held ex parte only, and an officer of the rank of Brigadier or higher shall represent the petitioner.

(c) If the Judge declines to give permission as petitioned, the Attorney General, or his representative, may appeal this decision before a Justice of the Supreme Court has been appointed by its President.

(d) The identity of the computer's possessor, and the place where the computer is located, as far as they are known, as well as the means of penetration, shall be specified in a permit under this section.

(e) The period of its validity shall be specified in the permit. This period shall not exceed three months from the date the permit

was granted, but the permit may be renewed from time to time.

(f) The Inspector General Of Police shall forward a monthly report to the Minister of Police of the permits granted under this section and their conditions. The Minister of Police shall forward copies of these reports to the Minister of Justice every three months.

18. *Preservation and Liquidation of Information.*

The Minister of Justice, with the approval of the Constitution, Law and Justice Committee of the Knesset,[45] shall make regulations regarding preservation and liquidation of the information obtained by permit under this part.

CHAPTER 3: TORTS

19. *Wrongs.*

An act or omission described in §§ 2-9 shall be deemed wrongs under the Torts Ordinance (New Version).

20. *Interpretation.*

For purposes of the Torts Ordinance (New Version), and § 19, software, information, and data shall be considered "property," and their alteration, copying, or use as "damage."

21. *Application.*

The provisions of this chapter shall apply whether or not the computer, software, data, or information are as specified in § 10.

22. *Reservation of Rights.*

Nothing in the provisions of this chapter shall derogate from any right of action under any other law.

CHAPTER 4: SOFTWARE AUTHORS' RIGHTS

VERSION A:

23. *Definition.*

For purposes of this law, version A, "new software" means software that is the result of the mental efforts of its author.

45. The Israeli Legislature.

24. *The Rights of Software Authors.*

The author of new software, and his substitute (referred to in this chapter as "author"), shall have the right to prevent the following acts from being done to his software, or any part of it, without his consent:

(1) Storing the software, or using it in a computer;
(2) Using the software for the purpose of preparing either a parallel version of it or software essentially similar to it;
(3) Copying the software electronically, electromagnetically, or by any other means;
(4) Publishing the software, or any part of it that is original, before access to it has been given by the author;
(5) Possessing, for the purpose of sale or for some other transaction, an article in which the software is contained. For the purpose of this provision, any possession of new software shall be presumed to be for such a purpose; but in circumstances in which it seems fit to the court, the court may oblige the claimant to prove the said purpose.
(6) Making any transaction therewith, importing, or exporting it.

25. *The Rights of an Author of Similar Software.*

A person who has independently compiled new software identical to an author's software, a parallel version of it, or software essentially similar to it, shall have the rights described under § 24, and the restrictions therein shall not apply to him or to his substitute or to any other person who has acquired rights in the software from the other author.

26. *Expiration of Rights.*

The rights under § 24 shall expire after fifteen years from the date of compilation of the software, unless none of the following has happened within ten years thereof, whereupon they shall expire ten years after the date of compilation:

(1) Commercial use has been made of the software, with the author's consent, to operate a computer, within or outside of Israel;
(2) The software was made available for public sale with the author's consent.

27. *Remedies.*

(a) Upon an infringement of an author's rights under this law, the court may award him damages for the infringement, except against a person who has acquired the software in a bona fide manner on the open market.
(b) Upon an infringement of an author's rights under this law, or if the court anticipates that such rights are about to be infringed, the court may, upon the author's petition, issue a prohibitory injunction to prevent the infringement.

(c) If software, in respect of which there exists a right of authorship under this law, has been obtained unlawfully, the court may, upon the author's petition, order the software, or any article containing the software, to be surrendered to the author.

28. *Notice of Rights.*

(a) No software in which there exists any right under this chapter shall be transferred, by the author or by any other person, to another, except with a written notice of such a right and the time of its expiration, insofar as it is known by the transferor.
(b) If software has been transferred without a notice as required under subsection (a), the transferor shall be held liable for any infringement foreseeable by him at the time of delivery.

29. *Reservation of Rights.*

The provisions of this chapter are in addition to those of any other law that gives any right to a software author and are not to derogate from them.

30. *Application to Software Made Outside of Israel.*

This law shall not apply to software made outside of Israel except to the extent ruled by the Minister of Justice, who may rule according to the place of authorship or in any other way.

VERSION B:

(If this version is adopted, the numbers of the other sections shall be adapted accordingly.)

23. *The Rights of Software Authors.*

Software shall be deemed, for all purposes, a literary work as defined in the Copyright Act.

CHAPTER 5: EVIDENCE

31. *Authenticity and Admissibility of Computers' Output.*

(a) There shall be prima facie presumptions regarding computer output:
  (1) That when the output is a result of feeding, the data fed in is as registered in the sources from which it is fed if the trustworthiness of the feeding, input, and output mechanisms of the computer is shown.
  (2) That when the output is a result of self-feeding, the data is as received by the computer if the trustworthiness of the input and output mechanisms of the computer is shown.
  (3) That when the output is a result of data processing or of eval-

uation, the processing of the data and the evaluation of the computer are trustworthy if the trustworthiness of the operation and of the translation process and the effectiveness of the program under which the data was processed or the evaluation reached is shown.

(b) If the output is obtained from a system of computers, the provisions of sub-section (a) shall apply to each computer in the system.

32. *Records of a Public Institution Kept in the Course of Business.*

(a) The output of a computer that is used for registering or processing data, or for evaluation by a public institution in performing its duties, or by a business in its regular course of business, or by any other enterprise, when the computer use is part of its regular activities, shall be presumed accurate as provided in § 31(a) without proof of the relevant particulars.

(b) When the conditions specified in subsection (a) apply, and it is the regular course of the institution or business to rely on such records, the records shall be admissible as prima facie evidence of the truth of its content.

33. *Approved Modes of Proof.*

The Minister of Justice may prescribe regulations to govern the methods/conditions of proof of credibility or orderliness under § 31. If so prescribed, credibility and admissibility shall not be proven except as prescribed, unless the court allows proof in some other way.

34. *Reservation of Laws.*

Nothing in this chapter shall derogate from any pleading with respect to computer output as admissible evidence other than its being indirect evidence not given by a witness (hearsay).

CHAPTER 6: MISCELLANEOUS PROVISIONS

35. *(Not relevant for the purposes of this Article.)*

36. *Transitory Provisions.*

(a) The provisions of Chapter 2 shall not apply to acts committed before enactment of this law.

(b) The provisions of Chapter 3 shall apply to software compiled before this law's enactment but shall not apply to an infringement committed before its enactment.

(c) The provisions of § 28 shall not apply to software compiled prior to enactment of this law.

37. *Implementation and Regulations.*

The Minister of Justice is responsible for the implementation of this law and may issue any regulations necessary for its enforcement.