2002-11987

LAW LIBRARY OF CONGRESS

FRANCE:

COMPUTER SECURITY AND PROTECTION OF COMPUTER INFORMATION

France envisioned in the mid-70s the risks that electronic data processing would cause with respect to personal data and privacy. As a result, a Data Protection Law was enacted in 1978 and an independent agency, the National Commission on Data Processing and Liberties, was created to enforce its provisions. This Law is under review by Parliament. The government 's aim is to increase the powers of the Commission and to further strengthen data protection. In addition , the Penal Code defines several specific offenses against the security of computer systems. These provisions are currently used to combat, among others, viruses, software bombs, "Trojan horses" and spy software. Provisions contained in the Code of Intellectual Property protect computer databases and software.

France has no specific legislation to fight the dissemination of illegal and/or harmful content on the Internet. It applies existing laws such as the Law on Freedom of the Press or broad provisions of the Penal Code. As far as procedural issues are concerned, the Code of Criminal Procedure does not contain provisions adjusting the general provisions to the specific needs of the computer area.

Within the past three years, the government has set up specialized units and created two new offices to further fight crime associated with information technologies. It also wants to create a "citizen electronic card" allowing each individual to access, verify and modify data contained in the various government databases on that individual.

I. Introduction

In today society computer technology has spread into almost all areas of life. Businesses and individuals depend to a high degree on the efficiency, reliability, and security of computers and computer networks. Unfortunately, these new information technologies are also being used to facilitate or perpetrate various criminal activities, thereby posing a major threat to the society and making computer security of essential importance.

The number of criminal cases linked to information technologies is constantly rising in France. For example, between 1997 and 1998, the number of cases increased by 33.49 percent. In 1999, there were at least 20,000 attacks on computers systems. However, it is hard to collect precise statistical data, as these offenses are not systematically reported to the judicial authorities. The reason likely is to preserve the credibility of the security system and the image of the company that has been victimized. The above figures relate only to attacks on computer systems; the number of common law offenses carried out by means of networks is not known.[1]

What is new is the greater ease with which computer-related offenses can be committed and disseminated throughout the world. In many cases, it is difficult to prosecute the perpetrators because of the international dimension of the Internet and other computer networks, and the fact that many offenders operate from countries in which there are no appropriate laws. In addition, computer-related crimes are committed across cyberspace, raising new procedural issues which may challenge the existing national rules of procedure.

[1] Daniel Martin & Frˈdˈric-Paul Martin, *Cybercrime: menaces, vulnˈrabilitˈs et rispostes*, (Presses Universitaires de France, 2001) at 16-19.

This report will first focus on the legal protection for computerized systems and information, addressing successively the Data Protection Law, the provisions of the Criminal Code defining specific offenses against the security of computer systems, and the copyright protection of computer databases and software. It will then address the dissemination of illegal and /or harmful content on the Internet. Finally, it will briefly cover procedural issues, in particular, the jurisdiction of French courts in matters of computer-related offenses and some of the recent government initiatives to combat crimes associated with information technologies.

II. Legal Protection of Computerized Systems and Information

A. The Data Protection Law of 1978

A Data Protection Law was enacted in 1978 and an independent agency, the *Commission Nationale de l'Informatique et des Libertés* (CNLI) (National Commission on Data Processing and Liberties), was created to enforce its provisions.[2] The Law provides for procedures insuring the confidentiality of personal information held by government agencies and private entities. Its first article states that "Data processing must be at the service of each citizen. It cannot infringe upon human identity, the rights of man, privacy or public and/or individual liberties."

The provisions dealing with infringements on personal rights resulting from data processing have been incorporated into the Penal Code. Articles 226-16 through 226-24 define eight offenses:

- Collecting automated data without complying with the prerequisite formalities;
- Collecting automated data without taking all the necessary precautions to preserve the security of such data;
- Collecting information by fraudulent, unfair or unlawful means or collecting data concerning a person despite the person's reasonable objections;
- Collecting health data without informing the persons of their right to access, rectification and objection or despite their objection;
- Storing data which directly or indirectly discloses the racial origins or the political, philosophic, religious opinions, trade union membership or morals of a person without the explicit agreement of such person;
- Storing automated data without the authorization of the CNLI beyond the period originally authorized;
- Diverting automated data from its intended use;
- Making automated data available to a third person not qualified to receive such data witho

[2] Law N° 78-17 of Jan. 6, 1978, J.O. Jan 7, 1978, p 227.

ut the consent of the affected person.

Penalties range from one year imprisonment to a maximum imprisonment of five years and from a minimum fine of 15,000 _ to a maximum fine of 300,000 _.

The Data Protection Act is currently under review by Parliament to make it consistent with a Europ ean Directive dated October 24, 1995. The draft law has three objectives: (1) improve data protection; (2) increase the powers of the CNLI; and (3) standardize prerequisite formalities required for the creation of a utomated data bases containing information on persons.

B. The Penal Code

In addition to the provisions listed above, the Penal Code contains specific offenses against the se curity of computer systems. Furthermore, the definitions of many traditional offenses are broad enough so that they can be interpreted to be applicable to offenses facilitated by or linked to the use of computers.

Offenses against the security of computer systems

The following provisions were introduced into the Penal Code in 1988. They are currently being us ed to combat, among others, viruses, software bombs, "Trojan horses," and spy software used for keeping a site or a system under surveillance. These provisions provide penalties as follows:

- Fraudulently obtaining or maintaining access to an automated data processing system is punishable by one year imprisonment and by a fine of 15,000 _. When such access result s in either a deletion of information contained in the system or an alteration of the functioni ng of the system, the penalty is increased to two years imprisonment and to a fine of 30,0 00 _.[3] The offense is committed even though the system is not protected. The legislator did not want to impose an obligation of protection.

- Hindering or altering the functioning of an automated data processing system is punishabl e by three years imprisonment and a fine of 45,000 _.[4]

[3] CODE P'NAL,(C.P'N) art.323-1.

[4] *Id*., art. 323-2.

- Fraudulently introducing information into an automated data processing system or fraudul ently deleting or modifying information it contains is punishable by three years imprisonme nt and a fine of 45,000 _.[5] This article addresses the introduction of worms, viruses or an y other similar attacks to computer systems.

- Participating in a group formed or an understanding reached for the planning of one or mo re of the offenses specified above, when evidenced by one or more overt acts, is punisha ble by the penalties specified for the offense itself or for the offense most severely punish ed.[6]

In addition, the Penal Code provides that attempting to commit the offenses listed above is punish able by the same penalties.[7] Furthermore, the above offenses are acts of terrorism when they are "intenti onally" connected to an individual or collective enterprise having the purpose of seriously disturbing public order by intimidation or terror.[8]

Traditional offenses

Traditional offenses are often broadly defined with terms such as "by any means whatsoever," whi ch make it possible to take into account the use of new means of publication or communication.

C. Copyright protection of computer databases and software

[5] *Id*., art. 323-3.

[6] *Id*., art. 323-4.

[7] *Id*., art. 323-7.

[8] *Id*., art. 421-2.

The Code of Intellectual Property defines a database as "a collection of works, of data, or of other independent elements, methodically or systematically arranged and individually accessible by electronic or any other means."[9] French law makes a distinction between the container, i.e., the database's structure and the elements required for its running or its consultation, and the content of the base. In order for the container to be protected on the basis of authors' rights,[10] it must meet the requirement of "originality"imposed by the Code.[11] As for the database contents, its producer has a monopoly without need of originality; an investment is sufficient.[12] Infringement of the rights of a database producer may result in up to two years of imprisonment and a fine up to 150,000 _.[13]

Computer software and materials used for their conception are also protected by authors' rights laws. Infringement of the rights of the creator of the software will carry the same penalties as above.[14]

---

[9] Code de la propriet, intellectuelle, art. L112-3.

[10] French authors' rights protect any and all original "works of the mind." Authors' rights cover two components " moral rights," and "economic rights."

[11] Code de la propriet, intellectuelle, art. L112-4

[12] *Id*. art. L341-1.

[13] *Id*., art. 343-1.

[14] *Id*., art. 335-4.

III. Dissemination of illegal and/or harmful content on the Internet

There is no specific legislation or regulation restricting Internet content. To try to block material th at undermines public order and security, national defense, racial and religious harmony and morals, the go vernment applies existing laws such as the Law on Freedom of the Press or general provisions of the Pen al Code.[15] These laws or provisions have been either drafted broadly at the origin or amended at a latter d ate so as to include any new means of publication or communication.

The Law of July 29,1881, on the Freedom of the Press as amended,[16] and the Law of September 30, 1986, as amended on audiovisual communication,[17] govern all offenses committed by way of the pres s or "any other means of publication." Therefore, these laws are applicable to the Internet with the exceptio n of private messages.

[15] For example, the two following provisions of the Penal Code protect minors from pornography and violence. They have been applied to material found on the Internet.

> Article 227-24 of the Penal Code provides that manufacturing, transporting, or disseminating, by any means wh atsoever, a message of a violent or pornographic character or a message likely to seriously injure human dignity...is punisha ble by a three years imprisonment and a fine of 75,000 _ when that message is susceptible of being viewed or perceived by a minor.
>
> Article 227-23 provides that disseminating a pornographic picture or representation of a minor by whatever means to import or export it or to have it imported or exported is punishable by the same penalties.

[16] Law of July 29, 1881, CODE PENAL, Appendice, at 1861 (Dalloz, 2001).

[17] *Id*., at 1982.

Among other offenses, the 1881 Law punishes any direct incitement, in the case when such incitement is not acted upon, to voluntary manslaughter, violence against the person, sexual offenses, terrorist acts, discrimination, and hatred or violence against persons based on racial, religious, ethnic or national origin. It also prohibits a defense of war crimes, crimes against humanity, and terrorist acts. These offenses are punishable by five years' imprisonment and a fine of 45,000 _.[18] In addition, the Law prohibits the denial of one or several crimes against humanity, for example, denying the existence of the Nazi concentration camps and of the gas chambers in the World War II era. [19]

Individuals or groups that would publish information on how to build a nuclear weapon or a bomb would fall under the provision of the 1881 Law and could be charged with incitement to terrorist acts.[20] It should be noted that when incitement to commit one of the offenses listed in the above paragraph is acted upon, the 1881 Law provides that the actors of the incitement shall be charged as accomplices.[21]

In addition, French courts have applied by analogy the law setting forth the liability of the director of publication and/or producer of audiovisual communication services to web sites. They have held Internet servers and hosts responsible if illegal material detectable by a search engine is discovered on their servers. They therefore have a legal duty to be prudent and diligent and ensure that material presented on their servers does not infringe the rights of third parties and does not violate laws or regulations. If such material is found, they are required to take reasonable measures to remove it from their sites.[22]

The Law on the Press was also the basis for the court ruling against Yahoo rendered on November 20, 2000, by a Paris judge. The judge ordered Yahoo, Inc., to keep French citizens from seeing its American-based sites that auction Nazi-related items even though the computers, content, and company are physically located in the United States. Yahoo's French subsidiary, complying with an earlier court ruling, had stopped posting Nazi items. The judge found that the sale or exhibition of the Nazi memorabilia incited racial hatred.

---

[18] *Supra* note 16 , art. 24 at 1881.

[19] *Id*., art. 24 *bis* at 1885.

[20] Christiane F•ral-Schuhl, *Cyber Droit*, at 95-96 (Dalloz 1999). The author recalls several terrorist attacks which took place in Paris in 1995 and that at the same time, one could freely find on the Internet a manual entitled le *Manuel du terrorist* which detailed all the steps necessary to prepare a very powerful bomb.

[21] *Supra* note 16, art. 23 at 1876.

[22] *Supra* note 20, at 102 to 107.

The judge gave Yahoo three months to bar French nationals from accessing its U.S. sites. If Yahoo did not comply, it would be fined 100,000 French *francs* (U.S.$13,000) for each day it exceeded the deadline. The case raised the issue of whether the laws of individual countries can govern a web site based abroad. Yahoo complied with the order of the French judge and removed almost all of the Nazi memorabilia links on its auction sites.[23] However, it also moved an American court for a declaration that the ruling of the French judge was not enforceable in the United States and that Yahoo did not need to comply with the French decision. The U.S. District Court for the Northern District of California held that the directions of the French judge could not be enforced in the United States, as they were in violation of the first amendment of the U.S. Constitution. An Appeals court upheld the decision but the League Against Racism and Anti-Semitism and the Union of Jewish Students, which had initiated the lawsuit in France have appealed again and have vowed to take the case to the U.S. Supreme Court if necessary. They are arguing that the issue is not about free speech but about national sovereignty.[24]

IV. Procedural issues

Most of the discussion of the legal consequences of computer-related offenses have focused on substantive law and have neglected procedural law aspects. The Code of Criminal Procedure does not contain any provision adjusting the general provisions to the specific needs of the computer area. The traditional powers of the investigative judge, who is empowered to order all informative acts which he considers helpful for finding the truth, may be broad enough to adequately cover most cases.

In addition, the victims must know whether French courts have jurisdiction over the matter. Under articles 113-6 and 113-7 of the Penal Code, French law applies where (1) a felony is committed by a French citizen outside of French territories; (2) a misdemeanor is committed by a French citizen outside of French territories and if such an act is punishable under the law of the country where the offense was committed; and (3) an offense was committed by a French citizen or a foreigner outside French territory, if the victim in the case is a French citizen. These provisions are applied even in cases where the offender has become a French citizen only after the offense took place.[25]

The Criminal Procedure Code furthers provides that offenders and accomplices to a crime committed outside of French territory may be prosecuted and tried by French courts when French law applies as seen above or when such jurisdiction is allowed by other legislative documents, or by the text of internatio

---

[23] LE MONDE, Oct 21& 23, 2000, via Lexis/Nexis Presse.

[24] Ariana Eunjung Cha, *Rise Of Internet "Borders" Prompts Fear for Web's Future*, THE WASHINGTON POST, Jan 04, 2002 via Lexis/Nexis News.

[25] C. PEN., arts 113.6 & 113.7.

nal conventions.[26]

V. Government Initiatives

[26] C.CRIM.PROC, art. 689.

Considerable efforts are being made to coordinate the various agencies involved in the fight against crime associated with information technologies. In addition to specialized units which have been set up in various ministries (Defense, Economy and Finances, Interior, Customs), the government created two new offices to further ensure the security of computerized systems and information. An inter- ministries office, the *Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication* (Central Office to Combat Criminality Linked to Information Technologies), was created in May 2000 [27] to coordinate, at the national level, the fight against specific computer offenses and traditional offenses whose commission is facilitated by or linked to the use of information technologies. In addition, a *Centre d'alerte et de secours sur l'internet* (Computer Emergency Response Team/Administration) has been operational since the end of 1999. One of its missions is to detect attacks against the State's computer systems and to prevent them. In addition, Prime Minister Jospin has announced that the government plans to build near Marseilles a college dedicated to the Internet and digital technology. This college would promote Internet-related research and development.[28]

The government also wants to create a "citizen electronic card" that would allow each individual to access, verify, and modify the automated data contained in the various government databases on that individual.[29]

At the international level, on November 23, 2001, France signed the Convention on Cybercrime adopted earlier by the Council of Europe's Committee of Ministers. The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing in particular with infringements of copyrights, computer-related frauds, child pornography, and violations of network security. Its main aim, as set out in its preamble, is to pursue "a common criminal policy aimed at the protection of society against cybercrime by adopting appropriate legislation and fostering international co-operation."[30]

Conclusion

France has in place many specific tools to prevent and punish computer misuse. In addition, many of its laws are broad enough that they can apply to this new environment even though certain adjustments may be necessary here and there. France is also in the process of further strengthening its Law on Data Protection. However, information technologies transcend frontiers and a state alone cannot be completely successful. Therefore, great emphasis must be put into developing international dialogue and cooperation in this area.

Prepared by Nicole Atwill
Senior Legal Specialist
Western Law Division
Law Library of Congress
April 2002

---

[27] J.O. May 16, 2000, at 7338.

[28] United Press International, *French to set up cybercollege*, May 17, 2000, Nexis/Lexis/News.

[29] <http://www.premier-ministre.gouv.fr>.

[30] <http://conventions.coe.int./