Criminal Law Aspects of Computer Crime

General Theory of Computer Crimes and the Proposed Bill to Modify the Brazilian Penal Code

OTTO BANHO LICKS, JOÃO MARCELLO DE ARAUJO JUNIOR

Les temps modernes sont souvent, dans les pays hautement industrialisés, caractérisés par le terme de révolution informatique. Le temps que précédent, à partir de la moitié du siècle passé, se voit, de son côté, caractérisé par la notion de révolution industrielle, le développement presque explosif, et l'usage répandu, des machines.

1. Introduction

Technological development has changed the history of the world and transformed society. The invention of the printing press, of the telephone of the automobile and the discovery of electricity, just to cite a few examples, has led to a fundamental redefining of social, political, commercial and military behavior.

During the second half of this century, we have witnessed one of the most farreaching technological advances: the evolution and widespread dissemination of computers. Ten or twelve years ago, a veritable revolution took place when personal computers started to become common. Now, another revolution, unquestionably greater than the first, is under way. It is the advent of computer networks.

The velocity and irreversibility of these changes have brought about what is commonly called the computer revolution, and what Bell defines as the post-industrial society. In view of this fact, we should say right from the

---

1 The modern age is very often characterized, in the highly industrialized countries, by the term computer revolution. The previous age, beginning in the mid-19th Century, is seen in its turn as being characterized by the notion of industrial revolution, in view of the explosive development and the prevailing use of machines. TIEDMANN, Klaus, Science and Crime policy in Honor of Heleno Fragoso, Organizer prof. João Marcello de Araujo Junior, Brazilian Group of the International Association of Penal Law, RJ Editora Forense, 1992.

start that we do not have to consider computer crimes as the price of progress. To protect ourselves and our computers, we need to replace the myths of the past by the reality of the present. The notion or false idea that computer crime is a problem related to computer techniques, according to Bloombecker, would be the worst myth of all.

The change undergone by society through technological advances has brought as an mediate and predictable consequence a transformation in the Law and in jurial relations too. Today, we are obliged to adjust the Law, particularly Criminal Law, to adapt it to a new form of criminal behavior.

This study will take a look at the present stage of the institutions related to computer crimes. The concepts and definitions of these crimes will be analyzed in the light of international and internal doctrine. A number of solutions already adopted by other legislations will be put forward and discussed.

We will carry out our analysis based on a critical study of already existing comparative legislation in order to suggest some theoretical elements that should guide Brazilian’s penal law reform in the area related to computer crimes. This study will try to deal with the subject in a systematic way, because there are no prior studies of this type in the native doctrine.

Our research covers three specific fields. Firstly, will look at Penal Law related to information technology and the definition of its terms. Secondly, we will analyze the general theory of Penal Law applied to computer crimes. And thirdly will examine the juridical institutions that deal with the criminal law aspects of copyright, privacy protection and trade secrets.

All these subjects will be considered as separate topics. The first topic will be devoted to the study of the changes in positive criminal law arising from situations produced by the information society. Also current Brazilian legislation will be discussed and the proposed bill to modify Brazilian Penal Code will be presented.


The information technology field is a fertile one for practicing a crime. Current studies on computer crimes reflect very strongly the international

---

community's concern and indignation about the dependency of computerized society on computers. This, however, leads to exaggerations in criminal legislation.

Such concern seems to have brought back the days of the Inquisition. Definitions of computer crime as any illegal, unethical, or unauthorized behavior involving automatic data-processing and/or transmission of data lead us to deny certain basic individual rights, pillars of faith in most States and in the international community. It is interesting that in the name of these same rights, computer crimes law itself deals with such fundamental values as individual privacy.

First of all, we should make it clear that we prefer a more restricted understanding of computer crimes. Taber at the beginning of the 1980's defined a computer crime, albeit rather imprecisely, as being a crime that, in fact, occurred and in which a computer was directly and significantly instrumental. Taber's contribution to Criminal Law relating to information technology, though not jural, was very important. His pragmatic view, came to influence jurists and scholars like Parker. He was the first to restrict and delimit the scope of the acts which could be defined as computer crimes.

Hence Parker, immediately afterwards, differentiated Computer Crime from Computer Abuse, a term he defined as any intentional act associated in any way with computers where a victim suffered, or could have suffered a loss, and a perpetrator made, or could have made, again. While Computer Crime would be any act as specified in a computer crime statute in the applicable jurisdiction of the statute.

From these preliminary studies carried out in a empirical way, we can thus conclude that the bases and principles of what we call Criminal Computer Law and Computer Crimes have emerged in the USA.

---


5 TABER, John, *A Survey of Computer Crime Studies*, 2 Comp. L.J. 275 (1980). BloomBecker, in his book *Spectacular Computer Crimes*, op. cit., p. 67, defines Taber's contribution in the following way: Taber returned to the obscurity in which he had previously lurked. In two very influential law review articles, and in testimony before Congress, this IBM programmes, threw down the gauntlet to all those people who argued that computer crime was a serious problem requiring legislative attention.

2.2. Computer Crimes and Developments in Legislation

On the international level, the United Nations congress on Computer Crimes has a similar understanding when it says that:

... the resolution urges Member States to intensify their efforts to combat computer crime by:
1) modernizing national criminal laws, including the institution of measures to:
   a) ensure that existing laws adequately apply to the commission of such offences when committed within the computer environment;
   b) create new offences where required;

In our view, the dichotomy between modernizing existing laws or creating new ones is the basis of the difference between Computer Crime and Computer Misuse.

The international community began to realize during the 1980's that traditional criminal law was proving inadequate for dealing with certain types of abuse in the use of computers. Hence, we have witnessed the appearance in the so-called more developed countries of specific legislation in response to the absence or unsuitability of traditional penal law. However, this response, in the form of specific laws against computer crime errs through lacking in uniformity and has an even more serious drawback.

The drawback to most legislation that has initially appeared lies in the fact that it treats the new facts belonging to the technological environment of digital data processing and the computerization of society with the same penal law principles applicable to tangible or corporal crimes. However, to mention a difference, as an example, for other types of crime, it can be said that the laws of physics support and are related to criminal laws. The same cannot be said of computer crimes. This factor will lead to other ways of dealing with these acts and behavior requiring severe punishment.

2.3. The Objectives of Computer Crimes

There is still today a bi-polarization concerning what is the fundamental juridical property protected by the Criminal Computer Law, whether it is the computer system or the information. Some have adopted clear positions,

8 By abuse is understood, any unethical behavior, deserving the severest censure in the light of the society’s values and the prevailing penal system.
like prof. Sieber in Germany, or Parker in the USA, in favor of protecting information, based on a new definition of the term “information” in the post-industrial society.

On the other hand, The National Center for Computer Crime Data in the USA, defends the view that Criminal Computer Law be conceived to protect the computer and communications systems, besides the information\(^9\). This would be *prima facie* our position, although not so extreme as to consider, for example, the physical destruction of a computer as a computer crime, as Bloombecker suggests\(^10\).

We believe Criminal Computer Law’s main concern with computer and communications systems is fundamentally due to the need to protect their immaterial or intangible components, that is to say, the software and the data which still lack the same protections as the other component, the hardware, and particularly what we call an available resource, resulting from the use of computer systems in computer networks.

We should stress that when we refer to software protection or computer network resources we are not referring to the protection of intellectual property by copyright or patent law, but rather the protection of such juridical property from all other forms of misuse other that piracy, unauthorized copying, or counterfeiting. In our view, unauthorized copying, counterfeiting or piracy of computer software are already provided for in specific legislation, which in the Brazilian case are the software law, Act n° 7646/87, the copyright law, Act n° 5.988/73, and the Penal Code, section 184, modified by Act n° 8.635/93. The same approach has been followed in other countries, like Holland, where software piracy is also not considered as Computer Crime\(^11\).

Although the distinction between hardware and software is quite clear from technical and factual points of view, the same can hardly be said of their juridical implications. The Law is moving very slowly towards implementing a juridical system which protects incorporeal and immaterial property as well as material property. In this respect, we agree with prof.\(^9\) According to Prof. YAMAGUCHI Atushi, the National Law-Enforcement Agency in Japan defines computer crimes as being crimes including negligent acts or accidents which obstruct the function of a computer system or use it illegally. *International Review of Penal Law, Computer Crime and Other Crimes against Information Technology*, Érès 1st and 2nd trimester 1993, p. 433.

\(^10\) BLOOMBECKER, *op. cit.*, p. 71

Davis\(^{12}\) who supports a similar position towards the juridical protection of intellectual property in the field of artificial intelligence, which is worth quoting:

“As computer scientists learn early in their education, hardware and software are essentially interchangeable. More precisely, they are what we might call behaviorally interchangeable: any behavior we can accomplish with one we can also accomplish with the other...

If hardware and software are behaviorally interchangeable, the choice of which to use in any given circumstance becomes what is termed an “engineering decision”...

While hardware and software are interchangeable in the technical world, notice the enormous difference in the variety of intellectual property protection available depending on which of those we choose...

2.4. Differences between Existing Institutions

When one considers the protection of immaterial property, the example that first comes to mind is intellectual property, such as copyright, one of the oldest provisions for protecting immaterial property, designed to protect the author of a work.

Prof. Santos\(^{13}\), explains the theories which justify Copyright Law. According to him, Joseph Kohler’s theory of immaterial juridical property recognizes an author’s absolute right sui-generis, a natural right. At the same time, he declares that there is a juridical relationship of a personal nature between the author and his work, which does not constitute a copyright element and retains the characteristics of pure personal right.

As one can see, intellectual property has a firmly entrenched position today in the Science of Law. Copyright institutions date back more that 250 years in the positive law of certain jurisdiction\(^{14}\). Likewise with patents.


\(^{14}\) One example would be the law passed by Queen Anne Stuart of England in 1710, fixing privileges lasting 21 years for author of literary works and 14 years for other types of work. For a more detailed study, see the work of prof. L. Ray Patterson, particularly *Copyright in Historical Perspective and The Nature of Copyright*. 


In more modern terms, one can mention the new protection *sui-generis* granted by the 1989 treaty of Washington to integrated circuits. In view of the above one should add a new proposal. For many years non-material juridical property was generally confused with rights protected by intellectual property institutions. Just because properties like invention or creation, which come under intellectual property, were for a longtime the only non-material properties able to be measured and protected by property law, one should not think that they are the only non-material properties of relevance to the Law today. One institution which is different from intellectual property is the industrial or trade secret, also provided for in various legislations, where the property in question is essentially a piece of information or know-how and not an intellectual creation.

Outside the property sphere of private law one also has in the field of basic human rights the safeguarding of non-material property, in this case of a more subjective measurability, but nonetheless existing and important. Such rights are also guaranteed and protected by legal provisions, both in international community and in various national jurisdictions. In the case of crimes already provided for by these three forms of "corpus legis" against these protected juridical properties, the computer is going to bring new challenges and new forms of committing such violations. The detection and effective prosecution of already prescribed crimes, in which the computer is used, is becoming much more difficult. There is also likely to be a growing demand to punish such behavior, in view of the growing damage caused by crimes against such property employing information technology. The computer then is used to practice a crime in the same way as other weapons. The discussion then focusing on the criminalization of certain practices, particularly as certain crimes are becoming impossible to classify, prove and prosecute when perpetrated in a computer environment.

Provisions of a legal nature for the protection of non-material property by these juridical institutions, when related to information technology, are

---

15 This treaty signed under the auspices of the World Organization for Intellectual Property dates from 26 May 1989 and still has not come into force.

16 The right to privacy, beginning with the Universal Declaration of Rights of Man, has been repeated in various constitutions and in international charters. More specifically, however, in the information technology field, a number of laws for protecting against infringements of privacy appeared in the USA in 1974. In Germany and Finland in 1977 and Austria, Denmark and France in 1978.

to be found in a study of what is commonly called Criminal Computer Law, although in our view they do not constitute genuine Computer Crimes, as we will see later.

2.5. The Property or Interest to be Safeguarded and Protected

The protection of juridical properties of newly defined importance, such as data, information, and computer networks, will now be discussed. Their importance stems, as was mentioned before, from the changes undergone by post-industrial society with impact caused by modern information technology.

Firstly let us define these terms.

“Data” can be understood as any part of information or as something which has the power to bring any information. It can also mean, when related to computers and information technology, a piece of numerical information in a comprehensible format processed or stored by a computer or component part of a computing system; or a piece of information ready to be processed, operated or transmitted by computing system or computer program. The data can express facts, precise statements or commands and instructions.

Information, on the other hand, is something through which one acquires some form of knowledge. It is commonly referred to as a collection of data which describes or integrates a body knowledge.

For the computer, all data are bits of information, whether as a register, or as an instruction, i.e., ends and means respectively, but for us only certain data or group of data constitute information which may or may not form or be part of a certain type of knowledge.

Neither data nor information are products of the post industrial society. Information has always been highly valued, its control representing a true form of power. Information has always been power. This easily verified looking back at history. To give only one example, the Pharaohs in Egypt used to surround themselves with wise men.

Data when referred to in relation to computer or communication systems represent tangible objects, because they are individualized, albeit in a very tenuous way, through microscopic orifices and smooth areas with different reflective properties in the case of digital technology, comparable for example to the corpus mechanicum of Copyright Law.

The data, therefore, serve as supports for the subjective non-material objects, which are the bits of information, equally comparable to the corpus mysticum. The data have also recorded their importance thought history,
in such instances as the destruction of the Alexandria Library by Saracen armies under the command of the Caliph Omar in 638 AD\textsuperscript{18}.

We, thus, do not agree with Sieber, who in basing his theory, assesses and defines information as a new economic, political and cultural asset, which, furthermore, has a specific potential for danger, because we believe information has always been a precious asset. We agree, however, with his claim that modern information technology has altered the very characteristics of information, especially in extending its importance and in treating it as a factor which works without man’s intervention, in automated data processing.

We believe that when a quantitative change reaches an extraordinary scale, at some point it changes into a qualitative change. Information technology has brought a new challenge in handling information and data. It is this change that is now affecting the law\textsuperscript{19}.

Information quantified and checked though objectively stored data in an information system, generally a computer system, becomes a fund of wealth, knowledge and power in the post-industrial society.

The data and information, once their importance have been maximized in the post-industrial society, should receive the protection of criminal safeguards, in every respect.

However, it is necessary to pay close attention to the difference between information and data. In terms of pure Computer Crimes, including the way they are treated in the proposed bill of law, the term “data” should be used as being more subjective than information. This is because information, as has already been explained, is a very vague concept to be used in penal law. “Vox” should only be employed in dealing with privacy infringement. This is also Kaspersen’s\textsuperscript{20} view to be found in the Exposition of Motives of the Dutch Ministry of Justice when he asserts:

\textit{The term information applies to the result of a process rather than to the object of any (illegal) act. Under the present substantive criminal law, information or equivalent terms occur only in provision in which the process of obtaining}

\textsuperscript{18} Alexandria Library, an Egyptian library founded 290 BC by Ptolemy Soter of Alexandria and enriched by successive rulers. Destroyed by Saracen and armies the Caliph Omar in 638 AD, it is thought the collection totaled 700,000 volumes.

\textsuperscript{19} Maggs, Peter B., Soma John T., Sprowl James A: op. cit., p. 504.

information (illegally) is at stake, e.g. espionage, professional secrecy, trade secrets, insider trading. Therefore, the term computer data will be introduced in the Criminal Code, which not only refers to the content and meaning but also to the form and technical environment of the potential information.

2.6. Computer Networks

Computer networks, from the very simplest services to the most complex EDI or the transfer of electronic credit, are characterized by being computer systems linked to telecommunications equipment. Such systems become the autonomous ways and means for producing wealth and providing services, forming the basis of many complex and essential services in our society. As Wasik says, "computers are today at the very center of the whole financial market, as well as other sectors of the economy". The computerization of the London Stock Exchange, in compliance with the law, will not require any physical proof of the transactions effected. Accordingly thus, if the City of London's computers break down, the whole financial complex will grind to a halt.

Those networks, though not constituting in themselves a juridical property, can be described as an available resource of proven reliability, resulting from the use of computer systems, programs, data banks and communication systems.

This is not a new juridical property, but it is a new means stemming directly from modern technology. The network may represent a set of resources provided by the environment resulting from the junction of different linked computer systems. Nowadays, networks have become so important that they to be protected and kept free from any interference and misuse. Besides being invested with the confidence of various sectors of the economy as the ways and means of production, they require a huge quantity of financial resources to maintain them and, furthermore, have a processing capability and a range of information and data which should not be subject to unauthorized use or interference by any person whatever. The use of the network and use isolated computers vary. To give an easy example in the academic world, one only has to imagine what the resources of WW, WAIS and Gopher, found in Internet, would be reduced to, if it were not the computer networks.

21 Some examples of these networks are: Access, Westlaw, Nexis, Lexis, EFT, Swift, Bitnet, Arpanet, UUCP, Internet, DECENET, Videotext, GEnie, Compuserve, Reuters, etc.
22 Wasik, op. cit., p. 32
2.7. Definition of Computer Crimes

Basically, "computer crime" is characterized as being injurious behavior, which does not necessarily correspond to obtaining an illicit advantage. In this concept, behavior which characterizes traditional crime, that has as the material object computer systems, their components, or peripheries, such as, for example, the theft of hardware or software material, is not included.

Thus, anyone who takes a personal computer with the purpose of selling it for money, would be guilty of common theft and not a "computer crime". We will define computer crime, therefore, firstly from the standpoint of a protected juridical property. Computer crime is any prejudicial conduct against the natural state of the data and resources provided by a system of processing, storing or transmitting data, whether in the form only understood by the elements which make up a data processing, transmitting or storage system, or in the form understood by Man. Such conduct should be directed at the data which, in its turn, will operate without the intervention of man, and constitute the material object of the crime.

It should be said, therefore, that those two elements cannot be dissociated, since should only one of them prevail, one would not be dealing with a computer crime, but rather a common crime, as already typified, perpetrated though the use of the computer. Thus, someone who perpetrates an explosion in a building to destroy files contained on magnetic tapes which were stored there is acting against a highly valuable property which is at first sight the data contained on those tapes and which can be translated into information.

Nevertheless he would not be committing a computer crime, due to the absence of the second element. In the same way, someone who uses a computer to kill a gravely ill patient connected to life-support equipment in an ICU would be committing homicide and not a computer crime, due to the absence of the first element.

Thus, we should stress that not every act direct against data, information and computer networks constitutes a computer crime. It might constitute any of the crimes already typified or even civil or administrative illicit acts, as the same juridical property may be attacked and consequently protected in various fields of Law.

23 This is also the of Michele M. Correra e Pierpaolo Martucci: I Reati commessi con l'uso del computer, CEDAM, Padova, 1986, pag. 26.
3. CONSIDERATIONS ON THE CRIMINALIZATION OF CERTAIN CONDUCT

3.1. Criminalization of New Conduct

The new section of the Penal Code to be presented by the Executive to the Brazilian Congress, in respect of penal safeguards to interests and properties stemming from, or redefined in their importance, by the post-industrial information society marks a new approach by Brazilian authorities to the question based on arguments already examined.

The suggested draft is contained in an Chapter entitled “Crimes against the Socioeconomic Order” in the Special Section of the Penal Code, where computer crimes will be inserted. The said Chapter has only eight sections. Three of them will deal specifically computer crimes, as previously defined, while another three provisions will deal with the modification of already existing norms to cover intangible properties redefined in their importance. The final two sections will cover serious infringements of individual privacy, perpetrated through the computer.

In sum, while three sections will deal with the Computer Crime, the other five will be related to Computer Misuse.

3.2. Legal Provisions and the Brazilian Federal Constitution

The Constitution of the Federative Republic of Brazil establishes in its article 220 that “thinking manifestation, creation, expression and information of any form, process and means will suffer no restriction, according to this Constitution”. In its paragraphs 1 an 2, this article completes the general norm while determining that: “No law shall contain disposition constituting impediments to the plenty journalistic information freedom in any means of social communication, according to the article 5, IV, V, VII and XIV” and that: “every and any censure of a political, ideological and artistic nature is prohibited”.

In order to guarantee these principles, the Constitution determines in its article 21 that it competes to the Union: n° XI - “to explore telephonic, telegraphic and data transmission services and other services of telecommunication directly or by means of concession to companies under the control of the State, being assured to entities of private law the right of reentering information service by means public nets of telecommunications explored by the Union”; n° XII - “to explore, directly or by means of authorization, concession or permission: a) services of sound broadcast, of sounds and images, and other services of telecommunication”. Faced with this, the article 22 of the Constitution states that: “it competes privately to the
Union to legislate about": n° IV - “waters, energy, information, telecommunications and broadcast”. According to the article 48, XII of the same Constitution, this is a private competence of the National Congress (Legislative Power).

In addition to this, the Brazilian Constitution consecrates the principle of information freedom among its “Fundamental Rights and Guaranties”, so that the Chapter on “Individual and Collective Rights and Duties” establishes in its article 5 that:

“All people are equal before law, without distinction of any nature, being assured to Brazilians and to foreigners living in the country the inviolability of the right’s to life, freedom, equality, security and property in the following terms:

“IV. the thinking manifestation is free, being prohibited the inanimate;
“V. the right to response proportional to the offense is assured, besides indemnification for material and moral harms;

“IX. the expression of intellectual, artistic, scientific and communication activity is free, regardless of censure or license;
“X. the privacy, the private life, the honor and the image of all people are inviolable, being assured the right to indemnification for material and moral harms resulting from transgressions;

“XII. the secrecy of correspondence and telegraphic communications, of data and telephonic communications is inviolable, except in the last case for a judicial order in the hypothesis and in the way established by law for purposes of criminal investigation or procedural instruction;

“XIV. the access to information is assured to all people, being protected the secret of the source when the professional activity requires it;

“XXVII. it belongs to the authors the exclusive right of using, publishing, reproducing their works, being this right transmissible to their inheritors for a period fixed by law;

“XXXIII. all people have the right to receive information on their private interest as well as on collective or general interest from public organisms in accordance with the law, under penalty of liability, being excepted those information whose secrecy is necessary for the security of the society and the State;
"LXXII. Habeas data shall be conceded:
"a) to assure the access of information related to the applicant from registers or data banks of governmental or public entities;
"b) to ratify data, when the solicitant does not prefer to make use of a confidential, judicial or administrative process;

"LXXVII actions of Habeas Corpus and Habeas data, as well as all acts necessary to the plenty exercise of the citizenship are free".

Besides the constitutional field, there is a national policy of information technology, whose implementation began in 1979. Nevertheless, this policy only assumed configuration in 1980, when the first computer based on an entirely Brazilians project was concluded.

For orienting and executing the national policy of information technology, the National Council of Information Technology and Automation (CONIN), the Special Secretary of Information and Technology (SEI) and the Foundation Technological Center of Information were created.

The law number 7.232 of 29.10.84 disposes about the National Policy of Information Technology. Looking forward protecting our market, this law created an “official Register of all Information Technology Services Renders” and determined that public organisms can only contract information technology services from foreign countries when there is no similar service offered by a national company. This law created the software official register and also established rules for contracts of commercialization of computer programs and complementary services like installment, maintenance and technical support. In addition to this, it established a concept for program; required approval for all contracts; created obligatory covenants; and established some determined prohibitions.

The CONIN was reorganized by the Decree number 90.754 of 27.12.84, and the SEI was re-structured by the Decree number 90.755, while the Decree number 90.756 approved the Statute of the Foundation Technological Center for Information Technology.

The first National Plan of Information Technology and Automation was established by the law number 7.436 of 17.04.86 and is addressed to promoting the development of national technology, to increasing activities in this sector and to generating new employment’s by means of a system of market reservation, according to which fifty per cent of the market should be covered by Brazilian companies.

According Bittar, “that basic objective of this system is the national qualification in activities of information technology, in advantage of the
general development of the country, while increasing the level of national autonomy and the productivity of national companies.\(^{24}\)

As we have already seen, the law number 7.646 of 18.12.87 disposes about the protection of intellectual property of computer programs and their commercialization within the country, while establishing other provisions. This law was regulated by the Decree number 96.036 of 12.05.88. The Decree number 90.750 of 27.12.94 establishing the organization and the functioning of the CONIN was altered by the Decree number 97.695 of 26.04.89 and also by the law number 8.249 of 16.10.91 and the Law of Information Technology (Law number 7.323 of 1984) was modified by the law number 8.248 of 23.10.91. This law reduced enormously the system of market reservation previously established.

### 3.3. Substantive Criminal Law

The Brazilian Legislation related to "computer crimes" is very poor. The Criminal norms disposed in our positive law date from a period when these crimes were not under major discussion. For this reason, these norms of Penal Code, whose Special Part dates from 1940, can only be applied incidentally to those hypothesis.

As we have said in another part of this study, our present legislation has focused its main concern on crimes of software piracy what we consider as a computer misuse and not a computer crime.

The orientation of the Brazilian doctrine has followed major international tendencies protecting software as copyrights material. This doctrinaire position was accepted by our legislators who created two crimes expressing such understanding in the articles 35 and 37 of law 7.646 of 18.12.87.

The article 35 establishes the penalty of imprisonment varying from 6 months to 2 years and fine for those who "violate right's of authors of computer programs". The article 37 establishes a crime we can critically call "smuggling of non registered software", that is defined as "to import, export, keep in deposit non registered computer programs from a foreign country for purpose of commercialization penalty: imprisonment from 1 to 4 years and fine". The second crime has an economic nature, since it seeks to strengthen the rules of market reservation established by our national policy of information by means of a penal sanction, as we have already seen.

A simple reading demonstrates that the legal rules already mentioned

---

are clearly imperfect and insufficient for the purposes they intend to achieve. As a result of the changes occurring in our policy of market reservation, the crime of “smuggling non registered software” will be soon discrimina-
ized”.

The Brazilian law protects intellectual property of computer programs as manifestation of immaterial property, the same way our Penal Code punishes general transgressions of copyrights. Nevertheless, its penalty is heavier than that imposed by the Penal Code (imprisonment from 3 months to 1 year and fine).

The recent law number 8.137 of 27 December 1990 defines crimes against the tributary and economic orders and against consuming relations and creates new forms of “computer misuse” related to the tributary order. This crime is defined as the action of “using of disclosing data processing program to permit the active subject of the tributary obligation to maintain information related to bookkeeping which are different from those presented to the Public Treasury - Penalty: imprisonment from 6 months to 2 years and fine”. As we can see, it is the case of a computer program whose specific destination is to permit frauds. In this case, information technology is being used as a criminal instrument.

This is our whole legislation in relation to “computer crimes”.

Faced with this normative limitation, the judge is obligated to make use of rules of traditional crimes to combat this new form of criminality.

It is possible to understand some conducts as traditional larceny by fraud. Nevertheless, both questions related to the nature of the fraud and relations between subjects of the criminal relation do not permit the establishment of a crime definition, especially in cases of espionage and sabotage, in addition to those where there is no economic advantage for its agent. From these questions result the need for the creation of a new criminalization process. And, in this field, many new problems emerge.

As we know, in the present moment of the scientific development, main thinkers involved in the criminalization phenomenon propose a wide program of discriminalization. The neo-defensists support this point of view based on the lack of social interest in punishing some determined crimes. Both supporters of the Critical Criminology and of the Alternative Criminal Policy present the same understanding, although basing their analysis on a minimum Criminal Law, limited by the Fundamental Human Rights, according to determination of Baratta’s.

Alessandro Baratta: Principios del Derecho Penal Mínimo; in Anais da Conferência
For both neo-defensists and critical criminologists the modern criminal policy is determined by a double way. According to this theory, beside the movement of discriminalization there is another one, whose objective is to criminalize new facts related to the modern forms of criminality.

Faced with this theoretical and practical configuration, Brazil tends to create some specific crimes. Such tendency is manifested in an analysis of the present projects under discussion in the National Congress.

Presently, the following projects are being discussed in the National Congress:

A. Project of law of the Senate number 75 of 1989 that “Disposes about inviolability of privacy, private life, honor and individual image”. Such project was assimilated by another one (number 137 of 1989) that has the following text:

"Article 1. Constitute crimes against individual freedom:
I. to violate guard of photo, image, writing or word about someone’s private life, by means of technical process or any other means - Penalty: imprisonment from 3 months to 1 year.
II. to provide or to use unduly information present in automatized file about someone’s private life - Penalty: imprisonment from 3 months to 1 year.
"Article 2. Penalties established in the anterior article will be increased until their double if the agent has acted looking for profits or by means of abuse of power.
"Article 3. The penal action established for the crimes this law depends on representation".

This Project is presently under discussion in the Chamber of Deputies.

B. Project of law of the Chamber of Deputies number 4.597 of 1990, substituted by the project number 597 of 1991 that “disposes about the crime of interference in information technology systems” with the following text:

"Article 1. Practices crime someone who, having in view an illicit advantage for himself or for someone else, or also looking forward causing prejudice to someone, to system, to computer or to equipment that composes a system or program:

“a) destroy or alters fraudulently or uses unduly computer program he has access to:
“Penalty - imprisonment from 1 to 5 years and fine corresponding to the value of the advantage in view or of the risk of prejudice imposed to the victim.
“b) abuses by any means of his right to accessing system of computing, data transmission or processing of any nature:
“Penalty - imprisonment from 1 to 4 years and fine corresponding to the value of the advantage in view or of the risk of prejudice imposed to the victim.
“c) introduces fraudulently into computer a program or command-instruction destructing or altering a program stored in the computer, or alters in any way its functioning:
“Penalty - imprisonment from 1 to 4 years and fine corresponding to the value of the advantage in view or of the risk of prejudice imposed to the victim.
“d) uses someone else’s password to obtain an undue access to a system or a computer:
“Penalty - imprisonment from 1 to 3 years and fine corresponding to the value of the advantage in view or of the risk of prejudice imposed to the victim.
“e) obtains intentionally access to system or computer without previous authorization:
“Penalty - imprisonment from 1 to 3 years and fine corresponding to the value of the advantage in view or of risk of Prejudice imposed to the victim.
“Article 2. A non-intentional interference resulting from negligence, imprudence and unskilled fullness constitutes a fault crime:
“Penalty - fine corresponding to the prejudice caused. Minimum fine: Cr$ 170. 000, 00 (one hundred seventy thousand cruzados). In case of reincidence imprisonment for 3 months and the same fine”.

In relation to protection of computer programs, the President of the Republic while giving sequence to his policy of information technology liberation has send the message number 229/91 to the National Congress. This message that assumed the denomination of Project of Law number 997/91 disposes about the protection of intellectual property of computer programs and their commercialization in the country while establishes other providence”. According to the “Exposition of Motives” that followed the presidential message, this project is fundamentally in accordance with the following directives: a) elimination of restrictions for national companies to distribute and to commercialize foreign computer programs within the country; b) elimination of the exams of similarity involving foreign and national products; c) elimination of the cadastre of computer programs; d) possibility of importing computer program without a contract of distribution, in order to establish a bigger competition in this sector; e) reinforcement of right’s and guarantees of computer programs users.
Considering the present situation of this project in the National Congress, we can say that it will become a law soon. Based in this law, we will not have the crime of “smuggling of non-cadastre software”, established in the article 37 of the law of intellectual protection of computer programs, anymore.

The crime of violating copyright of computer program (article 35 of the present law) is not altered by the Project either in its definition or in the quantity and quality of its penalty.

Major innovations are established in the Project of Law of the Senate number 152 of 1991 presented by the Senator Maurício Corrêa and also in a substitute one. According to this Project, one understands that the major concern of the legislator is guaranteeing data belonging to the user. So, data inviolability and its communication is under protection.

In addition to this, the author of the Project understands that, save some important exceptions, the use of information technology did not create new crimes, but only established new means for the commitment of traditional ones. For this reason, in addition to creating some new crimes, this law establishes legal mechanisms for the use of norms of the Penal Code.

The Project adopted an old idea of ours established in the article 11 of the bill of Law of Financial crimes. We have elaborated this bill representing the Rio de Janeiro State’s branch of the Brazilian Bar Association in 1985. Since that time we have understood that not only sheets of paper can contain information of juridical relevance. For this reason, we understood in that bill that electronic registers of data processing have the same value of documents.

Faced with new crime establishes in the Project, one has to detach the undue access to other people’s information. Such crime destinates to giving execution to the constitutional command that establishes the data secrecy.

In relation to “virus”, penal liability should not be restricted to the individual who creates the program. It should also reach the person who introduces it in other people’s system. So, the crime must be defined as the action of “putting in circulation a virus program”. The “virus” program does not necessarily have to bring an advantage to the agent nor an economic prejudice to its victim in order to be criminalized. It is only necessary to happen an undesired effect within the system. So this is the text of the substitutive Project number 152/91:

"Article 1. It constitutes crime against data inviolability and their communication the practice of the conducts described in the article 2 and 3 of this law.

"Article 2. To violate data secret by accessing information contained in other people's physical support or system without the due authorization:

"Penalty - imprisonment from 1 to 6 months and fine.

§ 1. If the access is practiced by means of undue use of someone else's password or magnetic identification process:

"Penalty - imprisonment from 3 months to 1 year and fine.

§ 2. If the access results in an undue economic advantage to the detriment of the system's owner, the fact is punished as a qualified larceny by fraud in accordance with the article 4 of this law.

"Article 3. To insert into physical data support or into data communication program designed to work clandestinety in other people's system causing an undesired effect:

"Penalty - imprisonment from 1 to 6 months and fine.

§ 1. If there is a definite loss of information contained in the system:

"Penalty - imprisonment from 6 months to 2 years and fine

§ 2. If, in addition to the loss of information there is an economic prejudice of any owner of the system:

"Penalty - imprisonment from 1 to 3 years and fine.

"Article 4. The commitment of conduct described in this law for the practice of any other crime turns it into a qualified crime, having its penalty increased in a period between one sixth and its half.

"Article 5. Information or data contained in electronic system having any sort of relevance for human relations are considered "documents". Their material or ideological adulteration is punished in accordance with the Penal Code and with the article 4 of this law.

"Paragraph Unique. For purpose of this article, one understands "public documents" as information or data of a system:

"a) belonging to or under service of public organism of direct or indirect administration, financial institution, Stock Market or recognized establishment of public instruction:

"b) in condition to authorize payment, quittance, movement of bank account or any other transference of values:

"c) designed to access public payable or free commercial, economic and financial information".

This was the tendency of the Brazilian law. It was sure that the criminalization of "computer crimes" would take place in a singular law, and not in the Penal Code.

Now we hope that our contribution to the bill may represent an evolution to the actual stage of the criminal computer law in Brazil.
3.4. Proposed Bill to Modify Brazilian Penal Code: Crimes against Computer Systems or Data Communication Systems. Violation of Computer System or Data Communication System

**FIRST SECTION:** To violate a computer system or data communication system belonging to another, by obtaining or trying to obtain unauthorized access, making it produce any function: penalty... fine and a ban on exercising activities connected with information technology for... years.

Qualifications:
Paragraph 1. If the unauthorized access has the intent to cause damage to another person or obtain any advantage. penalty... fine and a ban on exercising activities connected with information technology for... years.
Paragraph 2. If through the unauthorized access the perpetrator produces a temporary or permanent alteration to data, instruction or computer program contained therein or accessible through a computer system or data communication system: penalty... fine and a ban on exercising activities connected with information technology for... years.
Paragraph 3. If the unauthorized access or the alteration of data, instruction or computer program is done through the use of an identification code or other such identification process belonging to another: penalty... fine and a ban on exercising activities connected with information technology for... years.
Paragraph 4. If through unauthorized access the perpetrator violates the confidential status of the data, contained therein or accessible through a computer system or data communication system: penalty... fine and a ban on exercising activities connected with information technology for... years.
Paragraph 5. If through unauthorized access or the alteration of data, instruction or computer program the perpetrator causes damage to the other obtains any advantage: penalty... fine and a ban on exercising activities connected with information technology for... years.

*Unlawful Acts against the Integrity of Computer System or Data Communication Systems*

**SECTION 2:** To develop a command, instruction or computer program able to clandestinely delete, wipe out, alter, store or transmit data, instruction or computer program or to provoke any other result different from that expected in
a computer system or data communication system with the intent to cause
damage to the other person, to obtain undue advantage or satisfy personal or
interest:
penalty... fine and a ban on exercising activities connected with information
technology for... years.

Contamination of a Computer System or Data Communication System

Sole Paragraph. The same penalties will apply to anyone who introduces the
command, instruction or computer program to which this section refers to in
a computer system or data communication system belonging to another:

Computer Sabotage

SECTION 3: To destroy, damage or impair the operation or capacity to operate
of a computer system or data communication system belonging to another
with intent to harm the other person, obtain advantage or satisfy personal
whim or interest.
penalty... fine and a ban on exercising activities connected with information
technology for... years.
Sole Paragraph. The same penalties will apply to anyone who, with same intent:
I. deletes, eliminates, alters, stores or transmits data, instruction or computer
program in a physical support, or outside computer system or data communi-
cation system;
II. provokes any other result different from that expected which violates the
integrity or readability of the data, instruction or computer program found in
a physical support or outside computer system or data communication system.

Theft of Time in Data Computer System System Network

SECTION 4: To make unauthorized use of the resource of government agency
or public computer system or data communication system networks.
penalty... fine and a ban on exercising activities connected with information
technology for... years.

Personal Data Traffic

SECTION 5: To send data or information of a personal nature contained in a
data computer system or any physical support system to unauthorized person(s)
or with a different intent to that which the information is designed for, without
the permission of the interested party.
penalty... fine and a ban on exercising activities connected with information
technology for... years.
Sole paragraph. The same penalties will apply, in the terms of this section, to
anyone who obtains data or information of a personal nature.
Violation of the Duty to Inform

SECTION 6: To fail to acknowledge or rectify personal information found in or accessible through a computer system or data communication or physical support system of a government or public service agency when requested by the interested party: penalty... fine and a ban on exercising activities connected with information technology for... years.

Accredited Documents

SECTION 7: A document shall be construed, for penal effects, as data or computer program employed in the computer system, data communication or any physical support system.

Crimes Specified in Other Articles

SECTION 8: A crime not specified in this article, when committed through the employment of a computer system or data communication system, will be subject to an additional penalty of...

4.0. Acknowledgement

We recognize the contribution of prof. Nadia de Araujo from PUC-RJ and we are grateful for her thoughtful comments.