October 30, 2001 Official Gazette No. 37,313

SPECIAL LAW AGAINST COMPUTER CRIMES

THE NATIONAL ASSEMBLY OF THE BOLIVARIAN REPUBLIC OF VENEZUELA

DECREES

The next,

SPECIAL LAW AGAINST COMPUTER CRIMES

TITLE I
GENERAL DISPOSITION

Article 1. Purpose of the Law. The purpose of this Law is a greater comprehensive systems that use information technologies, as well as the prevention and punishment of crimes committed against such systems or any of its components, or of crimes committed through the use of said technologies, to the terms provided in this Law.

Article 2. Definitions. For the purposes of this Law, and complying with the provisions of Article 9 of the Constitution of the Bolivarian Republic of Venezuela, is understood by:

- **Information Technology:** branch of technology that is dedicated to study, application and processing of data, which involves the obtaining, creating, storing, managing, modifying, operation, movement, control, visualization, transmission or reception of information automatically, as well as the development and use of the hardware, firmware, software, and related telecommunications and all procedures associated with data processing.
- **Systems:** any *organized arrangement of resources and procedures* designed for the use of information technologies, *suited and regulated* by interaction or interdependence to fulfill a series of functions specific, as well as the combination of two or more components interrelated, organized in a functional package, so that information technology can accomplish functions or satisfying a requirement within specified specifications.
- **Data:** facts, concepts, instructions or characters represented in an appropriate way to be communicated, transmitted or processed by human beings or by automated means and to which a meaning is assigned or can be assigned.
- **Information:** meaning that the human being assigns to the data using known and generally accepted conventions.
- **Document:** record incorporated in a system in the form of writing, video, audio or any other medium, containing data or information about a fact or act capable of causing legal effects.

- **Computer:** device or functional unit that accepts data, processes it according to a saved schedule and generates results, including arithmetic or logical operations.
- **Hardware:** physical equipment or devices considered *in* independent of their capacity or function, which make up a computer or its peripheral components, so that they may include units, implements, instruments, connections, assemblies, components and parts.
- **Firmware:** program or program segment incorporated in such a way permanent or semi-hardware component.
- **Data or information processing:** systematic performance of operations on data or on information, such as management, merger, organization or computation.
- **Safety:** condition resulting from the establishment and maintenance of protection measures, which guarantee a state of invulnerability of the information and data, that is free from danger, risk or damage, to the data of unauthorized persons, or that affect the operation of the functions of a computer system.
- **Virus:** intentional program or program segment that develops within other computer programs, destructive or disruptive effects on a program or system component.
- **Smart card:** label, identification card or card that is used as identification instrument, access to a system, payment or credit, and that contains data, information or both, of restricted use about the user authorized to carry it.
- **Password (password):** alphabetical, numeric or combination sequence of both, generated by confidentiality code, and to verify the authenticity of the authorization issued to a user to access the data or information contained in a system.
- **Data message:** any thought, idea, image, audio, data or information, expressed in a known language that can be explicit or secret (encrypted), prepared in a format suitable for be transmitted by a communication system.

Article 3. Extraterritoriality. When any of the crimes provided for in the present Law, committed in whole or in part, affects or causes harm to the entities subject to its provisions if, within the territory of the Republic, produced effects of the prosecuted act, and the person responsible has not been tried by the same fact or has evaded trial or conviction by foreign courts.

Article 4. Sanctions. The sanctions for the crimes provided for in this Law will be main and accessory.

The main sanctions will consist with the accessory penalties and both may also coincide with each other, according to the particular circumstances of the crime which it is, in the terms indicated in this Law.

Article 5. Liability of legal persons. When crimes provided for in this Law were committed by managers, administrators, directors or dependents of a legal entity, acting on its behalf or representation, they will respond according to their guilty participation.

The legal person will be sanctioned in the terms provided in this Law in the cases in which the punishable act has been committed by decision of its organs, to the scope of its activity, with its social instrument or in its exclusive interest or professional.

TITLE II
OF CRIMES

Chapter I
Of Crimes Against Systems That Use Information Technologies

Article 6. Improper access. Any person who, without proper authorization or exceeding that which has obtained, accesses, intercepts, interferes or uses a system who uses information technologies, will be sentenced to imprisonment from one to five years and a fine of one to fifty tax units.

Article 7. Sabotage or damage to systems. Anyone who intentionally destroys, damages, modifies or disables the data or the information contained in any system that uses information technologies or any of its components that make it up, will be punished with imprisonment from four to eight years and a fine of four hundred to eight hundred tax units.

Anyone who destroys, damages, modifies or disables the data or the information contained in any system that uses information technologies or in any of its components.

The penalty will be five to ten years in prison and a fine of five hundred to one thousand units, if, if the offenses indicated in this article are carried out through the intentional creation, introduction or transmission, by any means, of a virus or similar program.

Article 8. Improper error of sabotage or damage. If the foreseen offense in the previous article is committed by recklessness, negligence, incompetence or breach of duty to the security of systems that use information technologies, will be applied depending on the case, with a reduction between half and two thirds.

Article 9. Improper access or sabotage to protected systems. The sentence provided for in the previous articles will be increased between one third and half, when the crimes provided there or their effects fall on any of the components of a system that uses information technologies protected by security measures, that is intended for public functions or that contains personal or patrimonial information of natural or legal persons.

Article 10. Possession of equipment or provision of sabotage services. Whoever imports, manufactures, distributes, sells or uses equipment, devices or programs, with the purpose of using them to violate or eliminate the security of any system that uses information technologies, or provide for the purpose of these services to unlawful ends, will be punished with imprisonment from three to six years and a fine of three hundred to six hundred tax units.

Article 11. Computer espionage. Any person who improperly obtains, discloses or disseminates the data or information contained in a system that uses information technologies or any of its components, or any crime against them, will be imprisoned from three to six years and a fine of three hundred to six hundred tax units. The penalty will be increased from one third to one half, if the offense provided for in the present article is committed in order to obtain some kind of benefit for himself or for others.

The increase will be from half to two thirds, if the safety of the State, the reliability of the operation of the affected institutions or will result in damage to third parties, or if it occurs as a consequence of the disclosure of confidential information.

Article 12. Forgery of documents. Who, through any means, create, modify or delete a document that is incorporated into a system that uses information technologies, causing damage to third parties or to create a false same, or incorporate a non-existent document into said system, it will be punished with imprisonment from three to six years and a fine of three hundred to six hundred tax units.

When the agent has acted in order to procure for himself or for another some type of benefit, the penalty will be increased by one third to one half.

The increase will be from half to two thirds if the fact results in damage to other.

Chapter II
Of Crimes Against Property

Article 13. Theft. Who through the use of information technologies, accesses, intercept, interfere with, manipulate or in any way a system or means of communication to seize tangible or intangible assets or values of transcendental economic, will be imprisoned from three to six years and will be subject to a economic gain forfeited to the another, will be punished with imprisonment from two to six years and a fine of two hundred to six hundred units.

Article 14. Fraud. Anyone who, through the improper use of information technology, information, using any manipulation in systems or any of its components, or in the data or information contained in them, manage to insert false or fraudulent instructions, that produce a result that affects property, or that affects the property of third parties, will be sentenced to imprisonment from three to seven years and a fine of three hundred to seven hundred tax units.

Article 15. Improper obtaining of goods or services. Who, without authorization to carry them, use a third party smart card or instrument intended for these purposes, or the one who improperly uses information technologies to require the obtaining any effect, good or service, or to provide your payment without disbursement or assume the commitment to pay the consideration due, will be punished with imprisonment for two to six years and a fine of two to six hundred tax units.

Article 16. Fraudulent handling of smart cards or similar instruments. Who, for the purpose of obtaining any effect, benefit or service, unlawfully duplicates or defeats the data or information contained in a smart card or in any instrument intended for the same purposes, or the person who, through any means of information technology, creates, captures, duplicates or alter the data or information in a system, in order to incorporate units, accounts, registrations or information, for himself or for third parties, will be punished with imprisonment for five to ten years and a fine of five hundred to one thousand tax units.

The same penalty shall be incurred by those who, without having taken part in the previous events, but knowing the illicit origin of the cards or instruments, they carry out the commercialization of smart cards or instruments for the same purpose, or of the data or information contained in them or in a system.

Article 17. Appropriation of smart cards or similar instruments. Whoever appropriates a smart card or instrument intended for these purposes, that has been lost, misplaced or has been delivered by mistake, in order to retain, use, sell or transfer it to a person other than the legitimate owner or holder, will be punished with imprisonment from one to five years and a fine of one to fifty tax units.

The same penalty will be imposed on whoever acquires or receives the card or instrument from referred to in this article.

Article 18. Undue provision of goods or services. Anyone who, to knowing that a smart card or instrument intended for these purposes, has been lost, misplaced or has been delivered without, falsified, altered, provide whatever presents those with money, effects, goods or services, or any other thing of economic value will be punished with imprisonment of two to six years and a fine of two hundred to six hundred tax units.

Article 19. Polymorphic or counterfeiting. Anyone who without being duly authorized to issue, manufacture or distribute smart cards or analog instruments, receptor, area, transfer, market, distribute, sell, or in any way, use or provide for commercial purposes, devices of autonomous intended for the same purposes, or any equipment or component that captures, records, copies or transmits the data or information of said cards or instruments, will be punished with imprisonment from three to six years and a fine of three hundred to six hundred tax units.

Chapter III
Of Crimes Against the Privacy of People and Communications

Article 20. Violation of the privacy of the data or information of character personal. Anyone who knowingly violates the privacy of the data or information by any means, without the consent of its owner, the data or personal information of another or in which you have a legitimate interest, that are incorporated into a computer or system that uses information technologies, It will be punished with imprisonment of two to six years and a fine of two hundred to six hundred tax units.

The penalty will be increased from one third to one half if as a result of the violation of privacy will result in damage to the owner of the data or information or to a third party.

Article 21. Violation of the privacy of communications. Every person that through the use of information technologies access, captures, intercept, interfere, redirect, distribute or modify a third party's messages or signals of transmission or criminal communication, will be sentenced with imprisonment of two to six years and a fine of two hundred to six hundred tax units.

Article 22. Violation of disclosure of data or information of character personal. Whoever reveals, disseminates or assigns, in whole or in part, the facts discovered, the images, the audio or, in general, the data or information obtained

by any of the means indicated in articles 20 and 21, will be sanctioned with imprisonment for two to six years and a fine of two to six hundred tax units.

If the disclosure, dissemination or assignment had been made for profit, or if It will result in some damage to another, the penalty will be increased from one third to one half.

Chapter IV
Of Crimes Against Children or Adolescents

Article 23. Diffusion or exhibition of pornographic material. Anyone who, by any means that involves the use of information technology, exhibits, disseminates, transmits or sells pornographic or adult material, specifically designed to be seen or heard by people who are not of notice the minors to children and adolescents, will be punished with imprisonment from two to six years and a fine of two hundred to six hundred tax units.

Article 24. Pornographic exhibition of children or adolescents. Every person that by any means that involves the use of information technologies, uses to the person or image of a child or adolescent for exhibitions or pornographic, will be punished with imprisonment of four to eight years and a fine of four hundred to eight hundred tax units.

Chapter V
Of the Crimes Against the Economic Order

Article 25. Appropriation of intellectual property. Who, without authorization from his owner and in order to obtain some economic benefits, reproduce, distribute or sell in whole or in part, a work of the intellect that has obtained through access to any system that uses technologies of information, will be punished with imprisonment from one to five years and a fine of one hundred to five hundred tax units.

Article 26. Misleading offer. Any person who offers, markets or provides of goods or services, through the use of information technologies, and make false allegations or attributes uncertain characteristics to any element of said goods or services, or any other circumstance relevant to the same, sanctioned with imprisonment from one to five years and a fine of one hundred to five hundred units tax, without prejudice to the commission of a more serious crime.

TITLE III
COMMON PROVISIONS

Article 27. Aggravating factors. The penalty corresponding to the crimes provided for in the This Law will be increased between a third and a half:

1. If a password has been used to carry out the event
   also improperly obtained, taken away, withdrawn or lost.
2. If the act has been committed through the abuse of the position of access to data or reserved information or privileged knowledge of a professional, by reason for the exercise of a position in function.

Article 28. Special aggravating factor. The sanction applicable to legal persons for crimes committed under the conditions indicated in article 5 of this Law, will be

only fine, but for double the amount established for the referred crime.

Article 29. Accessory penalties. In addition to the main penalties provided in the previous chapters, will be imposed, necessarily without prejudice to the established in the Penal Code, the following accessory penalties:

1. The confiscation of equipment, devices, instruments, materials, tools, computer, or any other thing used to the commission of the crimes provided for in articles 10 and 19 of this Law.
2. Community work for a term of up to three years in the cases of the crimes provided for in articles 6 and 8 of this Law.
3. Disqualification from exercising public functions or jobs, for less disqualification for a period of up to three (3) years after the completion of the sentence, or the authorization for a period of up to three (3) years after the completion of or contested the main sanction, when the crime has been committed with abuse of the position of access to data or information or privileged knowledge of privileged personal, due to the exercise of a position or function public, the private exercise of a profession or trade, or the performance in an institution or private company, respectively.
4. The suspension of the permit, registration or authorization for operation, or the prohibition of the operation of institutions or companies related to the use of information technologies, up to the period of three (3) years after the main penalty has been completed or contested, if for reasons of the crime, the agent would have used or made appear a legal person.

Article 30. Disclosure of the conviction. The Court may
in addition, order the publication or dissemination of the conviction by the means that you consider the most suitable.

Article 31. Civil Compensation In cases of conviction for any of the crimes provided for in this Law, the judge, in the same ruling, will impose in the judgment of compensation in favor of the victim for an amount equivalent to the damage caused.

To determine the amount of the signed compensation, the judge will require the expert help.

TITLE IV
FINAL PROVISIONS

Article 32. Validity. This Law shall enter into force thirty days after of its publication in the Official Gazette of the Bolivarian Republic of Venezuela.

Article 33. Repeal. Any provision that conflicts with the present Law.

Given, signed and sealed in the Federal Legislative Palace, seat of the Assembly Nacional, in Caracas on the fourth day of September, two thousand and one. Year 191 "of Independence and 142" of the Federation.