

## **Costa Rica**

### **AMENDMENT TO VARIOUS ARTICLES OF THE CRIMINAL LAW AND ADDITION OF A NEW SECTION VIII TO THE TITLE VII OF THE CRIMINAL LAW DENOMINATED "CYBER CRIMES AND RELATED NORMS"**

**FILE N° 17613**

**ARTICLE 1.-** Articles 167, 196, 196 bis, 209, 214, 217 bis, 229 bis and 288 of the Criminal Code, Law N.º 4573 of May 4<sup>th</sup>, 1970 and subsequent reforms are hereby reformed as follows:

**Article 167.- Corruption. (Draft law)**

Who maintains or promotes corruption of a minor person or a handicapped person with erotic, pornographic or obscene purposes, while in exhibitions or public or private performances would be punished with imprisonment from three to eight years, even if the minor or the handicapped person consents to it.

The punishment will be from four to ten years of imprisonment if the author, using social networks or any other computer or telematic media, or any other communication means, looks for sexual encounters for oneself or for another person, or for groups, with a minor or a handicapped person, or uses these persons to promote corruption, or obligates them to perform perverse, premature or excessive sexually acts, even if the victim consents in participate in them or to watch when being performed.

**Article 196.- Violation of Mail or Communications. (Draft law)**

Who, with danger or harm for the intimacy or the privacy of a third person, and without his/her authorization, seizes, accesses, modifies, alters, eliminates, suppresses, intervenes, intercepts, uses, opens, diffuses or diverts from its

destination documents or communications that were address to another person, will be punished with imprisonment from three to six years.

Punishment will be from four to eight years of imprisonment if the conducts describe are performed by:

- a) People in charge of the collection, delivery or safeguarding of the documents or communications; or
- b) People in charge of administrating or giving support to the computer or telematic system or network, or that, in exercise of his/her duties, have access to such system or network, or to the electronic, optical or magnetic containers.

**Article 196 Bis.- Violation of personal data. (Draft law)**

Who, in his/her own benefit or the benefit of a third person, and with danger or harm to intimacy or privacy, and without authorization of the data's title, seize, modifies, interferes, accedes, copies, transmits, publishes, diffuses, compiles, renders useless, intercepts, retains, sells, buys, diverts towards a different end from which it were collected or give an unauthorized use to the image or data of a physical or legal person storage in a computer or telematic systems or networks, or in electronic, optical or magnetic containers, will be punish with imprisonment from three to six years.

Punishment will be from four to eight years of imprisonment, when the conducts describe in this article:

- a) Shall be realized by person in charge of administrating or giving support to the computer or telematic system or network, or that, in exercise of his/her duties has access to such system or network, or to the electronic, optical or magnetic containers.
- b) When the data are of a public nature or is within public data base.
- c) If the invaded information corresponds to a minor or a handicapped person.
- d) When the person's conducts affect data which reveal the ideology, religion, beliefs, health, racial origin, sex life or preferences of a person.

**Article 209.- Aggravated theft. (Draft law)**

Imprisonment from one to nine years applies will be levied on a person, if the value of the stolen information does not exceed five times the government defined base salary, and five to ten years if it is over such sum, according to the following cases:

- a)...
- b)...
- c) If does by picklock, false key or other similar instrument, or by the real key that has been stolen, found or kept, by access key, by magnetic card or by electronic devices.
- d) ...

**Article 214. - Extortion. (Draft law)**

Who, with the aim of profiting, forces another person, with intimidation or through a serious threat, to take a harmful patrimonial disposition for oneself or for another person, will be punished with imprisonment from four to eight years.

Punishment will be from five to ten years of imprisonment when the conduct is executed taking advantage of any computer, telematic, electronic or technologic manipulation.

**Article 217 Bis- Computer Fraud. (Draft law)**

Who, in detriment of a physical or legal person, manipulates or influences the entry, processing or results of the data of an automated information system, by way of false or incomplete data, improper use of data, programming, taking advantage of some computer operation, or technological device, or by any other action that affects the processing of the system data or that results in false, incomplete or fraudulent information, which endeavors or obtains a patrimonial or improper benefit for oneself or for another person, will be punished with imprisonment from three to six years.

The punishment will be from five to ten years of imprisonment if the conducts are committed against the public information systems, banking information systems, financial entities, or when the author is an employee in charge of administrating or

providing support to the computer or telematic system or network, or that in exercise of his/her duties, have access to such system or network, or to the electronics, optical or magnetic containers.

**Article 229 Bis.- Computer Damage. (Draft law)**

Who, without authorization from the owner or exceeding the one that has been granted and in detriment of a third one, suppresses, modifies or destroys the information in a computer or telematic system or network, or in electronics, optical or magnetic containers, will be punished with imprisonment from one to three years.

Punishment will be from three to six years of imprisonment, if the information that has been suppresses, modified, or destroyed is irreplaceable or irrecoverable.

**Article 288.- Espionage. (Draft law)**

Who procures or obtains in an improper way secret politic information or information from the national police bodies or security concerning defense matters or foreign relations of the Nation, or affects the fight against drug trafficking or organized crime, will be punished with imprisonment from four to eight years.

Punishment will be of five to ten years of imprisonment, when the conduct is executed through computer manipulation, malicious computer programs or by the use of information and communication technologies.

**ARTICLE 2.-** Addendum of a new subparagraph 6) from article 229 and an article 229 ter of the Criminal Code, law N.º 4573, from May 4<sup>th</sup>, 1970 and its amendments, which will be read as follows:

**ARTICLE 229.- Aggravated Damage. (Draft law)**

Imprisonment from six months to four years will be imposed:

[...]

6) When the damage is done to computer, telematic, or electronics networks, systems or equipment, or their physical, logical or peripheral components.

**ARTICLE 229 Ter. Computer Sabotage. (Draft law)**

Who, in his/her own benefit or the benefit of a third person destroys, alters, obstruct or disable the information in a data base, or impedes, alters, hinders or modifies, without authorization, the operation of an information management system, its parts or its physical or logical components, or a computer system, will be punished with three to six years of imprisonment.

The punishment will be of four to eight years of imprisonment when:

- a) As a consequence of the author's conduct, an unexpected collective danger or social damage may result.
- b) The conduct is performed by an employee in charged of the administration or support of the computer or telematic system or network, or because of his/her duties have access to such system or network, or to the electronic, optical or magnetic containers.
- c) The computer system is of a public nature or the information is on public data.
- d) Without being authorized, employ technological means that impede those who are authorized, the lawful access to telecommunications systems or networks.

**ARTICLE 3.-** Amendment of Section VIII of Title VII of the Criminal Code, Law N.º 4573, of May 4<sup>th</sup> ,1970 and its amendments and adjusts the numbering of the subsequent articles, to be read as follows:

**Section VIII**

**CYBER CRIMES AND RELATED NORMS**

**“Article 230.- Identity supplant. (Draft law)**

Who supplants the identity of a person in a social network, web site, electronic or technological information media will be punished with imprisonment from three to six

years. The same punishment will be levied on a person who, using a false or inexistent identity causes detriment to a third person.

The punishment will be from four to eight years if, following the previous conducts, a detriment is cause to a minor or a handicapped person.”

**Article 231: Computer Espionage. (Draft law)**

Who, without authorization of the owner or the responsible party, taking advantage of any computer or technological manipulation, seize, transmits, copies, modifies, destroys, uses, blocks or recycles, information of value to the normal economic behavior of the industry and trade, will be punished with imprisonment from three to six years.

**Article 232: Set-up or programming of malicious computer Programs. (Draft law)**

Who, without authorization and by any other means, installs malicious computer programs in a computer or telematic system or network, or in the electronic, optical or magnetic containers will be punished with imprisonment from one to six years.

The same punishment will be given in the following cases:

- a) Who induces another person into mistakenly installing a malicious computer program in a computer or telematic system or network, or in the electronic, optical or magnetic containers, without the right authorization.
- b) Who, without authorization, installs harmful computer programs or applications in legitimate web sites, with the objective of converting them in suitable vehicles for propagating malicious computer programs, known as Web Site Attacker.
- c) Who, with the aim of propagating malicious computer programs, invites other people to download or visit web sites that allow the installation of malicious computer programs.
- d) Who distributes computer programs which are design for the creation of malicious computer programs.
- e) Who offers, contracts or provides services of service denial, delivery unrequested mass communications, or propagation of malicious computer programs.

The punishment shall be from three to nine years of imprisonment when the malicious computer program:

- i. Affects a banking entity, financial entity, savings and credit Union, Solidarity Association or state entity.
- ii. Affects the functioning of public services.
- iii. Obtains remote control of a computer system or network, to become part of a zombie computer.
- iv. It is design to execute actions aim at obtaining a patrimonial benefit for oneself or for another person.
- v. Affects computing health systems and such damages can put in danger people's health or life.
- vi. Has the capacity of reproducing without the need of additional intervention of the legitimate user of the computer system.

**Article 233: WebPages supplant. (Draft law)**

Punishment of imprisonment, from one to three years, will be imposed on the person who, in detriment of a third, supplants illegitimate sites of the Internet.

Punishment will be from three to six years of imprisonment when, as a consequence of the supplant of the legitimate website, and through faking or making incur in a mistake, obtains confidential information of a physical or legal person for her/his own benefit or the benefit of a third person.

**Article 234.- Facilitating cybercrime. (Draft law)**

Punishment of imprisonment, from one to four years, will be imposed on the person who facilitates the execution of a crime that was carried out by a computer or telematic system or network, or by the electronics optical or magnetic containers.

**Article 235.- Drug trafficking and organized crime. (Draft law)**

The punishment will double when any of the crimes committed by a computer or telematic system or network, or the electronic, optical or magnetic containers, affects the fight against the drug trafficking or the organized crime.

**Article 236.- Diffusion of false information. (Draft law)**

Who through electronic, computer, or a telecommunication systems, propagates or diffuses news, or false facts capable of distorting or causing detriment to the security or stability of the financial system or of its users, shall be punished with imprisonment from three to six years.

**ARTICLE 4.** The article 9 of the Law about Registration, Seizure and Examination of Private Documents and Interception of Telecommunications No.7425 of August 09<sup>th</sup>, 1994 will be read as follows:

**“Article 9.- Authorization of Interventions.**

Within the procedure of a police or a jurisdictional investigation, the court can authorized the intervention of oral, written or another type of communications even the permanent, mobiles, wireless or digital telecommunications when it involves the clarification of the following crimes: **cyber crimes or executed through the use of computer, electronic, telematic, optical or by magnetic means**, kidnapping for the objective of ransom, aggravated corruption, aggravated pimp, manufacture or production of pornography, trafficking of persons and trafficking of persons to trade their organs; aggravated murder; genocide, terrorism and the crimes foresee in the Law on Narcotics, Psychotropic Substances, Drugs of Unauthorized Use, Money-Laundering and related activities, N° 8204 from December 26<sup>th</sup>, 2001.

In the same cases, such courts can authorized the intervention of communications between the presents, except what the second paragraph of article 26 of the present law establishes; when produce within dwellings and private spaces, the intervention can only be authorized if there are enough signs that an unlawful activity is being executed.”

This law will be valid when published.”