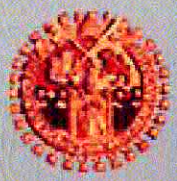

Universidad de Salamanca
fundación general

Juan Carlos Ferré Olivé, Ezno Musco, Barbara Kunicka-Michalska,
Jorge Almeida Cabral and other Autors

Grotius II Penal Programme

Penal Legislation in the Fight Against Financial Crimes, Fraud and Corruption, Computer Fraud and Internet Crimes

Financial Crimes, Fraud and Corruption: Fraud to the Interests of the European Union

Internet Crimes

Private Sector Corruption

Computer Fraud

Spain, Italy, Portugal and Poland

TABLE OF CONTENTS

Introduction II

The Subjective Type in Article 295 of the Spanish Penal Code
EMILIO JESÚS SÁNCHEZ ULLED 1

Computer Fraud: Provisions of Polish Law
BARBARA KUNICKA-MICHALSKA 11

Criminal Policy Regarding Private Corruption
ENZO MUSCO 20

Investigative Techniques and Procedural Problems in Computer Crime
FERNANDO VITORINO FERREIRA 29

Internet Piracy (Computer Crime: Practical Questions)
ROMULO AUGUSTO MATEUS 33

Conflict of Interest Between a Manager and the Managed Company With Public Funds
JAN SKUPINSKI 49

Sexual Abuse of Children: Child Pornography
JORGE DE ALMEIDA CABRAL 55

Fraud to the Financial Interests of the European Union: The Performance of the Portuguese Judicial Police
ANDRE INACIO 67

The Penal Responsibility of Internet Providers in Third Party Illegal Activities
LAURA LAURETI 73

Company Corruption in the Field of Unfairness: Connections With Article 2634 of the Civil Code
MARIA NOVELLA MASULLO 82

Child Pornography on the Internet
JUAN CARLOS FERRÉ OLIVÉ 88

Procedural Issues of Computer Offences in the Criminal Code of 1997, After the Amendments of 2003
LECH K. PAPRZYCKI 98

Computer Fraud in the Praxis
NIEVES SANZ MULAS 102

Embezzlement With the Use of Payment Cards
ANDRZEJ ADAMSKI 113

Embezzlement and Wrongful Collection of Subsidies Which Harm the State: Mafia Phenomenon, Illicit Winning and Management of State and Community Subsidies
ROBERTO ALFONSO 120

The Offence of Defamation With the Use of Internet in Polish Criminal Law
JOLANTA JAKUBOWSKA-HARA 132

Problems Regarding the Territorial Competence to Trial in the *Corpus Juris*
ANDRES PALOMO DEL ARCO 136

Corruption Between Individuals
LOREDANA ACIERNO 144

Fraud Detrimental to the Financial Interests of the European Community and the Polish Penal Code and the Polish Fiscal Criminal Code
JANINA WOJCIECHOWSKA..... 152

Hacking: Option in Favour of an Autonomic Penal Repression Model
NURIA MATELLANES RODRIGUEZ..... 164

A Brief Analysis of the Private Corruption Description
ANGELO CARMONA..... 169

Corruption in the Private Sector: Category Object of Articles 41-B and 41-C of Decree Law Nº 28/84 (January 20)
SONIA KIETZMAN..... 175

Computer Fraud
JORGE DE ALMEIDA CABRAL..... 184

Abusive Computer Access and Spanish Penal Law
MIGUEL ANGEL NUÑEZ PAZ and CARMEN RODRIGUEZ GOMEZ..... 194

Embezzlement Which Damages European Communities in Italian Jurisprudence
ROBERTO PASSALACQUA..... 203

Internet and the Right to Respect for Privacy
ADAM LOPATKA..... 211

European Council Agreement on Ciber Crime: An Analysis of Typical Conduct and Its Regulation Under the Spanish Penal Code
MIGUEL ANGEL NUÑEZ PAZ and CARMEN RODRIGUEZ GOMEZ..... 215

Telematic Reality and Illicit Connections
GIORGIO PICA..... 226

Computer Crime
RUI TEIXEIRA..... 233

Internet Offences in Poland: Analysis of the Practice
RYSZARD A. STEFANSKI and BARBARA SWIATKIEWICZ..... 239

Some Considerations Regarding Criminal Policy on Internet Crimes
MANUEL MORAN..... 251

State Police, Postal and Communications Police, Computer Fraud and Abusive Access in Internet
MARCELLO LABELLA..... 253

Computer Crime in Judicial Practice
A.A. SANTOS CARVALHO..... 258

Conclusions and Recommendations..... 269

COMPUTER FRAUD IN PRAXIS

NIEVES SANZ MULAS
Professor
University of Salamanca (Spain)

I. STUDYING THE PROBLEM.

Nowadays, the juridical world is certainly expected to face what seems to be a big challenge coming from the field of new information technologies. Evermore, looking from the most limited frame in Penal Law, its own nature as a repressor tool, with its fragmentary and ultimo ratio characteristics, would take us, inexorable, to the most negative side of the computer science, the most severe and evident consequences about our society. Or, what it is the same, the penal expert must face the perverted use of new technologies which are not just purely philosophical speculations, but more likely a reality supported by the "criminality numbers"[112]. The computer science, as defined by GARCIA PABLOS, "opens new horizons to the criminal minds, stimulates their imagination, favours the impunity and promotes the effects of the conventional crime"[113]. All of this, logically, without forgetting that the scientific and technological advancements are not inherently positive neither genuinely perverse[114]; because The positive or negative nature is directly dependent with the use that the human being does of such advancements.

II. COMPUTER FRAUD IN PRAXIS.

Concentrating on computer fraud, the United Nations, classifies the crimes in four different modalities, based on how the frauds are committed[115]:

1. *The manipulation on the data entry registration process.* This of computer fraud, also known as the subtraction of data, represents the most common computer crime, since it is easy to commit and hard to find out. The commission of this crime does not require of previous technical knowledge in the computer field and it can be done by any person who has access to normal processing functions in the data processing during the stage of data recollection.

---

[112] GUTIERREZ FRANCÉS, M.L., *Computer swindler and fraud. (Suitability of the type of swindler in the Spanish Law regarding the fraud by computer techniques),* Justice Department, Madrid, 1991, pp. 41 y ss.
[113] GARCÍA PABLOS DE MOLINA, A., "Computer Science and Penal Law", Socio-juridical implications by the information technology, Citema, Madrid, 1994, pp. 43-44.
[114] MESA, R., *The new International Society,* Center for Constitutional Studies, Madrid, 1992, p. 143.
[115] LEVENE, R., y CHIARAVALLOTI, A., "Computer Crimes", Published in the VIth Latinoamerican Workshop of 1998, in Colonia, Uruguay.

2. *Manipulation of computer programs,* which is very hard to find out and frequently goes unnoticeable due to the fact that the criminal must have some concrete technical computer knowledge. It is done by modifying the existing programs or inserting new programs or new routines in a computer system. A common method used by people with specialized knowledge in computer programming is the one known as "Trojan horse", which consist in the insertion of covered commands in a computer program, in order to allow it to perform a function which was not authorized originally to do, while performing its regular function, just as normal.

3. *Manipulation of the exiting data*, which is done by settling an objective to the functioning of the computer system. The most common sample of this is the fraud in ATM machines, done by introducing false instructions during the data entry stage on these machines. Originally these frauds were done by using stolen credit cards, but nowadays specialized computer systems and programs are used to codify forged electronic data in the magnetic band of bank cards and credit cards.

4. Finally, the UN report mentions the fraud committed by computer manipulation. In this case the fraud is done by the use of the automatic repetitions during the computer processing. It is a specialized technique which is known as "technique of _____"in which small portions of financial transactions, which are hardly noticeable, are taken repeatedly from one account and entered into another.

Regarding Internet, e-mail and e-commerce and the part that refers to the offering of goods and services, there is no doubt that these new technologies are making possible a better development of many business, and are very comfortable to use for the consumers. But the Net is also presenting a great window of opportunity for development of swindler on various levels. Internet has become a very susceptible way to commit swindler, due to the low security that the net still offers, as well as the smartness of the criminals working on this area, who do not hesitate in taking advantage of their knowledge in detriment of a third party. Among some of the most common acts of swindler in the net, are[116]:

- Products for sale offered in the Net but never send to the buyer, or if they are send, they have an increase in the final price notified after the client receives the goods.
- Products for sale which differ from the ones that the client ends up receiving.

For example, in some *sites*, such as some of the online auction sites, there are pictures of the products to be auctioned, for example a Rolex, and, after a client placed a bit and ends up acquiring the product, when the

[116] Shown by the *National Fraud Information* Center created in 1992 by the *National Consumer League (NCL)* of the USA. *Vid.*, en STRANO, M., *Computer crime,* Apogeo, Milán, 2000, pp. 153 y 154.

good arrives home, the client realizes that it is not the watch that you have buy and pay for, but the picture of the watch, such as it was sown in the site.

- Free services being offered on the internet, but which later on the client ends up paying, or services which differed from the ones that the client signed on for.

For example, an adult content site may offer to see images for free, by previously downloading a program needed. The site sexygirls.com operates like that. Its users downloaded a program necessary to watch the images, but such a program was really a "Trojan Horse"[117]. This Trojan Horse program silences the user's modem while unplugging it from its regular internet provider service. The PC then is plug and connect to a phone number in Moldavia (Soviet Union), and redirected later to North America, where the pictures are really located. The user's phone bill, therefore, is very expensive, because, even after the user logged out of the web site, its connection was still going throughout the Moldavia phone number.

- Also a common fraudulent practices are: selling hardware or software which never reaches the client, or, that after the buyer receives the merchandise, it differs from the ones advertised; offers on pyramidal investments and multilevel business ventures; opportunities of deceitful new business and franchises; offers to work at home previously acquiring the material to do so; money borrowing offers with a previous requirement for the payment of commissions (when the money is never given at the end) etc.

The e-mail is in itself as well, the best and more ideal way of increasing computer swindlers. These really are crimes that steal from individual users small amounts of money, but due to the humongous diffusion that electronic mail has, such crimes will give the swindlers large amounts of money. In this category, are procedures such as chains of letters, the pyramidal system and the *Ponzi*[118]*system.*

By the system of chain of letters the user is offer the guarantee possibility of getting a large amount of money by sending a very small amount to the person's name who is on the top of the list received. The victim, after sending the required amount, can delete that name from the top the list, and add his/her own name at the bottom of the list. The operation of this swindler is easy, the victim believes that after certain time, his/her name will be at the top of the list, and therefore, with the new names added to such a list, he/she will be

---

[117] This method consist the hidden insertion of specific commands which have different functions from the ones in the original program (or host program, which is automatically duplicated). This hidden commands act with total independency from the host program. Therefore, the computer will execute non authorized functions while in the meantime, it allows the host program to reach the ends to which it was created to begin with. This is the most common method in the commission of computer swindler and fraud. The Trojan Horse is a section of a code that is hiding, which does not have the capacity to auto replicate itself and which can be activate immediately or it can continue its operation as a legitimate software during a long period of time, before it activates itself.

[118] www.cnet.bigpond.com.

getting a larger amount of money than the amount that he/she send to begin with. But the reality is that the swindler, has send that same e-mail to thousands of people, obviously having his/her name on the top of al those lists, and therefore, receiving the adding small amounts of money from each one of the recipients of the mail, before the chain is deleted.

The pyramidal system, is done with more sophisticate and respectable looking letter chains, which offers the victim, the possibility to get involved in an investment venture that is expanding. In order to reach the top of the pyramid, the addition of more names to the base of the pyramid is a must. The swindlers also offer the possibility to acquire an extended list of personal e-mail addresses, so the victim can send an e-mail to, and therefore, escalate to the top of the pyramid. Needless is to say that none of the victims would ever reach the top of the pyramid, and therefore, start winning money.

Finally, the *Ponzi system* (named after a famous swindler in the field, Charles Ponzi) offers a user the possibility of getting aboard a promising investment venture, by giving a small amount of money upfront, and which guarantees a large return in a very short period of time. What makes this of swindler particularly believable, is the fact. that some times, in a relatively short period of time, some money is returned to the victim (with a small increase over the invested amount) to the victim, (usually until it reaches the second or third level of investors), and therefore, the victim gets more relaxed and trusting in the original investment. At this point, the swindlers will ask the victim to re-invest the recently acquire money, in order to get even better results, or even add a bigger amount, from his personal capital (at this point, they mention higher numbers, from 100 to 200 USD). The victims, who are feeling relaxed and trustful about the investment at this stage, frequently do send more money, but obviously, after sending the new amount, they would never hear from the swindlers again.

There is also, no doubt regarding the commission of fraud with credit cards. The interception of the credit card information, while is "travelling" throughout the net, and the utilization of such information to acquired product and services on Internet as well, have forced the business that operates selling goods and services on the Internet with the payment of such products via credit card, to adopt a secure and protected protocol for the transmission of such delicate information with very difficult decodification process[119].

At some Internet sites, for example, the user credit card information is required in order to verify that he/she is older than 18 years, if the user does not have the ability to realize that there is no possible way that with the credit card information the site operators can verify his/her age, then he/she would be suffering swindler.

---

[119] STRANO, M., *Computer crime, op. cit.,* pp. 156-157.

It is also possible to produce credit card numbers that are very believable, by using a software program that operates with various mathematic algorithms. Such activities, frequently allows the professional swindler to get small amounts of money.. The use of these method, is even available to people with very little technical knowledge and resources, since even Internet makes available to the public some programs with such a capacity to generate believable credit card numbers, which can be use later to acquire products on the internet for small amounts or money[120].

So in view of all of these different methods, it is surprising the number of possibilities to commit fraud and swindler by using computer procedures, and the question that remains is, how many of these cases are place on trial, and how many are sanction? To be totally honest, only a small proportion does.

Reviewing the Spanish jurisprudence since 1996, when art. 248.2 of the Penal Law was enforced —being this article the first one describing computer fraud in Spain—, it is surprising to appreciate that there are very few sentences related to these of crimes. Some juridical resolutions which generally refer to the punishing of fraudulent behaviour throughout the use of irregular credit cards are:

Sentence nº 14/2001 dictated by the Audiencia Provincial (Penal Trial Room , section 2ª), of March 10th, which qualifies as guilty of the crime of medium swindler (somewhere between generic swindler and computer swindler), stated on art. 248.2 on the Penal Code, to those individuals whom used various credit cards issued under their name, but the credit card's magnetic bands contain copies (data recorded electronically) of magnetic bands from original credit cards issued to different individuals. The Audiencia Nacional stated that "... it was not needed to materially swindler an individual in order to constitute computer swindler, but it was enough cause the fact. that the tool needed for computer manipulation, which is the element that can be consider as the constituent of the fraud using computer system".

Audiencia Provincial de las Palmas Sentence *nº 121/1998 (section 2nd), of October 19th, also* qualifies as computer swindler crime the act committed by any given individual who makes various purchases using various credit cards that have been previously stolen, since it considers that "...due to the fact that these of swindlers in which the operation is guarantee throughout an electronic signature, which is exactly the same as the identification code inserted in the magnetic band of the credit cards, these crimes differ from the traditional crimes of swindler, since there is a sophistication in the process, by commiting the fraud using a patrimonial active, throughout a transfer that has not been previously allowed...". This is also stated in Audiencia Provincial of Málaga Sentence *nº 128/2002 (section 3rd), of November 4th.*

---

[120] *Ibídem,* p. 159.

Other computer crimes of swindler tried and sanctioned are: those done by irregular accounting annotations in the computer system of a Bank entity[121]; taking advantage of computer failures in ATM machines[122]; duplicating fees of enrolment (to products or services) previously done[123]; duplication and substitution of product codes[124], etc. Although, honestly, such sentences are still just as small drops in the ocean of the real practical cases. Why is that?

III. VALORATIVE CONCLUSIONS

The first question to be asked is if art. 248.2 of the Penal Code for computer swindler with strictly patrimonial content is useful or not.

1. Legal regulation on computer fraud in the Spanish Penal Code.

The 1995 Penal Code, is well known, for not containing an independent chapter related to computer crimes, but for taking a political criminal decision to insert the different infractions all throughout the Code, taking into consideration the different needs for protection that in each case identified as juridical goods with different nature (intimacy, patrimonial, business secrecy, etc.)[125]. And regarding computer crimes referred to the patrimonial and economic sphere, the Spanish Penal Code classifies the computer fraud or swindler in the second paragraph in article 248, also considering guilty of swindler:

---

[121] The Audiencia Provincial of Granada Sentence *nº 208/1999 (section 1st), of march 23rd* considered guilty of a crime of computer swindler, the individual whom being a bank representative, took various amounts of money from the Bank Flow and deposit such amounts onto their own personal accounts, while using irregular accounting annotations in the computer system. Regarding this the Audiencia Provincial stated literally that the individual was committing this crime: "... based on the fact. that the accused, having the obtention of profit on mind and using computer manipulation, obtained the transfer not approved of a patrimonial active, money, which directly harmed the bank entity...".

[122] The Audiencia Provincial of Granada Sentence *nº 567/2002 (section 1st), of September 26th*, defines as computer fraud the crime committed by someone who after realizing the existent of a computer failure in ATM's, irregularly obtain money out of them.

[123] The Audiencia Provincial of Barcelona, Sentence*º 251/2002 (section 7th), of March 14th,* also described as computer swindler the conduct of the owner of a travel agency whom, in order to obtain financial aid for his/her business, duplicated and triplicate some of the charges already paid by clients who purchased their travel arrangements, by using the TPV machine. In this way, he obtained the new electronic transfers of the same amounts to his/her account, after obtaining the computer approval of the operation by the entity that issued the credit card.

[124] The Audiencia Provincial of Valencia, in Sentence *nº 14/2002 (section 4th),of January 30th,* sanctions the commission of a computer swindler crime stated in art. 248.2 of the Penal Code, to those whom forfeit the bar code of some products acquired at a cheaper price, by using a computer. The sentence states: "... throughout computer manipulation or a similar procedure, someone gets a not allowed transfer of any patrimonial active in detriment of a third party, by the requirement, against the previous consolidated doctrine of the supreme jurisprudence, that such a manipulation must be done with total awareness, it must fulfil the requirements needed to be considered proved enough the acquisition of a not allowed transfer, which would have never happen unless the manipulation would not have taken place, qualified as "enough" as the adjective of the deceit. Therefore one can reach the conclusion that in cases as the present one, in which the purchased good have been manipulated by the inclusion of a false bar code which does not match the original bar code of the some good as it was offered by the commercial branch, a deceitful mechanism has been placed, which causes the authorization of selling the product by the electronic reading of the false bar code by the laser reader.....".

[125] MORALES PRATS, F., "Penal intervention on the Net. The penal represion of traffiquing with children pornography: a concrete study", by AA. VV., *Penal Law, society and new technologies,* Colex, Madrid, 2001, p. 112.

"...those whom, with the obtention of profits in mind and using computer manipulation or a similar procedure, would obtain a not allowed transfer of any patrimonial active in detriment of a third party".

Is this definition enough to englobe the multiple cases of computer fraud or is this exactly the reason for the very small numbers in prosecuting and punishing this of crimes?

To answer this question, first of all, must be taken into account the fact that whatever the degree of complexity, sophistication and assigned functions, computers are mere tools, machines created by humans to serve humans, prepared, programmed and arranged so they can execute specific orders or commands. Regarding any fraudulent behaviour, this means that the computer is only a "tool", but can never be the "victim" or "subject of the fraudulent action"[126].

Next, we must interpretate the crime type stated in art. 248.2[127] so there is enough coverage for the majority of the suppositions[128]. At any rate, the typical action described in art. 248.2 of the Penal Code, describes as *"computer manipulation[129] or a similar procedure"*. In this way, and we agree with this, the legislator renounce to concrete on the different commission methods, which is something totally coherent with the fast technological development that is happening nowadays, where there is a risk of overdoing the classification of the typical modalities throughout the discovery of new ways of computer manipulation[130].

---

[126] GUTIERREZ FRANCÉS, M.L., *Computer fraud and swindler, op. cit.,* p. 584.

[127] In this new facet of swindler crimes, the typical action consist in the manipulation of a computer file or system, throughout which the active subject reaches a controlling capacity (transitorily) over the victim patrimonial, getting to transfer actives from the victim into the area of control of the swindler, and as a result, it goes in detriment of the patrimonial actives of a third party, for which, obviously, the relation between the casualty of the action and this previously mentioned detriment, is a must. *Vid.,* en MESTRE DELGADO, E., "Crimes against patrimonial actives and the socioeconomic order", LAMARCA PÉREZ, C., (Coord.), *Penal Law Manual. Special Part,* Colex, Madrid, 2001, p. 266.

[128] In relation to this, professor GUTIERREZ FRANCÉS redefine the elements as it follows: By deceit, we must accept that the falsification of the reality that the deceit implies, does not necessarily involve a direct and personal correlation between two different human beings, because while there is still a negative to take into account the possibility of the deception of a physical or juridical body, with help from sophisticated information technology, the criminal figure of swindler will be vetoed in the majority of computer fraud committed. In relation to the *error*, if we keep demanding that the swindler will maintained the state of error on the victim of the deception, as the detonant of the patrimonial use, then this crime has no place on the computer fraud arena. Finally regarding the reference to the act of patrimonial use, this must be re-study, considering that such patrimonial use can be made with the help of a machine, and that the "cooperation in the transfering of lesive patrimony" that is implied, can be extrapolate to the person, if he/she acts in person or with the help of machines. *Vid.,* GUTIERREZ FRANCÉS, M.L., *Computer fraud and swindler, op. cit.,* pp. 584-585.

[129] The computer manipulation can take place during the data entry process (by action or omission), as well as during the exit data process, in the same program. We are talking about cases related with computer transferring of actives, consisting in the introduction of false data or commands, or the modification of the programs that automatically manage banking transfers, deposits or credit approvals favouring the manipulator. These of criminal behaviours could not be included in the crime of stealing, since it is impossible to consider bank movements done over paper (implying accounting movements done directly by a computer giving as a result what are known as credit rights) as "goods", neither can it be included under crimes of swindler since there is no deceit committed against a "person" but against a machine. *Vid.*, GONZÁLEZ RUS, J.J., *Spanish Penal Law Course. Special Part,* Marcial Pons, Madrid, 1996, pp. 686-687.

[130] VALLE MUÑIZ, J.M., "Regarding fraud", QUINTERO OLIVARES, G., (Dir.), *Comments to the new Penal Code,* Aranzadi, Pamplona, 1996, p. 1135.

By transferring, one must think on the change of "something" from one place to another. In the text which it refers to is the accounting procedure which implies charging debits, taking actives or requiring deposits with the annotation correlative to a different subject, giving this subject the right to a credit or the beneficiary of a concrete service or benefit: the purchasing of travelling tickets charge to a third party, fictitious deposits in banking accounts, payment of non due salaries, charges for material that have never been delivered, false payment orders, etc[131]. Finally, it must be taken into account that the most common situation will be the one in which the transfer will be done directly using the computer system that gets the fraudulent order, and therefore, the reference to a not allowed transfer can not be think of as the existence of a concrete action of will against the transfer by the victim, since this will not exist, but more like the payment order done with a third party patrimonial actives, without having the legal right to do so.

Therefore, it looks like the legislative arrangement is accurate enough, but when taking into account the very small numbers on the computer fraud crimes known in Spain —from the point of view of the cases taking to Court—, the question to be asking at this stage is if this is a fictitious problem or if there is a high black number of criminality in this field. Usually the answer to this question is the second one.

2. The reason for the high black numbers on criminality.

The numbers given by Courts are not even close to be and indicator of the real dimension of this problem. The massive incorporation of the new information technologies in the majority of society fields –and specially in the economic field-, is a fact, and the computer dependency of small and big businesses, financial institutions, public and private entities, is also a fact. Therefore, it is an easy conclusion to realize that in this field, the "dark area" of criminality is specially high.[132]. ¿Why is this?

The small number of cases reported and the little publicity given to them, is due to various reasons, as stated by professor GUTIERREZ FRÁNCÉS[133]:

- The lack of technological devices developed enough to detect abusive behaviour.
- The lack of confidence in the capacity of our Courts to give a satisfactory solution to the problem, in short term and using the tools that the current law offers.

---

[131] GONZÁLEZ RUS, J.J., *Spanish Penal Law Course. Special Part, op. cit.*, pp. 687-688.
[132] ROMEO CASABONA, C., *Computer power and juridical safeness,* Madrid, 1988, p. 37. The author states that curiously the cases known use to have public sector entities as victims, probable due to the fact. that their managers have less capacity to take decisions, since they are basically just administrators of the public or private actives, and they are under the principle of hierarchy subordination.
[133] GUTIERREZ FRANCÉS, M.L., *Computer fraud and swindler, op. cit.,* p. 601.

- The victim's fear of the consequences that come from the public knowledge of the facts, which will be like the recognition of the system's vulnerabilities (loss of prestige, massive withdrawal or clients and investors, direct or indirect economic detrimental, etc).

It is also very difficult to create any of statistical numbers in relation to this issues, since it is complicated to find out and sanction these conducts based on the economic power of those committing the crimes, although the economic damage is really humongous. It is also important to take into account the extended difference in public opinion about the damages that caused by these crimes, affect society in general. Even society itself does not consider the subjects who commit these of crimes as criminals, it does not segregate, despise or devaluate them, but on the contrary, the perpetrator of these crimes is considered as a "respectable" citizen"[134]. In conclusion, it is not truth that in Spain these of acts do not happen massively, but, in fact, what happens is that either the acts are not known, or if they are known, they are not publicly exposed. .

On the other hand, considering the globalization phenomena of nowadays, our legislative system can not avoid getting involve with the international community in which is integrated. The elevated level of these criminal behaviours can, therefore, being explained by taking into account the difficulty of its international eradication, since the users are spread all over the world, and consequently, there is a high probability that the perpetrator and the victim can be subjects to different jurisprudences or national regulations. Although throughout international cooperation agreements and bilateral extradition treaties there is an intent to give a solution to some of the difficulties caused by computer related crimes, their possibilities are very limited. Therefore, the transnational dimension on computer crimes, which is aided by the development of computer science and the transnacional flow of data, calls for an administrative, police and legislative coordination, with an importance that has already been reflected by the initiatives and propositions that came from the bases of international organizations.[135].

In like manner, the juridical problem of computer systems, must take the combined information technology into account (chips, A.I., nanotechnology, nets, etc...) in order to avoid the maladjustment of juridical regulations from the context where are applicable. On the other hand, it is easy to realize the potential of computer activities as a research tool, mostly due to the absence of evidential elements which could allow the detection of the illegal acts committed using computers.

Finally, we must highlight the role of the State, which is the main and irreplaceable regulator for the management and control of the information flow, throughout its computer nets[136]. To do so, it is important to remember that the main tool in the fight against computer fraud has an extra juridical character (the physical

---

[134] www.abogaciaenlinea.com.ar/delitos%20inform%E1ticos.htm
[135] GUTIERREZ FRANCÉS, M.L., *Computer fraud and swindler, op. cit.,* p. 602.
[136] www.abogaciaenlinea.com.ar/delitos%20inform%E1ticos.htm

and technological protection of the computer systems)[137]. In this field, as well as in all the rest of criminal classified acts, prevention is the best fight against crime. In this frame of mind, it is irreplaceable to have a legislation on the issue, as well as to be able to invest some money in order to assure the total invulnerability of the computer systems of many entities, specially those entities that keep and operate with money.

Regarding the prosecution of crimes already committed, or the ones in the commission stage, the Spanish Guardia Civil, is pioneer in the research and investigation of computer crimes, in an effort to try to prevent that such crimes can be completed. Our virtual Guardia Civil professionals, meet with colleges operating in similar departments at some of the best police departments in the world, such as *Scotland Yard*, the FBI, the PAF or what it was the old KGB, and many other *undercover* professionals from the Secret Services in important countries. One of the main duties, undertaken by the brand new cyberspace department on Guardia Civil, is the prosecution of white collar crimes and capital evasion, as well as crimes that seem to be "in" or with a special scandalous surroundings, such as children pornography, or crimes that create social awareness and worries, such as terrorism and traffic of drugs. We hope that this would be an important step in the fight against these crimes. At any rate, our obligation lies in trying our best on this fight, and that is the philosophy that lies on International Experts Meetings, such as this Grotius one, which I sincerely wish, that will keep coming in the future.

BIBLIOGRAPHY

GARCÍA PABLOS DE MOLINA, A., "Computer Science and Penal Law", *Sociojuridical implications of information technologies,* Citema, Madrid, 1994.

GARCÍA, N., en www.delitosinformaticos.com/estafas/delito.shtml.

GONZÁLEZ RUS, J.J., *Spanish Penal Law Course. Special part,* Marcial Pons, Madrid, 1996.

GUTIERREZ FRANCÉS, M.L., Computer fraud and swindler. *(Correcteness of the swindler crime classificcation in the Spanish Law in relation to computer fraud),* Justice Department, Madrid, 1991.

LEVENE, R., y CHIARAVALLOTI, A., "Computer Crimes", Published for the VIth Latin American Conference on 1998, held in Colonia, Uruguay.

STRANO, M., *Computer crime,* Apogeo, Milán, 2000.

[137] GUTIERREZ FRANCÉS, M.L., *Computer fraud and swindler, op. cit.,* p. 622.

MESA, R., *The new international society,* Center for Constitutional Studies, Madrid, 1992.

MESTRE DELGADO, E., "Crimes against patrimonial actives and socio-economic order", LAMARCA PÉREZ, C., (Coord.), *Penal Law Manual. Special Part,* Colex, Madrid, 2001.

MORALES PRATS, F., "Penal Internet intervention. Penal repression on children pornography: a detailed study", AA. VV., *Penal Law, Society and New Technologies,* Colex, Madrid, 2001.

ROMEO CASABONA, C., *Computer Power and Juridical Security,* Madrid, 1988.

VALLE MUÑIZ, J.M., "Regarding fraud", en QUINTERO OLIVARES, G., (Dir.), *Commentaries to the New Penal Code,* Aranzadi, Pamplona, 1996.

www.abogaciaenlinea.com.ar/delitos%20inform%E1ticos.htm.

www.cnet.bigpond.com.