PARTICIPANTS' PAPERS

EFFECTIVE COUNTERMEASURES AGAINST ECONOMIC CRIME AND COMPUTER CRIME

*Ramon Crespo Carrilho Machado**

I. ACTUAL SITUATION OF ECONOMIC CRIME

Brazil is no exception to the late-century economic crime sweeping the world. On the contrary, it bears a long list of financial scandals, strenuously prosecuted or still unresolved serious cases and a widespread sense of impunity. The existing set of laws and regulations are under a continuous, although slow, improvement process in an attempt to fill legal gaps, stay abreast of criminal innovations and fulfill international agreements.

At the same time, criminal business activities constantly change their means of action, quickly adapting to the legal and economic context. Surely, money laundering constitutes one of the most serious problems to study and control. Money to be legalized come from countless illicit sources; drugs and arms traffic, corruption, import/export schemes, financial system fraud, contraband and organized crime, the most significant of them.

Economic crime seems to present a typology of special importance and frequent occurrence in Brazil. It concerns large corporations fraud, particularly banks and financial institutions. In the beginning of most cases, banks emerge as financially troubled institutions and later, after investigation, turn out to include a substantial criminal component. That was the case of *Banco Economico*. Its financial problems became public in December 1994 and upon continuous demand for official monetary assistance, Central Bank intervention amounting to USD $3 billion began only in August 1995. Later in the same month, the National Monetary Council approved PROER, which is a treasury fund that guarantees account deposits and finances to troubled banks for restructuring. *Banco Economico's* "good part" was sold to other banks while "the rest" remained under Central Bank administration, demanding USD $2.9 billion from PROER; due November 1996 and never paid.

As to the fraud, the police inquiry process came across several illicit actions entrusted to Banco Economico's owners who cooperated with the financial insolvency. Among these actions were money transfers to foreign accounts, the transfer of assets to associated companies and to controlled off-shore companies, simulated real state operations, bad loans, etc., which significantly reduced its asset guarantees. A remarkable fact was that the Central Bank noticed these frauds only after the police inquiry.

A private bank called *Banco Nacional* has an even more astonishing story. The Central Bank intervention of it took place in November 1995, although there is evidence that inspectors knew about misdeeds since September 1987. The inquiry process conducted by the Federal Police resulted in 700,000 pages, distributed in 900 volumes. Forensic computer experts went through 6,000 magnetic tapes containing 30,000 software programs used by *Banco Nacional*. They

* Federal Criminal Expert, Federal Police Department, Ministry of Justice, Brazil

selected evidence from over 50,000 backup magnetic tapes and developed over 100 data filtering programs in 'Easytrieve', 'Cobol' and 'Clipper' computer languages. One IBM 9672 mainframe and several personal computers were used to manipulate this material.

Accounting and computer forensic examinations managed to prove that *Banco Nacional* utilized up to 1,046 of its accounts to grant phony credit amounting to USD$ 16.9 billion over a period of seven years. There was no real money involved in these operations, but on manipulating accounting computer programs, those credits incorporated positive results into the audited balance sheets and made it look financially sound. *Banco Nacional* demanded USD $4.98 billion from PROER, due November 1996 and still unpaid. Again, its "good part" was sold to another bank.

Brazil's land border with Paraguay has also provided an opportunity for large scale money laundering after the Central Bank imposed limitations on foreign resident bank accounts and financial operations in 1996. Some exempt status was granted to a few banks and exchange bureaus, to remain working under the old rules in consideration of border intense commercial transactions. This exception attracted an enormous amount of money laundering operations to the border. Some of *Banco Nacional's* accounts analyzed during the inquiry process raised clues to the border operations, and investigation began. The present status of investigation points to operations amounting to USD $10 billion, under scrutiny through 152 police inquiry processes, with 50 more being started nationwide to identify these money sources. The Central Bank revoked the special status for that area and enhanced inspections.

Another instance of illicit money transfer being explored is related to "Annex IV", a Central Bank Ordinance that permits foreign investment in Brazilian capital and stock markets through Foreign Investment Funds. Together with legitimate investment money, money previously sent abroad as a result of corruption, tax evasion, parallel accounting schemes, etc., has an excellent method of legally returning to the country and leaving again in the same way. Finance specialists estimate that 50% of Brazilian foreign reserve is funded in Annex IV investments.

The most recently noticed economic crime typology, being followed closely by the Central Bank and the Federal Police, is related to NGOs (Non Governmental Organizations) and "Foreign Entities Assistance Funds". They are moving large amounts of money into Brazil, justified as relief assistance by NGOs and as social investment by Foreign Entities.

One of the few statistical data studies available on economic crime was developed by a Federal Public Prosecutor as a doctoral thesis. It became a book titled "Criminal Control on Crimes Against the National Financial System" (Ela Viecko Volkmer de Castilho) published this year. It researched all Central Bank communications to the Public Prosecutors Office related to facts defined as 'economic crime' by a 1986 law, which is the main legal provision defining crimes against the national financial system. This law places financial institutions under Central Bank inspection, thus greatly centralizing in it all information. During the Central Bank's exercise of this attribute, identified irregularities are addressed via an administrative process. When illicit facts come up, the Central Bank must refer the case to Prosecutors Office, which can dismiss it or request the Federal Police institute a police inquiry process. Upon

completion, police inquiries end up in the Federal Justice courts for trial. The research period covered July 1986 (when the 1986 law was enacted) to July 1995 and considers a selection of 606 Central Bank communications, as shown in Table 1.

TABLE 1

NUMBER OF CENTRAL BANK COMMUNICATIONS

Year	No.	fr %
1987	0	0.00
1988	8	1.32
1989	14	2.31
1990	25	4.13
1991	87	14.35
1992	117	19.31
1993	131	21.62
1994	125	20.63
1995	99	16.33
Total	606	100.00

Table 2 shows the information gathered about the average time, in years, calculated from the time the alleged criminal facts occurred and the date they were communicated to the Prosecutors Office.

TABLE 2

ELAPSED TIME BETWEEN FACT AND COMMUNICATION

Time	No. of years	fr %
0 to less than 1	63	17.36
1 to less than 2	93	25.62
2 to less than 3	102	28.10
3 to less than 4	72	19.83
more than 4	33	9.09
Total	363	100.00

Average time = 2.2 years

Table 3 shows the elapsed time, in months, calculated from the date of the Central Bank communication to the Prosecutors Office, and the date that the police inquiry process was instituted.

TABLE 3

ELAPSED TIME BETWEEN COMMUNICATION AND PROCESS INSTITUTION

Time	No. of years	fr %
0 to less than 1	63	29.72
1 to less than 2	46	21.70
2 to less than 3	43	20.28
3 to less than 4	25	11.79
more than 4	35	16.51
Total	212	100.00

Average time = 2.1 months

Table 4 shows the elapsed time, in years, calculated from the date of the police inquiry process being instituted and its conclusion by the Federal Police.

TABLE 4

ELAPSED TIME BETWEEN PROCESS INSTITUTION AND CONCLUSION

Time	No. of years	fr %
0 to less than 1	2	3.33
1 to less than 2	14	23.33
2 to less than 3	26	43.34
3 to less than 4	14	23.33
more than 4	4	6.67
Total	60	100.00

Average time = 2.5 years

Table 5 shows elapsed time, in years, calculated from the date of the police inquiry process being instituted and indictment by the Prosecutors Office, which is the beginning of the judicial process.

TABLE 5

ELAPSED TIME BETWEEN PROCESS INSTITUTION AND INDICTMENT

Time	No. of years	fr %
0 to less than 1	38	26.21
1 to less than 2	48	33.10
2 to less than 3	37	25.52
3 to less than 4	22	15.17
Total	145	100.00

Average time = 1.8 years

Table 6 shows the elapsed time, in years, calculated from the date of indictment by the Prosecutors Office and the sentencing by a Federal Justice Court.

TABLE 6

ELAPSED TIME BETWEEN INDICTMENT AND SENTENCING

Time	No. of years	fr %
0 to less than 1	5	25.00
1 to less than 2	4	20.00
2 to less than 3	9	45.00
3 to less than 4	2	10.00
Total	20	100.00

Average time = 2,5 years

Table 7 shows the number of adjudicated cases. The distinction between a dismissed sentence and a merit sentence is as follows. The first one is issued after the conclusion of the police inquiry or Prosecutors Office apprasial, when there is no basis for referral to a Federal Justice Court. The latter, after the conclusion of instruction in Federal Court, is provoked by referral.

TABLE 7

NUMBER OF ADJUDICATED CASES

Item	No.	fr %
Dismissed sentence	62	80.52
Merit sentence	15	19.48
Total	77	100.00

Table 8 shows the nature of merit sentences.

TABLE 8

NATURE OF MERIT SENTENCES

Item	No.	fr %
Acquittal sentence	10	12.98
Conviction sentence	3	3.90
Mixed sentence	2	2.60
Total	15	100.00

Additionally, table 9 shows the Federal Police Department statistics about the total number of police inquiry processes initiated based on the two main laws regulating economic crime. They amount to 7,742 inquiry processes since 1986 (when the first law was approved) up to the present day. Only 2,893 of these cases are registered as being concluded.

TABLE 9

NATURE OF MERIT SENTENCES

	Law 7.492/86		Law 8.137/90	
Year	Started	Concluded	Started	Concluded
1986				
1987	6	1		
1988	11	1		
1989	46	7		
1990	78	36	2	2
1991	154	35	60	17
1992	201	100	59	35
1993	481	235	280	114
1994	401	255	434	209
1995	369	190	518	288
1996	821	470	550	252
1997	629	228	851	257
1998	1,107	81	684	80
Subtotal	4,304	1,639	3,438	1,254

The research study and table data eloquently demonstrate the application of the economic crime law. The small number of registered criminal offences bear no proportional significance when compared to the total criminality registered in official statistics; estimated as one million Penal Code offences per year in the country. It shows the necessity to investigate the current interpretation of the legal provisions and to study the Central Bank, Public Prosecutors Office, Federal Police and Federal Justice system's operation and procedures.

II. PROBLEMS IN INVESTIGATION AND PROSECUTION OF ECONOMIC CRIME AND THEIR COUNTERMEASURES

The economic crime research mentioned before showed the Central Bank's predominant role in identifying illicit procedures and reporting them to justice authorities. Legal power to inspect the financial system's operating procedures places the Central Bank under a judicial duty to communicate crimes to the Public Prosecutors Office. This communication is not a requirement to start the police inquiry process or criminal justice process, but it has conditioned other instances of action in practice.

The 1986 economic crime law predicts the assistance of the Central Bank in prosecuting cases in the criminal process. However, it is not rendering greater and better scrutiny of economic crime. As became evident in the bank crash cases cited in the previous section, Central Bank monitoring has not prevented trouble in financial institutions. Its inspecting structure is oriented to law-abiding auditing actions, instead of real financial situations and assets quality evaluations.

Among other institutions with inspecting duties and illicit communication obligations are the CVM (Securities Exchange Commission), the Internal Revenue Service (IRS) and some government banks. Compared to the number of Central Bank communications, CVM has communicated a total of 85 cases to the Public Prosecutors Office, based on the 1989 law defining responsibilities for damages caused to investors on the Exchange Market.

The Central Bank's functions and autonomy are expected to undergo significant changes as further regulations are being debated in Congress. Its autonomy, in relation to Executive power, is intended to avert political influence in all areas. The same autonomy is desired for CVM as well, including a greater role in assisting prosecution.

III. CRIME PREVENTION MEASURES TO CONTROL ECONOMIC CRIME

The first step to preventive action on economic crime is a sound, effective set of laws. It is a prevalent belief that the resolution and significant change of serious problems can only take place in a country as a consequence of political motivation. Observation of recent trends in Brazil leads to the conclusion that important changes are taking place.

Recent developments include the March 1998 Congress approval of Law 9.613/98, incriminating money laundering activities. This long-awaited law filled an important gap in Brazilian criminal legislation, while at the same time complying with several international agreements, (among them the 1991 Vienna Convention). It also created COAF (Council to Control Financial Activities) responsible for monitoring the activities of money laundering suspects in financial and commercial operations. COAF is empowered to apply administrative penalties and request needed information.

Along the same line, the constitution of SGT-4 (Money Laundering Subcommittee of the Mercosul Financial System Commission) is intended to develop strategies for the Mercosul countries. They are presently evaluating the Brazilian proposal for a minimum regulatory code.

Another important initiative was the creation of the National Anti-drug Bureau, upon the recognition that Brazil has become a corridor for drug export, and the biggest manufacturer of chemical products in Latin America. The estimated consumption of illegal drugs in the country is USD $7.5 billion. Brazil has also become more attractive for money laundering and capital recycling, due to economic stability.

A new anti-drug policy is to be developed based on prevention and rehabilitation, including better laws and regulations, particularly on the concept of preserving national sovereignty and individual rights. This new policy will also pursue investigating the financial flow of drugs and Brazil's incorporation into FATF (Financial Activities Task Force). The Brazilian Federal Police Department also has improved its structure, aiming to become a more effective and specialized force against economic crime. A specific commissioners division was created to this end, namely DICOIE (Organized Crime and Special Inquiries Division), under the direct guidance of the General Director. Finally, its crucial to optimize international cooperation, especially with Interpol.

IV. ACTUAL SITUATION OF COMPUTER CRIME

The term "computer crime" is being widely utilized and is well established and defined. However, due to the fast pace of technological innovation, a comprehensive approach must be adopted to efficiently combat this type of crime. Based on the the Brazilian Federal Police Department's experience relating to computer crime, a specialized Computer Crime Investigative Division was created as part of the National Forensic Institute. In developing a cognizance for, and extending this category of crime, it was first necessary to devise three kinds of offences, as follows:

A. Computer Aided Activities

These are activities usually developed without 'computer demand', but the use of computers come from the assistance they provide. It presents the possibility of evidence retrieval when police action comes across these types of devices. Some examples are:

- computer organizers used by drug traffickers to store telephone numbers

and addresses, and computers storing information about their business;
- parallel accounting control in computers.

B. Technology as an Instrument

In this category, the presence of computers in the process is required to perpetrate the offence. Without the computer, the fact of the crime would not occur. This category is not intended to indicate the appearance of new criminal facts, although this might be the case. It is mainly for activities using computers as a new tool to gain efficiency, lower costs and improve crime member security. An illustrative example is counterfeit money, which migrated from labor intensive and costly printing processes to the average cost of a graphics workstation. Likewise, this is also the case for economic crime.

C. Virtual Crime

Labeled this way are those crimes targeting computers and the reality (data) stored in them. The intention is to alter the digital representation of goods and values in order to obtain unmerited advantages. For this purpose, all it takes is privileged access to computers, commanding transactions through keyboards, which is far more convienent than handling pistols and machine guns to demand and withdraw money from a bank.

Offenders in these cases seem to be motivated by the small probability of physical injury, together with the support that a device which processes millions of operations per second can offer, to use these operations to benefit them directly.

Its known that in Brazil, several credit card companies have been victims of credit card fraud; but they will not disclose these frauds throush fear of negative publicity and breach of client confidence. One of these institutions suffered a USD $800,000 loss through illicit Internet credit card purchases between July 1997 and March 1998, which were not reported to police.

Counterfeit money produced through graphics workstation resources, and printed on laser and inkjet printers, has increased dramatically since the introduction of the 'Real' (Brazilian currency denomination) in 1994, with newly designed bills. The number of forged currency bills made through this method and seized by the Central Bank increased as shown in table 10.

TABLE 10

NUMBER OF SEIZED COUNTERFEIT MONEY BILLS

Year	Bills
1994	1.046
1995	9.168
1996	75.283
1997	137.489
1998	101.182
Total	324.168

The enormous incidence of this type of offence compelled the Federal Police Forensic Section to develop a computer database intended to classify each counterfeit bill according to its:
- value
- printing process: ink jet, laser, off-set, copying machine
- individualizing details: type of paper, serial number, defects
- origin: city where bill was apprehended
- date
- inquiry process number
- names involved

This database registers money forgery occurrences in Sao Paulo since February 1996, storing information from 1,387 police

inquiry processes and totaling 4,177 currency bills classified to date.

A report containing matching characteristics keyed by value, printing process, details and name is then issued and attached to the forensic analysis report which is sent to the origin for further police investigation. Another benefit of this report is the possibility of quickly identifying and effectively charging the criminals also responsible for counterfeit money with similar characteristics found in distant locations.

V. PROBLEMS IN COLLECTING EVIDENCE OF COMPUTER CRIME AND THEIR COUNTERMEASURES

Within evidence collection, a more pressing and crucial problem is posed by tracking and identifying offenders, particularly when considering cases originating in large networks such as the Internet. The actual stage of WWW computer interconnection allows anyone, from the most remote location, to access information in unsecured systems virtually unnoticed. Moreover, his/her system might be used to store, diffuse and/or promote such crimes as pornography, bomb manufacturing, introducing computer viruses, etc.

Although most reported cases relate to pornography involving children and teenagers, damage caused by hackers is frequent, but seldom effectively prosecuted, due to criminal classification uncertainty. Questions to address in examinations of this nature are:

i) First, the existence of legal provisions for the crime;
ii) Correct identification of the criminal acts authorship. Most of the time, computer activities registers (logs) are obtained, but the possibility of forged computer access using third parties accounts must be considered, as it is a common procedure in hackers attacks;
iii) What can be considered as evidence? For example, one Internet page containing illicit material is initially noticed (browser). Usually, there's a responsible person for each page on the web, and he/she is identified by inquiring through the server operator (it must be remembered that servers will not take responsibility for users published material). To better support prosecution, these pages are apprehended in the server's system. Couldn't the hackers be those who inserted the pages, considering the previous item's (2) rationale?
iv) One computer being "invaded" by a hacker theoretically situated in a different state poses the problem of distance, in actions of search and apprehension.

In a recent and very much publicized case in Brazil, a TV presenter of a cultural program which shows its e-mail address on screen for viewers interaction, received 105 harassing messages from a "rapist@macho.com". Police were successful in identifying the author, a married systems analyst, who disguised his signature using software called Unabomber. In addition, he had 430 more messages in his HD sent to a newspaper columnist. He was charged with harassment and convicted to a one-year alternative sentence.

To track him, as has happened in other cases, police relied on the network service provider's cooperation. Obviously, this cooperation can not always be expected, as some service providers are resistant to disclose client registers; posing the problem of devising other effective means of investigation and mandatory disclosure

regulations.

A relevant case of child pornography was investigated by Interpol in Brazil, based on information received from counterparts in other countries and child protection groups. Working with remote monitoring, electronic surveillance and search warrants, Interpol managed to identify and arrest the service operator, and one of its users, in another state as responsible for furnishing several images.

The creativity component found in the practice of these particular offences is a continuous challenge for forensic specialists' knowledge improvement. Some useful technical concepts for evidence collection are presented below, although it is important to mention that it is difficult to list a detailed set of proceedings and techniques suited for all forensic examinations.

A. Evidence Retrieval

The title expression has been used for some time by special computer crime units in international organizations; meaning a whole set of proceedings to be performed in the forensic examination of computer materials. An elemental sequence in this set of proceedings is as follows:

i) Ambience Analysis: gathering all information concerning work environments, hardware and software adopted, user activities, data flow, connections configuration (e.g. isolated workstation, network station, modem connections, etc.), amongst others, is fundamental in reducing the possibility of error in the next steps;
ii) Search: after taking cautionary measures to preserve all the material (unchanged), useful data is searched in the equipment support;
iii) Translation: considering that any and every computer content is, in fact, a digital representation of the comprehensive information of human beings, translation processes are used to both insert into and retrieve information from computers, thus making it possible to obtain original unaltered information. It may look simple but, considering the possibility of a faulty translation, methods and proceedings must be defined to guarantee sufficient clarity and accuracy;
iv) Presentation: issuing a final report.

B. Search of Information

Special methods and tools are employed to recover data, information, or remnants of them, located in permanent memory computer media, such as hard and floppy disks, magnetic tapes, CD-rom, optical disks, etc. The usual proceedings are:

i) Searches adopting a user point of view, oriented to understanding the work ambience of the equipment's user, comprehending directory tree verification, main software programs and installed systems;
i) Meticulous search of scattered data, such as text and images fragments, deleted files and printing spools.

The above mentioned cautionary measures in handling examining material anticipate the following actions, taken in order to preserve evidence integrity:

i) Technical measures: boot control, media mirroring etc;
ii) Physical Care: packaging, transportation, magnetic fields etc.

VI. LEGAL FRAMEWORK AND CRIME PREVENTION MEASURES TO CONTROL COMPUTER CRIME

The existing legal framework on computer crime in Brazil still lacks a specific and comprehensive law defining principles, legal use of information, and related offences and punishments. There is a draft bill in Congress, which has not been submitted to debate yet, whose proposals contain:

- Principles to regulate computer network services;
- Rules for the use of computer and network information;
- Definition of computer offences and respective punishments, ranging from six months to six years imprisonment and fine.

Some existing laws provide partial support to the prosecution of determined offences. The relevant portions of these laws are summarized below:

i) Law 5.988 - 1973: when information turns to be original material and is related to literary, artistic or scientific work, its author has rights defined in this law;
ii) Law 7.170 - 1983: considering a given set of data as secret and of Brazilian state interest, its diffusion (communication, delivery, consent to communication or delivery) to foreign governments or groups, or organizations or groups of illegal existence, constitutes a crime against national security, political and social order;
iii) Law 7.492 -1986: the plain unauthorized access to extraneous data kept by financial institutions is already typical conduct. Article 18 defines as a crime the breach of financial institutions operational secrecy or rendered services;
iv) Law 7.646 - 1987: software is defined as original intellectual property.

In some cases, certain laws are being used with a broader interpretation of their provisions; to penalize computer-related crime conduct lacking a specific legal basis. According to one approach, "If computer equipment is considered someone's else property, actions of erasing or altering its digital representations directly affects the condition of its regular functionality. In this way, the equipment can be properly considered as an aggregate of its physical parts (hardware), in association with essential instructions to achieve its intended functionality (software), thus any such damage could be charachterised as a crime."