Surveillance, control, crime, terrorism, fraud: paradigm and syntagma

...skeptics, liberals, individuals with a taste for private life and their own inner standards of behavior, are objects of fear and derision and targets of persecution for either side... in the great ideological wars of our time.

Isaiah Berlin

The environment of hyper commerce, continuous consumption and electronic money, new equipment, programs and behaviors appeared evidencing a substantial transformation of what people until them called the *right to privacy*.

In the winter of 1992, the French philosopher Gilles Deleuze published, at the *MIT Massachusetts*

Institute of Technology, a short essay on what he called *Postscript on the Societies of Control*. In it, Deleuze described the emergence of a new type of society, which he called “societies of control”. Revealing the phenomenon generated with an intensive and specialized use of vision and its gradual disarticulation with the new virtual media, his text was a major impact among intellectuals around the world: «Foucault located the *disciplinary societies* in the eighteenth and nineteenth centuries; they reach their height at the outset of the twentieth. They initiate the organization of vast spaces of enclosure». – *Enclosure* is a term that came to be generally translated in different languages as “closing of the map”. «The individual never ceases passing from one closed environment to another, each having its own laws: first the family; then the school (“you are no longer in your family”); then the barracks (“you are no longer at school”); then the factory; from time to time the hospital; possibly the prison... (...) Foucault has brilliantly analyzed the ideal project of these environments of enclosure, particularly visible within the factory:

to concentrate; to distribute in space; to order in time... (...) We are in a generalized crisis in relation to all the environments of enclosure – prison, hospital, factory, school, family (...) ...everyone knows that these institutions are finished, whatever the length of their expiration periods. It's only a matter of administering their last rites and of keeping people employed until the installation of the new forces knocking at the door. These are the *societies of control*, which are in the process of replacing disciplinary societies. "Control" is the name Burroughs proposes as a term for the new monster, one that Foucault recognizes as our immediate future».

Interestingly, what Deleuze calls *enclosure* is exactly the phenomenon of *systasis*, typical in vision. No less curious is the fact that both Deleuze and Foucault were not able to realize that the transition from a society of sovereignty – or hierarchy – to a low power society with generalized control, is precisely the interpretation of the transition from a visual society to something that existed before, to a world made of acoustic cultures.

If, on one hand, we launch ourselves to the past as to explain the future we do not understand yet, on the other hand the universe of virtual cultures hold some curious traces of resemblance with ancient oral cultures – even because they are two-way communication systems.

Any acoustical society is a society of control. But now, the global scale and diversity of sensory palette produced by virtual systems changed the entire reality, creating something different of the oral universe.

In the 1950s, the great American anthropologist Edward T. Hall called *environment* what would later be termed as *enclosure* by Deleuze.

Enclosure seems to be not appropriate either for acoustical societies or for virtual ones – because, in both cases, what we have is a continuum. *Enclosures* are established by *departments*, which are typical in mechanical and literary cultures.

The concept of *enclosure* is typically a product of a literary thought.

In May 2002, Brandon Mercer – journalist of the television program *TechLive*, in the United States, which was on air between 1998 and 2004, launched the article *Can Computers Read Your Mind*? There he presented an interview with the engineer Dave Schraer who developed to *NCR* a new kind of ATM machine that was able to detect people's mood. So, the machine could change its own appearance and offer products of different natures depending on the mood of the user in that moment. On the other hand, the detected mood fluctuation could be registered in data banks, in a way to elaborate a profile of that user as well as of ensembles of users.

Depending on the mood of the person,

special information would appear on the screen, *mediocrizating* even more the entire communication system, eliminating important aspects of privacy and establishing a new step in the development of video surveillance.

In 2008, the Japanese company *Omron* presented a photographic machine that beyond taking pictures was able to identify the gender and the approximate age of a person.

In his book *2020 Les Scénarios du Futur*, published in 2008, Joël de Rosnay traced a curious image of what already was a reality when the book was launched: «Imagine entering inside an environment that identifies you personally. The environment immediately adjusts temperature of the place, starts playing the music you like or download in your personal computer the software on which you had worked if you have been in that place». In fact, the environment started knowing everything about the person.

In Brazil, illegally, since the beginning of the 2000s, security systems of several buildings only allow people enter after leaving picture, copy of an identification document, signature and fingerprints in their database.

Each time a site of sales like *Amazon* is accessed, a *cookie* is automatically installed in the user's computer, and it starts scanning all his movements but without his authorization or knowledge.

Digital surveillance programs such as *Spector*, are sold in large quantities through the Internet. On Spector's site, for example, there is a description of its many benefits: «Imagine a surveillance camera pointed directly at your monitor, filming away everything that is done on your Macintosh (or PC). That is the idea behind the number one selling Internet Monitoring and Surveillance software, Spector. Spector works by taking a snapshot of whatever is on the computer screen and saves it away in a hidden location on your computer's hard drive. A few seconds later, Spector takes another picture. In fact, Spector can automatically take a picture of your computer screen as frequently as once per second. You get recordings of all chat conversations, instant messages, emails typed and read, all web sites visited, all programs / applications run, all keystrokes typed – EVERYTHING they do on the computer and on the Internet. You can come back to the computer a few minutes, a few hours, a few days or weeks later and SEE EXACTLY what they were doing, because Spector has recorded it. Spector is appropriate for parents concerned about what their children do online, or worried about protecting their children from the dangers of the Internet. Spector is also ideal for businesses concerned about how their employees use company computers. Are your employees goofing off too much online? Sending sexually or racially offensive e-mail jokes? Spreading company confidential information in anonymous chat and message boards? You'll find out with Spector. And, if you're concerned about what your spouse or mate is doing online at all hours of the evening, there is no faster or more accurate way to find out than with Spector».

On the same site, the company adds its commitment to governmental authorities: «It is our mission at Spy Chest Inc to provide government agencies with equipment in a timely manner. By streamlining the procurement process to meet individual agency needs and resources, equipment can be obtained as needed within one of several avenues purchasing. We understand the urgent need of our government clients, therefore we insure orders are processed accurately and timely. We look forward to providing you equipment with unsurpassed professionalism and accuracy».

In addition to the virtual surveillance systems, Spy Chest offers a large number of espionage equipment, which could be in a James Bond movie, for extremely low prices.

Another American company of espionage is the Spy Associates: “We are dedicated to providing you with the finest surveillance and detection equipment on the market today. SpyAssociates.com supplies surveillance equipment to individuals, corporations, schools, private investigators, agencies and religious organizations. Our in stock inventory includes: hidden cameras, nanny cams, wireless mini spy cameras, CCTV, surveillance systems and covert recording devices, listening devices, digital phone recorders, wireless microphones, hidden digital and analog voice recorders, bionic ears and audio jammers, passive and real-time GPS equipment for tracking your car and / or assets; detection devices, home drug, alcohol and infidelity test kits, radio frequency detectors, hidden camera detectors, wireless camera detectors, counter surveillance monitors, voice changers, cell phone voice changers, professional voice changers and voice transformers, telephone security, tap Nullifiers, bug detection, notification wire tap, spy gear, spy equipment, metal detectors, book safes and can safes', among others».

In January 2009, the Spy Tools Directory launched a press release which reported the qualities of a new product: «Looking for a smartphone spy software program to help you secretly retrieve copies of text messages from an unruly teenager, unfaithful spouse, or suspicious employee’s company issued cell phone? Online spy technology resource Spy Tools Directory is now featuring Mobile Spy, a program which secretly captures all cell phone activity from a smartphone targeted an upload it for the user view remotely via the Internet 24 hours a day».

In April 2008, the company Record Cell Phones announced a spy program, with a popular format, which “enables any cell phone user to record cell phone conversations for playback via voice mail or download and storage in MP3 format. The service, known as Call Recorder Cards, enables users to re-route all cell phone calls through a telecommunications switch where the conversations are digitally recorded. The recorded calls can then be managed online via a website interface, or accessed for playback through a voicemail-type system. The service is purchased in a pre-paid format, currently available in 250 and 500 minute increments».

That, not counting with the called *malicious software*, like *Trojan Horse* programs and *network worms*, for example.

In 2005, in a news release reported that “Israeli police have uncovered a massive industrial spy ring that allegedly used Trojan horse software to snoop into some of the country’s leading companies. The case will have major implications for the business community in Israel - and possibly beyond - as all the companies accused of having used the software are themselves leading companies. A report in Ha’aretz details how a wide range of businesses – including TV, mobile phone, car import, and utility companies – used a Trojan horse program, believed to have been written by two people living in the United Kingdom, to spy on their immediate business rivals with a high degree of success».

In April 2009 the website with the suggestive title *Go Hacking* taught all the steps to make a Trojan Horse using C language for computers. The author explained that «this Trojan works pretty quickly and is capable of eating up approximately 1 GB of hard disk space for every minute it is run. So, I'll call this the Trojan Space Eater. Since this Trojan is written using a high level programming language it is often undetected by antivirus».

Between April 6 to August 6, 2009, specifically related to the instructions about how to build a Trojan Horse, the site *Go Hacking* received dozens of messages from more than sixty people from different countries, clearly all teenagers, one of which took on the nickname *Hitler*. The author of the site, said to be someone called Srikanth, apparently was a brilliant young student of engineering in India.

The same site also offered: a virus program to disable USB ports, a Virus Program to Block Web Sites, a Virus Program to Restart the Computer at Every Startup, other Trojans and backdoors.

At that same epoch there was also the *Sniffer* – besides many other tools of the network espionage. *Sniffer* records the data traffic, capture parts and decode its contents. It is an instrument that has been often used by hackers to obtain copies of files during their transmission, to obtain passwords and even to capture conversations in real time.

If, on one hand, active spy, like the use of cameras or computer programs, achieved a tremendous expansion in the early twenty-first century, passive spy – which operates with data voluntarily supplied by the people – was no less exuberant.

Every time a credit card is used, large quantity of information about the user runs through computer networks. Each time we connect to digital networks the serial number of our computer and its location are automatically identified – and the same happens when we use our cellular phones and even fix phones.

In July 2009, Brazilian newspapers announced a new wave in the country: the use of mobile phones also as credit cards. Such was already very popular in Japan. When a person makes a payment over the cellular phone, he is not only immediately sending all his personal data, but also his geographical location.

Glenn Hastings and Richard Marcus – two false names – knew a great editorial success, especially in the United States, with the publication of the book *Identity Theft Inc*. The book tells the story, presumably true, of how the authors became millionaires through theft and criminal use of identities. Throughout its more than three hundred pages, the entire process of identity theft is carefully described, step by step.

«Even at the beginning of the 1990s, federal and state banks operated a highly efficient computer network that stored oceans of detailed banking data on virtually everyone in the United States who'd ever had in the account. The system worked much like the FBI's National Crime Information Center. By punching in your name, bankers would have instantaneous access to every tidbit of information concerning your banking history, in addition to personal details such as your Social Security number, date and place of birth, and last known addresses. They could pry into your tax behavioral history as easily as credit bureaus viewed your \ credit files. They would know if you'd ever written a bad check, if your account had ever been overdrawn, if you'd abused any bank services such as overdraft protection and, of course, if you had ever been linked to any type of bank fraud or questionable banking activities», and the authors added that «the Federal Trade Commission estimates that more than ten million Americans have their personal and credit information stolen or misused in one way or another each year», in

2006.

In the end of 1997, the Swiss police secretly tracked the location of mobile phone users through telecommunications companies that record billions of movements every year. They were able, through Swisscom, to identify the location of users with an accuracy of a few hundred feet.

With ITV or interactive TV, also known as digital TV, the first time television was transformed into a two-way medium. All movements of the audience are recorded in real time by the transmission network. Thus, it is known, device to device, preferences for programs, movies, newspapers, timetables, services like message boards, buying theater tickets or games with others, creating a user profile with data that can be crossed with others of different nature – even fiscal.

So, what was once “blind” transmission has become *port surveillance*.

The same happened with the regular telephones, which passed to automatically record all calls, regardless of the authorization of the user.

In November 2002, William Safire published a startling article in *The New York Times* under the title *You Are a Suspect*: «If the Homeland Security Act is not amended before passage, here is what will happen to you: every purchase you make with a credit card, every magazine subscription you buy and medical prescription you fill, every Web site you visit and e-mail you send or receive, every academic grade you receive, every bank deposit you make, every trip you book and every event you attend all these transactions and communications will go into what the Defense Department describes as "a virtual, centralized grand database." To this computerized dossier on your private life from commercial sources, add every piece of information that government has about you, passport application, driver's license and bridge toll records, judicial and divorce records, complaints from nosy neighbors to the FBI, your lifetime paper trail plus the latest hidden camera surveillance, and you have the supersnoop's dream: a "Total Information Awareness" about every U.S. citizen. This is not some far-out Orwellian scenario. It is what will happen to your personal freedom in the next few weeks if John Poindexter gets the unprecedented power he seeks».

TIA, or *Total Information Awareness*, was designed to be a system controlled by computers, operational condition that would become known as *COMPUTINT*, and not controlled by humans, or *HUMINT*. Thus, like what happens with cameras and systems for speed detection on the roads, all information collected on people would be superficial and non-subjective, pretending to respect the rights of privacy. But, in last instance, humans would operate final data, after several previous levels of digital analysis, which were extremely unreliable – in some sense like what happens with Internet translation engines. That is, digital analysis could produce strong distortions in the crossing of information later be manipulated by humans. Furthermore, the whole project would be heavily outsourced, with an operation centered on the hands of private companies.

Poindexter's project – who years before had been the leader of the disastrous Iran-Contra operation (Irangate), causing a scandal in Ronald Reagan administration – was called *TIA Total Information Awareness*, and finished to not be approved by the American Congress after a great wave of popular protests in 2004.

Although the American Congress have not authorized *TIA*, other similar operations, often specialized on specific environments and conditions, with identical aims and methods, would eventually be created not only in the United States, but virtually in the entire planet.

DARPA Defense Advanced Research Projects Agency – created in reaction to the launch of Sputnik in 1957 and responsible for the appearance of the Internet – has a project that is totally independent of the *TIA*, called *LifeLog,* and intended to put in a fantastic database all kinds of possible information on human beings – from audio visual data to biomedical information. It is a so powerful database that its aspiration would be the establishment of true human memory banks.

In 2003, an anti-terrorism institute named *CAT Eyes* was created in New Jersey, United States. According to Reg Whitaker, a sociologist at the University of Victoria in Canada, «the program's founder ambitiously envisions an eventual one hundred million informers, the ratio of watchers of about one to two, as compared with the East German Stasi of one to eight».

Like these, many other similar projects have sprung up all over the world, such as the *Bio-Surveillance* and *BioAlirt – Bio-event Advanced Leading Indicator Recognition Technology*.

One of these systems, still in the United States, was known as *CAPPS II*, or *Computer Assisted Passenger Prescreening System*. Established in 2003, as a kind of compensation for the impossibility of a radical and immediate implementation of *TIA*, *CAPPS II* replaced the previous system, *CAPPS*, with the following privileges, required by Congress: the government, not the airlines, will control and administer the system; every ticketed passenger will be screened, for instance not just those who check bags; every airline and every airport will be covered by the system.

In July 2004, after strong criticism, Tom Ridge, then Secretary of Homeland Security, declared the definitive abandonment of *CAPPS II*.

Another program, almost entirely unknown, supported by the Department of Justice of the United States, using the same principles like *TIA*, was called *MATRIX Multistate Anti-Terrorism Information eXchange* – same name of the famous movie showing a society subjected to a totalitarian government controlled by computers. *MATRIX* would be operated by private entities, centered on the company *Seisint Inc*. – founded by Hank Asher who, according to the Associated Press, was linked to cocaine trafficking in the 1980s. *MATRIX* was officially ended in 2005, but its principles, which were the same of *TIA*'s, continued proliferating in many other projects around the world.

It became common to find surveillance and control programs that start and end suddenly, causing confusion and opening doors for that capture personal data procedures become considered something common and perfectly acceptable for most of the people.

As David Lyon, «a massive and increasingly interwoven network of surveillance technologies is surrounding and defining contemporary societies».

And accidents happen. For general astonishment, the newspaper *Observer* announced in November 2007 that the British government had lost personal data of twenty-five million citizens, because of two compact discs lost or theft! In London, few days later, despite the scandal, the same English government reinforced its firm determination to impose to everyone who wishes to travel abroad the obligation to give to authorities fifty-three different kinds of information to obtain the travel authorization! Justification, as always, was the defense against terrorist attacks.

In July 2008, according to the newspaper *El Mundo*, seven hundred and forty seven computers were stolen from the British Defense Ministry, containing top-secret information. Days before, the United Kingdom Secret Services had announced to have lost important digital information about *Al Qaeda* and the second Iraq war.

In August 2008, a new lost shocked the British public opinion: the government had lost personal data related to almost one hundred fifty thousand criminals. The information was stored in a *pen drive* that simply disappeared, sold or stolen.

To make everything worse, few days later a computer sold in the site *eBay* for symbolic price contained bank information of one million British citizens, including addresses, phone numbers and even signatures among other data.

Between the summer of 2005 and the summer of 2008, British government officially announced to have lost or to have been stolen forty-three portable computers and ninety-four cellular phones, with all information they had.

Between 1998 and 2008, authorities in Britain, specially the Ministry of Defense, announced that six hundred portable computers had been stolen from their installations.

Database managed by governments became true scenarios for a *Kafkian* novel.

Another British control and surveillance project called *ECCO*, which was tested in Edinburgh in the end of 2007, provoked a strong reaction among the local population. The system will put online, in free access to any social assistant, updated confidential information about people who had had problems with alcoholism, domestic violence or mental disturbances, permitting a permanent monitoring and flash interventions, even against the personal wishes – everything in name of the social comfort.

One of my dearest masters on architecture, beyond an unforgettable friend, Eduardo Kneese de Mello, who lived between 1906 and 1995, was not only responsible for a good number of excellent projects, but also the chief architect in the construction of the city of Brasilia, together with Oscar Niemeyer, Lúcio Costa, Burle Marx and Juscelino Kubitschek; he also was the first president of the *Brazilian Institute of Architects* and great friend of Alvar Aalto, Kenzo Tange, Marcel Breuer and Walter Gropius, and relatively close to Frank

Lloyd Wright and Le Corbusier among others.

Eduardo Kneese de Mello told me about his strange feelings when he visited the United States in 1965. After some years not traveling abroad, he was invited to receive the honorary member medal of the *American Institute of Architects*, in Washington DC. «Before there were practically no commercial aerial lines. There were relatively few routes. We always traveled by ship. Going to Europe from Brazil, the travel took weeks to cross the Atlantic Ocean. When we entered in the ship, people aboard already knew who was who. When we arrived at the destination, everybody knew each other very well. At the exit of the ships the presentation of passports was never requested. The document traveled with us just in case of an accident, of an emergency, only this. When the ship landed, local authorities knew well the commandant and trusted him. On the other hand, he knew us. So, it never appeared any problem. But when I arrived at the United States in 1965, flying from Brazil, the first think the authorities asked me was for the passport! I felt myself like a criminal. Why should I identify myself? I had not committed any crime!».

In the United States, passport was only established in 1914 and its use became regular only after the First World War, like what happened in European countries. Even so, the exhaustive control of its presentation at the entrance or exit of countries, especially the United States, only became a regular procedure after the 1950s.

John Torpey, a sociologist at the University of California, details the creation and development of the use of passports along the centuries in his book *The Invention of the Passport – Surveillance, Citizenship and the State*, published in 2000.

In a world where, in a more or less general way, the scale made personal knowledge impossible, official obsession has become security and control.

Until the beginning of the electronic era, practically anyone could immigrate with relative easiness. When, already at the end of the 20th century, immigration waves became overwhelming huge bureaucratic barriers appeared, making illegal good part of the migratory flux! A thing that would be unimaginable few years decades – the prohibition of the right to freedom of movement!

In fact, there already was some control of movement during the first half of the 20th century – what brought to death thousands of people in war periods.

But, after a few decades, the mechanisms of electronic control became so intense that a case like that of the famous Portuguese diplomat Aristides de Sousa Mendes – who, making use of the emission of passports, saved thousands of Jews in the Second World War, even if such heroic act had condemned his future and the future of his family – practically would no longer be possible.

Control and surveillance were quickly extended to products and services.

In the 1990s, the commercialization of a huge quantity of wine, cheese and non-industrial regional food production was prohibited by the European Union, because it was difficult to keep them under control. Some critics accused this devastating strategy – made in name of public health – to have been a way to reinforce tax collection, because home made regional products are far from the government's eager. This, they were simply forbidden.

Some special products with a tradition of thousands of years, like cheeses, cakes, breads or wines, simply vanished.

In practically all countries law passed to determine the obligatoriness of previous presentation of the fiscal identification number – in the United States, the social security number – for a commercial transaction, of any kind, be allowed to exist. The information was registered and automatically sent to the authorities, establishing a total control.

In September 2008, some critics considered the overwhelming financial crisis, announced as the beginning of a new and devastating international depression, as a violent mass manipulation in a planetary scale with the aim to create a better environment for one of the candidates fighting for the American presidency. With chaos spread out all over the world, an older and more conservative figure would have more chances to win. The tremendous world crisis happened exactly seven years after the terrible attacks of September 11.

But, Barack Obama – the younger and less conservative candidate – won the elections, making intensive use in his campaign of the effects of the crisis.

However, there was another scenario. Gradually after the nomination of George W. Bush in 2001 for the American presidency, and quickly after September 11, power changed in diverse countries, establishing a more conservative structure aiming to reach standards of control and surveillance never saw before. It was thought that if the 2008 elections would change the groups in power, those heavy – and many times illegal – systems of control and surveillance would tend to gradually disintegrate. But, it was not what happened.

In very few days, in the middle of confusion and financial panic of September 2008, several governs, in diverse countries, illegally intervened in the markets, creating instruments of control and surveillance that were established for long term, not only for that specific moment. The American government changed its orientation, but the control and surveillance tools became even more rigorous and comprehensive.

Thus, the 2008 world financial crisis would have served, in fact, to reinforce and turn definitive those instruments, eliminating old democratic procedures, erasing citizen's rights and establishing a reality closer to heavy controlled markets, like what happens in dictatorships – but oriented to intense credit and continuous consumption.

In September 26, 2009, newspapers around the world announced that the countries of the so-called G-20 had decided to create even more rigid control mechanisms, intervening even in private companies, in executive salaries, reminding old Marxist ideals of social intervention in the production means. Germany and France even urged for the establishment of limits for salaries of managers in large private groups. The British Prime Minister, Gordon Brown, stated that those measures of control would save "millions of jobs" – even if few months later, in early 2010, Europe and the United States reached record levels of unemployment.

In the middle of the 2008 financial hurricane, Durval de Noronha Goyos, a celebrated Brazilian lawyer, arbitrate of the *World Commerce Organisation* manifested his profound indignation: «The massive injection of capital in private companies, loans with symbolic interests, the expansion of monetary basis, all this made without approval of parliaments, without popular referendum, with no approval or even previous knowledge by multilateral institutions like the *World Trade Organization*, the *World Bank* or the *International Monetary Fund* are not only illegal but happen with total disrespect to those multilateral entities, heavily affecting their credibility».

A possible result of those acts would be the gradual disappearance of such institutions, diving the planet into a hyper controlled asymmetric market, benefiting even more small groups of interests and launching large decentralized networks of control, acting locally through huge sets of volatile laws, and eliminating popular participation in collective decisions.

Such violent cup in the last months of 2008 would implant in few days, in practically the entire planet, a heavy structure of laws and regulations – permitting the intensification of even more control and surveillance – that could survive for decades, practically immune to the oscillations of political power provided by a democratic system!

Probably, the nationalization of the bank system – that characterized the measures assumed by the States in September and October 2008, was a practical step as to complete annihilate any bank secrecy and establish another toll for total control on citizen's private life.

However, forces of control and surveillance divorced from public benefit are not new. In 1913, Charles Lindbergh – a Republican Congressman – was a firm opponent to the establishment of the *Federal Reserve Act*: «This Act establishes the most gigantic trust on earth.... When the President signs this Act, the invisible government by the money power, proven to exist by the *Money Trust Investigation*, will be legalized.... The new law will create inflation whenever the trust wants inflation.... From now on, depression will be scientifically created».

Even with the clear and frontal opposition of Charles Lindbergh – father of the famous aviator – President Woodrow Wilson approved the *Federal Reserve Act* in that year of 1913. Some years later, Woodrow Wilson would lament: «I am a most unhappy man. I have unwittingly ruined my country. A great industrial nation is controlled by its system of credit. Our system of credit is concentrated. The growth of the nation, therefore, and all our activities are in the hands of a few men. We have come to be one of the worst ruled, one of the most completely controlled and dominated governments in the civilized world – no longer a government by free opinion, no longer a government by conviction and the vote of the majority, but a government by the opinion and duress of a small group of dominant men».

On July 27, 1979, John Lewis was injured by a vehicle owned and operated by the Los Angeles branch of the *Federal Reserve Bank* of San Francisco, California. Three years later, the Ninth Circuit Court of the United States, established that «Examining the organization and function of the *Federal Reserve Banks*, and applying the relevant factors, we conclude that the *Reserve Banks* are not federal instrumentalities for purposes of the *Federal Tort Claims Act*, but are independent, privately-owned and locally controlled corporations».

In June 17, 2009, president Barack Obama announced the launching of a «new system of financial regulation that increases Federal Reserve's powers and created an agency for the defense of financial products consumer».

But, total surveillance and control are no longer an exclusive prerogative of the State and of the companies. One of the problems with which Law, in diverse countries, has dealt with difficulties – because of its increasing and large scale – are *non-wished pictures*, many times made with the use of cellular phones even in balnearies or bathrooms and later sold in the virtual world's black market.

Other times, *hackers* steal images from personal communication, which are later transferred to several people inside network – many times pornographic or erotic images – and start a process of blackmail.

Even the *personal image*, which along centuries counted with the rigor of shame and honor, passed to value almost nothing when inserted in the context of low cost universe, even when they are intimate images of sexual relations.

According to a report made in 2008, the *Suisse Romande* television showed that pornographic and erotic images stored in the memory of teenager's mobile phones, many times images of other teenagers colleagues, were considered by them as true trophies, strong signals of power. And those images existed in great quantity, non-rarely counting with the agreement of the other part.

Such scenario of a low power society or, a society of generalized power in low concentration, indicates a population oriented to entertainment and consumption.

The formation of groups of criminals and terrorists stopped to happen in a concentrated way, as it was common until the 19th century and good part of the 20th century, but started dynamically participating in all social spheres – even inside governments and police institutions.

Hollywood's movies give us always very good examples about how it happens.

In the same way, people pertaining to that new social dominium of criminals, where many times there is great poverty, non-rarely make use of the most advanced technology – and have access to the most advanced of what before was called *erudite culture*.

This complex phenomenon characterizes, yet, much of criminals' networks all over the world.

In 2006, the Brazilian filmmaker and writer Arnaldo Jabor launched, as true, a fictitious interview with Marcola, a dangerous criminal, leader of the most powerful syndicate of crime in the city of São Paulo. The fake interview was characterized by great intellectual refinement, showing in the fictitious figure of the real criminal a person with profound knowledge on philosophy, economy and sociology. The revelations announced by the interview were chocking, creating a national scandal. The objective defended by the criminal was to destroy medium class society and establish a dictatorship leaded by cruel murders. Even if the criminal proudly said that he had read more than three thousand books, nobody imagined it could be a fiction.

In a certain sense, the Brazilian filmmaker reedited, through the *old* medium newspaper, Orson Welles' great radio success with *The War of the Worlds* by H. G. Wells, which originally was destined to a *new* medium of communication.

People believed on what the text said because it revealed a real fact, which was absolutely clear to everyone: the medium class was being destroyed.

The most interesting fact is that, along several months, nobody put in cause the authorship of the interview. Practically nobody even cogitated that it would be impossible for someone like that prisoner, born in a miserable family, criminal since childhood, having lived practically abandoned in his whole adolescence, living in the streets when he was not in prisons or *houses of correction*, to suddenly reveal himself as an intellectual of such importance. But! Everyone considered that phenomenon a very natural thing! However, that would not be natural a few dozen of years before.

People were right because, however new, such a possibility was also true. It is a real fact and a new data in civilization terms.

In the United States, the *Unabomber* – presumably Theodore Kaczynski – the most wanted American criminal in the 1990s, a terrorist fighting against technology and against investigation labs in universities, launched a manifest, initially through letters sent after 1995 to *The New York Times* and soon also published by the *Washington Post* with the title *The Future of the Industrial Society*. Against the political left and against new technology, the terrorist revealed a surprisingly intellectual refinement.

Like the fictitious interview created by Arnaldo Jabor, other classic of literature seems to be in evidence in the *Unabomber*: *1984* by George Orwell.

In the book *1984*, the personage Emmanuel Goldstein launched an enigmatic manifest where he affirmed that «nobody has ever seen Big Brother. His function is to act as a focusing point for love, fear, and reverence; emotions which are more easily felt towards an individual than towards an organization».

On the other hand, *Unabomber'*s manifest, after have argued that there are three kinds of human drives – a first one that requires a minimum effort; a second that requires a great effort; and a third that is simply unreachable – defended that «social needs, such as sex, love and status, often remain in group two in modern society, depending on the situation of the individual. But, except for people who have a particularly strong drive for status, the effort required to fulfill the social drives is insufficient to satisfy adequately the need for the power process. So certain artificial needs have been created that fall into group two, hence serve the need for the power process».

Literature as *content* of a new medium.

The old condition of high concentration and high power, that leaded to the ideal of welfare in the defense of a relative social stability, and that designed a clear separation between honest and criminal people, simply tends to disappear with a low power society. The old barriers between classes, education or technological development finished to exist.

In many countries, police passed to have less sophisticated weapons than those used by groups of criminals and, in certain cases, even less powerful than the weapons used or hidden by population in general. It was estimated to exist about one weapon per habitant in the United States, in the beginning of the 21st century!

Even in the most developed countries, many times, murders and drug traffic networks are organized from inside prisons where they are detained. In some countries like Brazil, gangs of criminals even transmit illegal videoconferences in real time, connecting different prisons using computers and cellular phones.

In the early 2000s, drug traffickers transformed the Frederick Douglas Towers – a social housing in Buffalo, United States – into a center for illegal drugs commerce. Then, the monitoring system of that institution, composed of a large number of surveillance cameras, has been used to control the movements of police.

Data from the *World Health Organization* shows that, only in the United States, more than thirty-one thousand groups of identified criminal organizations were in frank operation in the year of 1996. A number that would surely impress someone like Al Capone. In that same year there were an identical number of groups producing clothes in the United States with around eight hundred thousand employees.

Organized groups of criminals compared to industrial complexes.

In 2008 the German company *BASF* was a cyber-extortion victim. Attacked by a devastating virus, they were obliged to pay an amount for a “release”, that is, for the tele-liberation of their digital systems and the elimination of the virus.

New types of *cybercriminality* appear, like the *clickjacking* –when a pirate is able to activate at distance the camera and microphone that are part of the majority of computers all over the world.

From time to time, young cybercriminals are arrested and have their sentences annulled in change for works to police, in the search of other hackers or in the spying on common citizens.

In 2004 it was announced that identity theft would have exceeded drug trafficking as the main criminal problem in the United States.

Between April 1998 and April 2003, as reported by the Federal Trade Commission of the United States, more than twenty-seven million cases of identity theft happened in the country, and of them around ten million had happened just in the last twelve months between 2002 and 2003. It was estimated that such number would exceeded the seventy-five million in a near future. The same report showed that half of the victims simply did not even realize they had been stolen.

Henry N. Pontell and Simon A. Cole – Professors of Criminology at the University of California – explained, in 2005, the ease with which it was an identity theft in the United States, a process that is very similar if not identical to other countries: «With just a name and Social Security number, the "specialist" can order a copy of a victim's credit report and obtain information on open credit lines. Credit card personal identification numbers can then be accessed, changed addresses to reroute fraudulent billings to addresses, and multiple users added to an existing account. The mother's maiden name can be obtained through contact with vital-records bureau. The final financial transactions usually occur through runners, who purchase expensive electronics that are then sold to another retailer willing them for about half the real value. Runners are paid about ten percent of the profit earned by ringleaders. The other players in the ring - eg, fake identification and addresses makers who allow delivery of items to their home - are paid in similar fashion. In addition to item purchases, runners can also be assigned to make large ATM and credit card cash advance transactions».

Governments, like that of China, are accused to use prisons with the objective to falsify products that would be disguised exported all over the world.

The governments in China and Russia are among those which have more intensely used hackers with the objective to attack other countries, elevating crime to the dimension of State – as it has also been common in accusations against the United States, United Kingdom, Canada, Australia among others by their use of Echelon.

In 2009, a hacker apparently hired by the French government stole from a Swiss bank in Geneva banking information on thousands of people – data that would later be used by the government of Paris to pursue French citizens. The theft led to the Swiss government to announce the suspension of the convention of double taxation with France. This agreement would allow the exchange of information in case of tax evasion. Once established the evidence of tax fraud, the government would provide the information, as the Swiss constitution requires. But the convention no longer makes sense in the context of theft by the other State.

To Nicolas Arpegian, it is about the explosion of a third World War, this time virtual, spread out through all sectors of society: the cyberwar.

In May 16, 2008, *Financial Times* announced that around seven hundred and fifty thousand computers pertaining to German companies would be contaminated by spy software.

In September 3, 2007, the Pentagon officially recognized that part of its digital network had been disconnected along some days, because it had been victim of a cyber-attack.

In October 2008 Kelly Humphries, NASA's spokesman, announced that the International Space Station had been attacked by a digital virus called W32.Gammina.AG, which was placed in the astronauts' portable computers. The virus' objectives, as announced, were only to capture information about video games.

Even so, that time had not been the first one of a digital virus invading the orbital station.

Three months before Humphries' announcement, the OSCE Organization for Security and Cooperation in Europe launched the Astana Declaration: «OSCE Parliamentary Assembly exhorts the governments to condemn under a moral plan the cyber-attacks, as it deals with human beings or pirate actions against copyrights, and to establish universal procedure rules for the cyberspace».

Beyond the establishment of universal rules on a medium that is open by its own nature, the question is also to know how it would be possible to establish a Law that escapes from the principle of land property, legacy from the Roman universe, an immaterial, transnational and transcultural Law.

Like the digital virus, surveillance systems known as Closed Circuit Television, or CCTV, equipped with facial recognition programs passed to be spread out around the world and would not be unknown by planetary criminal networks.

Only in Great-Britain it was estimated in 2002 to exist around four million and two hundred thousand CCTV systems in activity – what represented one camera to each fourteen people. They represented around 25% of the surveillance cameras installed all over the world.

In 2004, it was estimated that a person in a single regular working day, in England, would have his image captured more than three hundred times by surveillance cameras.

In 2003, it was reported that more than 75% of the new schools in the United States were already equipped with CCTV surveillance systems.

In 2009, the Government Computer News, in Great-Britain, announced that part of the surveillance video cameras would no longer be controlled by people, but yes by digital systems. The tendency was to have computers controlling all surveillance systems.

Curiously, the first CCTV was installed by the nazi regime in 1942, by *Siemens AG*, to follow the launching of V2 rockets.

Not less curious is the fact that the British police solved less than 3% of the crimes with the aid of surveillance cameras, accordingly to a report dated of 2008.

In New York City, since 1997, the Central Park, subway stations and other public places passed to be controlled by hidden cameras twenty four hours a day. One year later, in 1998, there already were more than three thousand surveillance cameras working in the city.

Great part of the surveillance video systems passed to count with the technology known as VCA – Video Content Analysis.

Sometimes, though rarely, a reaction against the movement for super surveillance and control appeared. In the end of August 2009, an article published by France Presse reported that the Swiss government had ordered the immediate suspension of the Google service called Street View – through which a person, anywhere in the world, can virtually walk in the streets of virtually any city. According to the Swiss government, that service was not meeting the legal requirements to protect people's privacy.

Most impressive, however, it was to note that some reactions of people in Europe – through comments in newspapers – was to classify of the attitude of Swiss government as hypocritical and reactionary!

Those people did not have in mind the principles of freedom that designed the Western world for centuries forging the aspiration to what Karl Popper called the *open society*. Neither were they aware that the Swiss government strictly follows the determinations set forth by the people and not the opposite, like what happens in all other countries.

Surveillance, as a generalized phenomenon, counts yet with systems like the *Total Information Awareness*, or simply *TIA*, which is design to detect behavior – many times considered absolutely normal and perfectly acceptable by great part of people.

So, the Australian government announced, in 2009, the definitive installation of the *Smartgate* system in the airports and other transportation stations of the country. It is a system that automatically identifies the traveler through sophisticated facial recognition processes among other process of identification.

In the airport of Schiphol, in Amsterdam, the Netherlands, it has been installed the identity recognition system known as *Privium*. Through it, captured data are automatically shared with the American government in an extension that is kept under the usual State secrecy.

In its page on “privacy policy”, the Schiphol airport promises to not use the information about the visitants of the site, but makes no reference about the information about the adherents to the *Privium* system! It also informs that is automatically installing a spy cookie in each computer that opens its site.

Even more impressive is the fact of the airport “sells” that service in the form of a club for special members. Who become member of the *Privium Clublounge* at the Schiphol airport will have right to faster admittance to the gates through iris image scanning, priority in the use of car parking, exclusive discounts for use of car valets, business class check-in, special assistance at the airport and several other discounts. They are benefits that aim, as it is obvious, to establish a new standard of surveillance and control on passengers.

There were no protest or relevant public manifestation against those actions by the Dutch government.

Despite the draconian measures announced by the airport of Schiphol, it was there that a Nigerian terrorist embarked in a flight, in December 26, 2009, to the United States. The deflagration of exhausting control and surveillance on all citizens is the cabal proof of complete bankruptcy of the secret services systems all over the world.

Because of this, in January 2010, Gilles de Kerchove, coordinator of the anti-terrorism policy of the European Union, declared that the European Commission was already convinced of the validity of body scanners use in airports – equipment that allows to electronically "undress" people. After its use, everybody will be obliged to go electronically naked before boarding – a procedure that resembles security measures in prisons.

A little as part of the almost collective hysteria that conquered great part of the world immediately after the September 11 2001 attacks, Larry Ellison, president of Oracle, offered to the government of the United States a free software for the creation of identity smart cards to the American population.

In Peru, the government established

the obligatory use of identity cards with facial recognition chip for all inhabitants.

In the United States, along the last years, it has been debated the inclusion of DNA data in chips of the future identity cards and even the implant of identity chips in people’s bodies.

In April 19, 2009, Solomon Moore wrote in the *New York Times* that «law enforcement officials are vastly expanding their collection of DNA to include millions more people who have been arrested or detained but not yet convicted. (…) But criminal justice experts cite the Fourth Amendment privacy concerns and worry that the nation is becoming a genetic surveillance society».

Smart cards passed to be imposed as identity cards by the governments of several places like Malaysia, Thailand or Hong-Kong.

Companies like the *L-1 Identity Solutions* passed to offer all kinds of surveillance and control technology, for governments, private entities or even individuals.

As the sociologist David Lyon says, «surveillance records, once kept in fixed filing cabinets and dealing in data focused on persons in specific places, are now fluid, flowing and global. (...) The delocalised border is a prime example of globalized border».

In 2006, David Stork, scientist at the *Ricoh* in California, said: «Soon, when taking a picture with our mobile phones, it will be able to discover who is the person, based on its location and contact list».

That is: facial recognition left, since a long time, to be an essentially human question.

That competence of human recognition, including the detection of all kinds of preferences, crossing information with bank account balances, consumption habits, preferred books, preferred restaurants and dishes, perfumes, behavior habits like night activities and average of sleep hours, territorial dislocations, musical preferences, conversation habits, if the person is more or less shy depending on the diversity of telephone contacts and social networks, political tendencies, consumption evidences and much more – everything will possibly be immediately crossed and associated by digital systems in real time.

All that information could be used both for commercial ends as by governmental authorities. In fact, in larger or smaller scale, this already happens.

Everything that has been imagined as *solution* for such complex situation is based on a logical approach of *concentration*, which tends to disappear.

For John Gilmore, co-founder of the Electronic Frontier Foundation, computers are literally extensions of our minds and, therefore, their contents should be kept private like our deepest thoughts.

The question is to know what the concept of *mind* is – if it continues being a closed compartment as the thinkers of the nineteenth century wanted, or if the mind can be in different places and if what we identify as individual consciousness is nothing more than a moment, like a kind of macro synapse in a complex framework of relationships.

Old notions of personal life, of profession or even of historical fate depend on the principle of concentration. But, the new kind of organization – and, among them, the criminal ones – expand through *nano-associations*, volatile groups, non-intentional collaborative strategies, unpredictable and unstable connections made by chance.

In the same way, among large economic groups, big companies subcontract all kinds of suppliers, forming a strongly distributive chain.

The appearance of the appeal to *downsizing* in the 1990s transformed the structure of thousands of companies all over the world, distributing functions and eliminating social benefits – *deconcentrating* and distributing risk. But *downsizing* also increases *rotation* of precarious labor force, eliminating much of the old concept of *profession*.

Social exclusion is no longer about a *total idea*, a *paradigm*, but yes about a *syntagma* – a phenomenon of complex nature indicating non-linear distribution to all sides and diverse dimensions.

In his famous work *The Structure of Scientific Revolutions*, of 1962, Thomas Kuhn established the principle according to which civilization metamorphosis happened in *paradigmatic leaps*, kinds of phase shifts, like what *Gestalt* showed many years before, in the beginning of the 20th century.

Like the laws of *Gestalt*, *paradigmatic revolutions* have a very strong visual nature, working very well in the industrial reality of literary society.

Not by chance Thomas Kuhn recalled from linguistics the expression he used to designate the revolutionary leaps of knowledge transformation. Ferdinand de Saussure started using in the 19th century the world *paradigm* to indicate a homogenous set of meaning.

The word *paradigm* appeared from the contraction of two Greek words, *para* and *deiknynai*, which respectively meant *side by side* and *to show*, indicating the idea of *model*, of *example*.

A glass, for example, is a *paradigm*. A car is a *sintagma* – because it is formed by diverse *paradigms*, like pneumatics, engine, doors, seats and so on.

Paradigmatic, visual, literary and strongly designed by the emergence of medium class, the industrial world was transformed into a world of services, which is trans-sensorial, transdisciplinar and *sintagmatic*, where metamorphosis happens in the most varied levels, in a turbulent and unstable way.

A universe where the image itself has become ephemeral and volatile. In the beginning of the twenty-first century, for the first time, it became impossible to identify a photographic falsification. David Brin said in his *The Transparent Society* that «one of our scariest predictions now circulating is that we are about to leave the era of photographic proof».

As an elegant paradox, the planet is take by unprecedented memory systems, with a countless number of images – but one will never be able to know which are true, because what we call *truth* essentially is a literary question.

Often, people seem to have difficulty

in understanding the extent of the serious implications arising from the absence of privacy, naively believing in increased safety. It is enough, however, to imagine what would have been if a regime like the nazi had the general control of information, to tremble facing to a devastating scenario.