FREEDOM LAW AND DIGITAL SELF REGULATION

"Society is an abstraction, people are real" Karl Popper

Bruce Schneier in "Secrets and Lies" has made clear that security is a complex solution, in which technical and organisational measures and law have to be properly co-ordinated.
I would like to remember the conclusion of his book: "***There are no technical solutions for social problems. Laws are vital for security***".
The further question is: can we all be free in a secured digital environment, or are we condemned to live like in an anti-atomic shelter ?
Security vs. Freedom. Is this true ?
I would like to explain why and how freedom in the Internet is possible: only in observance of proper regulations. Freedom and regulations: they need each other, according to the perspective of a liberal society. Let's see how this can work in cyberspace.
In discussing the dynamic of freedom in the cyber-world, we have to rely on the following helpful categories:

a) the dualism between the world of atoms and the world of bits (also called "Cyberworld"), proposed by Nicolas Negroponte.
b) the regulatory nature of software code and other IT products, as outlined by Lawrence Lessig

Point a) above stresses that Information Technology follows its own rules, largely influenced by the binary logic, and the architectural choices of the system's engineers. The structural problem outlined by Lawrence Lessig, is the conflict between the fundamental rules (constitution + law) of liberal open (democratic) societies (fundamentally avoiding self-enforcement) and the fundamental rules of cyberspace as defined by hardware, operating systems, protocols and applications (where the choice between corporate interests and users' interests is rarely balanced and often prone to self-enforcement). In many cases a clash between contrasting norms.
The second points out that Information Technology has a normative attitude and that therefore there are actual conflicts between technical and legal norms that, since the Internet cannot be simplistically solved affirming the priority of the law: through the Internet IT has become such an international infrastructure, that any attempt to rule it from a national perspective is deemed to failure (or to pose the end of individual rights). On the other hand there is a need of regulation of Information Technology and of the cyberspace that hasn't already found a proper and structured answer (The Economist, front cover article, August 11th-17th 2001).

1. NO FREEDOM OUT OF LAW (WAR AND ANARCHY: THE DOMINO EFFECT)

The word "anarchy" is used here in its etymologic meaning of no ("a?") command ("a???"): no common rule or ruler is accepted.
In fact, the first we need to be free in the world of atoms (human society) are stable commonly accepted rules: a legal framework.
Failing that, self-regulation totally depends from self-defence. If you are not able to self-enforce an agreement, it is useless to make it ! Therefore, there is no freedom out of self-defence. Moreover:

- conflicts tend to spread, involving friends/allies of both fighting parts (you never know where the enemy is)
- the need of self-enforcement transforms each conflict in a war (worsening potential of conflicting relations)
- alliances and friendships are more eager to produce conflicts then a neutral relation or no relation at all (worsening potential of non-conflicting relations)
- therefore ambiguous relations with other parts or no relation at all, are preferable in order to avoid third parties conflicts
- the best way to end a conflict is the destruction of the antagonist
- the best way to avoid dangerous alliances of your foe, is to be friend of your foe's friends (ambiguity as an asset)

We see how this grim picture matches with the historic records

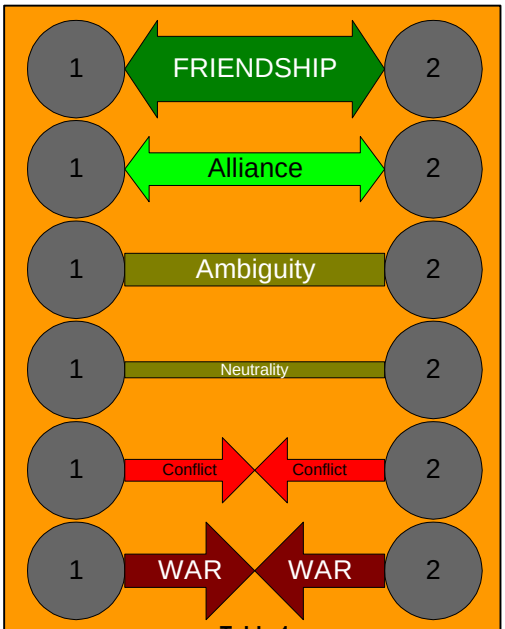

Table 1
Basic relations

on the warlords of the middle age, or of prehistoric societies. We will further see that it is also a suitable description of the current situation in the world of bits.

One of the most telling myths of the birth of a legal framework is the myth of the first strike. During secession to the Aventinum of Roman peasants opposed passive resistance to the knights under the slogan: "If the arms of a body refuse to work, how can the head survive?" It ended with the first written constitution of legal history. It could have ended in an endless bloodbath, if the knights had tried to self-enforce their rights.

There are two more probable evolutions of a lawless time:

a) monarchy/empire: if a party is stronger, then all the others involved. Often it is the degeneration of the effort to police the conflict
b) federation: if the parties conclude an agreement on (more or less) equal basis.

But these are not natural evolutions. The anarchy system is stable in itself, as the duration of the middle age reminds us.
There is the need of courageous initiatives in order to break the escalation of conflicts and self-enforcements.
In Table 2, the complex relational situation in a lawless environment.

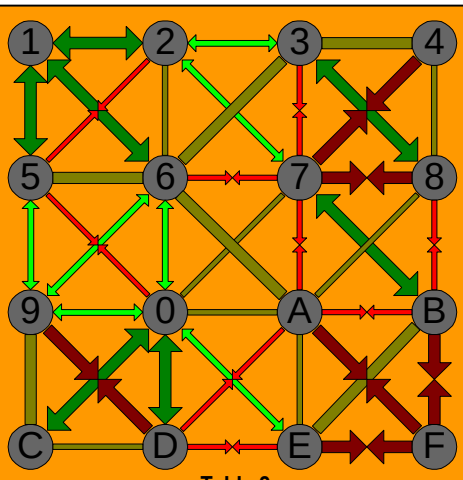

Table 2
Relational situation in a context without common legal framework

In Table 2, Friendship/Alliance cause war/conflict in following cases: 3-8 0-E 2-3 5-6 9-0 6-0 1-0 2-6 0-C 5-9 0-A
Ambiguity/Neutrality becomes Friendship/Alliance in following cases: 6-A 8-A 6-3

2. NO LAW OUT OF FREEDOM (THE SYNDROM OF THE EMPIRE)

In an absolute monarchy we begin to have a common legal framework, but it is sketchy and unable to cover all possible relations. In fact monarchy is not equal to freedom: it relies, more then liberal societies (federations), on strength in order to enforce the rules. Somehow it is based on a pyramid of strengths, and generally no ruling or law enforcement can move from the basis of the society to the top of it. Self-regulation and law enforcement are possible only horizontally, between equals.
In socially vertical relations no agreements are truly binding. The socially superior party rules on the inferior one, and has also the possibility of enforcing its ruling. The rule of law is flawed by many petty exceptions. Rule makers and judges, belong normally to the superior class and tend to act with partiality in its favour (see Table 3).

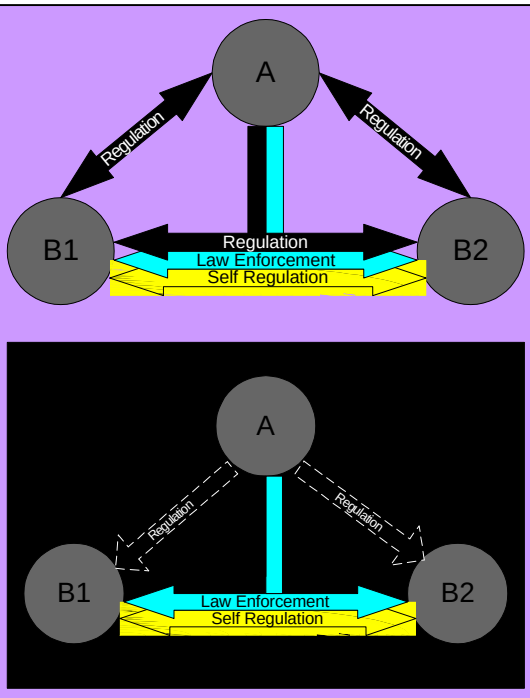

Table 3
Relations in a monarchic/monopolistic legal framework

Telling in this sense is the story of Friederich II of Prussia. His father, King Friederich-Willhelm I, accused his son and General Von Katte of treason, in 1730. A military tribunal chaired by Graf von der Schulenburg found both guilty. General Count von Katte was sentenced to life prison, to avoid that there could be the risk of a death penalty on the King's heir. The military tribunal ruled its incompetence rule the penalty for Friederich von Preussen. King Friederich-Willhelm, turned the life sentence of General Count von Katte into a death penalty, in order to discourage similar behaviour of Prussian generals. The execution was held at the presence of Friederich von Preussen, which later was graced: he was the only male son of the emperor. By the way, it was one of the most modern ruling kings of that century history.

Moreover:

- a system funded on the law of the stronger cannot at the same time be based on consensus: therefore petty ruling is frequent;
- law enforcement has to be cruel in order to be respected (it has to be enforced even if it is unjust)
- administrative regulation prevails on self-regulation

- judiciary is expression of the power of the crown (at the same time legislator and administrative power!) and therefore is not impartial and often not motivated
- self-regulation is weak and weakly enforced
- there are few common agreed rules, because also common agreed rules have extremely frequent exceptions (so called "*jura singularia*")

Anyway, this system is a great improvement compared to the lack of a common legal framework.
Because (see Table 4):

- conflicts do not tend to spread (the holders of privileges, if well advised, try to use them wisely in order to preserve them; the ruled class tends not to unnecessarily prevaricate the ruling class);
- few conflicts result in a war, threatening the existence of a common system (no worsening potential of conflicting relations);
- conflicts are polarized between the different social parties, and there is some kind of class solidarity: you know mostly who/where the enemy is (low worsening potential of non conflicting relations);
- ambiguous relations are only occasionally a good asset;
- there is no possibility to achieve the destruction of the antagonist (with the sole exception of revolutions);
- it is unusual to be friend of allies of your enemy.

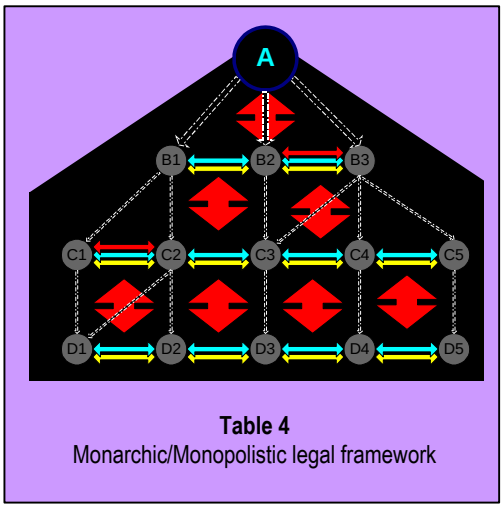

Table 4
Monarchic/Monopolistic legal framework

Justice is not the main virtue of such a system, but it is less violent and more transparent compared to anarchy. There is order to the price of freedom. Law has a secondary role compared to power. Violence is an option to (for an instance in order to achieve freedom), but it is no daily necessity any more.
The greatest virtue of this system is that it tends normally (through social conflicts) to reduce the amount of privileges and exceptions and to increase the area of law enforcement. It is a system, where the rule of the stronger gets weaker and weaker. It is just the second step towards an open and democratic society.

3. LAW AND FREEDOM: THE VIRTUE OF THE FEDERATION

The first known common legal frameworks have been characterized by a negotiated solution to long-standing conflicts of sovereignty. Already before the legal system of the ancient Romans, the federation of the Greek ?o?e?? (Nation-cities) was a generally shared and accepted legal framework, in which the Greeks evolved to the most rich and modern society of that time (V to III century B.C.). Each of the Poleis was abiding to some part of its power and sovereignty (to some part of its monopoly of the law) in order to achieve a common good.
And so in Britannia, during the mythological time of King Arthur, more then a millennium later. One millennium later, again, the birth of the North American Nation as "the" Confederation. In a federative system, each city, warlord, state, or single person, accepted, finally, that in order to achieve peace and greater wealth it was necessary to loose some sovereignty (see Table 5 and 6).
Looking at it from this peculiar perspective, also the European Union is already some kind of federation.
In such a context, negotiated politics keep conflicts peaceful, trying to achieve a compromise. Politics try to avoid self-enforcement. Politics try to keep social conflicts within the given legal framework.
Within a federation, there is a common legal framework as far as the rules are generally accepted.
Good rules are generally accepted rules. What else characterizes good rules ?
They are made according to an accepted procedure and they respect the funding values of the legal system.
From an HISTORIC perspective, this achievement was accomplished in two ways:

a) the merger of sovereign entities, accepting some significant limitations to their sovereignty, as it happened in North America or in ancient Greece with the federation of ?o?e?? (Table 5).
b) through the split of the power of the crown, separating from it the legislative and the judiciary powers, as it happened in Europe, about two centuries ago (Table 6).

The tri-partition of sovereignty in administrative, jurisdictional and legislative powers is the still working receipt to balance freedom with regulation.

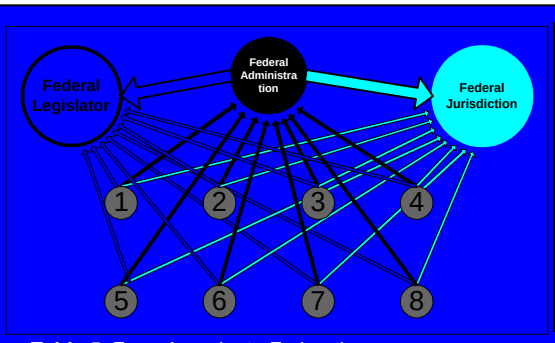

Table 5. From Anarchy to Federation

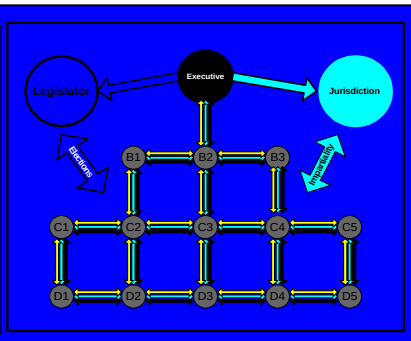

Table 6. From Monarchy to Federation

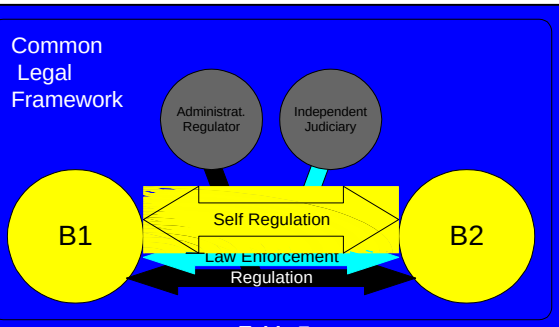

Table 7
Legal Framework in western democracies

So we can say that in western democracies, from each perspective, HISTORIC, ETHIC and POLITIC, good rules are those striking a good balance between individual self-determination and broader involved interests. The system works, thanks to **"Trusted Third Parties"**, exercising the sovereign legislative power, the judiciary power and the regulative power of the public administration (see Table 7). These are the reasons why the legislator and the public administration forbid (lawfully) only what can endanger or harm third parties: the first choice in an open liberal society is self-regulation. Only if broader collective interests are involved (i.e environment, privacy, food safety, consumer protection, financial markets, and so on) administrative regulation and/or supervision are advisable.

In such a system bilateral relations are generally self-regulated. Self-enforcement is strictly forbidden (only the state entitled to use the force). Third parties can determine the rules of a bilateral relation only exceptionally, whenever some general interest is involved.

The funding necessities of such a system are:

a) law has to respect the fundamental chart of the system (the "Magna Charta" of the federation), being this formulated by a legislator that is expression of the elected representatives of citizens
b) regulation has to be impartial and overrule self-regulation only if general interests are involved
c) law enforcement has to be impartial, transparent and motivated and effective

Under such conditions there is no "domino effect" of conflicting relations, the conflicts at legal level are most times individual (collective conflicts belong to the political sphere of competence). Therefore conflicts are minimized:

a) in violence,
b) in amount,
c) in ability to spread.

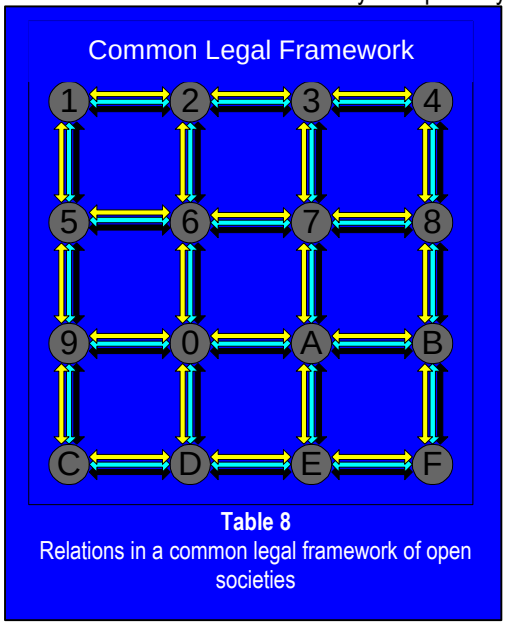

Table 8
Relations in a common legal framework of open societies

Open democratic societies make a limited use of force to achieve order. This is what we call normally "freedom". Something quite different from "*no limits*"; more like "*many well balanced limits*".
All members of a liberal democratic legal system can therefore concentrate in to find (also innovative) ways to self-regulate their economic or moral interests.
Freedom is endangered when a legal system:

a) has legislation which is not combining in the most effective possible ways all the renounced sovereignties and self-enforcements of citizens,
b) has oppressive or pervasive administrative regulation, compressing the opportunities of self regulation,
c) has ineffective or not transparent law enforcement.

All three pathologies are endangering freedom in the Cyberworld, as we will see below.

4. FREEDOM, SELF REGULATION AND INFORMATION TECHNOLOGY

Let's examine the relational structure on the Internet with actual technology and regulation.

4.1 RELATIONS WITHIN A SINGLE (NATIONAL) LEGAL SYSTEM

People interact only with other people of the same nationality and with servers, clients and services/products all placed in the same nation.
It is clearly an unusual situation today (besides in authoritarian regimes, such as the Peoples Republic of China). Some analysts start to guess that IT/Internet are going to become increasingly subject to national regulation. There are signs in this direction, but it is not already unavoidable or necessary.
Using the same relational parameters we used in discussing the issues of freedom, anarchy, self-regulation and self-enforcement in ancient societies, we get the following picture:

1. There is a common legal framework
2. There is also administrative regulation (i.e. tax, and recently electronic signatures)
3. There is law enforcement, despite costs and procedures that are barely compatible with the idea on-line transaction. Law enforcement can be deemed as weak.
4. Not all legal systems provide legal relevance of electronic documents and evidences (the European Directive to this purpose represents a significant improvement).
5. Very few legal systems provide an infrastructure for the authentication of parties (the European Directive is again significantly improving the situation).
6. The IT tools used by the parties are mostly proprietary. They are often products of de-facto monopolists. Moreover, IT is designed and engineered in such a way as to influence the behaviour of the parties in a quite unnatural way. It is not ergonomic. We see in every day's life on the Internet, the negative impact of not-ergonomic IT tools on the relation between the parties: it is like there would be a third party's regulation, strictly followed by both interacting parties. Sometimes it looks like technology would force interacting parties to behave like puppets. In Table 9 relations within a single (national) legal framework are illustrated. There is not only the conflict of interests between self-regulating parties, but also the interference of IT and the conflict between IT producers and the norms of the legal system. The law is not helping technology to work or to improve its functionalities. Technology is obstructing the normative effectiveness of the law. Today we can see several conflicts of the kind; we have seen analysing the anarchic context, because law enforcement cannot be effective, without coming into conflict with the fundamental rules of our liberal democratic open society.

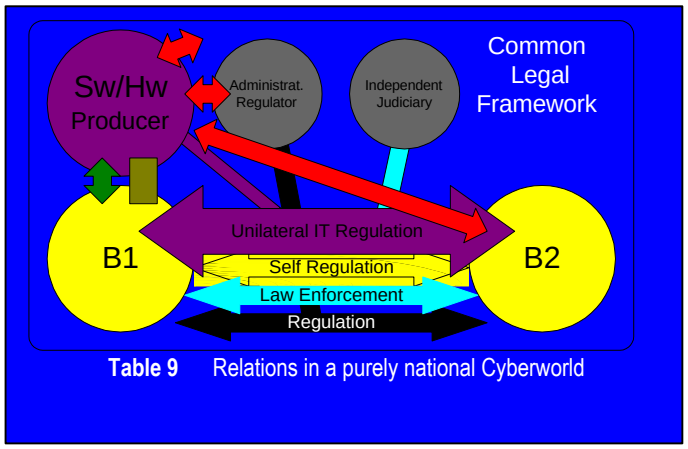

Table 9 Relations in a purely national Cyberworld

4.2 RELATIONS INVOLVING DIFFERENT (INTERNATIONAL) LEGAL SYSTEMS

If we then have a look to the international transactions on the Internet, the picture becomes even more alarming. Interacting parties belong to different legal systems and so do their servers, clients, products and services. The law of many states is involved in the definition of an apparently simple transaction, like booking a hotel.

1. There is NO common legal framework
2. There is NO administrative regulation
3. There is NO plausible law enforcement. Self-enforcement of rights is more then just an option. It is useful, perhaps, to remind some famous controversial issues, involving well known IT products or services:
    a. copyright protection vs. right to make a personal copy;
    b. marketing vs. privacy;
    c. copyright protection vs. right to configure the hardware of the PC;
    d. security vs. manageability and cost minimization;
    e. right to enhance a product vs. illegality of predatory practices;
    f. freedom of speech vs. desire to keep secret security flaws of IT products
    g. police activity vs. individual rights.
4. Few legal systems provide legal relevance of electronic documents and evidences (the European Directive to this purpose represents a significant improvement).
5. Very few legal systems provide an infrastructure for the authentication of parties (again the European Directive has significantly improved the situation).
6. The IT tools used by the parties are designed and engineered in such a way as to influence the behaviour of the parties in a quite unnatural way, as we have seen before. But there are moreover cultural and linguistic problems that can severely complicate things. All in one: there is a context in which people is unnaturally interacting, with great distrust of each other, all armed and ready to self enforce their interests.

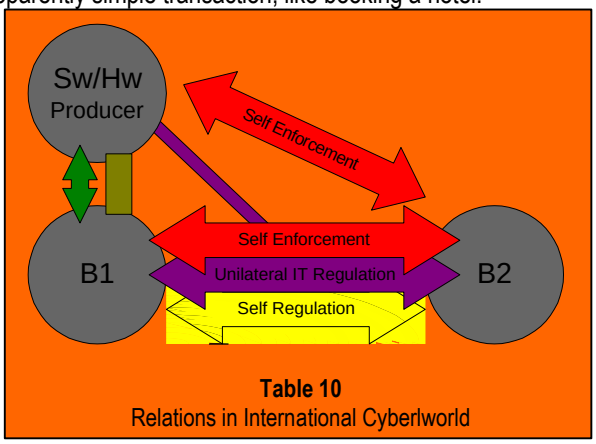

Table 10
Relations in International Cyberlworld

Such a legal context is more similar to the times before there even was a law, then to any legal system of the last 2000 years. **One thing is clear: things cannot go on like this,** regardless of the "Declaration of the Independence of the Cyberspace" written by John Perry Barlow in 1996. In fact today the only successful business strategy in providing goods or services to consumers is to abide completely to any self-enforcement (Credit Card companies, Amazon, E-Bay). Yet, can we nowadays make business like in the days of Marco polo's "silk route" to China (paying a toll to any individual, tribe, or organisation which is able to come between us and our counterparts) ? If today this is sustainable, it is only because the global amount of transactions is low (and slowly growing because of security and privacy concerns). Will this be sustainable forever ? The answer is: obviously not.

We see that, in both national and international self-regulation, the legal framework is worryingly shaky and unreliable. The analysis of the relational pathologies shows two groups of problems:

a) legal problems (Nr. 1 to 5)
b) technical problems (Nr. 6)

We will consider first the technical problems, because they have great influence on the legal ones.

5. THE TECHNICAL PROBLEMS: INFORMATION TECHNOLOGY INTERFERES UNDULY WITH PEOPLES SELF-REGULATION

There is a worrying pathologic regulative influence of Information Technology on the relational behaviour of interacting parties (as shown in Table 9). As in Orwell's "1984", most people cannot even dream of being able to act naturally on the Internet. The current architecture of technology is not transparent. Moreover often there is no choice between different technologies, because *de facto* monopolies are rather frequent today. Unregulated monopolies: something that brings us back to the beginning of last century. In fact, on the Internet:

1. We are asked to be identified, even before we can pose any question (or, worse, we get identified without being aware of it). At the same time no really trustworthy identification is possible (see the following nr. 3).

2. All kind of interactions have the appearance of a written transaction, but without the possibility of getting a proper, reliable documentation of it (the whole documentation is –eventually- in the hands of the commercial/professional party). Users have all the disadvantages of written transactions and none of the benefits. No tools to manage transactions are available for consumers.
3. No reliable identification is provided, besides the "Qualified Certificates" of the European Directive (and even these could prove, in case of pervasive use, a little simplistic in their conception). We are asked (per default) to rely on identifications that can be (and sometimes have been) quite superficial. The concept of identity has to be rethought in order to be used successfully on open networks (i.e. for electronic money, electronic liability, electronic enforcement, etc.).
4. We rarely can get immediately what we need: we normally pay and get a credit.
5. Law enforcement comes … "*from another world*" (the world of atoms), if it ever comes.
6. The most practiced form of self-defence, is "*denial of … transaction*": i.e. one of the two parties simply denies its agreed performance (delivery, payment, etc.) or even denies at all there has been some kind of agreement.

Let's look to **two purely technical examples**.

1. The operating systems and the applications of PABX telephone systems. After much more then a decade, there are still few efficient ways to connect a personal organizer with the desktop office telephone (all of those I have seen are more or less proprietary, at least from a commercial perspective). Also wireless headphones for office telephones are still missing. In fact hardware and software producers have no chance to market successfully their products within the captive market (and proprietary technology) of PABXs. I think it is a good example to show how much unilateral IT regulation, in this case in the form of a monopoly of the underlying infrastructure, can harm competition and innovation. It is not a consequence of bad will; it is a matter of fact.

Can this problem be solved imposing to PABX producers not to improve their systems enhancing the functionalities of their systems ? Or imposing them to accept innovation from other producers ? Probably not. But this is the only possible approach from the perspective of a national legal system. Is there any better option ? Yes !

Openness. To abide to some part of the monopoly, like ancient Greeks and ancient Britons did. There will be less individual power, but more shared strength.

2. PCMCIA I had (once again!) to transfer my presentation from my laptop to the PC of the venue of the conference. It did not work, despite we had computers of the same brand. It was because the floppy drives of that computer brand where incompatible. It worked with a PCMCIA card. PCMCIA is a standard, not a proprietary technology.

Open technology works better, improves faster, and because it is per definition no monopoly, it cannot be exploited ruthlessly.

Open technology is a technology that accepts the need to renounce to some monopoly in its ruling ability; it renounces to some ruling sovereignty. Like we all have to do in order to live in a peaceful and organized society.

All this has been marketed as normal, necessary, as a consequence of what technology can do. This is simply not true. Technology is, as it is, because of some (probably good) historical and economical reasons, but this is neither logical nor technical necessity for that.

As far as we can act naturally using any technology, there is no special need of regulation. The need of regulation grows, as soon as technology modifies our normal way to act.

Any technology aiming to determinate unilaterally how we shall act, is incompatible with any legal framework, with any individual freedom, with any digital self-regulation. It is incompatible with the funding and accepted rules of our societies, as egregiously remarked by Lawrence Lessig.

The supporters of Quality Of Service (QOS) on the Internet cannot see themselves as antagonists to the present situation of End to End (E2E). In fact, proper billing rules could be an appropriate compromise to combine QOS with E2E.

Technology openness (transparency + modularity) and ergonomic adequacy, in fact, are the possible ways to make top-down regulation unnecessary: if users can choice what sort of technology to use, they still can self determine their behaviour. If technology represents properly the rules of freedom of our society, it will become a true tool to express our liberty in cyberspace.

For this purpose Information Technology should:

- try to **be neutral**: i.e. avoid to choose unilaterally and per default what kind of interest are preferred among a series of conflicting interests of the relying parties (in particular to self-enforcing some competitive advantage of the IT producer);
- **be ergonomically appropriated**: i.e. do not impose radical changes to the ways things are done that cannot be managed culturally, socially or physically by users. Of course technology will radically change our habits and even our capabilities. But it cannot do it at once.

  Sometimes technology shall not change ways things are done. A digital signature performed today with a smart card on an insecure PC, can be meaningless, provided it has been proved easy to program worms able to substitute at the moment of signature the file to be signed, with other data. Secure viewer solutions and secure signature applications (secure terminals) are necessary in order to make digital signatures a true full substitute of handwritten signatures.

- **be modular**: i.e. allow technologies of third parties to be implemented onto it (renouncing to some competitive advantage of the producer);

- **be transparent**: make public full documentation of the technology to all interested parties (eventually under appropriate non disclosure agreements) in order to allow third parties to study and make publicly available the technologic/security weaknesses of such technology;
- **eventually allow third parties to improve such technology** and implement it within other systems, under the condition of full reciprocity.

A certain degree of openness (transparency + modularity) is necessary in order to:

a) be not considered (and ruled as) a de-facto monopoly
b) preserve the freedom to innovate from national legislators (see Chapter 6)
c) avoid mandatory legislation protecting users (in particular their security and freedom self determination), through mandatory requirements on technology.

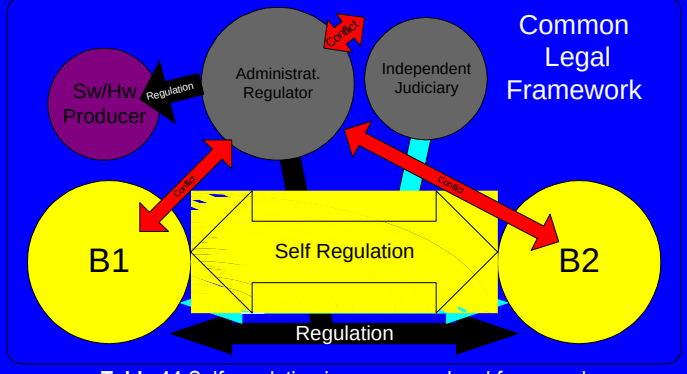

Table 11 Self regulation in a common legal framework with neutral and ergonomic technology. National legislator regulates technology to protect users and regulates Sw/Hw producers if they are monopolists. Freedom is at stake, regulation prevails on self-regulation

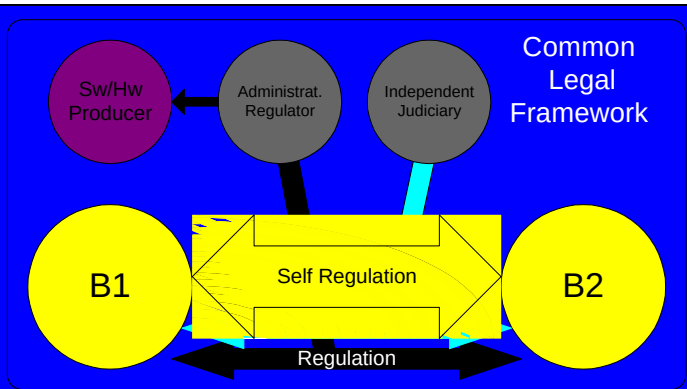

Table 12 Self regulation in a common legal framework with neutral, ergonomic and open (transparent + modular) technology. Legislator regulates Sw/Hw producers only if they are de facto monopolists.

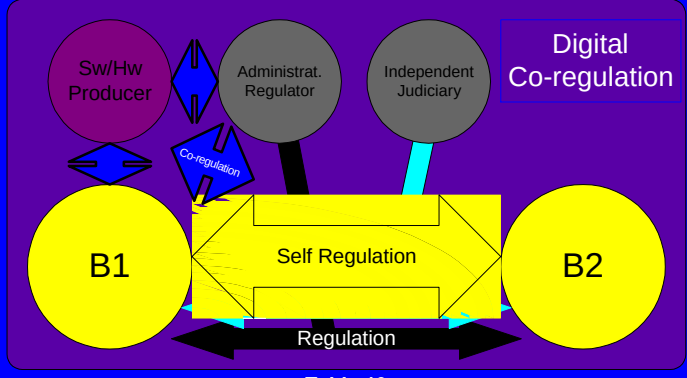

Table 13
Self regulation in a common legal framework with neutral, ergonomic and open (transparent + modular) technology and no de facto monopolies

The only existing business model going in this direction is "Open Source", despite many times products are poorly designed, from the ergonomic point of view. Since many of the leading IT producers embraced the open source approach, most IT research is moving towards the right direction. But presently, still very products are available. In fact, still, it is often the intentional choice of the producer to prefer certain (own?) interests to the legitimate expectations of relying parties.

How many times have I been asked to minimize the legal risk of some IT solutions ? The problem is that to become successfully the new central infrastructure of human acting, some (legal) risk is unavoidable. To avoid it, means just to be unable to accomplish such a relevant function !

IT industry, de facto ruling many aspects of human behaviour in the cyberworld, is asking for:

- exemption from the rule of law
- largest possible exemption from legal risk (liability)

To my eyes IT companies look like vile rulers, feared (or not interested) to rule the society relying on them: they rather go on fighting with competitors, then take care of the relying parties. Some kind of balkanisation of IT competition, that needs some third part ruling, if it is not able to achieve peace on its own.

We all agree that in our legal system self-regulation is (and has to be) the first option.

But if people are, at the end, unable to self-regulate their own interests, because of the competition's clash in IT industry (i.e. the rush to become or to stay as a monopolist), then administrative regulation (or prohibition) is the only remaining option (like at the time of the Rockfeller's industrial empire).
This option should be avoided (as better explained in the next Chapter), but cannot be excluded in principle, if self-regulation (self-restraint) does not happen or does not work properly.
Self-regulation through technology can only happen if IT tools are neutral, transparent and ergonomically appropriated.

6. THE LEGAL PROLEMS: INADEQUACY OF NATIONAL LEGISLATIONS

Law must regulate human behaviour, not Technology. The opposite approach of many governments, is a consequence of the difficulty to enforce rules on open networks. This is a real thread to innovation and entrepreneurial freedom (see Table 11). The correct answer of IT producers, is not the defence of their captive markets and/or de-facto monopolies. This is short sighted, because the next step of the legislator approaching IT will be to define the functionalities of IT. The most effective answer of IT industry to the top-down approach of the legislator is openness. National legislators cannot rule something which is truly international. The failure of national legislators to rule cryptography is the most telling example of the inability of national laws to rule technology. If in the days of the US SAFE Act of 1997 there had been a monopoly of cryptography, there would not exist any cryptography at all, without backdoors and key recoveriesanymore. Only those, who presently have a de facto monopoly can hope that legislation (or law enforcement) on IT functionalities will strengthen their monopolies. On the other hand, legislator and law enforcement bodies will acrimoniously work to weaken such monopoly. There are not good perspectives for IT innovation and self-regulation, basing on such ambiguous relationship between IT monopolists (or national IT champions) and the state..

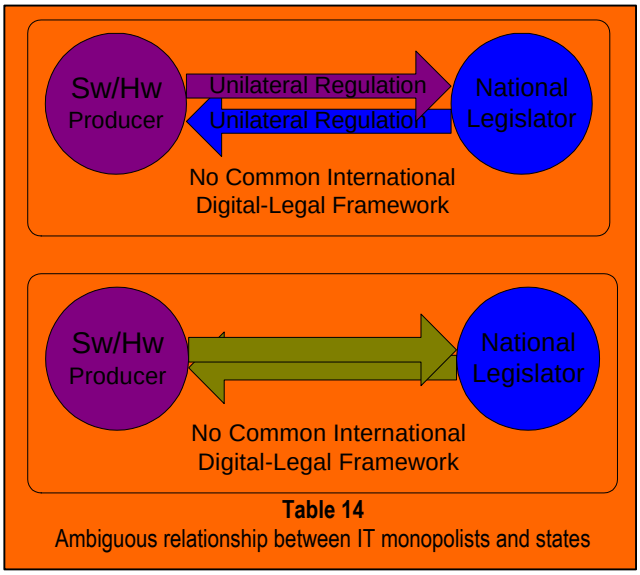

Table 14
Ambiguous relationship between IT monopolists and states

The European Directive on Electronic Signatures is exactly going in the direction of openness through an appropriate legal framework: moreover, the EU is supporting openness through the EESSI standardisation process.
In the end, law can avoid to regulate technology, only provided that there is no de-facto monopoly of some widespread technologies. In case of monopolies, a strict regulation, from the point of view of legislator, is unavoidable (see Table 12). The European approach will thus succeed only in a context where open technology will thrive (like that of Table 13).
Even the legislator is submitted to the rule of law. Why should not IT producers be submitted to it in the long run?.

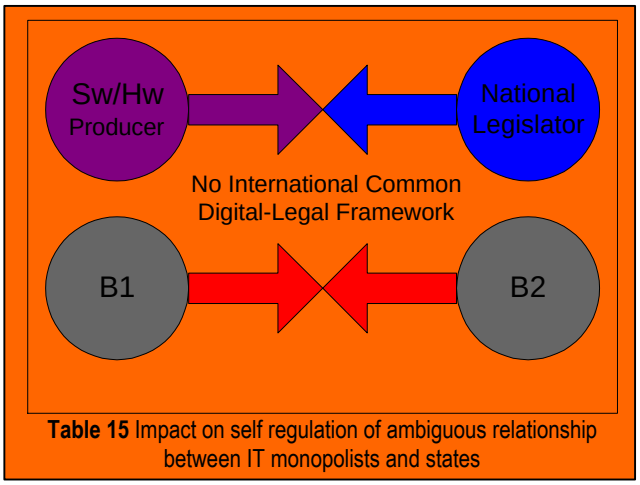

Table 15 Impact on self regulation of ambiguous relationship between IT monopolists and states

Surprisingly, this strange situation is accepted in the cyber-world, and the discussion goes about what default settings should be preferred.
Personally, I believe that the discussion is missing the point.
Openness is the only principle that might work. The expansion of the Internet technology will be strong, only if it is open. Still openness is growing faster then anything else.

Any other option will have a heavy toll on freedom or on technologic innovation or even on both, in a worst case scenario (we can see in Table 11) .
The way private self-regulation transactions are managed today is neither logical nor a necessary consequence of binary logics, or of any strict Internet protocols! It is a consequence of the present architecture of the Internet, which could be differently engineered, to allow freedom and self regulation, in order to respect the fundamental principles of our society: freedom of self-regulation, restraint in self-enforcement, the rule of law, the effectiveness of law enforcement.
The present conformation of Information Technology (No. 6 of the above mentioned problems) and its utilisation - which is much wider then within national borders - are the reasons why IT is handled by legislators and regulators more like a force of the nature, then a human activity.
as we have seen, this does not happen for good reasons.
Open and transparent technologies are technologies to which legislator can refer in order to give to the cyber-world a legal framework. Proprietary solutions, if endorsed by legislators or public administrations, can only create new monopolies, endanger fair competition and stifle innovation (as we have seen in the PABX example).
At this point, given that sometimes it is easier to enforce national regulation (or policy) towards (or with the support of) monopolists, (and/or proprietary technology) legislators try to regulate technology unilaterally.
The legislator (a legal monopolist) has instinctively tried to be an ally of other monopolists, or to use them in order to achieve his goals (National Railways, National Utilities, National Airways, National Telecoms and even national IT champions, sometimes!). This did not work, in the long run, because technological monopolies are a permanent thread to market freedom, to the individual freedom and to the rule of law. States always had conflicting relations not only with de facto monopolies, but also with their legal monopolies. They just subtract some relevant economic activities from the rule of economy.
The resulting situation is a conflict between two entities having a different kind of funding values, different sovereignties, both jealous of their own supremacy. No true alliance. It is an ambiguous relationship, like the one which could exist between two warlords, believing more in the strength of power, rather then in the power of self-restraint and agreement to rules.
Thus Technology should not be produced by monopolists. It should be open: transparent + modular (see Tables 14 and 15).
Despite open technology is harder to regulate at a national level, it is the true ally for a democratic government, which is trying to strengthen the rule of (democratic) law, and weaken the rule of autarchy.
A strong ally is not necessarily a bad ally. Given that the true supporters of open technology are the open society, they are sharing the same funding values of our democratic open society.
The allies refrain from self-enforcing their competitive advantage. They accept that a natural leadership in IT is not going to last forever: see the Palm Company business case.
Some legislators have started to introduce grim law enforcement legislations, compressing those individual rights, which in the world of atoms nobody would dare to touch. This will not work, exactly for the same reasons why torture never has made law enforcement more effective. Our system is working better then others thanks to its wide support. To attack individual rights will only weaken the legal system (see Table 11), which is funded upon individual rights. Moreover the conflict between different national legislations will, whereas possible, even increase (see Table 16 and 17).

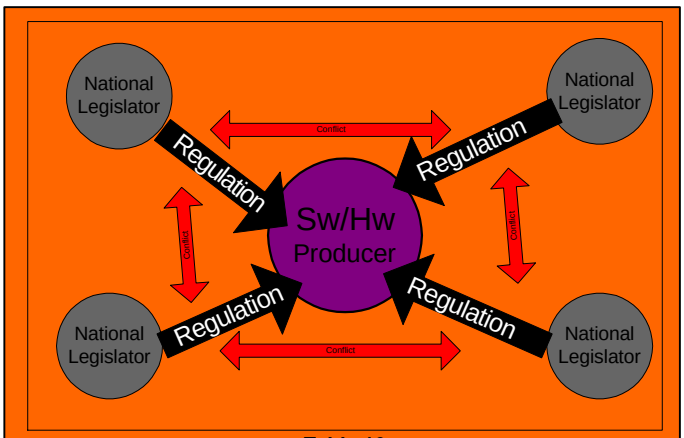

Table 16
National legislation's impact on freedom of technical innovation

Such an authoritarian approach is even more astonishing, considering that there are technologies that would make on-line criminality easier to tackle, without depriving citizens of their constitutional rights. Most of these technologies are based on cryptography, which some legislators still treat as a thread to security. These technologies should be at first understood, and then supported, funded, enhanced by the governments, before changing the rule of law in such a way that can only harm the credibility of institutions.

Therefore legislators should:

1) work on an international treaty to give international e-transactions a clear framework, respectful of the millenary rules of private law, possibly striking a good compromise between administrative and tax aspects (the same kind of compromise that has been done in shipping, aviation and banking).

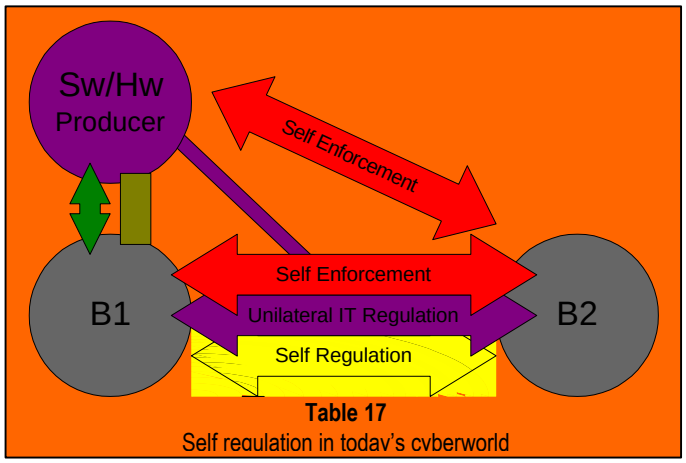

Table 17
Self regulation in today's cyberworld

2) internationally co-ordinate administrative regulations, like in the area of supervision of Service Providers, where it has been urgent to issue qualified certificates, according to the European Directive 1999/93. The Common Criteria have been chosen as the IT security evaluation system. It is the most widely shared IT security assessment system available: preferring the more global Common Criteria to the European ITSEC, EESSI has shown a strong interest towards openness. Also law enforcement and police should co-operate internationally, in order to be at the same time effective and respectful of the values shared by liberal democracies.
3) endorse and support all transparent forms of on-line voluntary arbitration, providing proper supervision, to avoid abuses.
4) give international relevance to digital documents and electronic signatures.
5) provide a trustworthy infrastructure for identification of persons, conceived and organized in a way suitable for on-line authentication. Existing forms of identifications have not been conceived to be used for an undetermined lapse of time as well as for any other purpose: they have been conceived for specific uses or functions. This is something IT companies cannot provide. Only legislation can. But the legislative solution should comply with the individual right on the own identity and at the same time with the IT infrastructure in place. How to do this without co-regulation ?

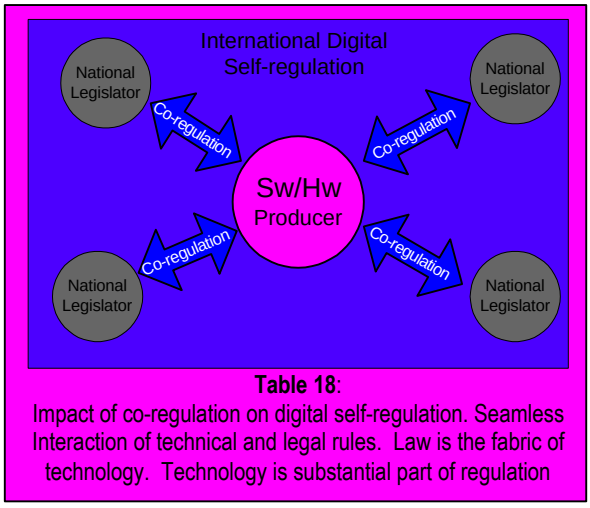

Table 18:
Impact of co-regulation on digital self-regulation. Seamless Interaction of technical and legal rules. Law is the fabric of technology. Technology is substantial part of regulation

The European Directive on electronic signatures has clearly addressed the tasks 4 and 5. The Directive on Electronic Commerce is endorsing task 3. Discussions on how to address task 2 are in progress.
It is impossible today to dream of a world legislator, dealing with global issues, like environment or international trade. International existing organisations are struggling, because nations are jealous of their sovereignty. The national interests come first. But national legislators can and should:

- endorse international standards and open technology
- avoid to make Internet a national issue, like it is happening in China, and
- sustain an international open legal framework.

This is exactly what the European Union has done with the Directive on Electronic Signatures (1999/93/EC).
The European legislator has defined goals and legal frameworks, specifying to the technologic community and users how to realize such goals. This goals are: technologic security, technologic transparency, market openness, mutual recognition, data protection, consumer protection.
In order to accelerate the co-regulative process, the European Union is funding two standardisation open workshops within a program called European Electronic Signature Standardisation Initiative (EESSI). The two open workshops are:

a) ETSI ESI, managed by the European Telecommunication Standardisation Institute and

b) Cen-ISSS E-Sign, managed by the European Committee for Norms (Cen), within the Information Society Standardisation System (ISSS)

This new approach, called CO-REGULATION is having great support, not only from European companies, but also from important overseas companies.. Consumer and user organisations, of course, are supporting it too.
I believe that this process, is going to be something more important, rather then just a standardisation process for the European Directive.
I think it is a first good step in the right direction in order to combine the rule of law with the rules of technology.
Being already a panel of this conference dedicated to the European Standardisation process, I will not go into details. I would only like to invite you to participate to that panel, where, I was told, there will be enough time for discussion. International experts not directly involved in the European Standardisation, like Steve Kent, will expose their point of view about such a process.
Anyway, I would like to stress here, that EESSI and the European Directive on Electronic Signatures are a process enabling more openness in technology, more freedom of innovation, only by sharing the funding values of our society in making new technologies. Industry is widely supporting EESSI and only eventually some companies have tried to halt the standardisation process.
Considering the wide support of the co-regulative approach of EU and its success, it is even harder to understand why still some legislator believe in an illiberal top-down approach to both IT and state security through IT. Maybe more dissemination activity is needed, particularly in the United States, where the legislator has one of the most authoritative approaches presently known.

7. SCENARIOS

By looking at the potential evolution of the present situation, at national and international level, we can make the following assumptions:

1) NATIONAL EVOLUTION:
   a) **Information technology stays as it is,** not open (modular and transparent), persisting to unduly influence the self regulation of the user: national regulation will start to limit the freedom of IT producers, as long as they are in conflict with the needs of law enforcement and the rights of the users, and will increasingly submit the Internet to national regulations. We have seen that such a process has had a few chances to be successful, yet antitrust cases in the USA and Europe, legislation in UK, jurisprudence in France are worrying signals that such a trend is already in progress. This will cause more problems at international levels, because the differences between national regulations will become wider. Eventually freedom to go abroad, will be even limited through firewalls or similar solutions. National legislation is not going to end this anarchic situation. Islands of Quality Of Service will be (artificially) created … Swiss will buy Swiss …. Italians will buy Italian … like in the Middle Age!

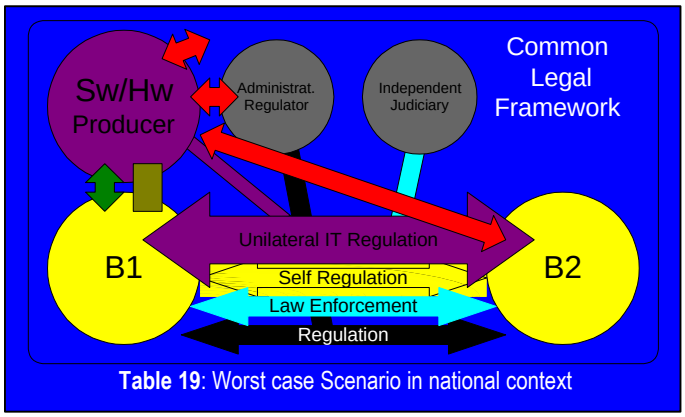

Table 19: Worst case Scenario in national context

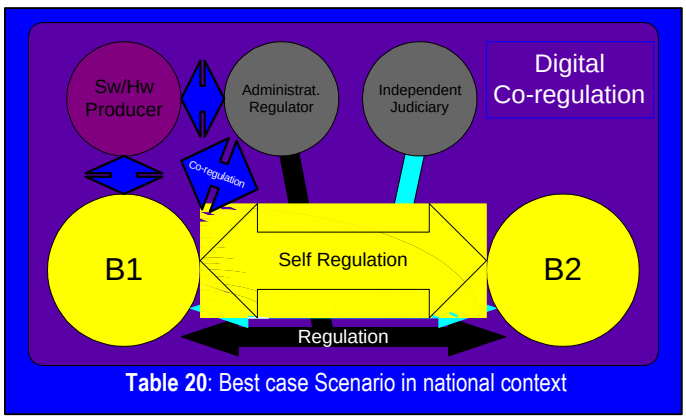

Table 20: Best case Scenario in national context

   b) **Information Technology gets more transparent**. Legislator will have a great interest to endorse somehow such technology in order to:
      i) become able to make effective the rule of law in the cyber-world

ii) build a transparent IT infrastructure for the nation, providing a competitive advantage for all kind of activities.

This trend is clearly recognizable in the following cases:

- The support of open source technology for public administration
- The endorsement of international standards as part of the European legal framework of electronic signatures provided by the Directive 1999/93/EC.

2) INTERNATIONAL EVOLUTION

a) **Information technology stays as it is**, proprietary, neither modular nor transparent, having a heavy handed impact on self regulation of the users. The present anarchic situation will persist, the trust in the Internet and technology will fade, the phenomenon of hacking will increase in numbers and quality. National legislation will have a point in asking to reduce individual rights in cyberspace, in order to fight criminality. The widening differences in national legislation will make any kind of law enforcement (even the voluntary arbitration) more difficult, if not impossible. In one sentence, we will get back to prehistory. We also have here clear signs that this is already happening: malicious attacks are increasing, national legislation tries to tackle that also at the price of individual liberty ….. Yet, can an illiberal Internet co-exist with a liberal society ? Only illiberal societies are having today the Internet seriously filtered. Can we really think that, in the end, they are right in acting this way ?

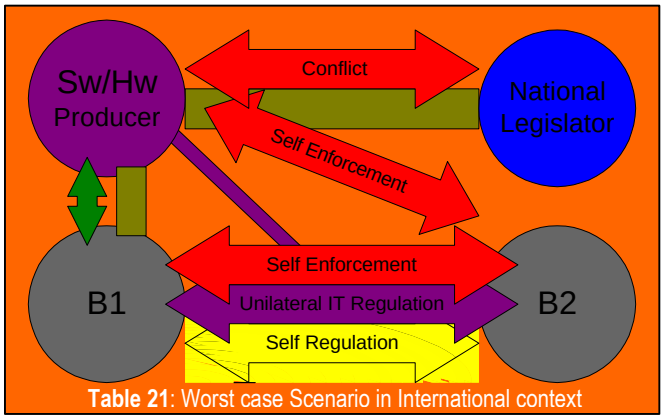

Table 21: Worst case Scenario in International context

b) **Information Technology gets more transparent** and abides to some of its ability to influence users in their free choice (the ruling ability of IT). This means that the relevant IT infrastructure will be somehow shared (this can happen in many ways) and will not be anymore a complex mixture of different proprietary technologies with some internationally agreed standards. In this scenario international standards and open source will have a key role. The support of national legislator is urgently needed, as seen before under 1b. IETF has a central role in this process, but still needs more (appropriate) support from national regulators, such as endorsement of its open standards.

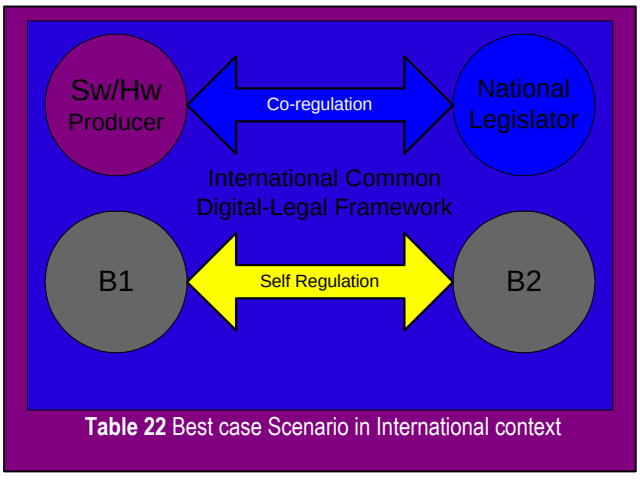

Table 22 Best case Scenario in International context

8. CONCLUSIONS: DIGITAL SELF REGULATION

I tried to explain how, in order to achieve digital self regulation, there is the need of:

a) a common legal framework, exceeding the limits of national legislation. A first step in this direction could be the co-regulatory approach chosen by the European legislator

b) open technology and ergonomic IT solutions in order to allow self-regulation.

The problem is that open technology is a better business only in the long run. Monopolies still score better !
Legislator is tinkering. Legislation is still not enough supporting open technology.
Anyway, I do not believe that there is no market for electronic signatures, as some say. On the contrary: applied cryptography is the essential technical answer to IT security. Only, it is not already properly linked with services

like URL identification, personal identification, corporate identification, and it is not efficiently (nor ergonomically) linked with IT products, like browsers and operating systems (the PABX syndrome).

I believe it is more correct to say, that there is no legal framework for any kind of self regulation in the (inherently international) cyberworld. So, why should a user ever desire an electronic signature, if there is nothing trustworthy to sign and nobody to trust? The best security solution is to avoid participating to such an insecure game.

The European Directive on Electronic Signatures and the European Standardisation processes are setting a landmark change towards self-regulation in a defined common legal framework. The impact can be so huge, that we should already consider how to improve such a regulation.
If such co-regulative approaches succeeds, electronic signatures will become as common as the handwritten ones. In fact, the PKI security infrastructure has been build, but

- it is not already integrated with the needed innovative services and
- it is not already integrated with any of the tools we daily use (PCs, PDAs). Mobile phones score better, but no real success story is already there. The area AA of EESSI is presently dealing with the integration of signature creation devices in existing devices that are fit to sign and to provide authentication.

One more reason why electronic signatures, as conceived until now, were not a success, is that the idea behind them is still far away from human ergonomics. I mean that too much security, might also degenerate into insecurity. Today we sign only relevant transactions and, if not made in cash, even payments.
Many have tried to convince their customers that they need the digital signature. But to which purpose ?
If people will be asked to digitally sign all kinds of transactions, from a taxi call to a life insurance, at the end their (digital) signature become meaningless. To sign will no longer have a warning function.
I believe that while enhancing our freedom, IT should also make us free to have security, despite not signing any transactions at all (or just very few of them).
We should also be allowed to execute verbal agreements in the Internet transactions. Who is providing us such a technologic solution ? Who allows us to have proper reliable documentation about a message sent via email, without having to digitally sign it?
We need to manage all our on-line identities. Who is providing an ergonomic solution for this?

I see that documentation, data storage, data protection, legal and technical security will be an underlying infrastructure. Just as they are today in verbal transactions, using a credit card: they will be a feature of a service provided by a trusted third party (credit card companies would love to be such a trusted third party, but it is still unclear whether or not they have the proper trust of their customers).

Such a trusted third party, could be a service provided by professional E-Witnesses, and for a good reason: because the witness was existing at the beginning of any legal civilisation, even before written law and signatures.
Who is providing a solution for this ?

In such an anarchic context, where still self-enforcement prevails over self-regulation, I looked at IT (security) providers and felt uncomfortable. On the one hand, they were fighting to hold their monopolies, defending their right to hold on proprietary solutions, by imposing them as the only available technology (despite cumbersome and not ergonomic); on the other hand, by asking users to trust them, to believe that a “digital pen” is enough security. I saw people armed with swords, asking other people to trust a pen ! Now the sword-holders are disappointed. Maybe they did not notice their own sword, but customers did.

Let’s try the possible, instead of marketing the impossible.
This is why we convened here all together.
The organisation asked me to remind you: “Please, leave your swords at the cloakroom”.
Here I show you my pen. Let’s share the knowledge !

RICCARDO GENGHINI
CHAIRMAN OF CEN/ISSS WS E-SIGN