Journal of Information, Law and Technology

A Code of Practice for the Globalisation of Electronic Commerce and Government

Fernando Galindo
Professor of Philosophy of Law
University of Zaragoza, Spain
cfa@posta.unizar.es <mailto:cfa@posta.unizar.es>

This paper was presented at the 20th IVR World Congress, Amsterdam, June 2001

This is a **commentary** published on: 22 March 2002

Citation: Galindo F, 'A Code of Practice for the Globalisation of Electronic Commerce and Government', Commentary, *The Journal of Information, Law and Technology (JILT)* 2002 (1). <http://elj.warwick.ac.uk/jilt/02-1/galindo.html>

1. Introduction

This paper presents a code of practice for e-commerce and e-government. This code is the result of a project undertaken to apply the concepts of the communicative philosophy of law in order to frame criteria by which competent institutions may assess the appropriateness of solutions applied to disputes in those fields of activity that have come to be known as electronic commerce and government, meaning financial and administrative transactions entered into using telecommunications systems[1]. Insofar as it performs this function, the code proposes an appropriate mechanism for the resolution of problems originating from the spread of the globalisation phenomenon through tools such as the internet. It is also intended to uphold respect for democratic principles in the regulation of e-transactions.

The code is not solely a regulatory proposal, however, but has its own institutional legitimacy, having been designed by a not-for-profit association formed by private citizens, companies and public institutions.

The efficacy of the code is guaranteed by an organisation set up to enforce compliance and sanction breaches of its rules. This organisation is an independent institution taking the form of an e-commerce guarantee agency, which will act in consort with the existing mechanisms of the democratic State for out of-court dispute resolution.

The code, guarantee agency and out-of-court mechanisms are accepted as an appropriate self-regulatory framework by all parties who may adhere to these arrangements as a secure way of carrying out e-commerce and e-government transactions with other individuals or organisations.

In the absence of the international legislation and institutions that would ideally provide the mechanisms to create the legal framework for the resolution of disputes arising from the spread of electronic transactions, the key to the initiative presented is that its action is grounded in respect for the law, for democratic principles and for the values and beliefs proper to the wide range of cultures that co-exist in the free society.

As this paper will show, this attitude differs markedly from the stance adopted in the self-regulatory initiatives that have until now taken shape in the internet. Traditionally, such initiatives have sought to base the legitimacy of the solutions proposed in response to the tensions generated by the roll-out of e-commerce and e-government on compliance with industrial standards designed ad hoc as the internet has grown or, since 1992, those imposed by a commercial enterprise: Network Solutions Incorporated. This company, which is now a part of VeriSign, has transferred its exclusive hold over admission to the internet to framing the rules by which admission is granted in a context where enterprises, citizens and institutions of all kinds are now active on line.

Section 2I of this paper will present a general outline of self-regulatory initiatives based exclusively on technical developments or the application of market rules, followed in Section 3 by the key principles underlying the e-commerce and e-government code

proposed, as well as the organisations involved in its preparation and application. Section 4 refers to the underlying principles and methodology developed by the philosophy of law, on which the Code and its institutions are based. The conclusion to the paper is contained in section 5.

2. Technical Initiatives

2.1 Self-regulation on the Internet: An Overview

The development of the network that would come to be known as the internet came about in US universities, companies and defence agencies during the 1960s, as a result of the work of computer scientists and researchers on projects forming part of the programmes launched by the Advanced Research Projects Agency (ARPA, itself a part of the Defense Advanced Research Projects Agency). Their research papers and projects already included the concept of self-regulation, meaning the acceptance of a succession of agreed rules for the operation of the network, which were proposed, developed and accepted by the various communities of developers and users [2]

This understanding was mistaken from a legal and political point of view, because the developers and researchers involved always lacked sufficient authority or power to establish rules ex natura or per se for the development of a resource such as the internet. In point of fact, the pioneers of the internet made up the rules for its operation as they went along within the framework of the projects that United States government commissioned, either through the Department of Defence or through the Education Department, from the companies and Universities involved in the development of what computer scientists initially called the Galactic Network[3].

It is therefore an incontrovertible fact that the US Government has played a key legal role in the birth and spread of the internet, as well as being the initial driver behind the development and testing of its rules of operation.

It is in this context that one must understand the active co-ordination role played by the US Government since the end of the 1990s, by which time the internet had spread internationally, and the scope and sophistication of applications had increased considerably. This coordination function is needed. It is a response to the fact that the internet is no longer a Galactic Network permitting the military or researchers to send and receive messages worldwide, but has become an effective tool for action in the fields of electronic commerce, democracy and government with global reach and consequences. This situation clearly requires new guidelines and practices for the use of the internet.

The key issue at stake here is that the ad hoc regulatory practices developed over time for the operation of the early internet were taken up in 1992 by a private company, Network Solutions Incorporated (NSI) as a precedent for creating a basic ad hoc rule for the award of domain names, an essential mechanism for the use of the internet, in consideration of an annual subscription fee. This rule thus establishes priority in favour of whoever pays the subscription or applies for the use domain names, regardless of any possible industrial

or intellectual property rights that the applicant may or may not have over the domain name.

The need for a change in regulatory practice was recognised, in view of the difficulties it caused, in a US Department of Trade White Paper issued on 5‘h June 1998[4], which noted considerable pressure for change from many quarters:

> •’There is widespread dissatisfaction about the absence of competition in domain name registration.
>
> •conflicts between trademark holders and domain name holders are becoming more common. Mechanisms for resolving these conflicts are expensive and cumbersome.
>
> •Many commercial interests, staking their future on the successful growth of the internet, are calling for a more formal and robust management structure.
>
> •An increasing percentage of internet users reside outside of the U.S., and these stakeholders want to participate in internet co-ordination.
>
> •As internet names increasingly have commercial value, the decision to add new toplevel domains cannot be made on an ad hoc basis by entities or individuals that are not formally accountable to the internet community.
>
> •As the internet becomes commercial, it becomes less appropriate for U.S. research agencies to direct and fund these functions.’

In view of the significance of developments, the increasingly pro-active stance adopted by the US Government in recent years (since 1998) is understandable. Intervention has consisted in attempting to resolve the problems mentioned in the white paper by explicitly recognising the regulatory role and instigating a complex process to transfer the management of the network, and particularly the Domain Name System, to a group of enterprises and institutions acting as the administrative registration entities for high-level domains (i.e. .com, .net and .org), which are by far the most numerous groups[5], allocated by the Internet Corporation for Assigned Names and Numbers (ICANN), the organisation recognised by the US Department of Commerce for technical domain name system management. ICANN is discussed in more detail in the following section.

It should be noted at this point, that these companies and institutions act in concert with the Central Domain Registrars, and with other companies and public or private organisations responsible for the administrative registries of existing high-level (.com, .net, .org, .edu, .gov, .mil, etc.) and country (.es, .be, .de, etc.) domains.

The first step toward change was taken on 25th November 1998 when a Memorandum of Understanding was signed between the United States Department of Commerce and ICANN, the new institution formed from the coalition of technical and business organisations that had run the development and spread of the internet until that time[6].

This agreement is a consequence of the US Government's recognition of ICANN as the most appropriate organisation to act as the agent of change, in view of its membership and functions. In accordance with the Memorandum of Understanding, ICANN is responsible, among other matters, for technical standardisation and supervision of the action of the companies and institutions responsible for the management of the Domain Name System.

2.2 ICANN

As defined by ICANN itself[7], it is a 'non-profit, private-sector corporation formed by a broad coalition of the internet's business, technical, academic and user communities'.

It has been recognised by the Government of the United States 'as the global consensus entity to coordinate the technical management of the internet's domain name system, the allocation of IP address space, the assignment of protocol parameters, and the management of the root server system.'. Its mission is to 'operate as an open, transparent and consensus-based body that is broadly representative of the diverse stakeholder communities of the global internet'.

ICANN's first objective is to bring about change in the internet's present technical management system, created by the US Government, in order to produce a new, privatised and internationalised system. The Chairman of ICANN's Board is Vinton Cerf, Vice President of Internet Architecture and Technology for WorldCom, who is regarded as one of the fathers of the internet. The remaining Directors (in total 19) were appointed by specialist internet organisations, discussed below, or were chosen in open election, online elections held worldwide. The role of elected Directors is to represent internet users from each continent. The shortlist of candidates for election was prepared by ICANN on the basis of their technical qualifications[8].

ICANN builds consensus through the action of the Board of Directors and the work of its three supporting organisations: the Domain Name Supporting Organisation, the Address Supporting Organisation and the Protocol Supporting Organisation. These bodies represent a broad consensus of business, technical, academic non-commercial and internet user communities.

ICANN is an organisation responsible for technical co-ordination and, accordingly, its mission does not consist of running the internet. Its duty is rather to oversee specific managerial and policy development tasks requiring central co-ordination, such as the assignment of the internet's unique name and number identifiers. In the area of domain names, it functions through the central and administrative registries and the territorial domain registries.

To complete this description of ICANN, let us remember that two earlier attempts to implement a system of this nature failed, overtaken by the speed with which events unfold on the internet. In 1987, the US Government ceded the organisation and governance of the internet to the National Science Foundation, and in 1992 this body in turn partially transferred registration, co-ordination and high level domain name system

(.com, .org and .net) maintenance functions to Network Solutions Incorporated, the private company mentioned above. The effects and negative consequences of these initiatives still persist and were the reason why VeriSign purchased NSI, which retains its monopoly hold over the .com, .net and .org domains, in 2000. These monopolies will not lapse until 2007, 2006 and 2002 respectively, in accordance with the agreements entered into by ICANN and VeriSign in March 2001.

2.3 Normalisation

In view of the foregoing, it appears that concrete progress has at last been made, at least in the form of a declaration of intentions in areas as sensitive to the internet as the registration and management of domain names, self-regulation under the terms of the Memorandum of Understanding made between the US Government and ICANN, and the functioning of the latter as a corporation subject to US law.

Nevertheless, one cannot fail to recognise the future hazard represented by VeriSign's takeover of NSI. The replacement of NSI means that the poor practice of the administrative registries recognised by ICANN criticised by the Department of Commerce in the White Paper of 5th June 1998 will persist for some years to come (until 2007) in the domains with the most numerous registered names. This is because the practices criticised were in large part those of NSI, and they persist in the current practice of VeriSign and the new administrative registries that provide access to high level domains.

The codes governing the practices of these organisations provide ample evidence for this, being anchored in rules derived from the 'first come first served' principle applied to the management of internet domains by NSI, under which it is sufficient to have made the first downpayment to gain a privileged position to use the name. The failure of the administrative registration agency to require proof of applicants' rights over domain names is consistent with this principle. Moreover, both the administrative and central registrars claim exemption from any liability, thus remaining free from any obligation to withhold or refund application fees and annual dues for the upkeep of domain names paid by users[9].

As a consequence of these practices, the promise of self-regulation far from becoming a reality has remained in the grip of one party, as has been the case since 1992, which is able to impose on all others a series of conditions created ad hoc from a position of monopoly power. This clearly shows the weakness of the organisation set up by ICANN with regard to the regulation of e-commerce, e-government and electronic democracy. It is these weaknesses that recommend the creation of the mechanisms, organisations and instruments described in the following section.

3. The Code of Practice

3.1. Introduction

As we have already seen, the internet's early history of develop in academic, military and industrial research carried out in the United States during the 1960s had a marked impact on the initial characteristics and common culture of the network. ICANN itself is a direct product of this tradition. Now that internet use has spread to citizens all over the world, however, it has become necessary to progress further with the construction of a culture that takes the use of the network by a diverse community, rather than narrow academic, business or military interests into account. The whole of society now has a stake in the operation and governance of the internet. Naturally, domain names, the main field of internet regulation, will remain an area of regulatory concern, but it has now become necessary to safeguard other rights such as data protection, ensure implementation of reasonable commercial practices, oversee internet content and establish dispute resolution mechanisms, to give but a few examples.

This is the context of the organisational and regulatory framework outlined in this section, which is representative of the will and opinion of citizens and social organisations. This organisation, which was established in April 2000 under the name APTICE (Asociaci6n para la Promocidn de las Tecnologias de la Informacidn y el Comercio Electr6nico - Spanish Association for the Promotion of Information Technologies and E- Commerce), has drawn up its own code of practice and implemented it through the creation of an independent institution, AGACE (Agencia para la Garantia del Comercio Electr6nico Agency for the Guaranteeing of E-Commerce).

3.2 The APTICE Association: Membership

The Association for the Promotion of Information Technologies and E-Commerce, (APTICE: (www.aptice.org) was founded in Zaragoza, Spain, in April 2000.). The association currently has 83 members comprising private individuals, enterprise (telecommunications companies, banks, communications media, etc.) and public institutions, and is the fruit of a year-long period of debate and preparation by its founders (individuals, businesses and the Aragonese Development Institute, an independent government agency). APTICE reflects the conclusions reached from the joint R&D activities undertaken at the University of Zaragoza by companies and research teams, mainly associated with the Philosophy of Law Department.

APTICE is currently engaged in building a network in various European countries together with interdisciplinary teams in universities and with the co-operation and assistance of private enterprise and public institutions. Its key achievement to date has, however, been the creation
of a Code of Practice and a quality seal organisation, AGACE (Agency for the Guaranteeing of ECommerce), which is responsible for implementing the code and spreading its use.

We shall concern ourselves with the latter two issues in the next section.

3.3 The APTICE Code

APTICE has framed its code of practice/conduct for e-commerce and e-government in consultation with all of its members. The code was thus drafted in a spirit of consensus. The quality seal and guarantee infrastructure created in parallel with the code are charged with its implementation using the organisational machinery specifically designed for that purpose, which is embodied in the AGACE Agency

The Code of Practice[10] is intended to provide a self-regulatory tool for the use companies and public institutions in their relations with users, whether be citizens, other businesses or government agencies carrying out electronic transactions with subscribers. The code has been prepared on the basis of prevailing legislation in Spain and the European Union, taking into consideration the practices required by other similar codes worldwide, expert opinion on the issues involved and the experience of companies operating in the e-commerce industry.

The aim of the code is to improve the quality of services offered through the websites of organisations conducting e-commerce and e-government operations, thereby fostering consumer and business confidence, and trust in government agencies, which have increasingly turned to the internet as a means of communicating with the citizen. A further aim is to establish a channel for handling the complaints and disputes that may arise through an out-of-court dispute resolution system.

To achieve its purpose, the APTICE Code of Practice contains seven general principles covering the key elements for building trust between the parties entering into on-line transactions over the internet and defining service quality and improvements needed in the activities and internal procedures of businesses and public institutions. These principles are as follows:

Principle #l: Identification of the Organisation.- In accordance with this principle, any organisation subscribing the APTICE code of practice must provide sufficient activities regarding its nature and activities in its web pages. The organisation must also comply with the domain name requirements established by the internet's central domain registries and with registration requirements established by legislation governing intellectual and industrial property. The future need for the use of advanced electronic signature systems and server authentication certificates is also provided for, as well as monitoring of legislation applicable to the establishment and its commercial activities.

Principle #2: Guarantees concerning claims and performance.- This principle requires that key commercial information (e.g. prices, delivery conditions, product descriptions, warranties, and many others) be displayed in the web site, together with instructions and procedures for carrying out on-line transactions, customer service details, and information concerning logistics, usability of web pages and contractual and extra-contractual liability.

Principle #3: Security and technology infrastructure.- This establishes mandatory security policies for subscribing organisations.

Principle #4: Data protection.- This principle requires organisations subscribing the code

of practice to comply fully with the Spanish Data Protection Act.

Principle #5: Content quality.- This centres on issues such as the organisation of illegal and offensive content, the protection of children and advertising practices.

Principle #6: Rules for out-of-court dispute resolution: The APTICE code of practice categorically requires subscribers to adhere to out-of-court dispute resolution systems. In principle, these would be bodies such as Consumer Arbitration Tribunals (business to citizen relations) and Chambers of Commerce (business to business relations). The intention is to ensure that any possible dispute that might arise between a company or public institution and customers (be they private individuals or other legal entities) is resolved as quickly and smoothly as possible, without the need for action in the courts, which are not sufficiently adapted to the exigencies of the new technology industries. APTICE will act as a mediator in disputes, which it will seek to resolve amicably or by referring cases to the most appropriate arbitration tribunal in the circumstances.

Principle #7: Requirements for the implementation of the APTICE Code of Practice.- This principle establishes the requirements that must be met by a company or institution intending to implement the code. These requirements refer, in particular, to the preparation of procedures manuals and records in accordance with the instructions provided by the institution or agency responsible for the performance of Code compliance audits. This principle will therefore allow auditors accredited by APTICE (to date only AGACE is an accredited auditor) to carry out appropriate procedures to examine the activities of an organisation and assess its compliance with the rules enshrined in the code of practice and, accordingly, its readiness to receive the award of the quality seal. Principle #7 also includes the sanctions mechanism established for cases of non-compliance by any subscribing organisation with its obligations upon accepting the code of practice as a guide for its own conduct.

The enumeration of these principles brings us to the need for a mechanism to implement the code of practice. This mechanism is now in place and comprises the quality seal and the organisational structure for its implementation. This infrastructure goes under the name of AGACE (Agency for the Guaranteeing of E-Commerce).

3.4 Guarantee Agencies

For some time now, it has been clear that the practicalities of the internet require the existence of specialised services, known as quality seals[11], to underpin the reliability of on-line transactions. Seals thus cover a different range of issues from guarantees referring to the identity of the parties entering into electronic transactions and the security of the messages exchanged between them. In view of the similarity of the goods affected, it seems appropriate in terms of the European legal tradition for such services to be able to guarantee both public and private operations.

Such services are already being implemented through initiatives such as TRUSTEE[12] which concentrates on compliance with data protection regulations, BBB on line[13], which is concerned with on-line trading practices, and Web Trader[14], which designs

codes of practice for on-line businesses.

The AGACE[15] e-commerce guarantee initiative bears a certain similarity to the above initiatives, but differs in that it is concerned with the various aspects of reliability and trust taken as a whole. Accordingly, the AGACE seal will be awarded only to those e-commerce and e-government activities that demonstrate compliance with the requirements of the APTICE code of practice, as described above.

AGACE has only recently commenced its activity, having carried out pilot consultancy work in the fields of e-commerce and e-government.

AGACE is at present a fully integrated division of APTICE, charged with the performance of compliance audits in connection with the Association's code of practice. In the coming months, however, it is planned to incorporate AGACE as a separate entity from APTICE with its own legal personality.

AGACE is currently formed by a team of legal professionals, computer scientists and economists specialising in the new technologies, who are responsible for the audit of organisations applying for the agency's e-commerce and e-government quality seal accrediting compliance with the APTICE code of practice.

In view of the above, we may then conclude that the functions and norms described in this section differ significantly from the ad hoc rules applied by the companies and institutions recognised by ICANN, which were discussed in the preceding section.

4. Philosophical and Legal basis of the Code

The discussion so far clearly shows the need for the process of self-regulation set in train by the US and European authorities and for the framing of rules in the form of codes of practice for companies, public institutions, organisations and citizens using the internet in the context of the existing situation, which has given preference to technical bodies such as ICANN. In this light, it may be considered appropriate for specialists of philosophy of law to consider the self-regulation process and make their own proposals, such as those indicated above. This is, of course, nothing new. Since the Renaissance treatises on natural law, it has been the mission of the discipline to debate and propose the conceptual framework on which systems and procedures capable of generating legal rules should be based, as well as studying regulatory and self-regulatory processes and the rules and codes drawn up.

The philosophy of law is, then, under the obligation to make concrete regulatory proposals. This is especially so now, since it came to be understood with the rise of theories on legal argument in the second half of the 20`h century that one of the main fields for the discipline is the study, review and formulation of the basic arguments applied in the activity of legal professionals working within the framework of the, currently numerous, institutions with normative powers[16].

From a philosophical point of view, the key questions are those already mentioned in this

paper. To what extent is the self-regulatory process in the internet a reality and what are its limits. What are the rules that express such self-regulation? What are their limits? What are the alternatives to the self-regulatory process and to codes of practice? This paper has tried to provide some concrete answers to these questions.

5. Conclusion

On the basis of the discussion set out above, it may be possible to provide an answer to the question inherent in the title, which might be expressed as agreement with the need for codes of practice in the internet; but what codes?

A tentative answer could be that codes are needed provided they are consensus-based and, as a rule, involve all parties concerned and not just the technocrats.

The example presented is proof that this is possible. It is the result of a regulatory process concerning the internet in its existing form undertaken by a significant number of different individuals and entities and implemented taking account of the rules and procedures approved by the democratic state, in a similar manner to the legal and extra-legal practices employed in dispute resolution.

The solution consists of establishing independent mechanisms and instruments that are representative of citizens, business interests and public institutions, have sufficient regulatory capacity, and, of course, are fully compliant with existing law. These structures comprise a democratic organisation and code which is consistent with the law and, naturally, with the principles for action propounded by the communicative philosophy of law.

Footnotes

1 The philosophical and legal foundations for this paper are set out in: GALINDO, F, La puesta en prdctica de la regulaci6n de Internet por la Filosofia del Derecho comunicativa ('Practical regulation of the Internet in accordance with the communicative philosophy of law'), to be published shortly in the Proceedings of the World Philosophy of Law Congress held in New York in 1999.

2. This explanation is based on the version of events set out in LEINER, B., CERF, V. G., CLARK, D., D., KAHN, R.E., KLEINROCK, L., LYNCH, D.C., POSTEL, J., ROBERTS, L.G., WOLF, S., Una breve historia de Internet, published by the Asociaci6n de Tecnicos de Informatica (Spanish Computer Science Association) in February 1999, as translated from the original English, which appeared in the May-June and July-August 1997 editions of the Internet Society journal On the Internet.

3 'In the past, many of the essential technical coordination functions of the Internet were handled on an ad hoc basis by US government contractors and grantees, and a wide network of volunteers. This informal structure represented the spirit and culture of the research community in which the Internet was developed.

<http://www.icann.org/general/fact-sheet.htm>, consulted 22nd September 2001.

4 <http://www.icann.org/general/white-paper-05jun98.htm>, consulted 22nd September 2001.

5 A few figures. At 7th September 2001 the numbers of names registered in key domains are: 22,373,097 .com; 4,244,092 .net; 2,688,657 .org. A total of 36,114,885 domains names of all kinds have been registered. These data were obtained from <http://www.netnames.com>.

6. <http://www.ntia.doc.gov/ntiahome/domainname/icann-memorandum.htm>, consulted on 22nd September 2001.

7. <http://www.icann.org/general/fact-sheet.htm>, consulted 22nd September 2001.

8. <http://www.icann.org/committees/nomcon/>, consulted 22nd September 2001. Criteria for candidate selection: the potential candidate must have... a 'reputation for integrity and hard work; ability to exercise independent judgement [and] willingness to disclose obligations and potential conflicts of interest; professional/volunteer roles and accomplishments; understanding of the internet's architecture and history; experience with the internet's architecture; specific experience in international and/or multicultural environments; educational background; [bring] relevant skills or experience that are otherwise absent from the ICANN Board; commitment, available time, energy and interest; [and] indications that the individual will find broad support in the At Large Membership.'

9. See an example of these practices in: <https://secure.nominalia.com/01/dna.addd.intemic.php>, consulted 30th September 2001.

10. The full text is available in <http://www.agace.org/en/index.html>, consulted 30th September 2001.

11. It is common for standards agencies to award seals to companies manufacturing products or providing services subject to accepted quality standards. See: MOLES I PLAZA, R.J., Derecho y calidad. El regimen juridico de la normalizacion tecnica, Barcelona, Ariel, 2001, p. 29.

12. <http://www.truste.com/>, consulted 30th September 2001.

13. <http://www.bbbonline.com, consulted 30th September 2001.

14. <http://whichwebtrader.which.net/webtrader/>, consulted 30th September 2001.

15. <http://www.agace.org acge.ore.org>, consulted 30th September 2001.

16. It is proper to the communicative philosophy of law to formulate and propose the

main arguments at the centre of legal debate, whatever their nature. The content of such discussions today frequently concerns the organisation of communications infrastructure. This is particularly so when the subject of debate is the use of codes of practice to regulate basic behaviour. And this is the case with the internet. The communicative philosophy of law is thus concerned with framing criteria and designing organisations capable of fostering the participation of the parties involved and the search for consensus as a basic principle for equitable treatment in the legal systems of democratic society. The foundations of communications theory on which this research is based are set out in GALINDO, F., 'The communicative concept of law', in ARNAUD, A.J., CHIBA, M., (eds.) Legal concepts in cross-cultural perspectives. Journal of legal pluralism and unoffcial law, vol. 41, 1998, pp. 111-129. The expansion of the functions of the philosophy of law with reference to examples of legal activities carried out with the aid of computer technology is discussed in: GALINDO, F., Derecho a Informdtica, Madrid, La ley-Actualidad Juridica, 1999, see particularly p. 23 in this regard. For a presentation of Spanish internet regulation from the point of view of communications law, see: GALINDO, F., 'Le droit de]'internet en Espagne', in VIER, CH. (coordinator.), L'Internet et le Droit, Paris, Legipresse, 2001, pp. 115-125. A first approximation to the subject of this paper is to be found in: GALINDO, F., 'Public Key Certification Providers and E-government Assurance Agencies', in TJOA., A.M., WAGNER, R.R. (eds.), 12th International Workshop on Database and Expert Systems Applications, Los Alamitos, IEEE, pp. 345-349.