

V Jornada Anual del

FORO DE LA

GOBERNANZA DE INTERNET

EN ESPAÑA

27 a 29 de Mayo de 2015
Madrid

Organiza



Con el apoyo de



Coordinan



Colaboran



www.igfspain.com

#igfspain

Table of contents

Critical Internet Resources	1
Messages from the forum.....	1
Regulation and cybersecurity	3
Messages from the forum.....	4
Privacy and surveillance	6
Messages from the forum.....	6
Identity of children.....	8
Messages from the forum.....	8
Intellectual Property policy	10
Main messages from the forum	10
Other messages	11
Open Internet and Net Neutrality.....	12
Main messages from the forum	12
Internet Economy. Innovation and entrepreneurship	14
Messages from the forum.....	15

DRAFT

Critical Internet Resources

Critical resource supervision is one of the key elements to guarantee that the Internet keeps functioning as we know today, one global space with identifiers and unique addresses in the whole space, standards, etc. 2014 and 2015 are being especially intense in the sphere of these critical resources. ICANN, the international private organization in charge of its management under the supervision of the American Department of Commerce (DoC), is going through a deep change. The limitations in the management model of critical Internet resources have been evidenced along the years when distrust and suspicions among the stakeholders have become more obvious. Revelations in 2014 coming from E. Snowden over security in the Internet are the last elements that contributed to the start of these changes in the management model of the critical resources.

With the transition of functions from ICANN to IANA, the US Government is trying to achieve some basic objectives that consist on supporting a multistakeholder model that guarantees Internet openness as well as security and satisfies the needs of the users of the services of the 'new' IANA (IANA is currently an autonomous organization assigned to ICANN). In this moment, the debate of the changes that will have to take place in order to change the management model to a multistakeholder one that controls the critical resources is taking place.

The different countries stand up for the necessity of finding the way of providing the governments with a more significant presence in the governance of the Internet, much further than the current Governmental Advisory Committee of ICANN in which the different governments are represented. Other countries have been supporting multilateral models as the one used in the International Telecommunications Union (ITU) to manage these critical resources. After the last NET Mundial conference in Brazil in April 2014, the means to achieve consensus in the community to find a path towards transition of ICANN's most critical functions were reinforced, although this process is not free of obstacles and is taking more time than expected. The window initially established by the NTIA to perform the transition of ICANN's function to IANA expires in September 2015. The NTIA has already announced, that is it necessary the window will be extended until the community finds the most satisfactory model

Messages from the forum

On the political nature of some technical functions carried by ICANN.

- The importance of the management of critical resources that ICANN makes contrasts dramatically with the little knowledge that the vast majority of Internet users have of this body and its functions.
- The technological complexity of these functions, and the complexity related to the working mechanisms, timing and decision making, the fact that English is the dominant language and the high dedication required

hampers the possibilities of participating in the decision-making processes.

The political dimension of ICANN is also evident in the difficulties to modify the terms of the special relationship that has until now maintained with the US government.

- The Internationalization of ICANN and the withdrawal of US tutelage performed by the NTIA on the IANA functions will be carried out according to a set of principles, among which is the desire that the multistakeholderism and participation be strengthened.
- This Process is positive both, for its symbolic character as the gains in terms of openness, internationalization and participation
- Talking about multistakeholderism it is worth noting the difficulties in defining what is meant by the "multi-stakeholder" participation, since not all the parties involved or affected by ICANN decisions have equal chances to influence or participate in decision-making processes.
- Some civil society organizations have great difficulty to be represented in the ICANN process and face significant costs to assert its voice in this forum
- Willingness of the US government that this transition process by which ICANN's termination does not involve ownership or excessive influence by other actors, and especially of other states. One way or another, the US government will continue for some time an ascendancy and influence over ICANN, but not so formalized as heretofore has had.
- The transition drafts have circulated so far seem to adopt a conservative character, with which ICANN seems to "shielded" from different influences of the US government.

Full support of the transition process round table, putting focus on the great challenges both to keep it running what until now has done reasonably well for the world, as to make the model participation in the management is done in accordance with new parameters to provide more legitimacy in terms of representativeness and accountability.

Regulation and cibersecurity

In the digital ecosystem security is a key issue. Internet governance in this area has advanced in recent years at international level. There is a growing concern on the part of the community by the system dynamics and the continuing challenges in this area. Cyber-attacks are becoming more intense with a greater magnitude and complexity. The impact of these new cyber-attacks is often greater and more dangerous attacks than traditional risk because the damage they can cause is huge and vulnerabilities of the infrastructure or resources are not as visible.

Internationally, the origin of the attacks is often in the states themselves, for example, the cases of China and Russia, or other Western governments, or the US, as the revelations of Snowden revealed.

Another of the trends is the professionalization of cybercrime. In 2014 there have been identified criminal organizations that have found space on the network to commit their crimes. Internet does not set boundaries and in these criminal organizations it is common that individuals who are in different parts of the world work together. The most extreme claims in social groups have also found its place in the network, hacktivists, some linked to groups like Anonymous, perform their actions in cyberspace which in turn serves as a platform to attract new members and propaganda.

In Spain the Red.es and the National Cyber Security Institute Spain (INCIBE) agency analysed in different studies during 2014 and 2015 incidents and trends in this field in Spanish homes. Among the most common incidents in this area include unauthorized access. Situations of fraud over the Internet are also very common. However some safety measures such as using antivirus programs is widespread in homes, and Spanish citizens are beginning to show a growing interest in Internet security. The confidence of Internet users in Spain is high even though almost 13% of respondents express users have little or no confidence in the Internet.

Certain network services, such as banking and electronic commerce are outstanding examples of best practice in security applied by the Spanish users in 2014. The most prominent advocacy by users is spam or unwanted email, a situation that affects all kinds of Internet devices (PC, Smartphone, Tablet), as reflected by recent studies.

In the field of Public Administration and large companies 2014 it was a particularly busy year in attacks on Information Technology and Communications (ICT) from governments, public administrations and companies with high strategic value. This form of cyber espionage, along with cyber terrorism and organized cybercrime are new threats to Spanish society and the trend is clearly strong growth in recent years. 2014 was particularly strong, as indicated by studies of CEN-CERT (attached to the Spanish National Intelligence Center). Also, industry and operators of critical infrastructure in the country have suffered cyber-attacks increasingly complex over the last year.

Regulatory responses to cyber security vulnerabilities are continuing, although it is difficult to anticipate emerging challenges. In the European Union (EU) in September 2014 a new Regulation No. 910/2014 on electronic identification and digital trust it is approved. Other actions are in process during 2015 a proposal for a new Directive to guarantee a common level of security of networks and information within the EU or new regulation on the protection in the processing of personal data and circulation.

In Spain there are several bills in place since 2014, and the draft Organic Law of National Security or the draft amendment to the Criminal Procedure Law and the draft Law amending the Criminal Code.

Technological trends have varied widely during 2014 and remain so in 2015. These include the use of smartphones as proof of identity, the increasingly widespread network access anonymously, hiding the identity of the origin and destination communications, and it has also extended to the case of service providers. Other developments such as the use of cryptography, encryption in the cloud, routers, proxies and opaque specific browsers located in countries with a permissive legal environment complicate the work of the security forces to hamper traceability. The deep web is a space that offers many facilities to crime and concealment, which combined with their own forms of ecosystem as bitcoin virtual currency payment, even more difficult to control capital movements.

On protection and prevention strategy on cyber security public-private partnership remains essential. The involvement of end users is essential to maintain the confidence of citizens surfing the net. Harmonizing the legal framework globally on these issues is complex but essential and proper education of users, especially those training belonging to the most vulnerable groups.

Messages from the forum

- Various laws promote cybersecurity management at national, European and global level.
- The law should be developed in line with the evolution of technology, defining mechanisms acting against cybercrime but not at any price, as it should uphold the rights and values of citizens
- To carry out strategies to ensure the protection and safety time, financial and technological resources and human capital is needed. Although Spain has strategies against cybercrime, strategy is needed globally since there are no borders to cybercrime. Besides trying cybercrime globally, it is important that states are clear about the threats, the risks and opportunities that cybercrime poses, and to develop a well-defined strategy.
- The intention of the European Union to strengthen public-private partnerships, and facilitate the exchange of information evenly among the various relevant bodies in each member state, elected by the EU itself, in order to end the borders between Member States as regards to cyberspace. You cannot apply the same laws to the physical world to the

digital world and that there must be a change, in which you pass corrective legislation to preventive legislation.

- Regulation is necessary, but it is difficult to define a law for minors or adults, so that legislation for citizens and businesses due. It should seek a dynamic regulation, adapted to ongoing changes in technology, globally, not nationally. The current regulation safeguards some vulnerabilities, but certainly there is a change of mentality that requires a different approach than has been so far, which must be carried out with the help of companies and all areas, and that the state alone cannot yet being a very new and very big phenomenon.
- The legal operators have difficulties in implementing the various offenses because of their low technological training. However, a significant effort is being made so that there is a technological training of such operators.

DRAFT

Privacy and surveillance

Privacy is one of the most relevant topics of the subjects highlighted in the Internet Governance. The debate over this matter has been more alive than ever in 2014. Some of the questions have already been debated and are linked to massive espionage on the net. The most alarming cases for society have been the collaboration between democratic governments and private companies, especially in western countries.

In Europe the Court of Justice of the European Union published two rulings in April and May 2014 that have implied a significant change in the way of addressing the matter of the right to data protection. The first one supposes in practice the repealing of the 2006/24/CE Directive over data conservation of telecommunications while the second one is important because it establishes the Right to be Forgotten when the search criteria is the name of a person. The scope of both ruling is limited. However, in the European Union a new Regulation for Data protection is being debated and it will bring new aspects regarding this questions.

In Spain the legislation has tried to guarantee the private life of the citizens. Currently there are several on-going legislative initiatives that influence the protection of data. Some institutions as the Agencia Española de Protección de Datos (AEPD) have exerted a relevant role in 2014 in different lines of action including the training and exposure. In civil society, there have been several organizations that have developed an intense labour, for example in the guidance of children protection, users or professionals.

One of the main conclusions obtained in all of the Internet Governance Forums in 2014 was that privacy must be guaranteed to improve the confidence of the users and guaranteed safety. There are new opportunities appearing as the Internet of Things or the access to multiple devices permanently connected to the internet on the progress made in the treatment of information with Big Data that also brings new problems for security and privacy, as it already happens with Internet consent related to, in many occasions, the appearance of “free” apps and services directed to the users.

Messages from the forum

- First, the interventions of the States, as the Snowden case and the Court of Justice of the European Union ruling in the case Digital Rights Ireland have shown still constitute a threat for privacy. At both sides of the Atlantic, the random tracking and indexing of the whole population is generating a relationship of distrust towards the State regarding the guarantee of the rights.
- The second risk factor derives from the behaviour of the own user. While it is true that the legal information and privacy policies are not clear, it is not less so that the user already has enough evidence to be careful with its behaviour in the internet and the identification of trustable services. However, it does not seem that this is happening.

- Ethical and legal problems. It is considered to be necessary that companies take on ethical and legal compromises in order to guarantee privacy.
- The current regulatory framework is old, inadequate and also it is very difficult to apply. A new regulatory framework, designed for the current and future times is needed and should be based on flexible principles and should be possible to apply to the design of goods, products and IT services.
- A neutral technology was reclaimed. One in which it use guarantees the privacy and it is design the interaction between technology and rights yields positive results while being respectful to privacy.
- ICT can act as a catalyst of an improvement in democratic institutions and also in transferring ability, empowering the people through instruments of digital participation.
- The fundamental right to data protection and privacy can and must be one of the cornerstones that support our system of freedom in the Internet.
- The European system for privacy should constitute an opportunity of growth in a global digital market through an offer of services based on an offer of guaranteed privacy.

DRAFT

Identity of children

Every year more minors are connected to the Internet and they do so at earlier ages. In Spain, children start using ICT between their first and second year of life and it is lowering every year. The average time that young people spend in front of a screen, whether it is a computer, smartphone or tables is above 7 daily hours. Social networks have become a key tool for socializing among this public. External factors that minors find when accessing the Internet are very diverse and have consequences. How the access is done, the socioeconomic environment, the country, education system, etc. are all factors that influence that the use is mainly social and consumerist or has an educational and creative role. The possibilities of communications, to share interest and learn with other children or different people are enormous. Therefore, it is needed to guard the privacy, which is not always well managed by minors; from possible harassment that might surface.

Internet is an indispensable tool that new generations must learn to use smartly. The digital competences are not just instrumental, linked to finding a work orientation or leisure, but they must allow to improve the development of the personality, knowledge and a safe and creative use of ICT. It's a continuous and adaptive learning; indispensable to take advantage of the new possibilities associated to the digital ecosystem and their challenges in the evolution towards a new society of knowledge in the 21st century. Reinforcing the digital identity and education in values in the education centres is one of the remaining tasks. The use of the Internet as an educative tool with pilot programs developed by schools in Spain in 2014 by companies like Facebook for example, are a great starting point in that necessary evolution.

Messages from the forum

- An identity must be given to children and young people on the Internet in order to guarantee infancy protection
- Positive uses should be encouraged to maximize the benefits associated. The biggest risk is to waste the potential that ITC bring to the development of children.
- Perspective and agility to study, talk and regulate the detected risks and putting in place systems designed to protect. It is needed multidisciplinary specialized units with much more operative capabilities than current ones.
- There is a lack of solid studies in which all the parties are involved, including children, which allow a better, more solid decision-making.
- Competencies should be given to the main characters of change so they become the real builders of knowledge, capable of stabilising better relationships on the Internet and leading innovation in a workplace where they will join as digital natives.
- It is indispensable a new framework for digital competencies worth real applications.

- Health environment is a great channel for the prevention, study and help for children and young people.
- Technology evolves very quickly and has caused that the conclusions from previous panels have become obsolete.
- We are not ready to grow along children in their growth with technology. WE should insist once more in the need for training for parents and education professionals as the prevention and only way to pass on the positive values of network identity. This close groups are being joined by health professionals and this is great news because it is a natural prevention channel.

DRAFT

Intellectual Property policy

The questions regarding the rights over the contents and management of intellectual property in the digital ecosystem are an element of key importance in the debates over Internet governance.

The contents in the digital ecosystem are competitive elements on a global scale. Europe and Spain in particular must adapt to a new scenario, more competitive every day in the production, distribution and monetization.

Given the economic and strategic impact of knowledge and creative developments, progress must be made faster towards a Digital Single Market, as it is happening in other developed economies as the USA.

In 2014 and 2015 several milestones have been reached (legislative and strategic as well as in the jurisprudence), both in Spain as in the scope of the European Union and even further because the digital environment does not know of borders.

- In Spain, in 2014 a modification of the intellectual property law was passed. It tries to improve the defence of the intellectual property rights on the Internet, although it has caused different reactions and an important controversy between the addressees of the norm, which is still pending on development and an integral modification in the future.
- In the European Union, on May 6th 2015, the strategy over a Digital Single Market was released. It expects to, among other things, progress toward a better regulatory harmonization in the matters of intellectual property between the member states.
- At the same time, since 2013 the Transatlantic Trade and Investment Partnership (TTIP) is being negotiated and should be followed and examined to find in what measure does it affect the commerce of cultural products and digital content.

Main messages from the forum

The main message from the roundtable was a stake for the value of Author's Rights and Intellectual Property in the digital Environment, protecting the freedom of the author to decide what to do with its work, whether it is to spread it for free or to look for a profit.

Also there has been an agreement that the Digital Single Market is not just for Europe but also on a global scale and there should be a tendency to establish a level playing field for everyone because the problems and challenges presented globally must tend to have a global solution in order to be able to compete in equal conditions

In third place, it has been verified that ICT have caused a revolution that has not been totally perceived yet and it forces us to rethink intellectual rights and business models, being possible the coexistence of individual and collective management of intellectual property rights.

Other messages

1. The sector of contents and Internet are forced to understand each other.
2. Digital content is and will be one of the main forces driving growth of Europe's economy.
3. The cooperation between Ministries and Administrations is key.
4. Public-Private-Partnerships and sectorial auto-regulation is key because Internet cannot be regulated nor controlled by governments.
5. In the Digital Single Market the role of Europe and Spain in the future of the global environment is at stake.
6. It is needed a harmonized framework so competitive companies can emerge.
7. Geo-blocking measures harm the value chain of content.
8. New business models must be promoted, but Intellectual Property rights will stay as the cornerstone if we want to encourage and industry that gives employment to thousands of people.
9. We must remain vigilant of how the Terms and Conditions in the use of multinational digital platforms affect intellectual property rights.

DRAFT

Open Internet and Net Neutrality

Past February 26th 2015 the FCC redefined the Broadband Internet Access Service (BIAS) as a Telecommunications service under the Title II of the Telecommunications Act. The new regulation, widely defended by the Obama administration, expects to safeguard the essence of an open Internet and places the FCC in a best legal position to guarantee it, given the difficulties arisen in past years in which tribunals have considered that regulating Internet access services was outside of its competency scope.

The regulation establishes rules of no blocking no throttling, no paid prioritization and enhanced transparency of traffic management in the Internet access service, which apply both fixed and mobile networks.

Meanwhile, in Europe a Regulation for a Telecommunication Single Market is under development, which has already been amended by the European Parliament and is being debated in the Council. The text deals with diverse questions related to the open Internet and net neutrality, including provisions for specialized services.

The panel took place in the V Internet Governance Forum in Spain and it aimed at analysing the differences between the US and Europe in this case, and debate which were the main challenges that Europe must face in the short term, not just in the grounds of net neutrality but in order to safeguard the openness of the Internet as a whole.

Main messages from the forum

The messages that we would like to transfer to supranational forums, especially to the EuroDIG, which will take place on June 4th and 5th, 2015 in Sofia, Bulgaria, are:

- The concept of the open Internet is subjective and open for debate, but it must cover all aspects of the value chain of the Internet: from user terminals to networks, platforms and the information in the network.
- The protection of the open Internet must preserve the freedom of choice of the users and respect Human Rights (Freedom of expression and privacy) as well as encourage innovation broadly.
- In respect to access networks, the US case is very different from the situation in Europe, where there is a reasonable level of competition, especially at very fast speed access.
- In the case of Europe, the formula of well-executed competition and transparency can be sufficient in most of the cases to avoid *ex ante* regulation for net neutrality.
- In Europe zero rating rates represent a commercial formula in which operators do not receive any kind of compensation from managing the data traffic –included in this formula- consumed by the clients. In this sense, there are many differences between countries in Europe and developing countries: for instance, in India, the use of these schemes is

generating an intense debate because of the effect it may have on freedom of speech.

- Regulation, neither in the US nor in Europe, has been able to address the similarities between electronic communications networks, managed by operators, and content distribution networks, (CDN) used by other economic agents that intervene in the Internet value chain, which is generating asymmetries.
- Europe needs to tackle the problem of Internet openness as a whole, with a review of sectorial regulation to study what aspects need to be protected through sectorial regulation and which ones should be covered with a horizontal scope.
- Innovation that has allowed the Internet until this point must be taken into account while the decisions are being made facing the review of the regulatory framework, given the difficulty to generate start-ups in Europe compared to other regions as the United States.

DRAFT

Internet Economy. Innovation and entrepreneurship

The economic environment has been deeply transformed by the digital ecosystem. In this digital revolution, the Internet Governance develops a valuable role that must become more visible due to its relevance in the coming years.

Internet is a very dynamic environment in which to create new business opportunities are enormous. Innovation, entrepreneurship and the Internet go together. Product and service innovation, process innovation, marketing innovation and organization are also technological innovations that have increased productivity in many productive sectors. However, the problem of growth, competitiveness and employment require an effort on the part of governments, businesses and society itself towards digitization. In this endeavour, the role of entrepreneurs as catalysts of innovation is indispensable. In the new environment the need to foster entrepreneurship, which requires a new way of thinking and understanding the world and the digital ecosystem is evident. Creativity, ability and motivation traits of an entrepreneur should not be considered only individual or personal items but be encouraged as a society, at the organizational level and also regulatory environment.

Provide adequate telecommunications infrastructure to ensure connectivity and access speeds at all times, it requires huge investments in infrastructure, an adequate regulatory framework in coordination with public policies that provide businesses with a more predictable and stable stage, without regulatory asymmetries; but this is not enough. It is necessary that in addition to Internet access, the new technologies are fully incorporated in production processes, among other effects automation of processes is, E-commerce agreements are instituted globally to establish uniform rules on tariff, tax, payments and trade, or even in terms of quality assurance and consumer protection transactions.

One of the main challenges in Europe and also in Spain is unemployment. The digital ecosystem means, in this sense, a great opportunity. One of the biggest challenges in the digital ecosystem is that much employment in the ecosystem is carried on the network and geographical location of the worker is irrelevant, so the competition is global. Fortunately, opportunities are also proportionally much higher than in a restricted national or regional stage.

The space of the Internet has led to new economic models, in the case of collaborative economy. Technology sharing creates, interacts and establishes new patterns of relationship in which the figure of the players involved and their roles can be various and dynamic, with citizens increasingly are also producers and consumers in this ecosystem.

The evolution of the Internet ecosystem is possible to discover new models of social and economic relationship that offer new opportunities to increase the growth of economies and spread the news and improvements in quality of life for people around the world more easily. Global network space is unique for growth, innovation and new digital entrepreneurs who dare to embark on a new adventure every day.

Messages from the forum

- There are several opportunities to generate employment within ICT, especially in sectors like videogames, mobile app development, and added value services for mobile devices or data Analytics.
- There are several positive externalities to Internet employment that could be enhanced by the Digital Single Market
- Machines are absorbing jobs that require a lower skillset. New, more creative, profiles are needed to shift to a knowledge-based economy.
- Strengthening of freelance professional profile, which requires more participation in corporate projects without losing its independence and capacity to deal with other initiatives.
- There is a high regulatory difference between telecommunications companies and Internet services.
- The Internet is not an economic sector and this should be taken into account when measuring its impact.
- Interesting growth of alternative funding with different modes and functions that are able to adapt to both the investor and the entrepreneur.
- Innovation policy cannot be limited to a single department inside the company. Society must become the main agent for innovation.
- Self-employment is not entrepreneurship. It cannot be assumed that political measures taken are the base to support entrepreneur activity. Individual business are so “despite of” the socio-political environment.