

# EuroDIG

European Dialogue on Internet Governance



Messages from Lisbon  
20 - 21 June 2013

*Internet for society -  
How to serve the public interest?*

*„The global public interest is not the sum of all national interests and it thereby cannot be defined by a conference of diplomats. The global public interest can best be defined by the people.“*

*„Surveillance measures are only legal when they pursue a legitimate aim necessary in a democratic society and are of an intensity proportionate to the aim pursued. Blanket surveillance and systematic data collection and data-mining without a clear purpose and independent judicial control violate human rights.“*

## Content

Information about EuroDIG	page 4
EuroDIG 2013 sessions at a glance	page 5
Messages from Lisbon	page 7-9
EuroDIG 2013 - Facts and figures	page 10
E-Participation	page 11
EuroDIG 2013 Programme	page 12-13
EuroDIG 2013 Reports	page 14-27

*Printed with the support of the European Broadcasting Union (EBU)*

## What is EuroDIG?

The European Dialogue on Internet governance (EuroDIG) is an open network to discuss and exchange on emerging issues and challenges concerning the Internet, including who and how we set the rules in cyberspace, between stakeholders (governments, international organisations, business and civil society) and other interested communities, covering the 47 member states of the Council of Europe.

EuroDIG was launched in 2008 and, so far, has held six annual events (Strasbourg-2008, Geneva-2009, Madrid-2010, Belgrade-2011, Stockholm-2012, Lisbon-2013).

## EuroDIG aims and objectives

The overall aim of EuroDIG is to provide an inclusive, open and transparent process, coupled with an annual event, to bring together stakeholders to help shape pan-European perspectives about the Internet, and in particular to prepare for the UN-led Internet Governance Forum (IGF). One of EuroDIG's strengths is its ability to include and outreach to new communities thereby sharing European experiences on a range of issues such as security vs. integrity, open internet and human rights, critical resources and infrastructure, net neutrality and so on. EuroDIG is a dynamic process which is in constant evolution and has a growing membership.

***EuroDIG is always open, always inclusive,  
and it is never too late to get involved.***

## EuroDIG, Lisbon 20-21 June 2013

EuroDIG 2013 was hosted by the Internet Society (ISOC), Portugal chapter, the Foundation for Science and Technology (FCT) of the Ministry for Education and Science, the Department for the Media (GMCS) and co-organised by the Council of Europe, the Federal Office of Communications of Switzerland (OFCOM), the European Broadcasting Union (EBU), with the support of the European Youth Forum, the European Commission, ICANN's regional At-Large organization (EURALO) together with other organisations.

During two days the EuroDIG 2013 brought together more than 600 participants, of which around 100 participated from 9 regional remote hubs across Europe.

Participants from the private sector, governments, international organisations, youth, media, civil society and the academic and technical communities came to discuss public policy issues and challenges related to the Internet.



## *Internet for society -*

### *How to serve the public interest?*

...was the overarching theme in 2013.

The rights of Internet users and the need to protect privacy on the Internet were present in many of the discussions, reflecting recent revelations about PRISM, XKeyscore and Tempora. Raising user's awareness of their rights and the consequences of their actions when managing personal data online was stressed based on a shared responsibility between public authorities, industry and civil society.

The wiretap operations have the potential to compromise many fundamental rights, such as those expressed in the European Convention on Human Rights. The secrecy about the all-around surveillance of European citizens, calls into question the enforcement of fundamental human rights. There was agreement in related debates that the line between secret service and law enforcement is increasingly blurry.

Questions related to the end of state sovereignty in cyberspace – and of the usurpation of sovereignty outside of state borders, are at the heart of EuroDIG and the IGF. In Lisbon, many plenaries debated alternatives to conventional national law such as “horizontal problem-solving” which was argued as more effective than top-down or bottom-up regulation.



## **EuroDIG 2013 sessions at a glance**

### **6 Plenaries:**

- How to serve the public interest?
- Governing Cyberspace – How to keep the Internet safe, free and open?
- Privacy and E-Commerce – Implications for children and young people.
- Under which jurisdiction(s) are European citizens Online?
- Multistakeholder approach to fighting Cyber-crime and safeguarding cyber security.
- Who makes money with content? Who should pay for content?

### **8 Workshops:**

- Governance challenges in the technical space: The impacts on users
- Culture, copyright and the future of access to digital content in Europe
- Searching for a common European model on network neutrality
- Towards a human Internet? Rules, rights, and responsibilities for our online future
- Connected TV – regulations and consequences
- Security as a multistakeholder model
- Accessibility and inclusion - digital participation and democracy for all!
- Cross-border hate speech and defamation – living together online

### **4 Pre - events**

- EURALO meets ICANN
- EURALO General Assembly
- EURid Board meeting
- New Media Summer School

### **2 Side - events**

- Celebrating 25th anniversary of .pt
- National IGFs – how can Europe build bridges in the post-WCIT

### **1 Opening session**

### **1 Closing session**

### **13 Flash sessions (30 min)**

### **1 Internet 101 session**

## Messages from Lisbon

*After each session a reporter is compiling the discussion and results. In the following we extracted the most important messages. Read the complete reports to go into detail!*

### Plenary 1: How to serve the public interest?

- Understanding that the global public interest is in the nature of the Internet itself as being a commons, managed collectively and inclusively through participatory democracy.
- Preserving the value of distributed Internet architecture.
- Balancing stakeholder interests in order to bring benefits of free and open Internet to all.
- Warning about regulatory approaches (done in silos) including their unintended consequences
- Understanding the real danger of the NSA 'Prism' revelations may lie in the various reactions to them; we must work together to prevent damage to the freedom and trust on the Internet



### Plenary 2: Governing Cyberspace – How to keep the Internet safe, free and open?

- Overcoming the "If it ain't broken, don't fix it" mantra and by addressing the different political expectations of societies concerning trust in stakeholders.
- Addressing the need for scalable models for consensus building and investing into education.
- Changing regulatory paradigms towards regulation based on principles.
- Noting that the multistakeholder model has most proximity to universal regulation.



### Plenary 3: Privacy and E-Commerce – Implications for children and young people.

- Understanding that children and young people have very different needs and interests, they must be addressed differently.
- Accepting that there is no common solution for conflicts amongst particular user groups.





#### Plenary 4: Under which jurisdiction(s) are European citizens Online?

- Ensuring that there are appropriate frameworks which are needed to ensure fair process and interoperability between heterogeneous legal orders.
- Considering that procedural interfaces between states, platforms or operators and users could diffuse the tension and creeping fragmentation of cross-border online spaces into realigned national cyberspaces to comply with geographically defined national jurisdictions.



#### Plenary 5: Multistakeholder approach to fighting Cybercrime and safeguarding Cyber security.

- Noting that there are different approaches to the legal frameworks for cyber security and cybercrime, such as Council of Europe conventions and the possible approaches from the ITU and UNODC.
- Noting also that the cyber security problem is a powerful tool that needs safeguards to

be implemented to keep the balance between government intervention and data protection.

#### Plenary 6: Who makes money with content? Who should pay for content?

- Best practice recommendations, worked out by all stakeholders jointly would help ensure fairness throughout the value chains.
- If we want to reach effective solutions, we need collaborative approaches among the various stakeholders.



#### Workshop 1: Governance challenges in the technical space: The impacts on users

- Identifying issues where non-technical stakeholders might have an interest.
- Bringing technical and non-technical communities together to enhance cooperation.
- Identifying the appropriate role for governments and regulators in IPv6 promotion.
- Noting that there is no need for states to substitute this liability with regulation.





### Workshop 2: Culture, copyright and the future of access to digital content in Europe

- Considering whether access to digital content being regulated by contractual terms and conditions of private companies instead of copyright law and the work of cultural and educational institutions
- Publicly funded content should be licensed under sharing license & made available through central repository(ies).
- Better metadata about cultural content, including licensing details.
- More niche websites catering for niche interests and more legal offerings for paying.
- Focusing on more on large-scale 'pirates' than on non-commercial use.
- More studies needed on the effects of technological innovation on creativity.
- Need a better understanding how to create a copyright regime that encourages innovation, with clear boundaries between commercial and non-commercial use.



### Workshop 3: Searching for a common European model on network neutrality

- ISPs interest lies in looking out for their customers and offer exactly what they are asking for.
- Defining an “appropriate” traffic management
- Managed services can be good in terms of innovation, user experience and dynamism in the ecosystem, but it needs to happen “beside the open Internet”.
- Calling for complete transparency in ISPs’ offers.



### Workshop 4: Towards a human Internet? Rules, rights, and responsibilities for our online future

- More transparency and accountability needed from industry and public sector providers.
- Awareness and education are essential!
- More educational initiatives that is broad based about how digital literacy and knowledge about rights are intertwined.
- Calling on policymakers need for holistic, human-centred and locally embedded approaches to decisions that affect internet infrastructure, we-design, access, and use.

### Workshop 5: Connected TV – regulations and consequences

- Less regulation needed because there will be a shift in responsibility from the media to the citizens / viewers and to the intermediaries.
- Protecting through design and by default
- Balancing regulation and self-regulation which is validated between European stakeholders





### Workshop 6: Security as a multistakeholder model

- Governments should act as facilitators, give incentives and encourage the dialogue between the stakeholders, the capacity building and education
- Security should be a multistakeholder model and therefore a shared responsibility of all stakeholders.



### Workshop 7: Accessibility and inclusion - digital participation and democracy for all!

- Continuing awareness raising activities and develop fora for discussion in the multistakeholder format.
- Need for national strategies on digital inclusion, as an outcome of European policies, to be implemented in close cooperation and engagement with local authorities.

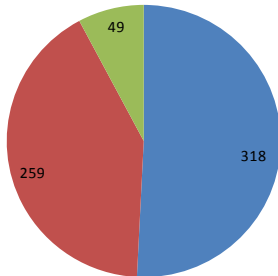


### Workshop 8: Cross-border hate speech and defamation – living together online

- Fragmentation: Current piecemeal solutions in different national jurisdictions to tackle the problem of hate speech and defamation entail the danger of a fragmentation of cyberspace, e.g. through techniques like Geo-IP Filtering or ISP blocks.
- Transparency: Companies dealing with the definition and restriction of free speech by prohibiting hate speech and defamation must be transparent in their terms of service.
- Education: The prevention of hate-speech and defamation through education plays an important role.
- Tools: Hotlines and safer internet centres are currently the most common tools for internet users to handle online hate speech and defamation.
- Multistakeholder: The problem of hate speech and defamation has to be discussed in multistakeholder process to avoid disproportionate measures.

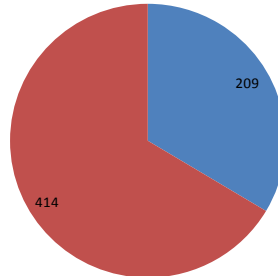


## EuroDIG 2013 - Facts and Figures



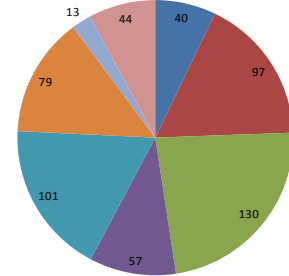
**Country**

- Portugal
- European countries
- Non-European countries



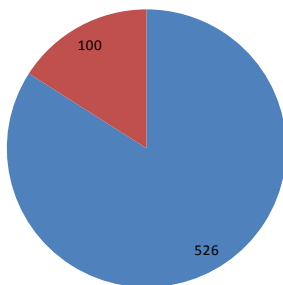
**Gender balance**

- female
- male



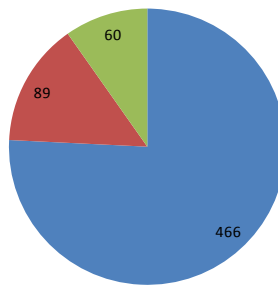
**Stakeholder group**

- Academia
- Business
- Civil society
- Europ. & int. Organisations
- Governmental
- Others
- Press / media
- Technical Organisations



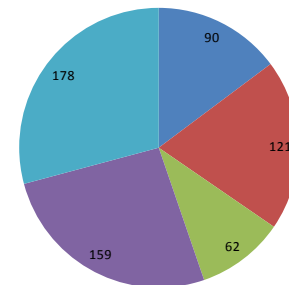
**Type of participation**

- present
- remote



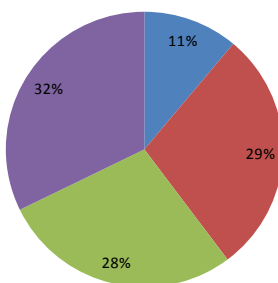
**No of EuroDIG attended**

- First timer
- 1-2 EuroDIG
- 3-5 EuroDIG



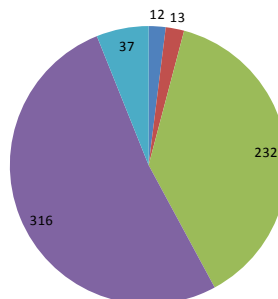
**Source of information**

- Info letter
- Attended EuroDIG already
- Newspaper / Magazin / Flyer
- Friend / colleague
- other



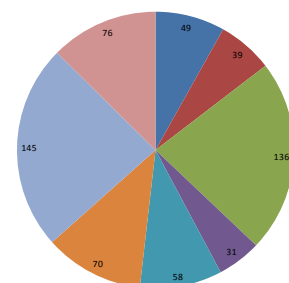
**Expectations**

- Business opportunities
- Dialogue
- Education
- Networking



**Reasons for attendance**

- Attractiveness of the city
- Availability of funding
- It is part of the job
- Because of the programme
- Because of the speaker



**Workshop preferences**

- Accessibility and inclusion
- Connected TV
- Future of access to digital content
- Hateful comments and abuse online
- Impact of technical aspects
- Network Neutrality
- Rights and responsibilities of I-net users
- Security as a multistakeholder model

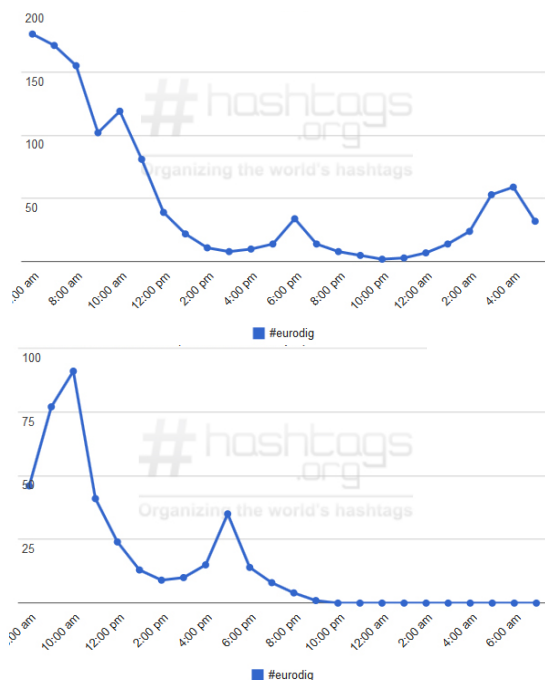
**625 participants did pre-register for EuroDIG**

## E-Participation

Remote participation facilities and captioning were put in place in order to reduce the different gaps related to the Internet. Several factors may hamper physical attendance, such as professional commitments and travel costs. But it does not mean you can not participate actively and make your voice heard.

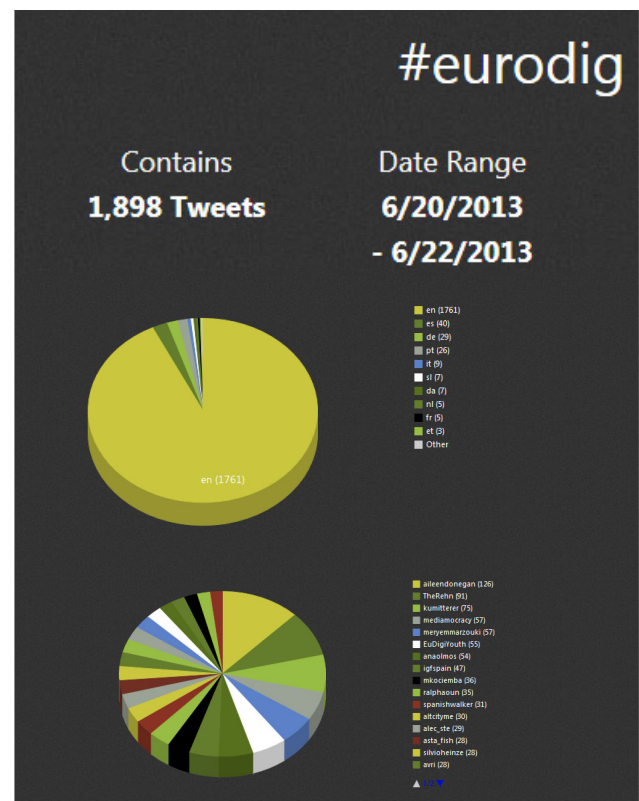


Twitter plays a more and more an important role for e-participation. Attendees agreed that both the audience and speakers benefit when tweets are being displayed and thereby feed directly into dialogue to improve interaction.



Hubs where organised in 6 European countries:

- Armenia
- Belgium
- Bosnia and Herzegovina
- France
- Spain
- Ukraine



*Thanks to all who made e-participation possible!*

## EuroDIG 2013 programme

Thursday, 20 June 2013

### 9:00 Welcoming address(es) and opening

Pedro Veiga, ISOC Portugal, Pedro Berhan da Costa, Gabinete para os Meios de Comunicação Social (GMCS), Pedro Carneiro, Fundação para a Ciência e a Tecnologia (FCT), Jan Kleijssen, Council of Europe, Christian Hermansson, Charge d'Affairs at the Swedish Embassy in Lisbon, José Manuel Durão Barroso, President of the European Commission (video message), Leonor Parreira, Secretary of State of Science of Portugal

### 9:30 Plenary 1

How to serve the public interest?

Co-moderators: Ayesha Hassan, International Chamber of Commerce, Luis T. Magalhães, Lisbon Technical University

Key participants: Nigel Hickson, ICANN, Francisco Pinto Balsemão, European Publishers Council and former Prime Minister of Portugal, Markus Kummer, ISOC, Ross LaJeunesse, Google, Alberto Da Ponte, Rádio e Televisão de Portugal, Jimmy Schulz, German Parliamentarian for the liberal Free Democratic Party, Giovanni Seppia, EURid

### 11:00 Coffee break

### 11:30 Plenary 2

Governing cyberspace: How to keep the Internet safe, free and open?

Co-moderators: Wolfgang Kleinwächter, University of Aarhus, Ana Neves, Foundation for Science and Technology

Key participants: Fadi Chehadé, CEO ICANN, João Confraria, ANACOM, Luigi Gambardella, ETNO, Sir Richard Tilt, Internet Watch Foundation, Edward Zammit Lewis, Ministry for the Economy, Investment and Small Business of Malta

**11:30 Flash 1** Illegal drugs in cyber space

**12:15 Flash 2** Web accessibility

### 13:00 Lunch

### 14:30 Parallel workshops

WS 1: Governance challenges in the technical space: The impacts on users

Moderator: Chris Buckridge, RIPE NCC

Key participants: Wim Degezelle, CENTR, Marco Hogewoning, RIPE NCC, Jan Malinowski, Council of Europe

WS 2: Culture, copyright and the future of access to digital content in Europe

Moderator: Stuart Hamilton, International Federation of Library Associations

Key participants: Sarah Kelly, The Coalition For A Digital Economy, Marco Pancini, Google, Olav Stokkmo, International Federation of Reproduction Rights Organisations, Ben White, British Library  
Comments by: Carlos Romero, Sociedad de la Información, de esta Secretaría de Estado

WS 3: Searching for a common European model on net-neutrality

Co-moderators: Frederic Donck, ISOC Europe, Vladimir Radunovic, DiploFoundation

Key participants: Jean-Jacques Sahel, Skype, Pedro Veiga, University of Lisbon, Narine Khachatryan, Media Education Center, Giacomo Mazzone, EBU

WS 4: Towards a human Internet? Rules, rights and responsibilities for our online future.

Breakout session facilitators: Lee Hibbard, Council of Europe, Marianne Franklin, IRP Coalition / Goldsmiths University, Abbe Brown, University of Aberdeen, Meryem Marzouki, Sorbonne Universités, Thomas Schneider, OFCOM

Key participants: Paulo Foncesca, Associação Portuguesa para a Defesa do Consumidor, Rikke Jørgensen, Danish Institute for Human Rights, Matthias Kettemann, IRP Coalition / University of Graz, Michael Rotert, eco

### 16:00 Coffee break

### 16:30 Plenary 3

Privacy and e-commerce - implications for children and young people

Moderator: Sophie Kwasny, Council of Europe

Key participants: John Carr, eNASCO, Conelia Kutterer, Microsoft Clara Guerra, Portuguese Data Protection Authority, Peter Matjasic, European Youth Forum

**16:15 Flash 3** Google, media system and news aggregation

**17:00 Flash 4** Internet of things

**17:45 Flash 5** How to empower vulnerable children online?

**18:30 Flash 6** Is the porous garden scenario becoming reality?

### 19:30 Gala dinner by ISOC Portugal, FCT and GMCS

## Friday, 21 June 2013

8:00 Education session about concepts in Internet infrastructure

Marco Hogewoning, RIPE NCC

8:00 Flash 7 Human rights and Internet surveillance

9:00 Key note speech

Digital Agenda Assembly – highlights / reporting-in from the European Commission by Linda Corugedo Steneberg

9:30 Plenary 4

Under which jurisdiction(s) are European citizens online?

Moderator: Bertrand de la Chapelle, Internet & Jurisdiction Project

Key participants: Linda Corugedo Steneberg, European Commission, Maria da Graça Carvalho, Member of the European Parliament, Jan Kleijssen, Council of Europe, Wolfgang Kleinwächter, University of Aarhus, Erika Mann, Facebook

09:30 Flash 8 Big data and user controlled architecture

10:45 Flash 9 InfoZipper, Ukraine

11:00 Coffee break

11:30 Parallel workshops

WS 5: Connected TV – regulations and consequences

Moderator: Elisabeth Markot, European Commission

Key participants: Ross Biggam, Association Commercial Televisions, John Carr, eNACSO, Marianne Franklin, Goldsmith University London, José Maria Guerra Mercadal, Euralva, Sophie Kwasny, Council of Europe, Antoine Larpin, Panasonic Europe, Mario Rui Miranda, RTP, Michael Wagner, European Broadcasting Union

WS 6: Security as a multistakeholder model

Moderator: Oliver J. Süme, EuroISPA

Key participants: Sabine Dolderer, DENIC, Marco Hogewoning, RIPE NCC, Richard Clayton, University of Cambridge, Michael Rotert, eco

WS 7: Accessibility and inclusion – digital participation and democracy for all!

Co-moderators: Yuliya Morenets, Together against cybercrime, Stuart Hamilton, International Federation of Library Associations

Key participants: Sébastien Bachollet, ICANN, Dorina Bralostiteanu, Public Library of Fillasi, Jorge Fernandes, Ministry of Education and Science of Portugal, Irena Kowalczyk, Council of Europe, Mikus Ozols, Telecom Latvia

WS 8: Cross-border hate speech and defamation – living together online

Moderator: Paul Fehlinger, Internet & Jurisdiction Project

Francisco Seixas da Costa, North-South Centre, Council of Europe

Key participants: Adriana Delgado, The No Hate Speech Movement, Konstantinos Komaitis, ISOC, Marco Pancini, Google

Comments by: Rui Gomes, Council of Europe

13:00 Lunch

14:30 Plenary 5

Multistakeholder approach to fighting cybercrime and safeguarding cybersecurity

Moderator: Tatiana Tropina, Max-Planck Institute for Foreign and International Criminal Law

Key participants: Sophie Kwasny, Council of Europe, Richard Leaning, Europol, Michael Rotert, eco, Christine Runnegar, ISOC, Pedro Verdelho, Cyber-crime Office within the Prosecutor General's Office of Portugal

14:30 Flash 10 Internet principles

15:15 Flash 11 ICANN's new gTLD program

16:00 Coffee break

16:30 Plenary 6

Who makes money with content? Who should pay for content?

Moderator: Marianne Franklin, Goldsmiths University of London

Key participants: Francisco Pedro Balsemão, Imprensa, Mike Holderness, European Federation of Journalists, Marco Pancini, Google

Comments by: Konstantin Komaitis, ISOC

16:15 Flash 12 ICANN strategy for the next 5 years

17:00 Flash 13 Gaming and Tel-technology enhanced learning

17:30 Wrap-up, reporting-in and conclusions

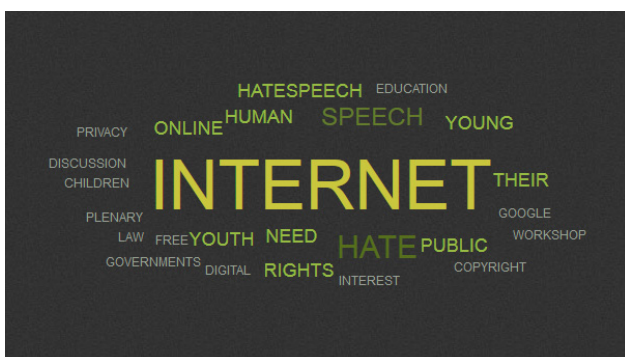
## Reports from plenary and workshops

*Last but not least, we would like to express our special thanks to all focal points and session organisers, moderators, remote participation moderators, and reporters, as well as many key participants for their contributions which helped to shape EuroDIG 2013.*

*We must underline that in 2013 we found all reports were of high quality what made it easy for us to formulate the EuroDIG Lisbon messages. We therefore agreed to publish the reports as they were submitted by the session reporters.*

*Year by year, the EuroDIG process is being reviewed, in particular to enhance the inclusion and dynamics of interaction between stakeholders – this can only be done with your help and support.*

*Thank you for time, efforts and expertise!*



## Plenary 1: How to serve the public interest?

Predictably, the session didn't come up with a clear and generally applicable answer to the question, and rather raised more questions. Who defines public interest, and what is the framework: national or global? Governments claim the right to define public interest within their borders, but the Internet does not care about borders and the Westphalian system. Global actors have to deal with different national conceptions of public interest ranging over a wide spectrum. (During the dictatorship, censorship was motivated in Portugal by public interest!) There is no ready-made international and certainly no intergovernmental solution either.

Instead, participants suggested looking for global public interest in the nature of the Internet itself as commons, managed collectively and inclusively by participatory democracy; in the definition of Internet Governance of the Tunis Agenda about principles, rules etc. shared by all stakeholders; and using variable geometry on different issues. The IGF was held up as a model for defining public interest related to the Internet, better suited for that purpose than intergovernmental fora, such as UN or ITU.

Drawing on the experience of their own organizations, speakers suggested different approaches to serving public interest. ISOC works to preserve values of distributed Internet architecture. ICANN balances stakeholder interests both internally and externally. Council of Europe wants to turn the question around: instead of telling people what public interest is, they are asking them to define it. Even parliaments could use a multistakeholder process to find out what public interest is. Google works to bring the benefits of free and open Internet to all. (Stressing the importance of the adjectives, Ross LaJeunesse – with 3 years experience from working in China - pointed out that even if China is doing well, none of its successes is attributable to the Internet)

Regulatory approaches were discussed and warnings about unintended consequences and silo mentality were heard. It is not useful to discuss whether the Internet can or cannot be regulated.

Instead, public interest has to be defined differently in different contexts. On the other hand, need for equal regulatory treatment for old and new media came up.

Inevitably, recent revelations of the extent of global surveillance activities of the NSA and allegations about the collusion of major global actors were reflected in the debate. The Google representative stressed that surveillance was not just a U.S. issue. He denied that any government had been given direct or blanket access to data on their servers. Google has to comply with the laws of dozens of countries, but does it willynilly, trying to push back. Markus Kummer quoted Benjamin Franklin: those who are willing to give up a little bit of their liberty for their safety reserve neither. Jimmy Schulz pondered the limits of the acceptable as far as surveillance is concerned. He called for transparency and clear rules: is something happens with our data, at least we should know about it. Nigel Hickson stated that the real danger of the revelations may be in the reactions to them; we must work together to prevent damage.

**Reporter:** Yrjö Länsipuro, ISOC Finland

**Co-moderators:** Ayesha Hassan, International Chamber of Commerce, Luis T. Magalhães, Lisbon Technical University

**Key participants:** Nigel Hickson, ICANN, Francisco Pinto Balsemão, European Publishers Council and former Prime Minister of Portugal, Markus Kummer, ISOC, Ross LaJeunesse, Google, Alberto Da Ponte, Rádio e Televisão de Portugal, Jimmy Schulz, German Parliamentarian for the liberal Free Democratic Party

### **Plenary 2: Governing Cyberspace: How to keep the Internet safe, free and open?**

The plenary analysed the different regulation categories, i.e. technical regulation versus political regulation and therein the diverse models of regulation with regards to deliberation and policy making. ICANN president Fadi Chehade pleaded “to overcome the if it’s working don’t fix it” man-

tra and addressed the different political expectations of societies concerning the trust on stakeholders like the private sector and governments in different continents.

The deliberations addressed the necessity of further developmental progress in several aspects, stressing specially first the need for scalable models in the process of consensus building which should provide for global inclusion and second, the educational aspect, since digital technologies are developing fast and steadily causing a growing gap between technological innovation and the understanding of its social consequences.

The concluding debate focused on several proposals for specific intergovernmental treaties and international law to regulate global issues such as cyber-security, copyright or data protection. Jānis Kārklīš, UNESCO’s Director of Communication and Information emphasized the importance of changing the regulatory paradigms towards a regulation based on principles and not on particular technologies. Some other concerns raised with respect to international law alluded to the standard quality of international treaties, since they constitute a compromise on the lowest common denominator, and to the implementation of those norms and principles, since the existing national law systems are different.

All arguments considered, the plenary led to the conclusion that the closest approach to universal regulation is the multistakeholder model which has already generated agreements fostering stability, security and innovation in the internet.

**Reporter:** Lorena Jaume-Palasi, Ludwig Maximilians University Munich

**Co-moderators:** Wolfgang Kleinwächter, University of Aarhus, Ana Neves, Foundation for Science and Technology

**Key participants:** Fadi Chehadé, CEO ICANN, João Confraria, ANACOM, Luigi Gambardella, ETNO, Janis Karklins, UNESCO, Sector for Communication and Information, Sir Richard Tilt, Internet Watch Foundation

### Plenary 3: Privacy and E-Commerce– implications for children and young people

Plenary 3 outlined the special status of children and young people on the internet. Young people should be considered stronger as users, digital natives and more media literate people. Young people were in particular referred to as users between 13 and 18. Children on the other hand are still very impressionable and „digitally naive“. They learn fast but the learning process runs many risks if unsupervised. Children were discussed for youth below the age of 13.

There are disparities also amongst young people themselves and children alike. They should not be considered as a homogeneous group but they are easy to reach for educational measures to set a basic level of media competency. An arising problem is that young people and their parents do not necessarily „speak the same language“ in terms of media use, a lot of media learning happens through peer learning.

Spark for the debate was the EU draft regulation on privacy and e-commerce, which in its current form would loosen the regulatory framework for ISPs, eg. reduce the role of parental consent in online forms. It would also reduce the minimum age for people to register online and share their data to the age of 13. The age is picked arbitrarily; the plenary was missing reasoning for that exact age limit. Furthermore the regulation lacks enforceability. Similar to the current status ISPs can shift the responsibility towards the parents and are not requested to check the information provided.

The debate quickly moved towards the problem of child abuse. Numbers for child abuse on the internet are apparently increasing. There seems to be a lack of police and international cooperation to deal with the topic. At the same time the organisations pledging support to the fight against child abuse are grow in numbers. Many questions arose on the implementability and effectiveness of current technology to track child abuse but remained unanswered. Young people from the audience largely stressed the relevance of privacy of every user and the potential loss of

freedoms on the internet due to implemented measures.

This showcased two different approaches towards the topic: blocking and taking offline. The European states have different ways to deal with it. With blocking the content remains online but is harder to access, yet with high media competency still easy to obtain. With taking offline content remains available until the source is found and then prosecuted. Questions evolved around the inflicted harm of pictures remaining online, the effectiveness of blocking, the communication ways of child abusers and the traceability of those.

The plenary did not come to a common solution but outlined ways to address the issues and conflicts amongst particular user groups. Young people and children have very different needs and interests and need to be addressed differently.

**Reporter:** Martin Fischer, Young European Federalists

**Moderator:** Sophie Kwasny, Council of Europe

**Key participants:** John Carr, eNASCO, Conelia Kutterer, Microsoft Clara Guerra, Portuguese Data Protection Authority, Peter Matjasic, European Youth Forum

### Plenary 4: Under which jurisdiction(s) are European citizens online?

**ABOUT:** When online, European citizens can be subject to multiple normative orders according to their place of residence, the services they use, as well as the location of the servers and DNS operators involved. How to address the resulting tensions and enable the coexistence of different normative orders in shared cross-border online spaces?

#### **TAKE-AWAY: NEED FOR INTEROPERABILITY FRAMEWORKS**

The session highlighted the fact that the transnational nature of online interactions necessitates appropriate frameworks to ensure fair process and interoperability between heterogeneous le-



gal orders. In the absence of specific international treaties or a universal harmonization of Internet related laws, procedural interfaces between states, platforms or operators, and users could diffuse the tension and creeping fragmentation of cross-border online spaces into realigned national cyberspaces to comply with geographically defined national jurisdictions.

## DISCUSSION HIGHLIGHTS

- **PATCHWORK:** As states increasingly strive to regulate the online interactions their citizens participate in or are affected of, a multitude of potentially incompatible laws and corresponding implementation procedures are proliferating.
- **SOVEREIGNTY:** Given the particular geography of cyberspace with the dispersed physical locations of platforms, operators and servers, the exercise of national sovereignty can have transboundary effects on other states and their citizens.
- **LEGAL UNCERTAINTY:** Both companies and users face increasingly major legal uncertainties regarding applicable laws and jurisdictions to which their online actions are subject to.
- **ENFORCEABILITY:** States struggle to enforce their national laws in cyberspace as existing frameworks for inter-state cooperation face their limits to scale up to the transnational nature of the Internet.
- **PRIVACY:** Without frameworks that ensure the interoperability between different privacy orders transnational data flows and the development of decentralized cloud computing capacities could be hampered. How to determine the rules for the protection of personal data if multiple jurisdictions are simultaneously involved in online interactions?
- **HATE SPEECH:** How to deal with cross-border hate speech in online spaces?
- **COEXISTENCE:** How can citizens who are subject to both their national laws and the Terms of Service of cross-border online platforms they use, coexist peacefully in cyberspace? How to prevent jurisdictional arms races and tension resulting in overlapping normative orders?

- **INTEROPERABILITY:** How to guarantee the interoperability of divergent laws and procedures of nation states and rules stipulated by cross-border online platforms?
- **FAIR PROCESS:** How to ensure that fair process is maintained in the interactions between states, platforms or operators, and users?
- **REDRESS:** The current legal patchwork renders redress for users often highly complex. How to ensure that users can better interface with states, platforms and operators to protect their rights?
- **INSTRUMENTS:** What are appropriate governance instruments for fair process frameworks for procedural interfaces in a multi-stakeholder setting?

**Reporter:** Paul Fehlinger, Internet & Jurisdiction Project

**Moderator:** Bertrand de la Chapelle, Internet & Jurisdiction Project

**Key participants:** Linda Corugedo Steneberg, European Commission, Maria da Graça Carvalho, Member of the European Parliament, Jan Kleijssen, Council of Europe, Wolfgang Kleinwächter, University of Aarhus, Erika Mann, Facebook

## Plenary 5: Multistakeholder approach to fighting cybercrime and safeguarding cyber security

The aim of the workshop was to discuss technical, legal, regulatory efforts to tackle cybercrime and safeguard cyber security from the perspective of the technical community, industry, law enforcement and international organisations. This approach was reflected in the selection of key participants from Council of Europe, eco, Internet Society, Portuguese law enforcement.

The plenary discussed the recent developments in multi-stakeholder environment such as public private cooperation in fighting malware, botnets and child abuse online, trans-border access to the stored data from industry and law enforcement perspective, the need for striking a balance bet-

ween privacy, data protection and government intervention. The main controversies of the discussion were focused on the issues of the failure of mutual legal assistance mechanisms and the different perspectives that industry, civil society and law enforcement agencies have concerning the validity of law enforcement requests. Different approaches to the legal frameworks for cyber security and cybercrime, such as Council of Europe conventions, the possible approaches from the ITU and UNODC. The cyber security problem was considered as a powerful tool that needs safeguards to be implemented to keep the balance between government intervention and data protection.

**Reporter:** Nicolas von zur Mühlen, Max-Planck Institute for Foreign and International Criminal Law

**Moderator:** Tatiana Tropina, Max-Planck Institute for Foreign and International Criminal Law

**Key participants:** Sophie Kwasny, Council of Europe, Richard Leaning, Europol, Michael Rotert, eco, Christine Runnegar, ISOC, Pedro Verdelho, Cybercrime Office within the Prosecutor General's Office of Portugal

### **Plenary 6: Who makes money with content? Who should pay for content?**

The aim of this session was to address, from different perspectives, the following questions: who makes money with whose content, on whose terms? And who pays for this content?

The panel session underlined that, if during the pre-digital world, the answers to these questions were relatively uncomplicated; the evolution of the Internet has led to significant changes in terms of production, distribution of and access to content, thus making it more difficult to have straightforward answers. The technological changes have been creating "disruptions" in the content-related business, have led to an increase in the quantity of available content, and have created new possibilities for users to access content.

When copyright was introduced, its aim was to reward artists, while at the same time allowing access to content and progressing science. But the new realities of the online space have overwhelmed the copyright model and created challenges that need to be addressed in order to ensure that the interests of all parties (content producers, publishers and consumers) are taken into account and protected.

### **Three main issues were raised in relation to the existing copyright model:**

- **The matter of choice:** while there is a need to allow creators to have an economic gain from their creative activities, we need to take into account the fact that there are creators who do not necessarily want to make money out of their content and they should be entitled to exercise this choice;
- **Access:** the main question to be addressed here is to what extent the existing copyright-based models allow access to content, under what circumstances and with what limitations and exceptions;
- **Efficiency:** to what extent content creators really benefit from the economic value of their content, taking into account, for example, the complicated matter of collecting society and the fact that the existing royalties are uneven?

Some participants emphasized that there are alternatives to copyright which offer solutions for some of these existing challenges, and one of them is the Creative Commons. But there were also opposing views showing that Creative Commons and similar solutions do not address the need for people to have sustainable ways to support themselves from their creative activities; the need to protect authors' rights was one example. The question, however, is whether we should stick to the current model or move towards a new model. Some of the participants mentioned that a suitable approach would be to have all stakeholders work on best practice recommendations (eventually, and if needed, with the aim to transform them into national/international legislation), which would help ensure fairness through-

hout the value chains. If we want to reach effective solutions, we need collaborative approaches among the various stakeholders.

All these debates illustrated the fact that the current discussions about copyright tend to focus on a traditional approach. But what if not the content is the problem, but the circulation of the content? Do we think about content too narrowly? If yes, how do we move forward with this debate?

**Reporter:** Sorina Teleanu, Parliamentary assistant, Parliament of Romania

**Moderator:** Marianne Franklin, Goldsmiths University of London

**Key participants:** Francisco Pedro Balsemão, Impresa, Mike Holderness, European Federation of Journalists, Marco Pancini, Google  
Comments by: Konstanin Komaitis, ISOC

### **Workshop 1: Governance Challenges in the Technical Space: The Impacts on Users**

Workshop 1 looked at some of the governance issues of specific concern to the technical community, and the implications that these issues might have more broadly in terms of social, economic or security impact. The goal of the workshop was to identify issues where non-technical stakeholders might have an interest and consider how they might contribute to the development of policy solutions.

Marco Hogewoning of the RIPE NCC discussed the example of IPv4 depletion and the deployment of the IPv6. He highlighted the problems with the transition from the one protocol to the other and how this may affect Internet users in the long term. Discussion also considered what issues would convince Internet users to take an interest in behind-the-scenes technical matters – issues such as privacy, traceability, or the breakdown of basic Internet services. Participants also considered what is the appropriate role for the government and regulators in IPv6 promotion.

Wim Degezelle of CENTR provided an further example of a technical governance challenge in the deployment of DNSSEC, security extensions to the DNS. He talked about the successful adoption of DNSSEC by many ccTLDs, but he pointed out that there is still a long way to go in convincing registrars and Internet Service Providers to employ DNSSEC. The role of government was again discussed, with agreement that leading by example was an important public sector strategy.

Participants, including panellist Olivier Crépin-Leblond (ISOC UK England and ICANN At-Large Advisory Committee), discussed possible ways to bring technical and non-technical communities together to enhance their cooperation. Technical community engagement with law enforcement agencies was highlighted as a successful example of this.

Jan Malinowski of the Council of Europe helped lead later discussion on the issue of whether government should be regulating in these areas. Participants considered the argument that users have an expectation that their state will ensure a secure environment; while on the other hand, we cannot expect a “clean Internet” any more than we can have a perfectly safe offline world. Ensuring that companies are liable for the services they provide to their customers is important, but there is no need for the state to substitute this liability with regulation. Participants also noted that security must not be a justification for state intervention against freedom of speech.

The workshop concluded with some comments on future EuroDIG discussions in this area that could perhaps look at different specific challenges or issues.

**Reporter:** Athina Fragkouli, RIPE NCC

**Moderator:** Chris Buckridge, RIPE NCC

**Key participants:** Wim Degezelle, CENTR, Marco Hogewoning, RIPE NCC, Jan Malinowski, Council of Europe

## Workshop 2: Culture, Copyright and the Future of Access to Digital Content in Europe

### Subject

- Starting from the premise that being able to access, share and re-use cultural content is in the public interest, and that the current European copyright framework was not providing the best support, the workshop discussed what issues would need to be addressed in any reform of copyright in Europe

### Obstacles

- Policy makers don't seem to understand that copyright also refers to scientific and educational content, not just content produced by the entertainment industry. It was suggested that this situation does not favour the public interest
- It's important to note that in many contexts what is regulating access to digital cultural content is not copyright but contracts - contracts are overriding copyright law and cultural and educational institutions are particularly affected.
- It was noted that Portugal is one of the few countries in the EU that ensures that limitations & exceptions cannot be overridden by private contacts
- Complex licensing agreements, as well as a lack of information on who owns the rights to what, are therefore preventing access to and re-use of content
- Conditions for some activities – such as text and data mining – are better outside of Europe, leading some tech startups to relocate. It was suggested that if Europe wants to compete with the rest of the world we can't just look at our system and say it works for us. Many SMEs are looking at starting elsewhere for legal reasons.
- Many startups hire a lawyer before they hire an engineer. This is a demonstration of a broken system.
- DRM in eBooks – it was asked why publishers have learned nothing from the music industry's experience?

### Reform

- Address overriding of copyright by private contract
- Private copying – the issue of copyright exceptions for private copying needs to be addressed
- Better metadata about cultural content, including licensing details
- Still too few fresh legal offerings for paying for cultural content. We need more niche websites catering for niche interests
- In terms of illegal content, enforcement approaches should change to focus more on large-scale 'pirates', and move away from non-commercial sharing
- More studies needed on the effects of technological innovation on creativity
- There was some support for the sorts of pay-what-you like models pioneered by Radiohead and available on Bandcamp. However, concerns were expressed that if we accepted a cultural economy based on 'free' then we would develop a winner-takes-all situation that suits big players such as Amazon and Apple more than European content creators
- Seemed to be an emerging consensus that all publicly funded content must be licensed under sharing license & made available through central repository(ies)

**Conclusion:** If we want to be pioneers we need to figure out how to create a copyright régime that encourages innovation, with clear boundaries between commercial and non-commercial use.

**Reporter:** Mike Holderness, European Federation of Journalists

**Moderator:** Stuart Hamilton, International Federation of Library Associations

**Key participants:** Sarah Kelly, The Coalition For A Digital Economy, Marco Pancini, Google, Olav Stokkmo, International Federation of Reproduction Rights Organisations, Ben White, British Library

**Comments by:** Carlos Romero, Sociedad de la Información, de esta Secretaría de Estado

### Workshop 3: Searching for a Common European Model on Net Neutrality

All speakers agreed with Ms. Kroes's recent statement that "transparency, customer choice, competition and the ability to switch providers" are the key aspects to net neutrality; however, while some stressed that this was sufficient in a competitive environment with strong regulatory bodies and consumer-oriented ISPs, others considered these aspects not enough: with statistics of restricted access in Europe and reference to trends in Europe (Slovenia, Norway, France, -just learned- Luxemburg and, of course, Netherlands choosing to legislate to protect net neutrality and the open character of the Internet), they argued that further issues need to be tackled.

Regarding the ISP's interest, it was laid out that ISPs will be tempted to block traffic as a way of eliminating competition with over-the-top players; on the other hand, it was argued that in a data-centric Internet with plenty of competition at the ISP level, it is actually in the best interest of ISPs to look out for their customers and offer exactly what they are asking for. Everybody seems to agree on the concept of "open Internet" and everybody is wary of restriction, whether it be applied in one sense (restricting traffic and over-the-top innovation) or the other (restricting innovation across the value chain).

The second question addressed was about defining "appropriate" traffic management. The Dutch law allows exceptions under which traffic can be managed: congestion, integrity and security, court orders.

On the issue of managed services, everybody agreed that it's a good thing in terms of innovation, user experience and dynamism in the ecosystem. However, some speakers pointed out, all of this needs to happen "beside the Open Internet". In the Netherlands, QoS services are encouraged, as long as they are offered "in addition" to the best-effort Internet, which must remain neutral by law. ETNO argued that ISPs do not want to lose customers and will offer the best-effort Internet in response to the demand, and that re-

gulators have enough mechanisms and power to control it.

Some argued that the future Internet is likely going to be mainly content-driven and geared towards entertainment. Interesting services can be offered but they need a guaranteed QoS. However, the question remains whether their interest would lead them to give preferential treatment to IP-based services, turning best-effort Internet into a dirt road, or if their interest would side with the customer. On this issue, the audience called for complete transparency in the ISPs' offers and there was some discomfort over the fact that public content may be contaminated in a managed services scenario.

On the challenge of regulating for an unknown future and the capacity to remain flexible and accommodating, Ørnulf Storm argued in favor of Norway's work on co-regulatory principles, instead of law, as most convenient. Marieke Pondman argued that the flexibility was achieved in the Dutch law by not regulating in a quantitative way (establishing QoS or minimum traffic) and opening the law to the idea of development of specialized services. ETNO, however, stressed the danger of regulation and alerted against the dangers of a fragmented Internet due to national regulations (instead of harmonizing a European approach).

**Reporter:** Ana Olmos, IGF Spain

**Co-moderators:** Frederic Donck, ISOC Europe, Vladimir Radunovic, DiploFoundation

**Key participants:** Jean-Jacques Sahel, Skype, Pedro Veiga, University of Lisbon, Narine Khachatryan, Media Education Center, Giacomo Mazzone, EBU

### Workshop 4: Towards a human Internet? Rules, rights, and responsibilities for our online future

This workshop, organized by the IGF Internet Rights and Principles Coalition and the Council of Europe, focused on a selection of practical

scenarios around internet infrastructure design, access, content provision, and use in the context of human rights. The workshop was an interactive, bottom-up session that drew on audience experiences and expertise. The aim was to unpack examples where selected human rights are at stake, overlooked, or potentially undermined. The objective was to raise awareness of these connections as well as consider ways to move these projects forward light of two ongoing projects; the Charter of Human Rights and Principles for the Internet (IRP Coalition 2011), and the Compendium of Existing Rights for Internet Users (CoE, 2013).

First, a panel of four speakers from industry, consumer groups, human rights advocacy, and legal scholarship provided brief introductions to the key issues from their perspective. The workshop then divided into 4 breakout/ brainstorming sessions who reported back in the concluding section along four specific rights-based lines of discussion articulated in the Charter of Human Rights and Principles for the Internet: 1) Freedom of Expression and Human Dignity; 2) Economic, technological, and physical barriers to access; 3) Right to Privacy and Security issues; 4) enablers and impediments to realizing human rights online. The outcomes of the breakout groups were reported as follows:

### **(1) Freedom of expression/Human Dignity**

Questions discussed: What is Freedom of Expression on internet / how can people learn more about it and protect their rights / How can they be protected?

Ways forward:

1. The European court is correcting decisions of national courts, e.g. in cases of Freedom of expression.
2. The Impact of the CoE guidelines: which have been adopted by companies and are adopted into legislation in some countries.
3. User groups are drawing on the CoE guidelines to make them user-friendly for citizens.
4. The Internet providers need to be more involved in informing and educating users.

### **(2) Internet Access/Economic, Socio cultural and Technological barriers**

Participants shared some concrete examples and issues from their experience about how internet service provision and infrastructure can create barriers for special needs or disadvantaged communities. Conclusions covered:

It is important that governments, civil society and companies are aware that digital exclusion exists and that excessive barriers are preventing groups of our society to have equal right to access the Internet ( These are not only physical barriers such infrastructure or physical disabilities and also cultural / educational barriers or bureaucracy.

More than just providing access it is important that governments ensure that the protection of the Human Rights online is safeguarded. This includes the right to access information basic and public services and the right to education.

It is also important that companies and the rights-holders industry don't prevent people from exercising their rights because of contradictory copyrights for accessing content by visually or hearing impaired users.

In sum, the session agreed that the issue is more than providing the means and the tools to access the Internet. It is important to educate people on how to use the tools and about the range of possibilities that the technologies and the Internet can open to them in order to fulfill their full potential as human beings.

### **(3) Right to Privacy/Security**

The outcomes of this session were in the form of 4 recommendations:

1. Message to EU on PRISM/NSA events: the revision of the EU data protection framework should guarantee that EU citizens are protected by EU law on privacy and data protection even when they use foreign online services or platforms
2. Message to EU and European States: Any EU or national legislation should be compliant

with European legislation on privacy and data protection. And any limitation to the right to privacy and personal data protection should be proportionate and absolutely necessary in a democratic society

3. More States should sign and ratify the Council of Europe Convention 108 to harmonize the level of data protection transnationally.
4. More education on privacy and data protection issues is necessary. This should be part of human rights education and should be introduced in schools's curricula.

#### **(4) Realizing human rights online/Enablers and Impediments**

The Question for general discussion was: Where and how do users need to know, and be able to exercise their rights?

After a round where specific barriers and impediments were shared from various perspectives (e.g. community projects for poorer neighbourhoods, issues around visually impaired programs, web uses for deaf persons, uneven funding and resources) immediate issues of concern were:

- Need for education: users, politicians, judges and prosecutors
- Need for transparency of procedures between states and platforms
- Need for quick and efficient remedies for users! Clear procedures

The question about whether Human Rights should be applicable online was not up for debate. This group then discussed procedures about how to make sure that those rights are actually being protected, and exercised e.g. how to ensure governments and corporations comply with guidelines that already exist.

The group noted that

- more transparency and accountability is needed from industry and public sector providers.
- Awareness and education are essential. Users and citizens need to know their rights and which tools are available for them to exercise

their human rights, their citizen rights or their consumer rights. They also need to trust the Internet and for that we may need legislation that not only exists, but can be enforced when this rights are violated.

- One point of disagreement was around the role that regulators should, or should not play, around the extent to which new laws are needed or existing laws are sufficient in ensuring that the above priorities are met.

Summing up the workshop as a whole, three broad themes emerged:

1. The need for concerted awareness-raising about the interrelationship between human rights and internet futures
2. The need for more educational initiatives across sectors (schools, higher education, the workplace) that is broad based about how digital literacy and knowledge about rights are intertwined
3. To advocate to policymakers the need for holistic, human-centred and locally embedded approaches to decisions that affect internet infrastructure, we-design, access, and use.

**Reporter:** Minda Moreira, IRP Coalition

**Breakout session facilitators:** Lee Hibbard, Council of Europe, Marianne Franklin, IRP Coalition / Goldsmiths University, Abbe Brown, University of Aberdeen, Meryem Marzouki, Sorbonne Universités, Thomas Schneider, OFCOM

**Key participants:** Paulo Foncesca, Associação Portuguesa para a Defesa do Consumidor, Rikke Jørgensen, Danish Institute for Human Rights, Matthias Kettemann, IRP Coalition / University of Graz, Michael Rotert, eco

#### **Workshop 5: Connected TV – regulations and consequences**

**Disclaimer:** This is a summary of the EuroDIG meeting, but does not represent the position of a specific organization or institution that attended the workshop.

The issues related to connected TV are so complex that the time available for the workshop was insufficient to cover all the topics outlined on the agenda. However, an exchange of views on most of the topics was possible, thanks to the massive participation of all the main stakeholders.

The exchange touched on, but was not limited to, issues addressed in the Commission's Green Paper (Preparing for a Fully Converged Audiovisual World). A summary was presented to the plenary. The discussion revolved around the following points.

1. One of the key elements discussed in relation to the audiovisual ecosystem (and especially connected TV), is bringing the citizen into the centre of the process. This involves the issue of citizens deciding what to access, when and from where on various platforms. However, in order to fully empower every citizen, a certain number of prerequisites are needed, such as access to media literacy tools and an understanding and full awareness of the role of intermediaries and/or gatekeepers. These tools were discussed in detail in this context. Media literacy is of crucial importance, especially in the medium and long term. It enables not only 'digital natives' but also the rest of the population to understand how to make the best use of the new tools and how to defend themselves from the new threats. When considering media literacy, it is necessary to go beyond definitions of technical skills alone. We need to look at the wider context of how young people use media, the provision of resources and curricula that encourage independent thinking, and literacy about media messages and production conditions. A more inclusive approach to media literacy acknowledges ways that audiences can exercise judgment about the provenance and types of content they consume. Media literacy therefore includes an understanding of protection and enablement in order for audiences and consumers to make informed choices when engaging connected media provisions in the context of social, cultural, and technological change. Understanding the role of the gatekeepers and intermediaries is fundamental. In the conventional TV world the relationship was bilateral: broadcasters to viewers or listeners, with the former deciding what to offer and the latter only able to decide whether they accept or refuse the offer and choose something else. Now the relationship is a lot more complex, with gatekeepers in the middle (for example, the providers of the device, network or software) that might decide what to highlight for the attention of the viewers, whether to alternate the signal, or prevent access to certain offers or provide access to others, etc.
2. The intense debate among all stakeholders has illustrated and confirmed the need to give special attention to some fundamental rights and values underpinning audiovisual policies, such as child protection, data protection, accessibility, media pluralism, cultural diversity, and vulnerable groups (elderly, not affluent). Child protection was recognized by all participants as by far the biggest issue. The safe haven that linear TV was considered as offering to families is no longer available in the world of connected TV. Protection needs to be discussed. Data protection is also one of the key issues, because applying various legislations to the connected TV screen (some of them outside of the European legal space) could endanger European viewers who expect the TV experience to give them the high level of protection that exists in Europe. Media pluralism and cultural diversity also need to be addressed, because the guarantees currently existing for media in the European area could be easily circumvented.
3. The workshop also identified the fact that there are huge opportunities arising from connected devices that could offer new solutions to long-existing problems, such as accessibility or language barriers. But in order to take full advantage of these opportunities, a certain number of conditions have to be met, and results could be achieved only through sincere and planned stakeholder cooperation.



**Conclusions:** We know little of the real consequences of this promising new media development resulting from the merger of broadcast and broadband. We are using conventional models of mass media analysis to look into a still emerging media process.

Connected TV represents a new frontier. So we are faced with a dilemma. It is too early in the game to forecast anything but it is not too late to avoid repetition of the old pitfalls of traditional TV. At the same time we are faced with a 'fast & furious' changing media process.

The final question that the workshop wanted to address was, in the light of all these considerations, how to regulate? Through hard laws, co-regulation or self regulation? From the consumers' or citizens' perspective, we could look into less regulation and/or greater self-regulation. Or even better, we could use rules of principle instead of fixed laws. That way we can adapt faster to this new media ecosystem and avoid the risk of establishing laws that become obsolete the very day they are enacted.

The general feeling was that this new world probably needs less regulation because there will be a shift in responsibility from the media to the citizens/viewers and to the intermediaries. But Europe cannot give up certain values and principles (such as the protection of minors, minorities, vulnerable groups, cultural diversity, media pluralism and privacy) that are pillars of its societal model and its lifestyle. Protection by design and by default could be one of the ways to achieve such goals. Consequently, applicable jurisdiction must remain firmly based on European principles. The issue of how to balance regulation and self-regulation is a process that needs to be decided between the European stakeholders, because it will shape the future of their citizens.

**Reporting team:** Elisabeth Markot, European Commission, DG Connect, Giacomo Mazzone, European Broadcasting Union, Sergio Silva, GMCS

**Co-moderators:** Elisabeth Markot, EU Commission – DG Connect, Pedro Bicudo, Journalist, RTP

**Key participants:** A broad range of stakeholders contributed to this exchange, including representatives from European institutions, national governmental representatives (GMCS); European public service and private broadcasting organizations (EBU, ACT); national broadcasters (Portuguese radio and television); consumer electronics industries (Panasonic); viewers' and consumers' associations (Euralva- IC medianet); child on-line protection associations (InSafe – Safer Internet); specialists from academia (Goldsmith University) and ISP.

### **Workshop 6: Security as a Multistakeholder Model**

**Abstract:** The Internet has become increasingly the key infrastructure and platform for social, political and economic activities. This implies strong dependency on the basic infrastructure and on the services and applications that use the Internet. Therefore it is essential to maintain stability, reliability, security and trust in the Internet. The Workshop covered different aspects and approaches of Cyber Security.

**Key Points:** The panelists are strongly committed to security and constantly improve, enhance and foster the security level on their services and apply most recent technical security standards (e.g. availability and accessibility of services, resilience, data security). The participants of the workshop agreed and concluded that security is shared responsibility. Therefore the key to improve security is working together with all relevant stakeholders in order to improve overall security. An essential aspect is transparency, exchange and information about security threats. Participants identified that the main challenge to improve overall security is to involve all stakeholders - especially on all levels / different sectors / all stakeholders ( IT Hardware Manufacturers, banking sector for example were mentioned).

### **The dialogue with the audience identified key questions:**

1. What is security (especially cyber security)?

A cross-border definition and common understanding of „cyber security“ is necessary. Because all operate globally, it is an global infrastructure, therefore close collaboration and cooperation is necessary to raise the overall security level.

2. What means Multistakeholderism in this context? A complex question, in brief cooperation, transparency, information sharing, engagement and collective learning.
3. How much security is necessary or do we need? There should be a balanced approach and interference with other aspects or fundamental rights needs to be examined (e.g. human rights).

**Summary:** It is essential to have common definition and common understanding of „internet / cyber security“ and Multistakeholderism on an European and likewise an international level. It was consensus that a bottom-up approach is target-oriented and preferable because a top-down approach from governments / regulators without much doubt will not work. Additional self-regulation is a good and efficient way to improve overall security level. Regarding the role of Governments: Governments should act as facilitators, give incentives and encourage the dialogue between the stakeholders, the capacity building and education. Disproportionate Governmental intervention and regulation could have negative impact, lead to less technological innovation and less cooperation. There was consensus that not law and regulation is the solution: Regulation and legal frameworks lead to control, monitoring and enforcement of the compliance with the legal framework and the bottom line to more and more regulation. This will not improve the overall security level. Leading towards the common aim is “smart regulation”.

**Conclusion:** The participants of the Workshop agreed without doubt that security has to be a Multistakeholder model and that there is a shared responsibility of all stakeholders (Industry, Users, Academia, Civil Society, law-makers, Regulators and Governments) in order to improve overall security level.

**Reporter:** Manuel Baros, Henning Lesch, eco

**Moderator:** Oliver J. Süme, EuroISPA

**Key participants:** Sabine Dolderer, DENIC, Marco Hogewoning, RIPE NCC, Richard Clayton, University of Cambridge, Michael Rotert, eco

### **Workshop 7: Accessibility and inclusion - digital participation and democracy for all!**

A successful and interactive discussion took place during the Workshop 7. It can be summarized in 10 recommendations.

#### **Recommendations / We need:**

1. To continue awareness raising activities on the issue and develop a European/Global Fora for discussion in the multistakeholder format;
2. To underline the need for European Framework and policies on the Inclusion of vulnerable, marginalized communities, people with disabilities (taking into account differences of handicaps) in the Information society;
3. To develop tools to measure the implementation of legal Framework and policies to ensure effective actions;
4. To continue developing technical solutions by engaging with private sector and ensuring financial support for European solutions. To continue the work on accessible infrastructure by creating support to European libraries;
5. To ensure the priorities of Universal Design are applied;
6. To recommend to the ICANN and communities working on the new gTLDs program, to develop particular projects for vulnerable communities to create new opportunities for this target group;
7. To adapt and continue working on e-educational solutions and media literacy methodologies to deliver access to content and capacity building tools, and also e-governmental solutions;
8. To focus on the needs of local communities by engaging local communities in the imple-

mentation of legal Framework actions and policies;

9. To present the issue of digital inclusion in business friendly language;
10. To underline the need for National Strategies on digital inclusion, as an outcome of European policies, to be implemented in close cooperation and engagement with local authorities.

**These recommendations can be implemented by:**

- Involving all stakeholders
- Developing a European framework
- Speaking to each other
- Taking care of each other
- Being proud of what we are doing

**Reporter:** Nadine Karbach, IJAB e.V.

**Co-moderators:** Yuliya Morenets, Together against cybercrime, Stuart Hamilton, International Federation of Library Associations

**Key participants:** Sébastien Bachollet, ICANN, Dorina Bralostiteanu, Public Library of Fillasi, Jorge Fernandes, Ministry of Education and Science of Portugal, Irena Kowalczyk, Council of Europe, Mikus Ozols, Telecom Latvia

**Workshop 8: Cross-border hate speech and defamation – living together online**

The aim of the workshop was discuss how to handle hate speech and defamation in shared cross-border online spaces, where not only different national laws but also different social values apply.

**Issues raised:**

- Are current tools to handle cross-border hate-speech and defamation effective?
- Can national laws or Terms of Service efficiently deal with cross-border online defamation and how do they interface?
- Do we have today the tools and frameworks to handle diversity in common cross-border online-spaces?

**Main points of the discussion:**

- **Fragmentation:** Current piecemeal solutions in different national jurisdictions to tackle the problem of hate speech and defamation entail the danger of a fragmentation of cyberspace, e.g. through techniques like Geo-IP Filtering or ISP blocks.
- **Transparency:** Companies are dealing with the definition and restriction of free speech by prohibiting hate speech and defamation in their Terms of Service. Therefore, measures taken by these entities (esp. takedown procedures) have to be transparent for the users to ensure granularity.
- **Education:** The prevention of hate-speech and defamation through education can play an important role, like for example the No Hate Speech Movement youth campaign does.
- **Tools:** Hotlines and safer internet centres are currently the most common tools for internet users to handle online hate speech and defamation.
- **Multistakeholder:** The problem of hate speech and defamation has to be discussed in multistakeholder process to create dialog and identify best practices and to avoid disproportionate measures.

**Reporter:** Nicolas von zur Mühlen, Max-Planck Institute for Foreign and International Criminal Law

**Co-Moderator:** Paul Fehlinger, Internet & Jurisdiction Project, Francisco Seixas da Costa, North-South Centre, Council of Europe

**Key participants:** Adriana Delgado, The No Hate Speech Movement, Konstantinos Komaitis, ISOC, Marco Pancini, Google

**Comments by:** Rui Gomes, Council of Europe

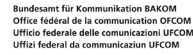
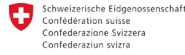
## HOST



Portugal Chapter



## INSTITUTIONAL PARTNERS



## THANKS TO OUR SPONSORS

