

**12<sup>th</sup> Informal Asia-Europe Meeting (ASEM) Seminar on Human Rights**  
**“Human Rights and Information and Communication Technology”**  
**27-29 June 2012 | Seoul, Korea**

**Key Messages**

Modern Information and Communication Technologies (ICTs) have had an unprecedented impact on the promotion and enjoyment of human rights. However, while access to ICTs has improved in recent times, the emergence of a global information society has also raised new challenges in terms of human rights protection. These issues were addressed at the 12<sup>th</sup> Informal ASEM Human Rights seminar, titled “Human Rights and Information and Communication Technology” (27 – 29 June 2012, Seoul).

The Seminar Series is organised by the Asia-Europe Foundation, the Raoul Wallenberg Institute (as delegated by Sweden), France and the Philippines. The 12<sup>th</sup> Seminar was hosted by the Korean Ministry of Foreign Affairs and Trade and the National Human Rights Commission of Korea. The Seminar brought together over 120 participants including official government representatives and civil society experts, representing 42 of 48 ASEM partners to discuss the challenges presented by new technologies in the protection and promotion of human rights. Events open to the public such as a special side event on privacy/data protection and the plenary sessions saw audiences of around 200 participants.

There was overarching consensus that the offline **safeguards that exist for human rights protection should be equally applied online, independent of borders, to all media and formats**. Given how there are multiple stakeholders involved, **the rights, duties and responsibilities of all stakeholders need to be clearly understood**. While governments bear the primary responsibility for protecting their citizens, the discussions highlighted the fact that **government restrictions on ICT usage should be provided by law, pursue specific public welfare interests and be proportionate**. States are also responsible for ensuring that human rights frameworks are equally applied to private and commercial actors who are key drivers in technological progress. Given their easy access to sensitive data, **private sector companies should be subject to appropriate regulatory frameworks and follow ethical Corporate Social Responsibility (CSR) guidelines**.

Civil society is also deeply involved in internet governance. Many organisations that protect online human rights exist but many netizens remain unaware of the assistance available to them. **Digital education, awareness and capacity-building about the appropriate use of new media for various purposes, including social activism, are needed so as to allow citizens and communities control and choice over how to use ICTs**. In particular, there is a need to increase awareness of the importance of data protection and privacy among young people. It was acknowledged that the **internet plays an enormously positive role in enabling access to knowledge and in particular access to cultural goods and cultural heritage**. Governments should ensure that content and technology tools and ICT skills education are available in as many minority, ethnic and indigenous languages as possible

The Seminar convened four working groups for direct and in-depth discussion on the relationship between ICTs and Human Rights. More specifically, the working groups focused on freedom of expression; the right to privacy; the digital divide; and the right to the cultural enjoyment of the internet. Detailed reports of the individual working group discussions can be found in the complete Seminar Report, which will be circulated by the organisers within four weeks’ time.

## General recommendations to ASEM States

1. States should use international human rights mechanisms, peer reviews, and bilateral dialogue to keep up with their Freedom of Expression (FoE) responsibilities. Clear, transparent and effective mechanisms should be spelled out for judicial redress, dispute resolution and mediation if there are accusations of FoE violations. Harmonisation of data protection laws should occur on a regional and global level. Journalists' associations should be strengthened to protect FoE.
2. Governments should publish lists of blocked sites, and the restrictions they place on Internet service providers. Governments should also open up more of their data for analysis and interpretation by citizen groups. For their part, citizens should learn how to protect themselves and their sites with respect to technology and media practices (eg. citizen journalism).
3. Recognition should be given to countries and companies that affirm rights not just in the abstract, but rights on the ground. More countries should be encouraged to expand the Freedom Online Coalition and more companies should join the Global Network Initiative.
4. There is a need for a common, coherent and international understanding of the concepts of privacy and data protection that is fully respectful of human rights guarantees. Common principles on privacy and data protection should apply, such as the right to know, to consent, to access one's own data and to the integrity and security of data. The collection and coordination of privacy legislation, especially in the Asian region, would benefit transparency and cooperation.
5. States not yet having privacy and data protection laws should adopt them – for reasons of human rights protection as well as for reasons of legal security and in order to facilitate trade in ICTs, e-commerce, and the general vitality of the ICT sector. Notably, States should consider the opportunity to join the Council of Europe Convention (No. 108) on Data Protection, which is open globally.
6. Internet gatekeepers, such as search engines and social network providers, are increasingly harvesting user data in order to monetize their services. Governments have a responsibility to provide – both for internet intermediaries and companies more generally – a regulatory framework under which the rights of individuals are protected from the profit-driven data demands from the private sector. Self-regulation is not sufficient. Privacy by design and privacy-enhancing technologies should be promoted. Remedies of individuals against violations of human rights must not only exist *de jure* but also need to be effective.
7. Effective remedies need to be provided on the various levels of regulation and people to be made aware of them. In particular, States should create independent data protection authorities and/or ombudsman institutions. Data protection officers should be installed in private companies handling large amounts of data. The corporate sector should agree to binding CSR principles, as contained in the Ruggie framework (protect, respect and remedy).
8. Digital inclusion is a right for all humans. ICTs are assuming an increasingly central role in all aspects of human and societal development across the world. As a result the ability to access and make effective use of ICTs has evolved into a necessary (albeit not sufficient) condition for the progressive realisation of a wide range of human and other fundamental rights.
9. This central importance of ICTs translates into strong and clear obligations for Governments to work towards digital inclusion by, inter alia, coordinating and intensifying investment in

infrastructure; exerting regulatory oversight to counter oligopolistic market structures; promoting open, non-discriminatory standards and universal design; providing targeted ICT education; protecting user rights and fair access to content; ensuring that alternatives to online services remain in existence; and leading by example and embracing open government principles – all with a particular focus on supporting the groups at risk of digital exclusion.

10. A pro-active, structural approach is required to close digital divides sustainably and prevent new ones from emerging in the context of rapid technological progress. This includes a focus on promoting the design of:
  - infrastructure and software architectures for maximum interoperability, language flexibility and accessibility by differently-abled persons;
  - internet governance institutions to fully incorporate the multi-stakeholder principle and affirmatively engage marginalised stakeholder groups.
11. Governments should actively encourage the development of localisation tools and technology for and by minority, ethnic and indigenous peoples. Localisation helps minority groups promote and preserve cultural and linguistic diversity; it removes barriers to participation and allows access to knowledge, culture and education as well as its dissemination within their own communities. Localisation includes not only content but also technology such as the ability to adapt software in local and threatened languages.
12. Where appropriate, Governments should provide policy frameworks in relation to publicly-funded information and culture that actively encourage the use of open standards where appropriate (open source, open data, open formats, open licences, open access and open education resources) so to ensure public access and re-use of publicly-funded information and culture.
13. Governments should always consider public interest when considering amending or introducing new Intellectual Property laws since they may have chilling effects on the right to access knowledge, culture and education and infringe on other essential human rights. Intellectual Property Rights (IPR) and overly stringent copyright protection, in particular, can threaten the enjoyment of human rights and hamper human creativity online.
14. There are concerns that international trade treaties such as the Anti-Counterfeiting Trade Agreement (ACTA) and the Trans Pacific Partnership (TPP) promote corporate interests at the expense of citizens' rights, and the interests of developed countries over those of developing countries. Governments should consider including the following provisions in multilateral and bilateral trade treaties and agreements:
  - a provision ensuring that any interference with human rights needs to be provided by law, pursue a legitimate purpose and be proportionate;
  - a provision that allows cross border sharing of copyright works created under an exception for the visually impaired;
  - a requirement for open-ended exceptions in copyright including anti-circumvention law;
  - a requirement for safeguards on internet enforcement policies to avoid undue threats to freedom of expression and freedom of Information;
  - an endorsement of international human rights of freedom of expression, freedom of information and other relevant rights.
15. Governments should ensure that the rights of users and public institutions—and the fundamental rights and freedoms such as freedom of expression, right to information, right to privacy—are positively affirmed in both domestic legislation and international agreements on intellectual property.