Keynote Address

Pavan Duggal
Advocate
Supreme Court of India and President Founder of Cyberlaw Asia

Mr. Chairperson
Ladies and Gentlemen

The world moves very quickly and yesterday something happened. Let's look on to the presentation to see what exactly happened yesterday.

This face has captured the world's attention. Who is this? A twenty two year old boy, Why is he in the news? Because he is Richard O'Dwyer who is facing extradition to the United States of America. What did he do? All he did was in 2007 he created a website called TVshack.net, this website enabled you to find free movies online. And then, apparently he committed certain copyright violations in the US. The United States pressed for his extradition and the British government accepted. And now just formalities remain. And while all of this is happening, the Wikipedia founder Jimmy Wales started an online petition to stop this from happening, arguing that "the internet as a whole must not tolerate censorship in response to mere allegations of copyright infringement. As citizens we must stand up for our rights online. Richard O'Dwyer is the human face of the battle between the content industry and the interests of the general public." Ladies and gentlemen, welcome to the new world of online human rights!

Traditionally, Human Rights have always been considered as rights existing in the physical world. Consequently, the entire treatment of the concept of human rights has been developed keeping in mind the physical world alone.

The advent of the World Wide Web and the Internet has brought a completely new dimension to our existence: cyber space. Is one domain that increasingly becoming relevant in our day-to-day lives. The Pentagon has formally recognized cyberspace as a "fifth domain", in warfare which has become just as critical to military operations as land, sea, air, and space.

The numbers of people who are today online are increasing with each passing day. The latest figure pertaining to total number of people since 2000 to 2011 is 528.1%. The internet has ceased to be merely tool for exchange of information. It is a paradigm shift of our lives. Internet is one of the most significant developments in human history after the advent of fire. No other event after the advent of fire had such a dramatic and remarkable impact upon the growth of civilization as Internet has.

And now we have the social media which is the flavour of the times. Increasingly people of the world are coming on social networking sites. Today, Facebook has got more than 900 million users, which is the third most populous nation of the world. And when an increasing number of people are online there is an increasing expectation of human rights and their expectation for protection. In that sense, it is increasingly clear that there is a need for recognizing existing human rights in cyberspace and on the Internet and that these human rights are capable of being violated by different entities in the cyber world, not necessarily states but also private entities and internet providers.

These human rights include the following basic human rights:

- Right to access the Internet as part of basic right to life and human dignity.
- The right to a meaningful life using the Internet.

- The right to use the Internet for living a well-balanced human life.
- The right to freedom of speech and expression on the internet.
- The right to education, knowledge and communication using the internet.

It all started with the advent of ARPANET as a military experiment in 1969. Consequently, the World Wide Web came in the early 1990's, which changed the way we communicate. Today in 2012, at just over four decades of the advent of the Internet, it is time for jurisprudence of the world to evolve in the context of human rights and cyberspace.

In fact, the entire concept of human rights has to be expanded to be interpreted in the context of cyberspace, the Internet and ICT. When one examines the jurisprudence of different countries across the world, one finds that there is hardly any development in the said jurisdictions pertaining to legal recognition of human rights in cyber space. Thus, there is a need for the legislations of different countries to enshrine and specifically legally recognize the concept of human rights in the context of cyberspace. There is also a need for amending the national legislations to provide with appropriate practices, procedure and processes which institutionalize the process of protection and preservation of human rights in cyberspace as also human rights in the context of Information and Communication Technologies. The abuse or violation of human rights needs to be specially deprecated and there is a need for providing penal provisions, which penalize such violations of such human rights. When one is to analyse such scenarios, one often finds that there is an intrinsic conflict between, the existence and preservation of human rights on the one hand, and the requirements of national sovereignty, interest, integrity, and defence on the other. The last four decades have demonstrated that the sovereign state would not hesitate to come down on any activity in cyberspace, which would tend to prejudicially impact or affect any aspects pertaining to national security, integrity, and defence of the relevant sovereign nation.

Violations of human rights in the physical world have had a direct impact in cyberspace. The Arab Spring Revolution is a case in point which has demonstrated in no unclear terms that contraventions of basic human rights in the physical world is likely to create rumbles and thunders in cyberspace which can be enough to impact and overthrow existing political regimes. There is a need for updating and expanding the scope and interpretation of the existing international legal instruments relating to human rights. These would include the Universal Declaration of Human Rights 1948; the International Covenant on Economic, Social and Cultural Rights 1966; and International Covenant on Civil and Political Rights 1966, so as to make the said interpretations relevant and in sync with the context of the evolution of ICT and cyberspace. It is my belief that a Charter on the protection and preservation of human rights in cyberspace needs to be drawn up and signed.

The existence of a digital divide can be found everywhere, not only between Asia and Europe as continents, but also as regions. And in the context of Europe and Asia, there is a need to learn from the experiences of each other.

Cybercrimes today are increasingly gaining the attention of sovereign nations. Broadly speaking there exist today three categories of cybercrime:

- Cybercrimes Against Persons
- Cybercrimes Against Property
- Cybercrime Against Nations

Cybercrimes today are becoming impediments and obstructions to the enjoyment of online human rights. The inability of the states to control cybercrimes effectively contributes to the violation of human rights in the ICT.

The advent of mobiles and Mobile Internet has given a unique twist to the entire issues. Mobiles can not only ensure the expeditions identification of human rights misuse but also can

be the target of immense state surveillance. And that is why a new branch of law emerging known as Mobile Law, which looks at all legal issues pertinent to the use of electronic devices and portable communication. This legal branch seeks to preserve human rights in the mobile ecosystem.

Clearly, the Internet is no longer a phenomenon, but rather it is a way of life and culture. The right to access and be a part of this way of life and culture is a pre-requisite in today's context. I would like to take this opportunity to mention a case study from India, the land from which I come from. The Indian approach is different and customized to the needs of India itself. In recent days, a number of media have reported social media censorship in India, but nothing is further than the truth. The Information Technology Act, 2000 has been amended in 2008. The Information Technology Rules, 2011 has stipulated certain due diligences to be done by intermediaries, while discharging their obligations under the law. The Indian approach to Unique Identification Number or Aadhaar Numbers is managed by the unique Identification Authority of India. Clearly, there are challenges in terms of privacy, data protection and cyber security- currently being worked out through draft legislation pending review. Hence, there are more advantages than challenges in the context of Indian eco-system.

Indeed, India has long played an important role on the Internet. And Indian approach to Internet Governance has been shown in the following ways:

- India has been partici[ating in the ICANN process
- India is a part of the WSIS process and committed to the Internet Governance Forum
- India hosted the IGF in Hyderabad 2008
- In 2011, India has mooted the establishment of a new institutional mechanism in the United Nations for global internet related policies, to be called the United Nations Committee for Internet Related Policies (CIRP)

The intent behind proposing a multilateral and multi-stakeholder mechanism is not to "control the internet" or allow Governments to have the last word in regulating the internet, but to make sure that the Internet is governed not unilaterally but in an open, democratic, inclusive and participatory manner, with the participation of all stakeholders. The idea is so that we can evolve universally acceptable, and globally harmonized policies in important areas, and further pave the way for a credible, constantly evolving, stable and well-functioning Internet that plays its due role in improving the quality of peoples' lives everywhere.

Moving from India to the international scene, there is going to be increasing tension between the existence, preservation and protection of human rights in cyberspace on the one hand and the inherent rights of sovereign nations to protect and preserve their national sovereignty, integrity, security and defence on the other. But clearly, on obtaining a meaningful balance between the two, relevant conflicting directions will lie the way forward for a meaningful growth and development of jurisprudence around human rights in ICT in the coming times.

It is my belief that nation states have to realize that if they continue to trammel upon and contravene basic human rights in cyberspace and ICT, there is a likelihood of more Arab Spring Revolutions evolving with much greater intensity which could have an immense impact upon the existing political regimes in different parts of the world. The governments of the world have to realize that cyberspace is a paradigm that is not capable of complete absolute control by the state. Sovereign nations will have to learn to respect, protect and preserve basic human rights in cyberspace. The violation of the same can only be an exception by the state and not by the rule.

There is an underlying necessity for recognizing that trammelling or violation of basic human rights in cyberspace and ICT would constitute crimes against humanity. It is indeed time to broaden the scope of definition of "crime against humanity". As new technologies cannot be

predicted it is important recognize the importance and potential threat of crimes such as cyber-terrorism, cyber-crime, breach of cyber security, and cloud computing and its ambiguities. “Crime against humanity” includes inhumane acts intentionally causing great suffering, or serious injury to body or mental or physical health when committed as part of a widespread or systematic attack directed against any civilian population, with knowledge of the attack. There is virtually no work happening in this direction. The beginnings have to be made.

It is in this context that organizations like the Asia Europe Foundation and ASEM Seminar on Human Rights could be the initial starting points for the development of work and steps in that direction. I would urge the 12th ASEM Seminar on Human Rights and Information & Communication Technology to come up with specific declaration in its conclusions which will encourage relevant stakeholders to recognise the existence of the concept of basic human rights in cyberspace and further work towards the evolution and development of jurisprudence around the protection and preservation of human rights in cyberspace and ICT. The future is a dynamic future! It is a completely dynamic evolving picture. All relevant stakeholders whether it is the state, civil society, lawyers, judiciary, law-enforcement and the netizen community at large, need to contribute to the process of development of jurisprudence around the growth and protection of human rights in cyberspace. Only in a sustained development and progressive evolution of human rights in the context of ICT and cyberspace lies the way forward for the healthy meaningful growth and evolution of cyberspace and concerned relevant jurisprudence in the coming times.

Thank you ladies and gentlemen.