UNITED
NATIONS

E

Economic and Social
Council

Distr.
GENERAL

E/CN.4/2005/NGO/266
10 March 2005

ENGLISH ONLY

COMMISSION ON HUMAN RIGHTS
Sixty-first session
Item 19 of the provisional agenda

ADVISORY SERVICES AND TECHNICAL COOPERATION IN THE FIELD OF HUMAN RIGHTS

Written statement* submitted by the Transnational Radical Party (TRP), a non-governmental organization in general consultative status

The Secretary-General has received the following written statement which is circulated in accordance with Economic and Social Council resolution 1996/31.

[11 February 2005]

* This written statement is issued, unedited, in the language(s) received from the submitting non-governmental organization(s).

In February, the Transnational Radical Party contributed with a document to a meeting organized under the auspices of the Netherlands National Commission for UNESCO, which focused on the World Summit of the Information Society (WSIS). The TRP believes that they may also interest the debate on technical cooperation in the field of human rights.

What follows is a question and answer session of the original document.

To what extent and in which ways are governments entitled to interpret and restrict human rights with an appeal to the culture and traditions of the country?

Too often "culture" and "tradition" are code-words invoked to keep at distance the notion of the universality of human rights and the need to implement measures to respect them the world over in a consistent way. If we are to accept "cultural relativism" as a guide in international deliberations, one could also argue that the "digitalization" of the world should not be considered appropriate, if not a priority, for developing countries that need more basic assistance and infrastructures.

The TRP, which for years has denounced the systematic violation of fundamental rights by dozens of governments, regardless of their political ideology, believes that the overall approach of the WSIS should be based on existing Covenants, Treaties and declarations, the so-called "international bill of rights", and that emphasis should be given to the need to promote their widespread ratification and just enforcement.

How are the interpretations and restrictions of human rights influenced by the arrival of the Internet?

Over the last few years, and for a variety of reasons, there has been a worrying development towards censorship in all countries. Restrictions of freedoms have also affected the virtual world and have been promoted mainly under the banner of "national security". The nature of those governmental concerns has made it almost impossible for international entities, be they inter or non-governmental, to "interfere" with the imposition and enforcement of such restrictions, as "national security" is THE top, and unquestionable, priority of any individual government.

Recently the Commission on Human Rights has tried to address these issues taking into consideration the ways in which States respect human rights while for instance combating terrorism. Such an exercise should also be extended to the WSIS also for the possible implications/suggestions it may have concerning the Information Society and human rights.

Despite the generally held view, the Internet is far from being a neutral space. In fact, the Net is a place where the code that has been used to design its architecture represents its own internal peculiar law. In such a context, the restriction of human rights, in particular those related to freedom of speech and of the press, but also those concerning all sorts of exchanges, can be conducted both through national legislations and technical modifications aiming at censuring Internet sites that Governments consider "dangerous" in general, a "threat to national security" or "blasphemous".

From a human rights perspective, it is regrettable, that prominent sites such as *Yahoo* and *Google*, among others, have for instance allowed the Chinese authorities to redirect "political" Internet searches to commercial and/or governmental websites. At the same time, it is extremely

worrisome that other developed nations have recently adopted, and are intent in promoting abroad, legislations that criminalize peer to peer file swapping. In fact, not only such a technique is mainly used to exchange personal files and/or information of all types, but it represents a medium for software programmers to work. Should these examples become a pattern of legislative decisions, the private sector, often considered to be the beacon of liberty, may become responsible of condoning censorship impeding the promotion of intellectual and political debates over the Internet posing an additional hurdle in the promotion of human rights.

Are international agreements on these rights sufficiently adapted to the digital era?

They may not be sufficiently adapted but certainly easily adaptable. The digital era has only created a new environment for all sorts of exchanges, new rules may not be necessary as long as existing ones are implemented fairly.

On the other hand, the TRP is concerned about several measures that have been devised to strictly enforce Intellectual Property Rights through penal law. While it is of utmost importance to ensure that inventions remain a profitable activity, at the same time, too strict regulations and/or too broad "patentability" can pose serious threats to different types of innovations.

The TRP has always expressed its concerns on the issue of cyber-crime, and cyber-terrorism, and the measures that several governments have adopted to prevent those phenomena. A series of governmental decisions has recently come under scrutiny exposing their shortcomings. In fact, while promoting non-violent responses to certain restrictive and intrusive laws may sound an appropriate activity in a democratic society, for a secretive and authoritarian regime it can amount to terrorism.

The TRP believes that once again, we are walking the fine line of "national security", which defines the ways in which governments treat "cyber-crimes". The fact that "new technologies" are also a hot item for the press has instigated harsher legislative reactions to activities carried out in the virtual world than on those pertaining to the "real" drastically changing the concept of individual criminal responsibility. To make just a couple of examples, it is in fact questionable to hold Internet providers accountable for the views and/or activities or their customers (be they political views, pornography or paedophilia), or to criminalize peer to peer file transfer or to impose on developing countries a high economic burden to enforce law and order policies on Internet piracy, without considering the overall budgetary constraints of those countries.

How should public authority ensure the safeguarding of these rights considering the international character of the digital environment and the role of private enterprises in facilitating digital communication?

Any penal code that is rooted in the norms contained in the International Covenant on Civil and Political Rights should be considered as fit to regulate any violation of the individual sphere also in the virtual world. The drafting and adoption of special, if not extraordinary, laws may not only delay the process of the launch of a universal Information Society, but also, may run the risk to subject the "necessity" to regulate the cyberspace to national legislations. International cooperation is certainly a pivotal component of 21st Century world affairs, but when it comes to "harmonizing" norms, the threshold should be set on the highest possible standards. To this end it is crucial that democratic governments prepare the ground for a successful outcome of the WSIS.

In the digital era, those laws on copyright, patents and licenses, which fuelled creativity during the last two centuries, making it become an incredibly lucrative business, are running the risk to slow down innovations or impede them all together if applied without taking into consideration the fact that the Internet should also be considered as a new form of "commons", where transactions can interest different types of fields and not necessarily only economic ones; a context where spontaneous collaboration may be the norm and not the exception.

Private enterprises with a high interest in the economic possibilities of the digital world should work towards the development of industrial models that take full advantage of the new medium and adjust to an interconnected world that relies on synergies, symbiosis and singularities rather than imposing existing standards on the virtual domain. The Net is also a community where individuals have demonstrated a sincere interest as well as professional skills in participating, in a collaborative way, in economic as well as humanitarian enterprises. Those extraordinary projects should not be prohibited by law.

Is the restriction of the freedom of private life with an appeal to protection of national culture and traditions compatible with fundamental human rights?

The need to combat terrorism is generating an increasing negative influence on political decisions vis-à-vis privacy rights. Many Governments are appealing for the inclusion of generalized and massive surveillance laws to strengthen national security in order to protect their citizens. The general data retention of individuals' electronic communications (via telephones, mobiles, SMS/text messages and Internet) by law enforcement authorities, will create new risks to personal privacy, political freedom, freedom of speech, and, many fear, also public safety. Moreover, because of the cross-border nature of Internet communications, a decision taken by a State, or limited to specific parts of our planet (e.g. the European Union) could have repercussions that may reach far beyond the targeted areas, posing legal and jurisdictional problems that, by now, the international community seems unable or unequipped to address.

Several studies carried over the last few years by major security analysts, have exposed the fact that the inability to prevent terrorist attacks is not due to the lack of information, but to the inability to process and analyze the information "routinely" gathered. Nevertheless, several democratic countries disregard this kind of analysis and have adopted the legal basis to implement generalized and systematic surveillance of citizens' communications.

Moreover, the bureaucratic/technocratic and illiberal procedures that have drawn this kind of legislations, not being adopted by clear, transparent and political decisions, may represent a new and worrying threats to civil and political liberties. The TRP believes that far from providing more security to citizens, these procedures divert energy and resources from more effective human intelligence analysis activities.

The TRP is of the opinion that the solution is not to expand the collection of data to the entire population, but rather to focus on the collection and analysis of the data and intelligence obtained. The TRP believes that among the root causes of terrorism, as well as instability, there is the lack of political freedom, therefore, there is an urgent need to promote the building of democratic societies based on the principle of rule of law also through "virtual" means.

Should states allow private companies to use information about citizens' behavior on the Internet for commercial purposes?

As in all transactions, all parties involved should be aware of their rights and obligations as well as the ways in which the information is gathered and processed. In any case, private companies should specifically request the possibility to retain the personal data of their customers and should not be allowed to buy or sell it to other companies. Moreover, the TRP believes that the use of proprietary software may pose a problem in cases when alleged mismanagements occur and inquiries are needed. There should also be a clear separation between commercial and governmental uses of the information gathered.

Or may States even oblige companies to keep these data for a certain period of time?

The issue of data retention is a very critical one and poses serious problems vis-à-vis individual privacy as well as those aspects that concern the ways in which private information is elaborated and shared with other public and/or private entities. It needs to be noted for instance, that existing European norms, impede the generalized use, also for security reasons, gathered for commercial purposes. In fact, article 6 (2) of the European directive on electronic reservation (EC 2299/89) clearly prohibits the transfer of personal data without the explicit consent of the passenger.

The TRP believes that in obliging private companies to discharge a mandate that is usually "institutional", we are running the risk of privatizing public functions without establishing transparent and clear accountability mechanisms to ensure the full enjoyment of individual rights. The non transparency in the procedures and the lack of individuals' consent in the exercise may, in the medium-long term, create more problems than the positive outcomes that it pretends to provoke. In any event, the TRP believes that individual prior consent should be requested for any data gathering and sharing, and, should national security issues be at stake, proper judicial procedures of due process and fair trial should be applied.

- - - - -