2012 4th International Conference on Cyber Conflict
C. Czosseck, R. Ottis, K. Ziolkowski (Eds.)
2012 © NATO CCD COE Publications, Tallinn

Impact of Cyberspace on Human Rights and Democracy

Vittorio Fanchiotti
Faculty of Law
University of Genova
Genova, Italy
vittorio@unige.it

Jean Paul Pierini
Fleet Command
Italian Navy
Rome, Italy
pierini.jeanpaul@libero.it

Abstract: This paper focuses on the asserted 'boundlessness' of cyberspace in order to examine how and to what extent jurisdiction, in its various meaning and forms (jurisdiction to prescribe, to adjudicate and to execute), over activities taking place in the cyberspace may be asserted and even exercised, based on traditional jurisdictional links and also on new trends. The paper also examines conflicts of law in civilian (mainly tort laws and laws on the protection of rights of the personality as well as intellectual property) and criminal matters. Determining what set of rules applies to a certain fact or situation implies a reference to those rules establishing where such a fact or situation has legally taken place and is to be localised (*locus commissi delicti*), and a reference to main criteria including those focusing on the conduct, the localisation of the hardware, the effect, the access to the informatics system, the accessibility of the information and future trends. The paper further highlights that the enforcement of activities in cyberspace appears to be affected by an assimilation to traditional forms of investigative activities, such as search or inspection or even the interception of communication or data flow, which are to a certain degree misleading in respect of the specific means employed. A specific reference to the role of providers in enforcement activities is also included. The second part of the paper deals with the traditional human rights relevant to cyberspace and to the broader concept of 'right to access' cyberspace, as well as the uncertainties derived from the fact that a plurality of state and non-state actors may limit and interfere with human rights in cyberspace. The paper specifically deals with the commercial dimension of cyberspace and with eventual corporate liability for human rights violation (multinational corporations violating rights to privacy in connection with or on behalf of states or enforcing censorship) based on US legislation and also taking into consideration European trends. The paper finally highlights the supportive role to the protection of human rights of regulatory bodies enforcing fair-trade and anti-trust regulations, and the multinational dimension of free trade in promoting human rights, by eventually considering restrictions in cyberspace and censorship as restrictions to trade under WTO agreements.

Keywords: *jurisdiction, enforcement, conduct, effects, antitrust, fair-trade, censorship, WTO*

1. IS CYBERSPACE REALLY WITHOUT BOUNDARIES?

Cyberspace, which is still lacking a standard and universally accepted definition, identifies a domain encompassing the digitalised information itself, as well as the infrastructure (including satellite telecommunications), server networks, computers and especially the internet, that makes the spectrum useful. However, cyberspace is mostly defined by how it is used and is identified with the World Wide Web.[1]

Accessing and transmitting information through the World Wide Web has become a significant part of contemporary lifestyles and entertainment, and has progressively developed into an awareness of a global community where the individual has the ability to connect socially and directly with other individuals without apparent political, social or racial borders. So called 'second life' social experiences, where the individual shows up through an 'avatar' giving them their identity of choice, have also reinforced the idea of cyberspace as a domain in which the individual may find, develop and exploit their own 'parallel reality'.

Influential literature from almost four decades ago significantly altered the perception of cyberspace and the web and, together with an increased awareness of the right to access directly information and knowledge (also as a substitute for declared but not sufficiently implemented human and social rights, to include the right to information), encouraged the perception of cyberspace as a 'global common'. The latter concept encompasses those goods and rights which are not suitable for appropriation by any state, entity or individual.

While 'virtual reality' has heavily contributed to the misconception of cyberspace as a space not marked or flagged by any state sovereignty, control or even governance, the potential for social connection and direct access to information and knowledge has contributed to the idea that within cyberspace (and specifically for those accessing it) exchange of information should be free and unhampered by rules and laws.

This said, in the authors' views, the assessment of the legal consequences of phenomena taking place in cyberspace, and the evaluation of the consequences of setting roles, should not be affected by the suggestion of cyberspace as a non-physical realm and, in general terms, by cyberpunk literature, as such phenomena always have a specific physical dimension. They are also linked to a clear geographical dimension represented by server location, point of access, human conduct and a legally appreciable effect.[2] Accordingly, the legal reasoning should not be altered by the social perception of cyberspace which is, to a substantial part, influenced by

1 For this purpose see Maj. Gen. Mark Barret, Dick Bedford, Elizabeth Skinner & Eva Vergles, *Assured Access to the Gobal Commons*, Supreme Allied Command Transformation, North Atlantic Treaty Organization, Norfolk Virginia, USA, April 2011, p. 35.

2 The idea is nonetheless reflected in the Explanatory Report to the European Cybercrime Convention, adopted on the 8th of November, 2001 at Budapest, CETS/SEV No 185, recalling, at § 7, the decision CDPC/103/211196, of the European Committee on Crime Problems (CDPC) reached in November 1996, stating that 'by connecting to communication and information services users create a kind of common space, called 'cyber-space', which is used for legitimate purposes but may also be the subject of misuse. These 'cyber-space offences' are either committed against the integrity, availability, and confidentiality of computer systems and telecommunication networks or they consist of the use of such networks of their services to commit traditional offences. The transborder character of such offences, e.g. when committed through the Internet, is in conflict with the territoriality of national law enforcement authorities'.

the idea that the web pages visited are hosted on a server somewhere in the unknown, simply because it is more exciting than associating the IP address to a certain location.

Wrongs committed through information technology almost entirely rely on the transmission of information and very often displace law enforcement mechanisms which do not benefit from equally advanced forms of judicial and police cooperation, effectively having the effect of a 'force multiplayer'. As such, certain legal difficulties in the repression of crimes, and also civilian torts, may have also contributed to the perception of cyberspace as a borderless domain, overarching a context of legal systems, each of which is jealous of its own prerogatives. Clearly, those willing to commit crimes find it easier to cross borders through the web than a law enforcement officer does in order to deter, stop, take evidence or arrest.

On the other hand, 'the critical nodes, or "gateways" to cyberspace … are entirely in the hands of commercial enterprises … internet service providers (ISPs) connect computers to the internet, while web hosting services maintain websites on the World wide web … browsers like Internet Explorer, Safari, Chrome, and Firefox make such content accessible.'[3]

Significant interest has been raised by 'cyber attacks' from the military perspective as an autonomous pillar standing aside from the traditional fight against cyber crime, with which it shares uncertain borders. This may be considered a consequence of the yet to be clearly determined threshold at which criminal activity becomes a military attack which may trigger the use of force in self-defence (to include offensive cyber responses under traditional principles of international humanitarian law, once the crucial issue of distinction between civilians and combatants/civilians directly taking part in hostilities has been addressed in a satisfactory way), but is also due to the fact that the reaction to a direct armed attack is easier to justify than violating the sovereignty of another state for a cross-border arrest.

Not being influenced by an indeterminist notion of one or more 'parallel virtual' universes does not mean that legal concepts, especially those defining enforcement activities (e.g. online searches) should not evolve to take technical developments into consideration and be correspondingly adapted in order to be more effective and also to preserve the essence of guarantees.

The social perception of cyberspace, and furthermore the role played by cyberspace in making knowledge available and a global community accessible, should be clearly taken into consideration when it comes to ascertaining if democratic rights stated in modern constitutions and human rights instruments have changed their essence and now encompass, through the web, a new dimension. These rights include those dealing with freedom of speech, the right to express opinions, the right to information (as well as the right to inform), and associative rights, as well as the right of the individual to develop him/herself in a social context.

On the other side of the coin, depicting the access to cyberspace is the dimension of data protection and the right to informational self-determination of the individual; a right which is endangered by the delocalisation of addresses.

3 Maj. Gen. Mark Barret, Dick Bedford, Elizabeth Skinner, Eva Vergles, *Assured Access to the Gobal Commons*, Supreme Allied Command Transformation, North Atlantic Treaty Organization, Norfolk Virginia, USA, April 2011, p. 35.

This new dimension of the right to access knowledge may pose specific problems with respect to copyright and related rights, which may in the future encounter the same limits as those set to advances in biotechnology and certain patents, and specifically the avoidance of 'excessive protection'.

2. CYBERSPACE AND STATE JURISDICTION

Despite the deceptive reference to cyberspace as a domain without boundaries, phenomena taking place within such domains are based on several criteria subject to state jurisdiction to prescribe, to adjudicate and to execute.

Establishing where a certain activity fulfilling the conditions for the application of a criminal provision took place has always raised legally harsh questions.

'Jurisdiction to prescribe', which identifies with the ambit of application of substantive laws which are eminently territorial, encounters in general terms the main limit of the prohibition to interfere with domestic issues of another state. Prescriptions issued extraterritorially to nationals and foreigners may be subject to the double criminality requirement as a postulate of justice. This requirement is commonly waived when the prescription pertains to the protection of core interests of the state or interests whose protection is generally recognised. In both cases, the effective protection of the interest may not be conditioned by the attitude of the state on whose territory the conduct took place.

Cyberspace is a highly regulated domain in which the territorial regulations may define legal obligations of ISPs, web hosting, commercial enterprises relying on the web in order to do their business, search motors, hardware, software and application producers and sellers, internet points, hot-spots, those collecting, storing, analysing and transmitting personal data, individuals accessing the web and downloading data, and even those travelling through the territory of the state with devices containing stored information. Territorial prohibitions under criminal law may well pertain to the establishment of criminal sanctions for hacking and illegal access to information systems located within the territory or accessed from such a territory, or simply disrupting public services on the territory of such a state.

Regulations eventually perceived as 'extraterritorial' may pertain to content of internet pages accessible from the concerned state, whereas evidence of access may well suit the requirements for the territorial commission of certain crimes, as in the case of libel, racist and xenophobic material, denial, gross minimisation, approval or justification of genocide, or crimes against humanity.[4]

Despite the instant or almost instant character of data transmission, consequences of the transit of certain information through the infrastructure and nets located in the territory of a certain state could be considered by the state for the exercise of jurisdiction to prescribe, based on the existence of available technical means. Current rules developed under international law on jurisdiction over space objects may sustain the exercise of jurisdiction to prescribe in respect of data flow through communication satellites.

4 For this purpose see the 'Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems', produced in Strasbourg on 28 January 2003, CETS/SEV No 189.

One current trend in law-making may be seen in the establishment of obligations for commercial enterprises offering cyberspace-related issues which are invested by a 'guarantee position' and increasingly held liable, either criminally and/or under tort laws, for content of hosted web pages including child pornography, commercial offers of counterfeit goods, libellous content and violation of copyright and related rights.[5] Such enterprises are encouraged to develop commercial arrangements with those benefitting from their services and establish proper procedures in order to control such contents through technical means.

The debate on the relevance of the conduct or the effect caused by such conduct, in order to establish the jurisdiction to adjudicate as a consequence of the definition of the crime as 'territorial' under the criteria for the establishment of the *locus commissi delicti*, dates back more than a century to the so-called 'Cutting case' of 1886.[6] This concerned the publication by a US citizen in the border town of El Paso of a defamatory article against a Mexican citizen, where the newspaper circulated in the Mexican city of Paso del Norte. Currently there is a wide practice for the sufficiency of either the conduct, or the realisation of part of the effect the criminal provision was aimed at preventing, in the territory of a certain state in order to consider the crime committed in the territory of that state (so-called ubiquity theory).

A recent issue which falls in between the jurisdiction to prescribe and the jurisdiction to adjudicate (at least where the latter is a consequence of the way the incriminating provision is drafted) is represented by the disclosure through the posting through an access point in State A of information classified in State B.

For this purpose it should be observed that some states consider a crime to have been committed in their territory when the crime aimed to realise its effects there but did not do so or, with respect to the crime of conspiracy, the (foreign) conspiracy aimed to commit a crime in the territory of such a state. Both variations imply the relevance of the mental element and do not seem to be of any particular value with respect to cyber crimes.

An interesting doctrinal debate dating back more than a century was aimed at clarifying the jurisdictional consequences of a libellous or an explosive letter sent from the territory of State A to the territory of State C, where it realises its offensive purposes, after having travelled through the territory of State B.[7] The concept of transit of digital data through the territory of a state (and its gateways, net, nodes, servers and even communication satellites as space objects) could be actualised in order to affirm that in such a state a material part of the conduct/ effect of the crime has taken place and in order to trigger its jurisdiction in a wider sense. The latter could be identified as a suggested trend in the development of the jurisdiction to adjudicate, with

5 Article 10 of the Cybercrime Convention refers to infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty and International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention).

6 References on the relevant documents in Lothar Bergmann, *Der Begehunsort im internationalen Strafrecht Deutschlands, Englands und der Vereinighten Staaten von Amerika*, Walter de Gruyter & Co., Berlin, 1966, p. 7ff.

7 The question on the relevance, for the determination of the *locus commissi delicti*, of that part of the conduct which, due to the intervention of other individuals (and also non human intervention), may further the conduct to its effect, is raised by Friedrich Meili, *Handbuch des internationalen Strafrechts & Starfprozessrechts*, Orell Füssli, Zürich, 1910, p. 119.

respect to crimes committed in or through cyberspace. It could also eventually be identified in the transit of data instrumental to a crime (eventually autonomous and not linked to the above referred broad definition of the *locus commissi delicti*) and also the prorogation of jurisdiction with respect to the violation or elusion of orders prohibiting or banning certain content from websites. Nevertheless, it should be taken into account that 'libel jurisdiction' in so called 'common law' systems currently requires, with respect to web-related cases, a 'substantial publication' which may well be considered an effect requirement of the conduct. Obviously the active and passive personality principles with respect to the exercise of jurisdiction to adjudicate may also provide guidance for crimes committed in or through cyberspace.

As a result of the evocative descriptions of cyberspace as a 'non space' and a legal limb – a description we currently do not agree with – cyberspace could be qualified as a 'non foreign' territory, similar to those ancient regimes labelled as 'lawless territories' (and the politically incorrect version referred to as 'non-civilised territories') where the jurisdiction to adjudicate was asserted without those limits, relying on the criminal character of the conduct in the place where it took place.

In order to exercise the jurisdiction to adjudicate, either of the criteria for the exercise of the jurisdiction to enforce should be fulfilled in order to prevent the further continuance of the crime, to identify the authors of the crime, to identify the victim and material witnesses, to gather and secure evidence and to prevent the escape of those having committed the crime. As an alternative to jurisdiction to enforce, suitable international agreements (or agreements within the EU domestic legislation implementing EU legislation on judicial cooperation) may assist.

Jurisdiction to enforce is eminently territorial and is exercised with respect to individuals, as well as goods, which can be found within the territory of the concerned state. With specific reference to conduct taking place in or through cyberspace, the territoriality principle implies the possibility to seize (physical) servers and data stored on servers located in the territory of the concerned state. Further (almost) territorial enforcement may refer to the so called expedited preservation of stored computer data,[8] the expedited preservation and disclosure of traffic data[9] and the 'production order' through a person or more frequently an ISP, even if the data are stored on a support physically located elsewhere as 'data in transit' until downloaded[10]. An enforcement activity with potentially extraterritorial reach is represented by the securing of information through an access point to the web.

The practice of telecommunications taping shows that, due to technical reasons, in specific circumstances the territorial state may not be in a condition to intercept a target within its territory and may need to rely on a third state which is able to enforce the measure. The latter state has a reduced interest in exercising supervisory jurisdiction, as the target is not in its territory and acceptance may be presumed after the expiry of a short notice. These issues have been partially addressed in the *Convention established by the Council in accordance with*

8 Such measures are established under art. 16 of the Cybercrime Convention.
9 Such measures are established under art. 17 of the Cybercrime Convention.
10 Search and seizure activity under article 19, paragraph 1, of the Cybercrime Convention, mentions the 'same territory' requirement only in respect of 'computer-data storage medium in which computer data may be stored' (lett. b) and not also in respect of a computer system or part of it and computer data stored therein (lett. a). The Explanatory Report § 192 states that 'the reference to "in its territory" is a reminder that this provision, as all the articles in this Section, concern only measures that are required to be taken at the national level'.

article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between Member States of the European Union, produced in Brussels on the 29th of May 2000,[11] article 18, 2, lett. *c*) .

Remote (live) access to information located on a physical support in the territory of a foreign state may to some extent infringe the territorial sovereignty of such a state. Remote (live) access represents one of the enforcement measures, to some extent similar to the traditional physical search of property.

In the recent past the German Constitutional Court confronted the issue of so-called 'online search' of hard discs, authorised under police laws of one of the German *Länder* for preventative purposes[12]. The Court set aside the law due to the inadequate definition of the prerequisites for the measure and deemed the constitutional provisions of measures impacting on communications rather than those on home search applicable. The judgment opened the way to several laws, including federal law.

Current practice shows that hard disc searches were performed through a trojan which infected a specific information system rather than through a remote (live) search. Furthermore, chronicles suggest that not only devices targeted with a specific authorised measure were infected, but in some case, devices were infected directly by customs when imported, by creating a *de facto* backdoor.[13]

This practice is questionable under the rule of law principle, as at least preparatory measures for a hard disc search and further measures, such as the parallel sending of calls to other unwanted recipients or the unwanted video-taping and photographing through the device, are adopted without judicial oversight even if the early infection of devices does not represent *per se* an interference with the individual who later purchases the device. Pre-installing a trojan in a device which will later connect with law enforcement activities instead of remote (live) access to a physical storage device in the territory of the state may determine a more vague interference with the jurisdiction and sovereignty of the foreign state where the device may later be located, as the interference may be considered a *de facto* effect of a previous law enforcement activity.

One aspect still to be examined is represented by the possibility that infection of information technology devices through trojans results in cross-border implications; that is, the element of provisions of criminal law in states where the device or system is located or from whose territory it is sending out unwanted information. Unclear legal procedures in the state enforcing its laws via trojans may result in the review of the authorising procedures and the denial of a claim for the legitimacy of the measure.

Apart from possible extraterritorial implications of the use of trojans as a law enforcement tool, state hacking methods, which are already a reality, imply the development of new patterns for

11 In EU Official Bulletin, C 197, 12th of July 2000: On the provisions dealing with telecommunications, *See* Barbara Huber, *Forschungsprojekt §12 FAG und Überwachung der Telekommunikation*, in, Wolter – Jürgen – Schenke, *Zeugnissverweigerungsrechte bei (verdeckten) Ermittlungsmassnahmen*, 2002, p. 61ff.

12 Marie-Theres Tinnefeid, *Online-Durchsuchung: Menschenrechte vs. virtuelle Trojaner*, in MMR, 2007, n. 3, p. 137ff.

13 Claim of the legal firm AFB *(Strafanzeige gegen den Einsatz des „Bayerntrojaners' gegen Staatsminister Joachim Herrmann, LKA-Präsident Peter Dathe sowie weitere Personen)* on the 17th of October 2011.

the judicial oversight of law enforcement activities which effectively take into account the risk of abuse by law enforcement agencies, as well as the risk of misuse by other subjects.

These patterns for judicial oversight should prevent systematic and mass infection of devices, establish an expiration date for pre-implanted backdoors, ensure proper and independent expertise on the part of the authorising judge, include inhibitory actions for those allegedly affected and, finally, establish proper liability mechanisms for those damaged by the measure.

In order to prevent conflict of jurisdiction in the form of conflicting decisions as to the legitimacy resorting to trojans for the surveillance of information technology devices, new international instruments should be developed and should refer to a mutual recognition of surveillance measures, based on information and access sharing. Further enforcement mechanisms could include tagging of IP numbers and real-time transfer to territorially competent authorities, as well as temporary blocking of the device used for violations until intervention by competent authorities.

Improvement of cross-border law enforcement may come from a reinforcement of the role of ISPs in enforcement activities, bearing in mind that, according to provisions already agreed within the EU Treaty on judicial assistance (art. 19), *'systems of telecommunications services operated via gateway on the territory, which for the lawful interception of the communications of a subject present in another State are not directly accessible on the territory of the later, may be made directly accessible for the lawful interception by that Member State through the intermediary of a designated service provider present on its territory'*.

Cross-border issues could perhaps be ameliorated by requiring multinational companies to preventatively agree (when authorised to operate) to execute requests for the storage, retrieval and seizure of data stored or accessible by them, even if the storage device is located in the territory of another state, and to develop 'standard service clauses' reserving them the right to execute foreign requests from the consumer.[14]

Beyond the above-mentioned contractual practice of cross-border cooperation, a much wider extent of multinational companies offering internet services should be included, in order to empower them to directly fulfil law enforcement tasks or at least delegated investigations with law enforcement purposes. The idea is to foster repression of cyber crimes through private actors acting as Private Law Enforcement Companies (PLEC) across state borders, throughout the company and its affiliates' reach, seeking (when needed under territorial criminal procedure law as *lex loci actus*) authorisation from judicial authorities and cooperating with prosecution offices for the repression of crimes, under territorial (for single act) or process (if prosecution starts) roles for oversight and liability. From an econometric perspective, requiring a contribution from those making money out of services in cyberspace for the repression of cyber criminality seems an acceptable onus and would justify budgets.

A topic partially related to the previous, and perhaps of more urgent character, is represented by

14 It should be noted that consent is currently a pre-requisite for the so called '*Trans-border access to stored computer data with consent or where publicly available*' under article 32 of the Cyberspace Convention.

'private' reactions to cyber attacks,[15] which may include the detection of intruders, disruption of attacks (by neutralising programmes as well as hardware) and gathering of information useful for the prosecution of those having committed the crime. Currently, intrusion detection may have cross-border implications and may trigger conflicting laws involving legal consequences. Far from advocating the right of companies targeted by cyber attacks to conduct 'private wars', there is the need to adopt uniform rules as to what represents a legitimate reaction under criminal defence and eventual liability patterns.

3. RIGHT TO ACCESS CYBERSPACE

The current social and democratic function of cyberspace is barely reflected in current human rights instruments and modern constitutions.[16]

In the cyberspace domain, the individual may express their personality, but the right to do so is properly defined in the negative, as the personality should not be affected by the fear of being subject to profiling through data collection and, in a wider sense, the individual should be granted the right to informational self-determination through a proper data protection regulation. The latter right is shown to be often affected in cyberspace by the acceptance of foreign data protection regulations offering a lower level of protection. There is, in this sense, a need for more homogenous regulations. Non-viable alternatives are represented by banning or restricting transactions, implying insufficiently strict data protection under foreign data protection rules.

Recent events show that the disclosure of personal information to authoritarian governments may lead to consequences under tort laws, while cooperation in order to implement censorship measures does not appear, currently, to be successfully challenged in court in order to obtain redress.[17]

A right for the individual to access cyberspace as a minimum social right is not currently recognised and taxes or fees are legitimate. Excessive taxes or fees could be considered a restriction to the right to access and provide information. From the perspective of free-trade agreements, taxes and fees, as well as limitations, may fulfil the requirements of a restriction to free trade and determine liability under WTO legal instruments.[18]

The so-called 'new media' which have developed on the World Wide Web, challenging traditional

15 For this purpose, See US National Research Council, *Technology, Policy, Law and Ethics Regarding US acquisition and use of cyberattack capabilities*, The National Accademies Press, Washington DC 2009, p. 77ff.

16 Even if focused on a state's responsibility in respect of cyber security, the *Letter dated 12 September 2011 from the Permanent representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary General*, A/66/359, deals in the annex *International code of conduct for information security*, with aspects related to the right to access cyberspace.

17 Michael Kwan, Kam-Pui Chow, Pierre Lai, Frank Law & Hayson Tse, *Analysis of the Digital Evidence Presented in the Yahoo!* Case, in IFIP Advances in Information and Communication Technology, Volume 306, 2009, p. 252ff.

18 Cynthia Liu, *Internet censorship as a trade barrier: a look at the WTO consistency of great firewall in the wake of the China – Google Dispute, in Georgetown Journal of International Law*, 2011, p. 1199ff.; Ritika Patni & Nihal Joseph, *WTO Ramification of Internet Censorship: The Google – China's Controversy in NUJS Law* Review, 3, 2010, p. 337ff.

media and specifically newspapers, derive the recognition of their roles under human rights and even democratic roles to include limiting restrictions from those media they are progressively replacing to those that are necessary in a democratic society. Specific preventative controls, counterbalancing in some countries the prohibition of any form of censorship and seizure of newspapers, may sometimes only work due to the parallel existence of the traditional media.

Social networks (such as *Twitter* and *Facebook*) which have proven to be drivers of social unrest in the so called 'Arab Spring' have also proven to represent a challenge for traditional media which, in an attempt not to be out-weighed by this form of new media, more often rely directly on such sources, while the traditional professional control over the reliability of information has become almost impossible. From this perspective, one could question if the individual's 'right to be informed' has, to a certain extent, been infringed by the speeding-up of information on one side and the information overflow on the other, while direct access to information by itself offers no guarantee of reliability, creating an illusion of access to first-hand news. The reverse side of the 'right to be informed', the 'right to inform' about relevant facts, has apparently overcome the tradition of freedom of speech for all and the role of traditional media, in favour of the faculty to post almost everything.

Apparently, social networks have recently played the role of drivers for democracy and have the potential to allow individuals to participate in not only political but also social and cultural life. However, they may also shelter discriminatory practices[19] including exclusion practices, the lack of protection against harmful content and the misuse of personal data.

The so called 'Arab Spring' shows that social media may to a certain extent fulfil the role of a command and control system in times of insurgency. The latter aspect should trigger the question of the real role of social networks as an efficient instrument for media and information operations and further, the role of leading multinational companies operating as non-state actors, which may be motivated by more than just profit-making purposes.

The risk of mass manipulation, which is *per se* one of the most difficult to counter with democratic means, has grown to a dimension which may no longer be managed or even mitigated by a single state. Perhaps governance mechanisms and social network management ethics could help in assuring that such instruments remain a driver for democracy rather than a means for non-conventional warfare.

Twitter has also shown an impact on legitimate law enforcement activities: the federal prosecution office of Brazil has requested an injunction to stop *Twitter* users from alerting drivers to police roadblocks, radar traps and drink-driving checkpoints. Such an injunction could make Brazil the first country to take *Twitter* up on its offer to censor content at governments' requests.[20]

Cyberspace has also become the domain in which information for educational purposes has become freely available and has become functional to the right to education of the individual, which has been universally recognised since the 1948 *Universal Declaration of Human Rights*

19 For this purpose we would like to recall the *Draft Recommendations of the Committee of Ministers to member states on the protection of human rights with regard to social networking services*, MC – NM (2010).003Final, of the Committee of Experts on New Media (MC – NM) of the Council of Europe contained in the document, adopted on 30th of November 2011 at Strasbourg.

20 Stan Lehman, Associated Press, 10 February 2012.

(UDHR, article 26). This has happened in an often spontaneous and non-institutionalised way, but often at the cost of copyright for material placed on the web.

The link between the internet and the right to education has been stressed by the Internet Rights & Principles Coalition,[21] which has attempted to define the implications of such rights on the internet. Organised attempts to make culture available through sites like *Google Books* have been ascertained as a violation of copyright and *Wikipedia* could also be affected by claims relating to the violation of copyright. In general terms, intellectual property rights are ensured in ways compatible with the aim to also grant the social function of such rights. Simply qualifying the posting of certain partial and limited contents covered by copyright on the web as a 'publication', despite proper quotation, may not properly balance copyright with the widespread educational purposes fulfilled by cyberspace. Accordingly one could question if, in this case, as in the case of advanced technology being beneficial to the wellbeing of mankind, a rule of non-excessive protection[22] of rights could apply in order to emphasise education and access to cultural aspects.

In cyberspace, access to information for any purpose is significantly influenced by search engines, responding to searches based on keywords. The result of the search is shown, as is well-known, as a hit-based list. Such an outcome may be influenced, and the hit list may neglect undesired content generally or based on the IP address of the individual making the search, supporting censorship mechanisms of authoritarian governments. The so called 'great firewall' developed for the Chinese market could also easily be used in democratic contexts. Such a threat also has an economic and anti-trust dimension, as *Google* could skew search results to favour its own services, making it hard for other businesses to win top advertising placements. *Google* came under the lens of data protection authorities not only for violations associated with *Google Street View*, *Google Earth* and *Google Maps*, but also in respect of the new social platform network *Google Buzz*. Besides, IP-associated storage of searches offers a unique potential for individual profiling and is correspondingly a unique threat to the individual's informational self-determination.

As in the case of social media, search engines have a unique potential for mass manipulation, and the multinational companies owning them have a dimension which allows them to outplay a single state. As such, the introduction of open oversight, governance mechanisms and company ethics should be promoted, oversight which should not be limited to a specific sector such as data protection or trade, but should cover a wide spectrum of all issues which may be associated with firewalls and search algorithms sensitive to democratic values. Mass manipulation may endanger democracy, but reference to the fear of mass manipulation evokes the risk of censorship and remedies which may be worse than the risk itself. Nevertheless, neglecting the risk no longer seems acceptable.

21 On the history of the development of the initiative, *See* Wolfgang Benedeck, Matthias C. Kettemann, Max Senges, *The Humanization of Internet Governance: A Roadmap towards a Comprehensive Global (Human) Rights Architecture for the internet*, Third Annual GigaNet Symposium, 2 December 2008, Hyderabad, India.

22 The debate on 'excessive protection' of intellectual property refers currently to protection of patents in agriculture, biotechnology, medicine and even ultra-high technology, which may have the effect of increasing economic and social inequality if the patents covering development are not made available as a consequence of excessive rights on such patents. Copyright could, in the authors' views, benefit from the debate as the Internet has intrinsically increased the need to access and disseminate the content of copyrighted works.

4. CONCLUSIONS

As the world became too small, some started dreaming and writing about virtual and infinite worlds that they could navigate without being affected any longer by daily problems. Suddenly they felt that the result of putting together internet service providers (ISPs), connecting computers to the internet and browsing websites maintained by web hosting services, was the emergence of a romantic new domain, global like no other, common to mankind and also border-free.

Perhaps the 'new romantic' view of cyberspace is misleading for the development of a clear vision from a legal perspective. Some of the problems posed by cyberspace are not really new, and resorting to ancient ideas may often appear to be beneficial. This could be true for those theories developed in order to clarify the role of transit of criminal instruments through the territory of a state.

Cooperation amongst authorities is often a matter of sovereignty and pride. Contractual development could foster judicial and police cooperation through the further development of contractual practice aimed at exploiting the potential role of multinational companies in the communications and IT sectors as an entry point for cross-border enforcement of requests. Further development could include the necessarily conventional development of a role for law enforcement functions to be carried out by private entities within multinational companies.

Obviously the reinforcement of the role of multinational companies presupposes the establishment of effective oversight mechanisms, also aimed at overcoming identified gaps.