

Communication Rights and the European Information Society

Cees J. Hamelink

Introduction

For the sake of convenience and coherence I shall use in this chapter the notion of the 'European Information Society'. I think it necessary however to preface this with some qualifying observations.

- *There is no European Information Society.* There are in the European region societies that are confronted with 'informational developments'. This notion refers to the growing significance of information products (such as news, advertising, entertainment, scientific data etc.) and information services (such as provided by the WWW), to the increasing volumes of information available, to the role of information technologies as part of society's infrastructure and to the contribution of information handling activities to key economic transactions in finance and trading in modern societies.

The confrontation with 'informational developments' occurs in different ways, at different levels, at different speed and in different historical contexts. Societies design their responses through policies, plans, and programmes both as centrally steered initiatives (for example by the European Commission) and as decentralized activities on national and local levels. The actors involved are both public institutions and private bodies and increasingly there are forms of public/private partnership. Society's responses may take the form of both legal instruments and self-regulatory arrangements. Most of these initiatives are driven by economic motives and are strongly technology-centric.

The key questions for academic inquiry address such crucial sociological issues as: what will be the distribution of benefits of these developments ('cui bono', or who benefits?), which actors will be included and which ones excluded from political participation in decision-making about these developments (who decides?), and which actors will be accountable in case these developments have adverse social effects.

- Discussing the European Information Society also raises the question about *the Europe that should be addressed*. The geo-strategically most comprehensive

Europe? From Alaska to Siberia? This is the Europe of 55 member states of the OSCE. Or the more restricted Europe of the Council of Europe (with its 42 member states), or the smallest, but expanding Europe of the European Union? Moreover, beyond the geographical descriptor there is also the more substantial differentiation between a European conception that is driven by commercial and trading interests and a European ideal that is motivated by the tradition of human rights protection. These different Europe's are not easily reconciled!

- *The European democratic deficit.* Europe may be en route towards an information society but it does so without adequate democratic institutional arrangements for a broad social debate and civil participation in the decision making on Europe's future. There is in Europe no broad public debate on how Europe can develop as a democratic project. The current EU decision making structure resembles more than anything else a TGV that races on at high speed with no alternative routes. Its political arrangement is an imposition from above which de-motivates citizens to take elections for the European Parliament seriously. There is at present not a European Public Space and its creation should be the foremost priority for any attempt to build the European Information Society.

European politics is mainly shaped by the secret deals that the European political leadership makes. The European Parliament has no matching power to control, expose and correct these deals.

The core of any democratic political deliberation should be formed by a shared value orientation (i.e. a *normative consensus*), a sense of 'imagined community' (i.e. a *feeling of belonging*), and a *common purpose*. The current efforts of the EU to construct a European identity through such legal instruments as the EU Charter of Fundamental Rights (2000) are doomed to fail since identity is a matter of social psychological processes and not of regulatory initiatives. *You cannot regulate people to feel European.* People in the European region will only become Europeans when they feel comfortable with this notion and when they conclude that it benefits them in direct, concrete and material ways. Actually, the adoption of the European Charter next to the already existing European Convention on Human Rights and Fundamental Freedoms (1950) does not help to promote the European feeling. It rather strengthens the impression that there are several Europes.

Communication Rights in Europe

Fundamental rights that are relevant to the 'European Information Society' are at present (in various legal provisions) found in connection with (a) the freedom of expression, (b) the protection of privacy and data traffic, (c) the security of information infrastructures, and (d) the protection of intellectual property rights.

The Right to Freedom of Expression

The basic legal instrument is the European Convention on Human Rights and Fundamental Freedoms (ECHR) of 1950. Its Article 10 reads:

“Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary”.

A supra-national court supervises the implementation of the provisions of this regional legal instrument and thus develops over the years a jurisprudence that helps to understand the meaning of the various articles of the Convention.

Over the past years a number of cases involving violations of Article 10 have been brought before the Court and through this case law important European jurisprudence on free speech is developing.

Between the beginnings in the early 1950s till 1970 there was only one case in relation to Article 10. In the 1970s there were three cases, in the 1980s twelve and since then the caseload is only growing. Between January 1990 and July 1999 the Court handed down some seventy judgments. In 50% of these cases the Court concluded that there had been a violation of Article 10. Between July 1999 and May 2002 the Court concluded in 36 cases that there was a violation of Article 10.

Most cases address forms of *direct and indirect interference by state authorities* in the freedom of expression. The Court uses as basic rationale in judging forms of state interference that free speech “constitutes one of the essential foundations of a democratic society and one of the basic conditions for its progress and each individual’s self fulfilment”. According to the Court the notion of free speech is applicable not only to “information and ideas that are favorably received or regarded as inoffensive, but also to those that offend, shock or disturb: such are the demands of that pluralism, tolerance and broadmindedness without which there is no democratic society”. The Court has repeatedly stated that in a democratic and pluralist society free speech is particularly essential to the political

debate. "Free elections and freedom of expression, particularly political debate, together form the bedrock of any democratic society" (the *Bowman* versus the UK case of 9 February 1998).

In this context the Court has stressed the *essential role of the media*. In the case *Bladet Tromsø & Stensaas v. Norway* of May 20, 1999, the Court stated: "One factor of particular importance for the Court's determination in the present case is the essential function the press fulfils in a democratic society".

The rulings of the European Court can be organised under the following headings (see <http://www.echr.coe.int/>).

1. Political Polemics

Exemplary is the *Janowski versus Poland Case of January 21, 1999*:

On 2 September 1992 Mr Janowski – a Polish journalist-- intervened when he saw two municipal guards ordering street vendors to leave a square in Zdunska. He argued with the guards and told them they had no legal basis for their action. The Zdunska public prosecutor instituted a criminal proceeding against Mr Janowski and charged him with having insulted the municipal guards. On 29 April 1993, the District Court convicted Mr Janowski and sentenced him to eight months' imprisonment suspended for two years and a fine plus the court costs. Against his appeal, also the Regional Court found him guilty of having used such insulting words as 'oafs' and 'dumb'. The Court found that Janowski had insulted state officials. His remarks were not part of a public discussion and he was operating as a private person, not as a journalist. Civil servants should allow for criticism but not to the same extent as politicians. To strengthen their credibility with the general public it may be necessary to protect them against verbal violence. As the Court states, "it cannot be said that civil servants knowingly lay themselves open to close scrutiny of their every word and deed to the extent to which politicians do and should therefore be treated on an equal footing with the latter when it comes to criticism of their actions". The Court concluded that the Polish authorities did not overstep their margin of appreciation in assessing the necessity of the measures. With twelve votes against five the Court held that there had been no breach of Article 10.

The margin of appreciation rule that the Court refers to is intended to leave space to national authorities to judge the pressing need for interference with free speech. Starting point here is the position that "it is in the first place for the national authorities, notably the courts, to interpret and apply domestic law. The Court's rule is limited to verifying whether the interference which resulted from the

applicant's conviction of that offence can be regarded as necessary in a democratic society" (Lehideux & Isorni vs France).

Following *Bladet Tromsø* the Court defines the margin of appreciation in this way: "According to the Court's well-established case law, the test of 'necessity in a democratic society' requires the Court to determine whether the 'interference' complained of corresponded to a 'pressing social need', whether it was proportionate to the legitimate aim pursued and whether the reasons given by the national authorities to justify it are relevant and sufficient... In assessing whether such a 'need' exists and what measures should be adopted to deal with it, the national authorities are left a certain margin of appreciation. This power of appreciation is not, however, unlimited but goes hand in hand with a European supervision by the Court, whose task it is to give a final ruling on whether a restriction is reconcilable with freedom of expression as protected by Article 10".

Whereas on the one hand the margin of appreciation is circumscribed by the need to show a pressing social need and by the essential role of the press in democratic societies, there is a much wider margin for national authorities in relation to matters of public order, in situations where there is incitement to violence or when "matters liable to offend intimate personal convictions within the sphere of morals or, especially, religion" are at stake (*Wingrove v. UK*, 25.11.1996). With regard to the latter, the Court has argued that "what is likely to cause substantial offence to persons of a particular religious persuasion will vary significantly from time to time and from place to place, especially in an era characterized by an ever growing array of faiths and denominations. State authorities are in principle in a better position than the international judge to give an opinion on the exact content of these requirements with regard to the rights of others as well as on the 'necessity' of a 'restriction' intended to protect from such material those whose deepest feelings and convictions would be seriously offended".

The margin is greater in cases of insults against officials, incitement to violence, or cases that refer to morals or religion. The problem with this flexible approach to the margin of appreciation is that the Court distinguishes in its protection of Article 10 between different situations where state restrictions obtain. The scope of the national margin of appreciation varies but, in the absence of explicit criteria, there is a margin of arbitrariness.

In the field of political polemics also the *Oberschlick versus Austria (No 2) Case of July 1, 1997* is interesting. The periodical *Forum* reproduced a speech held on 7 October 1990 by Mr Jörg Haider, leader of the Austrian Freedom Party. The editor of the magazine, Mr Gerhard Oberschlick, commented on the speech and called Haider a Trottler, an 'idiot'. On 26 April 1991 Mr Haider brought an action for defamation and insult. On 23 May 1991 the Court found Mr Oberschlick guilty of

having insulted Mr. Haider and sentenced him to a fine and also ordered the seizure of the relevant issue of *Forum*. In his application to the European Court Mr Oberschlick alleged that his conviction was contrary to Article 10 of the Convention. The Court stated in its judgment that the use of the word 'Trottel' should be seen as part of a political discussion in response to Haider's speech. As the Court expressed, "the applicant's article and in particular the word Trottel, may certainly be considered polemical, but they did not on that account constitute a gratuitous personal attack as the author provided an objectively understandable explanation for them derived from Mr Haider's speech, which was itself provocative". The necessity of interference with the author's freedom of expression was not shown, concluded the Court, and it found that there been a breach of Article 10.

2. Racism and Revisionism

The Lehideux & Isorni versus France Case of September 23, 1998:

On 13 July 1984 the daily newspaper *Le Monde* published a one-page advertisement bearing the title 'People of France, you have short memories'. The text basically called for a more positive attitude towards Marshal Petain and his role during World War Two as French Head of State. On 10 October 1984 the National Association of Former Members of the Resistance filed a criminal complaint against Mr Lehideux as President of the Association for the Defence of the Memory of Marshal Petain, against Mr Isorni as the author of the text, and against the publication manager of *Le Monde*, for publicly defending the crimes of collaboration with the enemy. In the judicial process that followed, the highest French court judged (16 November 1993) that the text defended a person convicted of collusion with the enemy and concluded that the finding of the lower court in favor of the complainants did not infringe the right to freedom of expression as protected by Article 10 of the European Convention. Mr Lehideux and Mr Isorni submitted an application to the European Commission on Human Rights which found their complaint admissible. The case thus proceeded to the Court which concluded that the criminal conviction of the applicants was disproportionate and not necessary in a democratic society. According to the Court there had been a breach of Article 10.

The Court clarified that the protection of Article 10 would not hold if the cruelties of the Nazis had been justified in a publication or if the Holocaust would have been denied. In its 'obiter dictum' the Court said that Article 17 of the Convention takes the protection of Article 10 away from those who deny the Holocaust.

3. The Use of Confidential Documents

The Case Bladet Tromsøe & Stensaas versus Norway of May 20, 1999:

The newspaper *Bladet Tromsøe* published some articles on the hunting of seals. In the first article scientist Lindberg, inspector for the Ministry of Fishing, talked about the unacceptable ways in which the animals are killed. The hunters got an opportunity to do their story. Then the newspaper published the official report by Lindberg for the Ministry. The report was withdrawn from publicity since there were allegations of criminal conduct that needed investigation and the accusations of Lindberg were not proven. The newspaper and editor Stensaas were sentenced for slander.

The Court expressed the need for careful scrutiny in cases where government interference may discourage the participation of the press in debates on matters of public concern. It confirmed the 'watch dog' function of the press even if reputation and name of people are at stake.

The Court's majority confirmed that the seal hunters have a right to the protection of their name and reputation and the right to be held innocent until their guilt has been proven in a court of law. However, the allegations were part of the contents of the Lindberg report and the newspaper had good reason to believe the report was reliable. The Court saw no evidence that the newspaper acted not in good faith! Therefore, the Court concluded that the interference with the applicant's freedom of expression was disproportionate. The Court sentenced the Norwegian government to a compensatory payment of 693.606 Norwegian crowns.

As may be expected the Court's opinions are not always without dissent and controversy. In this case the three dissenting judges argued against the consenting majority: "In our view the fact that a strong public interest is involved should not have the consequence of exonerating newspapers from either the basic ethics of their trade or the laws of defamation". They concluded that the judgment "sends the wrong signal to the press in Europe...Article 10 may protect the right for the press to exaggerate and provoke but not to trample over the reputation of private individuals". The dissenting opinions found the judgment undermines the basic ethics of the profession which imply that journalists should carefully check facts and should not trample over the reputation of private individuals.

4. Protection of Journalistic Sources

The landmark case is *William Goodwin versus The United Kingdom (March 27, 1996)*. This case provides the legal basis for the journalistic privilege in Europe. Until this case the protection of journalistic sources was only recognized in voluntary professional codes.

Journalist William Goodwin who worked for *The Engineer* received confidential information about financial problems at the company Tetra Ltd. He intended to publish an article on this. The company complained that the information in the article originated from a confidential business plan and requested a prohibition to publish the information. A court of law supported the request that would be valid for all British media. Moreover, as the judge found that 'the interests of justice' are at stake, Goodwin was ordered to reveal his source. Also in appeal the House of Lords confirmed "the importance to the plaintiffs of obtaining disclosure lies in the threat of severe damage to their business". Goodwin got a fine of 5.000 British Pounds for contempt of court and took his case to Strasbourg.

The European Court stated that freedom of expression constitutes one of the essential foundations of a democratic society and confirmed that the protection of journalistic sources is one of the basic conditions for press freedom. The Court finally judged that the disclosure order couldn't be regarded as having been necessary in a democratic society. The Court took a principled position in favour of the journalistic privilege and did not make it dependent upon certain conditions, like how information was gathered.

Relevant in the case was the concurring opinion of one judge who suggested that the injunction was an utterly unacceptable form of prior restraint; and even if there had been no injunction the disclosing order would have been illegitimate!

The Goodwin case is particularly important since the Convention does not provide for the freedom to gather information. This is a difference with the Universal Declaration on Human Rights and the International Covenant on Civil and Political Rights that provide for the right to 'seek' information and ideas. The Court concluded very strongly "Protection of journalistic sources is one of the basic conditions for press freedom. Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest".

Failing this protection "the vital public-watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected". The Court proposed that an order to reveal sources "must be limited to exceptional circumstances where vital public or individual interests are at stake". The Court also proposed that in these cases the national margin of appreciation is restricted since the interests of the democratic society are here at stake. The Court saw the legitimate interests of the Tetra company but considered that they weighed less than the vital public interest in protecting confidential sources.

A relevant dimension of this case was also that the Court made reference to the field of professional self-regulation through codes of conduct. "Protection of journalistic sources is one of the basic conditions for press freedom, as it is reflected in the laws and the professional codes of conduct in a number of

Contracting States and is affirmed in several international instruments of journalistic freedoms ”.

Also in the cases *Fressoz & Roire v. France* and in *Bladet Tromso*, the Court referred in its argumentation to the ethics of journalism. The reference was used against state interference and in support of professional secrecy (a.o. in *Bladet Tromso*, *Goodwin* and *De Haes & Gijssels*). However, reference to the failure of journalists to heed the provisions of professional ethics has also been used to justify state interference, as in the *Praeger & Oberschlick versus Austria* case of 26 April 1995, where the Court argued that the applicant could not invoke compliance with the ethics of journalism.

5. Freedom of Expression in Turkey

The complex and tense situation in Turkey has led to several cases involving journalists who wrote about or in favour of the PKK, the Kurdish Political Party. In most cases the government was considered guilty of breaching Article 10, but in some cases the Court also decided that there was hate speech or incitement to violence and thus legitimate interference.

The case of Zana versus Turkey of 25 November 1997:

Mr Mehdi Zana, former mayor of Diyarbakir, while serving sentences in the military prison of Diyarbakir, remarked in an interview with journalists, "I support the PKK national liberation movement; on the other hand I am not in favour of massacres". The statement was published in the national daily newspaper *Cumhuriyet* on 30 August 1987. By means of an indictment of 19 November 1987, the Diyarbakir military prosecutor instituted proceedings in the Military Court against Mr. Zana charging him with supporting an armed organisation whose aim was to break up Turkey's national territory. The Turkish National Security Court held in its judgment of 26 March 1991 that Mr Zana's statement to journalists amounted to a criminal offence.

When the case ended up with the European Court, the judges found Mr Zana's statement contradictory and ambiguous. "They are contradictory because it would seem difficult simultaneously to support the PKK, a terrorist organization which resorts to violence to achieve its ends, and to declare oneself opposed to massacres". The Court finally judged that the penalty imposed on the applicant could be regarded as answering to "a pressing social need" and that consequently there had been no breach of Article 10.

The Court voted twelve against eight. The dissenting opinions found that the restriction imposed by the Turkish government was not necessary in a democratic society. In one opinion, a dissenting judge stated, "Even if one accepts...that the maintenance of national security and public safety constituted a legitimate aim for

the purpose of taking measures in respect of the statement made by the applicant, his conviction and twelve-month prison sentence cannot, in my opinion, be held to be proportionate to those aims, considering the content of the statement". And in the rationale for his dissent, the judge wrote, "The mere fact that in the statement the applicant indicated support for a political organisation whose aims and means the Government reject and combat cannot, therefore, be a sufficient reason for prosecuting and sentencing him".

It is interesting to compare the Zana case with the *Incal versus Turkey case of June 9, 1998*. Mr Ibrahim Incal, lawyer by profession, was a member of the executive committee of the Izmir section of the People's Labour Party, dissolved by the Constitutional Court in 1993.

On 1 July 1992 the executive committee decided to distribute a leaflet criticizing measures taken by the local authorities against small-scale illegal trading and the sprawl of squatters' camps around the city. The leaflet concluded with "The Driving the Kurds out policy forms part of the 'special war' being conducted in the country at present against the Kurdish people. It is one of the mechanisms of that war, the way it impinges on the cities. Because the methods used are the same, namely enslavement, violence, terror and oppression through compulsion. It is a psychological war". The Izmir security police considered that the leaflet contained separatist propaganda capable of inciting the people to resist the Government and commit criminal offences. A criminal investigation was opened and Mr Incal was found guilty by the National Security Court and sentenced to six months and twenty days imprisonment and a fine. In a judgment of 6 July 1993 the Court of Cassation upheld the judgment. When the case came to the European Court the judges observed that interference with the freedom of expression of a politician who is a member of an opposition party, like the applicant, calls for the closest scrutiny on the part of the Court.

The Court further stated that the limits of permissible criticism are wider with regard to the Government than in relation to a private citizen, or even a politician. "In a democratic system the actions or omissions of the Government must be subject to the close scrutiny not only of the legislative and judicial authorities but also of public opinion". The Court was prepared to take into account problems linked to the prevention of terrorism. Here it referred to its judgment in the Zana case. However, the Court judged that Mr Incal's conviction was disproportionate to the aim pursued and therefore unnecessary in a democratic society. It is interesting that the Court finds contrary to the Zana case that found Mr Incal cannot be held responsible for terrorism in Turkey.

6. Operational Procedure

In its operational procedure the European Court follows the standard practice that it first decides whether there was an interference of Article 10.1 and then examines whether the interference is justified. The questions then asked are:

Was the interference prescribed by law? What is the basis for the interference in national law? Is the law precise enough? Did the applicant have adequate protection from arbitrary interference? Did the interference pursue a legitimate aim? Was the interference necessary in a democratic society? In other words can the interfering state authority demonstrate that there was a pressing social need for its intervention? The contracting states have a certain margin of appreciation in assessing whether a pressing social need exists but eventually the decision is with the Court.

The question about the pressing need will be followed by the question whether the measures taken by the state are proportionate to a legitimate aim and whether the proposed reasons are relevant and sufficient? In several cases the Court has judged an interference to be not legitimate since the information that was censored by the state was already available in the public domain anyway.

Challenges for the Future

A first challenge addresses an essential and far-reaching element in the Court's jurisprudence, which is *its interpretation of the right to receive information*.

According to the jurisprudence of the European Court, the European citizen has the right to be properly informed. In several opinions the Court has stated that not only do the mass media have a right to impart information, they have the task "to impart information and ideas on matters of public interest" and the public has a right to receive such information and ideas. The Court has ruled that the media are purveyors of information and are public watchdogs. This imposes a special public responsibility on the performance of the media. According to the Court, the media of information have a corresponding duty to provide information that properly informs their audiences. This is a vitally important position in view of the increasing commercialization of media and the trend towards trivialisation of information provided by them: the 'sound bites', the info-tainment formats, the 'media-hypes' which are a very provocative challenge to both practitioners and policymakers. The Court's position also deserves to be elaborated. It will turn out to be very difficult to find more precise formulations than 'properly informed' and even harder to operationalize such formulations. It is, however, a task urgently needed and very pertinent to the current media climate.

A second challenge deals with the *relationship between the European Convention and the European Union*. A peculiarity of the European region with regard to human rights is the fact that although individual EU member states have ratified the ECHR, the EU as an institution has not. This creates a situation in which it is unclear how robust the protection of human rights really is for EU citizens. At the end of 2000 the European Union has proclaimed at its meeting in Nice the European Charter on Fundamental Rights. The Charter formulates the freedom of expression in Article 11, "1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. 2 .The freedom and pluralism of the media shall be respected". In the commentary on this article, it is stated that restrictions of the right to freedom of expression should not exceed the limitations of the European Convention, Article 10, paragraph 2. It is regrettable that the Charter only refers to the interference by public authority and effectively excludes the interference from private parties and thus undermines the possible horizontal effect of the Charter. As with the European Convention, also here the right to seek information is not explicitly mentioned. It is also unclear whether paragraph 2 on the pluralism of the media does imply a positive duty on the part of governments to promote this media pluralism. It would be a constructive step if the EU decided to ratify the European Convention and if the provisions of the European Charter would be implemented in accordance with the jurisprudence of the European Court.

A third challenge concerns *the accession of Eastern European countries*. In recent years Albania, Armenia, Azerbeidjan, Bulgaria, Rumania, Russia and other Central and Eastern European countries have ratified the ECHR, and thus the number of parties to the Convention has risen to forty-three. The newly acceded countries bring different legal traditions and political experiences to the Court's proceedings and it will be of critical importance that the level of protection secured by the Convention will not be lowered. The expanded membership may also confront the Court with more complex cases about situations where gross and systematic violations of human rights take place and this raises the question of whether the Court is adequately equipped to deal with this growing burden of the caseload.

The fourth challenge regards the horizontal effect of basic rights. It may well be possible that in the years ahead there will be a considerable number of cases in which interferences with the right to freedom of information come from private parties. Will the Court be adequately legally equipped to deal with this? In the case of *Fuentes Bobo versus Spain* of February 29, 2000 (about an employee of RTVE, the Spanish public broadcaster, who criticized his employer and who was subsequently fired) the Court concluded that Article 10 also applies to horizontal

relations. There is therefore a legal precedent but more work needs to be done as the so-called 'Dritt-Wirkung' or horizontal effect of constitutional rights remains a controversial issue.

A fifth challenge for the Court will be *the need to apply in its opinions very substantial lines of argumentation and avoid non-essential arguments*. In some cases the Court has introduced peculiar (non-essential) arguments that tend to erode the principled nature of these cases. An illustration is the consideration in paragraph 55 of the *Incal* case where the Court refers to the fact that the security police had an opportunity to require changes in the leaflet. Also in the *Goodwin* case there is the odd consideration that the interfering party no longer had a claim to the exposure of sources since a judge had already prohibited the publication and thus limited the damage thereof.

A sixth challenge will be the find a *balance between the right to free speech and European efforts to secure safety of the Internet in particular for children*. The Council of the European Union approved on 21 December 1998 an Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks. Whatever the valid intentions behind this Plan it will imply limits on Internet contents and thus requires a careful consideration of the limitation of these limits.

A seventh challenge will be *the need to make the Court more accessible for European citizens*. Given the current caseload this sounds like a very irresponsible proposition. It should be realized, however, that the institution of the Court is a great historical example of how the protection of human rights can become a reality indeed. The ultimate success of the Court's functioning will depend upon its concrete effect on the lives of European citizens. It is evident that in this process a great deal could be done by national judicial institutions. In many cases national courts would have come to different conclusions if they had already introduced in their reasoning the test of the criteria that emerge from European Court's jurisprudence.

A last challenge is also provided by the need to have *robust rules on access to information*. Although the Council of Europe has declared work on a legal text on access to information a priority, no concluding document has been produced so far. The European Court has held in the *Guerra & Others versus Italy* case of 19 February 1998, that the Convention does not provide a general right of access to public information, but it does provide a specific right to information on environmental hazards.

As mentioned before, the right to freedom of expression is also part of the provisions of The Charter of Fundamental Rights of the European Union (Brussels,

October 2000). Article 11 of the Charter and more recently the right to freedom of expression was reconfirmed by the Bucharest Pan-European conference in preparation of the World Summit on the Information Society (November 2002). The participating states proposed a vision on an Information Society “where all persons, without distinction of any kind, exercise their right to freedom of opinion and expression, including the freedom to hold opinions without interference, and to seek, receive and impart information and ideas through any media and regardless of frontiers”. It should be noted that the Bucharest Declaration does include the right to seek information!

The Right to the Protection of Privacy

Throughout the 1970s several European countries began to adopt national data protection laws. These laws had several common features, such as “setting limits to the collection of personal data in accordance with the objectives of the data collector and similar criteria, restricting the usage of data to conform with openly specified purposes, creating facilities for individuals to learn of the existence and contents of data and have data corrected, and the identification of parties who are responsible for compliance with the relevant privacy protection rules and decisions” (OECD, 1980: 11). Differences between national laws existed in particular with reference to licensing requirements and control mechanisms, the definition of sensitive data, and the provision of individual access. When in the 1970s the data protection concern became an international issue, the prime venues for negotiation were the Council of Europe (COE), the European Communities, and the Organization for Economic Cooperation and Development (OECD).

The work of the COE was obviously inspired by the privacy provision in the European Convention (ECHR) of 1950 which states in Article 8: “(1) Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others”. It is important to observe here that the Convention protect citizens against interference by public authorities whereas increasingly the right to privacy is also under threat through the activities of private agencies (such as marketing firms and consumer databases).

Following the Convention the Committee of Ministers of the Council of Europe adopted in 1973 and 1974 two resolutions concerning data protection. The resolutions recommended that member countries would take steps to implement basic principles of protection relating to the collection of data, the quality of data, and the rights of individuals to be informed about data and data processing activities. On this basis the COE began to prepare for an international arrangement through a Convention. This became the basic European instrument in connection with privacy protection: the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data. The convention was opened for signatures on 28 January 1981. On 15 June 1999 the Committee of Ministers of the Council of Europe adopted an amendment to the Convention that allowed the European Communities to accede to the convention.

In the 1970s also the European Community began to study the possible harmonization of legal rules in connection with transborder flows of personal data and in 1978 the European Parliament held a public hearing on data processing and individual rights. The sub-committee responsible for the hearing prepared a report that was submitted to the European Parliament in 1979 with a resolution on the protection of individual rights in view of data processing.

The OECD programme goes back to the late 1960s and its studies on computer usage. In 1977 the OECD Data Bank Panel held a symposium in Vienna to discuss privacy problems in the context of transborder data flows. The symposium presented a number of guiding principles that recognized, '(a) the need for generally continuous and uninterrupted flows of information between countries, (b) the legitimate interest of countries in preventing transfers of data which are dangerous to their security or contrary to their laws on public order and decency or which violate the rights of their citizens, (c) the economic value of information and the importance of protecting 'data trade' by accepted rules of fair competition, (d) the need for security safeguards to minimise violations of proprietary data and misuse of personal information, and (e) the significance of a commitment of countries to a set of core principles for the protection of personal information' (OECD, 1980: 14). In 1978 a new expert group on Transborder Data Barriers and Privacy Protection was initiated and was instructed to work closely with COE and EC to 'develop guidelines on basic rules governing the transborder flow and the protection of personal data and privacy' (OECD, 1980: 14).

The work of the expert group led to the OECD Guidelines that were adopted in 1980. Although there are similarities with the COE Convention, the main difference is that the Guidelines are a non binding instrument, they define very general principles for a minimal international consensus, they contain no enforcement procedures, and their constituency is limited (although powerful). Another distinction is that the Guidelines apply to all personal data, also those handled

manually. The COE Convention addresses only automatically processed data. The COE Data Protection Convention is a binding legal instrument for states that ratify it. As the Council is a regional body, the constituency of the Convention is limited, although the instrument is open for accession by all countries. The basic principles of the Convention are the right to confidentiality, the right to be informed about the existence of data collections, and the right to data quality. The Convention is formulated rather generally and leaves the methods to deal with these principles to national legislation. The Convention does not say how people are to know about data being collected about them or how to obtain remedy in case data registers refuse either access or rectification.

There are also serious questions about the adequacy of the concepts that are used in the Convention. A core concept is the automated personal file. This was based upon the early situation in which large mainframe computers would hold files that could be accessed/processed by different users. Today files are ubiquitous, they are in personal computers, for instance. One can hardly apply the rules on all automated files. Also the notion of 'machine readable' has changed with the application of optical scanners.

The concern about the quality of data (COE Convention Art. 5. or OECD Guidelines, Part Two, para 8) led to the formulation of a right of access for the data subject. This is insufficient if the data subject wants to get all the data correct. The data in different collections may be in and by themselves correct, but their combination may create inaccurate statements. If you combine correct data on gross income from one database and combine them with correct data from another database on net income and then present them as income, the outcome is no longer accurate. There is also the development towards more automated data collection devices. The data subject does not provide him/herself the information which is collected by electronic systems, such as traffic control systems.

The Convention deals with the sensitivity of data (Art. 6) and refers to health, sex, and crime. The question is whether this is sufficient? How about data on political affiliation? Or data about race and religion? Sensitivity increases with the potential for discriminatory use of the data. What guarantees does the Convention provide against collective surveillance, for example the surveillance of suspect populations? 'The majority of those subject to surveillance are not actually criminals, but only persons qualified by coincidence as members of the suspect population' (Bing, 1992: 256).

There is also a problem with the provision of the right of access as a fundamental right of citizens. The question is whether this really functions as an instrument of control. 'It is a disappointing international experience that very few citizens make use of the right to access, regardless of how comprehensive this right is outlined in the different national statutes' (Blume, 1991: 17). Yet there is sufficient evidence to suggest that 'citizens feel very strongly about data protection and are worried

about the extent of knowledge that public authorities and large private firms can acquire about them in our modern, information society' (Blume. 1992: 17). Blume suggests that the fact that access has to be a personal initiative constitutes a major barrier to use this means of control. An alternative might be a system in which citizens would be informed about the data held about them. 'Denmark has discussed such a system. However, besides the practical difficulties of such a system, a file of files would also create political problems. It would mean that the state had one big file or database containing all available information on all citizens, which when seen from the point of privacy would be very dangerous' (Blume, 1992: 18).

On 24 October 1995 the European Parliament and the EU Council issued a Directive (95/46/EC) on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

On 25 October 1998 the European Union Privacy Directive took effect. The directive requires EU member states to implement personal data policies that include such principles as transparency, purpose limitation, data quality, special protection of sensitive data and the appointment of 'data controllers' responsible for all data processing. The Directive also stresses the need for individual redress thus providing the right of individuals to access information about themselves, to correct or block inaccuracies and to object to information's use. Article 1 of the Directive demands of EU member states that they protect "the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data". The EU Directive in fact recognizes the protection of privacy as a fundamental human right.

The substantial basis of the Directive is found in the reference to the right to privacy as contained in the 1981 COE Convention. The Directive reiterates that rights are conferred on individuals, the data on whom are the subject of processing. These rights include that those individuals are informed that processing takes place, that they can consult the data, request corrections and object to processing under certain conditions, for example if the data are being processed for the purpose of direct marketing. The preamble of the Directive states that the processing of personal data must be carried out with the consent of the data subject.

When decisions affecting data subjects are taken on the basis of automated data processing, the data subject must be able to know the logic on which these automated decisions are based.

In the Directive EU Member States are asked to establish exceptions or derogations from data protection provisions in such a way as to strike a balance between different but equally fundamental rights such as the right to privacy and the right to free speech.

On 23 February 1999 the Committee of Ministers of the Council of Europe adopted a recommendation which proposes guidelines for Internet users and service providers (among others on the means of protecting themselves) and advises on the implementation of data protection standards. The Guidelines also emphasize the users' responsibility when process or transfer information about other people. On 12 July 2002 the European Parliament and the EU Council adopted Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector. In its Preamble, para (2) the Directive "seeks to respect the fundamental rights and observes the principles recognized in particular by the Charter of Fundamental rights of the European Union" . This concerns in particular Articles 7 and 8 of the Charter. And in para (3) the Directives assures that "confidentiality of communication is guaranteed in accordance with the international instruments relating to human rights, in particular the European convention for the protection of human rights and fundamental freedoms and the constitutions of Member States".

Article 4 addresses security and provides "(1) The provider of a publicly available electronic communication service must take appropriate technical and organisational measures to safeguard security of its services.... and (2) In case of a particular risk of a breach of security of the network, the provider of a publicly available electronic communication service must inform the subscribers concerning such risk...." Article 5 deals with the confidentiality of communications and provides (1) that "Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, or storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users without the consent of the users concerned, except when legally authorised to do so....".

The Charter of Fundamental Rights of the European Union (Brussels, October 2000) provides for the right to the protection of private communication and personal data in Article 7 which states, "Everyone has the right to respect for his or her private and family life, home and communication". And Article 8 provides "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance to these rules shall be subject to control by an independent authority".

The protection of 'informational privacy' as provided in this article is clearly based upon Article 8 of the ECHR and the EU privacy directive.

Compared to Article 8 of the European Convention of Human Rights and Fundamental Freedoms with regard to the protection of privacy the term 'correspondence' was replaced by 'communication'. This obviously takes into account developments and innovations in information- and communication technology. The Charter provides no unequivocal recognition of the right of encryption and there is no explicit no right to anonymous communications. Yet, paragraph 3 of Article 8 represents an important step towards the establishment of an independent European data commissioner.

In the course of 2001 the EU Council and Parliament have given more power to law enforcement agencies to monitor telephone, internet and email traffic. This allows these agencies to develop a fairly complete picture of people's movements (from mobile phone records) and of their personal communications by phone and email as well as of their internet behaviour. To further reinforce this the Belgian government proposed in 2002 a text for a Draft Framework Decision on the Retention of Traffic Data and on Access to this Data in Connection with Criminal Investigation and Prosecutions. The text states that the use of telecommunications services has grown to the extent that the data relating to its use, and principally those relating to traffic are very useful tools for investigating and prosecuting criminal offences. Following this the proposal is made for the a priori retention of traffic data during a period of a minimum of 12 months and a maximum of 24 months. In order to protect the right to privacy Article 4 of the draft suggests that "Access to retained traffic data is given only to judicial authorities; Access to retained traffic data is not authorised when other measures are possible which are less intrusive in terms of privacy; Confidentiality and integrity of retained traffic data are ensured; Data to which access has not been asked are destroyed at the end of the period of mandatory retention".

Finally, it is remarkable that the Declaration that was produced by the Bucharest Pan-European conference in preparation of the World Summit on the Information Society (November 2002) contains no provisions on the issue of privacy protection.

The Right to Security

Among some of the early signals that pointed at the problem of technology-vulnerability was the 1978 report by the Swedish Ministry of Defense Committee on the Vulnerability of Computer Systems (SARK) 'The Vulnerability of Computerized Society'.

In 1981 the Organization for Cooperation and Economic Development (OECD) held a workshop in Siguënza (Spain) on the Vulnerability of the Computerized Society. In 1984 the Information Task Force of the Commission of the European

Communities published 'The vulnerability of the information-conscious society-European situation'.

In 1986 the Norwegian Vulnerability Commission presented a report called 'The Vulnerability of a Computer Dependent Society'.

In 1989 a committee of the British Computer Society reported that current skills in safety assessment were inadequate and therefore the safety of people could not be guaranteed (Forester and Morrison, 1990: 3).

These various commissions and reports began to identify the risks that the use of international computer systems entailed. Such risks could be incorrect transmissions either by technical malfunction or by the intentional act of an intruder. Incorrect transmissions could include the transmission to the wrong address, or of the wrong content, or of both. Transmissions could also be afflicted by delays or by the unexplained loss of data.

Another risk could be the unauthorized access to the data traffic or the data themselves or both. A third type of risk could be the possibility of communicating with fraudulent persons (Redeker, 1989: 19). Risks could also be caused by malfunctions of networks that take care of Electronic Funds Transfers and such malfunctions may be caused by environmental factors, by equipment failures, errors in design architecture, or by human errors in data processing. Such errors could cause inadvertent changes in the contents of payment instructions.

The 1986 OECD study referred to the international dimension of computer-related crime due to the internationalisation of information and computer services. The study pointed to the need for an international response since "international co-operation in the repression of computer-related offenses... would facilitate transborder data flows" (OECD, 1986: 7). In the summary the study stated that international co-operation is recommended in both areas of civil and penal law. "As far as civil and administrative economic law is concerned, international harmonized solutions are necessary also in order to secure equal conditions of competition, to facilitate transborder data flow, and to avoid the transfer of undesirable or detrimental actions in foreign countries... It is important to develop common approaches to penal and procedural law in order to protect the international data networks, to enable the functioning of international instruments of co-operation in criminal matters and to guarantee that evidence gathered in one country is admissible in court in another country" (OECD, 1986: 64). The report stated very clearly that any other solution "would lead to 'data havens' and 'computer crime havens' and therefore lead to restrictions in transborder data flow" (OECD, 1986: 64). The purpose of international cooperation would be the repression and prevention of computer crime.

It has been increasingly realized that international cooperation in the field of law enforcement and computer crime would demand directives regarding cases where several states are entitled to prosecute the same case, law enforcement authority

on foreign territory and the harmonization of criminal sanctions. Harmonization is required if the emergence of computer crime havens is to be prevented.

In October 1989 the OECD Secretariat submitted to the Committee for Information, Computer and Communications Policy (ICCP) a report on Information Network Security. The preparation of this report had been approved by the ICCP in October 1988.

Following the report the ICCP appointed a Group of Experts to draft guidelines for information system security. On 26 November 1992 the OECD Council adopted the Recommendation and the member countries adopted the Guidelines. In its recommendation to the member countries the Council pointed to the "increasingly significant role of information systems and growing dependence on them...the sensitivity and vulnerability due to risks arising from available means of unauthorized access, use, misappropriation, alteration and destruction". In the memorandum annexed to the Guidelines the group of experts has highlighted the growing dependence on information systems and its concern for the possibility of information system failure. 'Failures of information systems may result in direct financial loss, such as loss of orders or payment, or in losses that are more indirect or perhaps less quantifiable by, for example, disclosure of information that is personal, important to national security, of competitive value, or otherwise sensitive or confidential' (OECD, 1992: 17).

The Guidelines are presented as a general framework within which member countries can develop laws, codes of conduct, technical measures and user practices. Central to the instrument are a set of nine principles. The accountability principle which provides that responsibilities and accountability of those involved with information system should be stated explicitly. The awareness principle which provides that those interested should have access to information about measures for the security of information systems in order to foster confidence in such systems. The ethics principle which implies that the provision and use of information systems and the security of information systems should take into account the legitimate rights and interests of others. The multidisciplinary principle which states that the development of security measures and practices should take the whole range of pertinent viewpoints and forms of expertise into account. The proportionality principle which suggests that security needs vary and security measures should be in line with the value of information systems and the severity of potential harm. The integration principle which says that security measures should be coordinated and coherent security systems should be designed. The timeliness principle proposes that the timely response to security breaches is vital. The reassessment principle suggests that the dynamic development of information systems renders a periodical assessment of security measures necessary. And the concluding democracy principle says that the security measures should be in line with legitimate interests in use and flow of data and information.

The Guidelines conclude with a set of recommendation to member countries on the implementation of security measures through policy development, education and training, enforcement and redress, exchange of information, and cooperation. Presently, the OECD Guidelines represent the core of an emerging political practice and eventually a robust and effective agreement in connection with the concern about data security.

The Convention on Cybercrime adopted on 23 November 2001 by the member States of the Council of Europe represents the first international legal instrument to address crime and criminal investigation in relation to the new electronic environment (cyberspace). In connection with the protection of privacy one finds the most contested provisions in Articles 16 and 17 that deal with the preservation of data. The articles address the need to adopt legislative and other measures to obtain the expeditious preservation of specified computer data, including data traffic for a period of time as long as necessary, up to a maximum of ninety days to enable the competent authorities to seek its disclosure. This is particularly where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

In terms of fundamental rights the Convention refers to the provision (Article 15) that all procedures are subject to conditions and safeguards for the protection of human rights and liberties as arising from such instruments as the ECHR and the 1966 UN International Covenant on Civil and Political Rights.

The Bucharest Declaration (2002) proposes that "A global culture of cyber-security needs to be developed: security must be addressed through prevention and supported throughout society, and be consistent with the need to preserve free flow of information". The Declaration has nothing to offer in terms of the protection of basic human rights in this process of developing cyber-security.

On 7 August 2002 the OECD has adopted the Guidelines for the Security of Information Systems and Networks. The Guidelines aim to promote a culture of security among all participants as a means of protecting information systems and networks. This OECD recommendation provides no rules on the protection of citizen's rights to their privacy.

The Right to Anonymous Communications

This is a strongly contested issue. In general, law enforcement authorities are concerned that anonymous communications seriously hinders criminal prosecution. There are also industry representatives who find full anonymity undesirable in relation to network integrity and anti-fraud actions. However others, and in particular privacy experts, claim that fundamental rights to free speech and privacy cannot be guaranteed without anonymous communications. The issue of

anonymity represents a *classic dilemma* between conflicting public policy objectives and demands that a balance is sought between securing basic rights and permitting certain limits on these rights. The Declaration of the Ministerial Conference in Bonn on Global Information Networks (July 6-8, 1997) proposed the principle that where the user can remain anonymous off-line, this should also be possible on-line. By consequence the powers of authorities to limit basic rights should not be greater in cyberspace than they are in the off-line world.

The Right to the Protection of Intellectual Property

Unlike the Universal Declaration of Human Rights (in Article 27:2), the European Convention (ECHR) provides no protection of intellectual property. As a consequence there is no recognition in Europe's most important human rights instrument of the status of intellectual property protection as a fundamental human right. This is significant, because in case intellectual property rights are recognized as human rights this recognition shapes the political framework for all parties involved, producers, distributors, artists, and consumers. It implies that the protection of intellectual property rights is constituted by: the right to full participation in cultural life for everyone; the right of affordable access to information for everyone; the recognition of moral rights of cultural producers; the rights of creative artists; the diversity of cultural production, and the protection of the public domain.

As human rights always imply responsibilities, the human rights-based conception of copyright would follow Larry Lessig's proposal to add to 'copyright' a 'copyduty'. As he writes, "We may well see the day when our students are taught not of 'copyright' but of 'copy duty' – the legal duty of copyright holders to assure public access" (Lessig, 1998).

A human rights approach would give full meaning to the so-called 'fair use' doctrine. 'Fair use' is a principle in US copyright legislation that entitles the public to access and use copyrighted works in situations that would otherwise constitute an infringement on intellectual property rights. The principle (which is also known on UK and German copyright legislation, although not as liberally applied as in the USA) implies a limitation of the property rights of owners of intellectual products in cases of educational use, use for news media, criticism and review, private non-commercial copying and parody. Fair use limits the otherwise exclusive control of rights-holders over intellectual products and recognizes that in most cases copyrighted works could only have been created by using materials from the public domain.

The fair use doctrine is under serious threat through the use of advanced technologies that allow rights-holders the control over access by third parties of

works in digital form. The use of protective technologies (such as encryption, copy protection codes) strengthens the monopoly control of IPR owners. As consumers are likely to develop and apply circumvention technologies to undermine this control, the US administration and US motion picture industry have effectively lobbied the WIPO to incorporate in the 1996 WIPO Copyright Treaty the following Article 13, "Contracting Parties shall provide legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restricts acts, in respect of their works, which are not authorized by the authors concerned or permitted by law".

In the USA this provision was enacted in the 1998 Digital Millennium Copyright Act (DMCA) which went much further than the WIPO agreement. The DMCA prohibits the manufacture, sales, or import of technologies that can be used to circumvent protective technologies. This could make it impossible for people who buy perfectly legal items and want to make extra copies for private use (the extra CD or DVD in the car or second home, for example). It may also become impossible to play a copyrighted item – legally acquired – on different platforms (not the CD player but your PC).

The DeCSS case demonstrates where this could lead to. In 1999 Norwegian teenager Jon Lech Johansen was arrested on the accusation of creating a circumvention technology to crack the protection code for DVDs. Contrary to most media publicity cracking the DVD encryption was not an individual effort, but was the effort of the MoRE group that authored DeCSS. This is a software application to decrypt DVD movies that can be used among others to play DVDs on Linux-operated computers. When the magazine *Computer 2600* reported about this (and offered a link to the programme), the publisher was successfully sued by the Motion Picture Association of America. Fortunately, in January 2003 a Norwegian Court found 'DvD Jon' not guilty and judged that copying for personal use was not a legal offence. The Court found that the purchase of a legally produced carrier (such as a DVD disk) gives full access to its information. This would not be the case the Court emphasized if copies had been illegally obtained.

In the Norwegian case the film business lost its claim upon the DMCA against 'DvD Jon', but this will certainly not deter the contents-industry from future operations against digital copying. Such operations threaten to erode the fair use principle and as this has far-reaching implications for people's access to culture, information, and knowledge, the forthcoming United Nations World Summit on the Information Society (Geneva, 2003) should issue a strong statement on the need to protect the public dimension of IPRs. A statement from Andre Gide "Everything belongs to he who makes good use of it" fits very well into a human rights IPR

framework and it should provide guidance to the future of intellectual property rights.

In the European region the WIPO Copyright Treaty was implemented through the EU copyright directive (Directive 2001/29/EC of the European Parliament and the Council on the harmonisation of certain aspects of copyright and related rights in the information society) In the Directive the EU went much further than the WIPO provisions on technologies that could circumvent measures to protect copyrighted works.

“Article 6 (2) Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which (a) are promoted, advertised or marketed for the purpose of circumvention of, or (b) have only a limited commercially significant purpose or use other than to circumvent, or (c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures”. That goes beyond the WIPO WCT provision in Article 11, that countries should “provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures”.

Then under article 5 a long list of exceptions or limitations to copyrights is provided that do constitute a fair use exemption. However, the exemptions are (with a minor exception) optional. There is no obligation for Member States to apply the whole list. They can make their own choice. This is peculiar in the view of the fact that the Preamble of the Directive states several times that this is an effort at harmonisation! In any case, mandatory or optional, it seems an odd effort to present an exhaustive list of limitations in connection with technological conditions that may rapidly change. Moreover, in terms of communication rights the Directive has bypassed the essential matter of moral rights of authors altogether. This would seem to fit with the overall impression that the EU Copyright Directive serves the rights of the cultural industries much better than the rights of individual authors, composers and performers. The Directive has little if anything to offer for the protection of individual creative artists --the essential sources for copyrighted contents --against the powers (contractual and otherwise) of corporate publishing houses, broadcasters and music recording firms.

Conclusion

If one assesses the current provisions for communication rights in European information societies from the perspective of European citizens, they are clearly unsatisfactory. Even more so now that communication rights are facing strong

pressures from the 'war on terrorism' which seems a convenient argument for many governments to limit rights and freedoms in the field of free speech and privacy. Moreover, there are forceful commercial trends that tend to favour industrial interests over individual interests in the field of intellectual property rights. There is also the added problem with the trend that people are in the EU context increasingly seen as 'consumers' for whom modern communication technologies and networks offer commercial goods and services. They are not primarily seen as 'citizens' in need of public space for political deliberation. The 1997 European Commission 'Greenbook on convergence in telecommunications, media and IT' (December 3, COM(97) 623), for example, presents users of ICT exclusively as purchasers of goods and services on a market. There is little if any interest in ICT as vehicle for people's political interactions and exchanges.

Communication rights that would be more adequate from a citizen's perspective would imply at a minimum:

- A robust protection of the right to freedom of expression including a strong provision on access to information and an obligation on states to support media-pluralism.
- A robust protection of privacy and confidentiality including strong provisions on the use of encryption and anonymity.
- An understanding that these fundamental rights and freedoms can only be limited under the condition that restrictive measures should be temporary, proportional, effective and the only available alternatives.
- A robust protection of the 'fair use' principle in relation to intellectual property rights including 'copy duty' provisions that oblige parties to facilitate the public dissemination of materials that are essential to public life (in politics and culture). This requires a positive formulation of the fair use standard in copyright legislation, i.e. the provision that fair use claims represent basic rights. They are currently mainly formulated as an exception to a standard protecting the interests of owners of copyright claims.

It would seem that in most policy debates and media reports the essential question is about what the European region can do to promote the development of the European Information Society. It is however more relevant and urgent to turn this question around and reflect on what informational developments can do to promote a democratic European space. This is critical since a peaceful future for the economic, technological, and cultural aspirations of the European region depends upon the democratic quality of its political deliberations. If current informational developments are to contribute to this constructively, Europeans must begin – today -- with the design and implementation of a pan-European Bill of

Communication Rights that robustly secures the pivotal position of European citizens in the future of their region.

References

- Blume P. (1992), "How to control data protection rules?", *International Computer Law Adviser*, 6 (6): 17-21.
- Council of Europe (1990), *Computer-Related Crime*. Strasbourg: European Committee on Crime Problems.
- Forester, T. and Morrison, P. (1990), *Computer Ethics*. Oxford: Basil Blackwell.
- I-Ways (2002), *Digest of Electronic Commerce Policy and Regulation*, OECD Adopts Guidelines for Security of Information Systems and Networks, 3-4, 2/2002.
- Lessig, L. (1998), Life, Liberty, Copyright, *The Atlantic Monthly Unbound*, 10.9.1998.
- OECD (1980), *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. C (80) 58 (Final) October 1. Paris: OECD.
- OECD (1986), *Computer-Related Crime: Analysis of Legal Policy*. Paris: OECD.
- OECD (1992), *Guidelines for Security of Information Systems*. OECD/GD (92)190. Paris: OECD.
- Redeker, H. (1989), "Liability in telecommunication systems: the German case", *International Computer Law Adviser*, 4 (1): 18-21.
- Rodotà, S. (1992), "Protecting informational privacy: trends and problems", in W.F. Korthals Altes, E.J. Dommering, P.H. Hugenholtz and J.C.kabel (eds), *Information Law towards the 21st Century*. Deventer: Kluwer, pp. 261-72.

