Marzouki, Meryem (2006) "The "Guarantee Rights" for Realizing the Rule of Law", in: Rikke Frank Jørgensen (ed.) *Human Rights in the Global Information Society*, Cambridge, MIT Press, The Information Revolution & Global Politics Series, pp. 197-218.

# The "guarantee-rights" for the realization of the rule of law
# Fair trial, presumption of innocence, effective remedy, equality before the law, and the principle of no punishment without law

## Meryem Marzouki

### Introduction

When addressing the global issue of human rights in the information society, and how these rights may translate in such a context, one immediately thinks of civil and political rights that should be directly and naturally exercised through information and communication means, or protected against their misuse.

These obviously include the right to freedom of expression and to seek, receive and impart information, the right to access public information and to take part in the conduct of public affairs, and the right to privacy.

Then, following a vision of an inclusive information society where all categories of individuals, social groups, minorities and peoples should have access to information and communication – where access not only means access to infrastructure but also appropriation and use of technology for empowerment and social justice – come issues related to non discrimination, such as the right for men and women to equally enjoy all rights, rights for minorities to enjoy their own culture and to use their own language, the right to education and knowledge and to participate in the cultural life, to enjoy the benefits of scientific progress and its applications, the right to development and the principle of non-discrimination itself.

Furthermore, in an extended understanding of the concepts of association, assembly, movement, etc., the right to freedom of peaceful assembly and association emerges as an issue to be addressed in this context too.

However, despite intense regulatory and legislative processes occurring for almost a decade at the national, regional and international levels, and despite many references to the rule of law in official outcomes of the first phase of the World Summit on the Information Society (WSIS) in Geneva in December 2003, fundamental human rights like the right to a fair trial, the right to the presumption of innocence, the right to an effective remedy, the right to equality before the law, and the principle of no punishment without law are seldom if ever addressed in the information and communication context.

The purpose of this chapter is to provide rationale to the legitimate inclusion of these rights in the debate on human rights in the information society, showing how, as "guarantee-rights", they are necessary conditions to the realization of the rule of law and thus to the effective enjoyment of all other human rights; how they have been particularly challenged by regulatory and legislative processes that make procedural rather than substantive changes in the legislation; and, finally, how these rights may be upheld and effectively implemented in the information society.

**Historical and legal background**

The origins of the "guarantee-rights", protecting individuals against the arbitrary of the political power, date back to the *Magna Carta* (or *Great Charter*) promulgated by King John[1] on June 15, 1215. This historical document has been adopted as a peaceful settlement between the monarchy and the nobility of England, which was tired of paying extra taxes for the – unsuccessful – King's campaigns to regain lost territories in France. Among the 63 clauses of the *Magna Carta*, mainly addressing the elimination of fines and punishments considered as unfair by the nobility, and giving power and privileges to the catholic Church of England, to the feudality and to the merchants, three of them (38, 39 and 40)[2] address what has been later acknowledged as the right to the presumption of innocence and the right to a fair trial. The most famous of these clauses provides that "*No free man shall be seized or imprisoned, or stripped of his rights or possessions ... except by the lawful judgment of his peers*". Although still limited in its scope ("free man", "peers"), the *Magna Carta* is now seen as the first occurrence of the guarantees provided by law to individuals against the arbitrary of the power, at that time the monarchy, later the government or the State.

This concept has been further developed, extended and detailed during the 17th century, through legal Acts imposed by the English Parliament (House of Commons) to the monarchy [Lochak 2002]: the *Petition of Rights*, imposed to Charles I in 1628, prohibited arbitrary arrest and imprisonment and required the need to a regular defense procedure; the *Petition of Rights* resulted mainly from the *Five Knights* case where a writ of habeas corpus has been brought.[3] Such a protection against abusive detention has been later formalized with the *Habeas Corpus Act* in 1679, under Charles II. The Habeas Corpus (literally from Latin "*you have the body*") procedure is still present in most common law systems, and has a constitutional value in the United States. A writ of habeas corpus is brought to a court to have the legality of an imprisonment examined, and if the procedure is found illegal, have the person freed. Further, the *English Bill of Rights* has been imposed in 1689 to King William of Orange, who was required, together with his wife Queen Mary when they were crowned, to swear that they would obey the law of the Parliament and thus be subject to law.

As underlined by Danièle Lochak, a common feature of these legal Acts and documents is that they all aim at being remedies to precise abuses, by defining concrete rules of procedure to pragmatically guarantee the freedoms of English subjects [Lochak 2002]. It took one more century to see the first Declarations and Bills of Rights aiming at defining more abstract and thus more universal principles, with the mutual influence of French and British philosophers before and throughout the Enlightenment period. In the United States, the *American Declaration of Independence* (1776), followed by the adoption of the *American Bill of Rights* (which ratification was completed in 1791), and, in France, the *Declaration of the Rights of Man and of the Citizen* of 1789, after the French Revolution, are the main results of this historical movement establishing or reaffirming not only the fundamental rights themselves, but their universal protection by the law limiting the arbitrary of power.

---

[1] Or 'Jean sans Terre', so called in French since he lost English territory in France and kept trying to regain it, without success.

[2] As numbered in the translation into English of the original Latin text. See this translation provided by The British Library and based on J. C. Holt work [Holt 1992].
<http://www.bl.uk/collections/treasures/magnatranslation.html>.

[3] After five men (Sir Thomas Darnel, together with four others), called the Five Knights, were imprisoned for refusing to contribute to forced loans by King Charles I.

These "guarantee-rights", so-called since they provide for procedural means to protect, defend and recover the "substantive rights and freedoms" recognized by law, are nowadays affirmed in most of existing Declarations, Charters, Conventions and Treaties, so that they have, at least theoretically, acquired a universal status. Among the "guarantee-rights", five[4] of them have caused debate or even controversy, and may be challenged in the context of the information society, although they all are recognized in the Universal Declaration of Human Rights (UDHR) and are protected by the International Covenant on Civil and Political Rights (ICCPR). In addition, these rights are protected as well by most of the binding regional instruments for human rights protection. These instruments are: the African Charter on Human and People's Rights, (ACHPR, adopted in 1981, entered into force in 1986); the American Convention on Human Rights (ACHR, adopted in 1969, entered into force in 1978); and the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR, adopted in 1950, entered into force in 1953). These five "guarantee-rights" are:

- *The right to equality before the law* (Article 7 UDHR, Article 26 ICCPR, Article 3 ACHPR, Article 24 ACHR, Article 14 and Protocol N°12[5] to the ECHR), which implies that anyone, without any discrimination based on any ground, is entitled to equal protection by the law. This right is closely related to the general principle of non-discrimination.

- *The right to an effective remedy* (Article 8 UDHR, Article 2§3 ICCPR, Article 10 ACHR, Article 13 ECHR), which allows everyone, whose rights and freedoms have been violated, to claim for an effective remedy before the competent authority (judicial, administrative or legislative, as provided by the national legal system) and to see this remedy recognized, granted and enforced.

- *The right to a fair trial* (Article 10 UDHR, Article 14 ICCPR, Article 7§1 ACHPR, Article 8 ACHR, Article 6 ECHR), which implies that everyone has the right to be publicly heard by an independent and impartial court, where minimal guarantee of defense should be provided. This includes the right to be informed promptly, in a language he can understand, of the charges against him, to benefit from legal assistance and from the right to a contradictory debate, even if economic conditions of the person does not allow him/her to pay for legal assistance. In addition, no one should be forced to self-incrimination or to confess guilt. Finally, the right to a fair trial also implies the right to be tried without undue delay and to have his sentence being reviewed by a higher court.

- *The right to the presumption of innocence* (Article 11§1 UDHR, Article 14§2 ICCPR, Article 7§1(b) ACHPR, Article 8§2 ACHR, Article 6§2 ECHR), which states that everyone should be considered innocent until proved guilty of criminal offence after a fair trial. This implies, inter alia, that doubt should profit to the accused and that burden of the proof should rest to the prosecution.

---

[4] Other, more specific, procedural guarantees that are enshrined in some of the "substantive rights", like e.g. in the right to privacy, are out of the scope of this chapter. Some of them are extensively dealt with in relevant sections of this book.

[5] See the explanatory report of this Protocol (CETS N°177 adopted in 2000 and entering into force in 2005) for a better understanding of the limitation of Article 14 of ECHR with regards to equality and non discrimination. Available on the Council of Europe website at: <http://conventions.coe.int/Treaty/en/Reports/Html/177.htm>.

- *The principle of no punishment without law* (Article 11§2 UDHR, Article 15 ICCPR, Article 7§2 ACHPR, Article 9 ACHR, Article 7 ECHR). It provides the guarantee that no one should be held guilty of a criminal offence which was not recognized as such by national or international law when the act was committed, or be subject to a higher penalty than the one that was applicable at that time. Although this principle is mainly intended in time,[6] it can also be perfectly understood in space context, as analyzed in a Council of Europe paper [Jakubowicz 2004]. This specially applies in the cyberspace, where an important and still unsolved problem relates to the competence of jurisdictions, due to the contradiction between the territorial definition of jurisdictions and the borderless characteristics of the Internet.

Moreover, specialized Conventions and Protocols and, in many cases, their implementation into national legislations have detailed and reinforced the "guarantee-rights". The Human Rights Defenders Office (HRDO) of the International Service for Human Rights (ISHR), based in Geneva, has compiled the list of international standards sustaining the work of human rights defenders [ISHR 2002]. Chapters 13 and 14 of this reference manual, for instance, deal with the right to a fair trial and the right to an effective remedy, respectively, as protected by international and regional instruments. Such a publication shows, if needed, how universal has become the protection of these "guarantee-rights" in international, regional and national legislations.

**The "guarantee-rights" as part of the realization of the rule of law**

Despite the diversity of legal cultures and systems,[7] as well as the historical evolution of the theory of the rule of law,[8] this concept, or at least its main ideas, has progressed to the point that it has become "a true rhetoric from which the sovereignty of States cannot escape any more in their relationship with the international community",[9] as analyzed by Daniel Mockle [Mockle 2000].

It is however important to keep in mind the three main understandings of the principle of the rule of law [Chevallier 2004]. It is instrumental, when understood as the legal mean by which the State is acting. It is formal, when it qualifies the State as subject to law, a vision that embeds the principle of the hierarchy of norms, like in the French system. It is substantive, when it identifies the State which legislation shows intrinsic attributes, the closest system to the "British rule of law".

Yet, Jacques Chevallier notes that it is only recently, starting from the 90s, that the rule of law principle is put back on the political scene, in a somewhat renewed view embedding at the same

---

[6] As explicitly called e.g. in ACHR: "Freedom from Ex Post Facto Laws".

[7] To the extent that a group of members of the Council of Europe Parliamentary Assembly has proposed, in May 2004, a resolution regarding the coherent translation into French of the expression "principle of the rule of law", stressing their concern related to possible misinterpretation, through inappropriate translations, of the substance of this principle. The motion is still pending. See: <http://assembly.coe.int/Documents/WorkingDocs/doc04/EDOC10180.htm>

[8] For a general overview of this evolution, see [Chevallier 2004]. We use here the expression "rule of law" as the English translation of the concept of "État de droit", rather than specifically as the concept of the British rule of law. A more comprehensive discussion could be found in [Chevallier 2003].

[9] "Une véritable rhétorique à laquelle ne peut plus échapper la souveraineté des États dans leurs rapports avec la communauté internationale" [Mockle 2000].

time the principle of the hierarchy of norms and the respect of fundamentals rights, both by their recognition and by procedural means to guarantee them. According to Chevallier and Mockle, this evolution has led to a kind of syncretic model of the rule of law, with a more substantive than formal feature, and that cannot be dissociated anymore from human rights.

This trend has been formally acknowledged at the international level in binding documents. This happened first in 1990 with the *Charter of Paris for a New Europe*, adopted in Paris by 34 European and North American participating countries at the 1990 Summit of the Conference for Security and Co-operation in Europe[10] (CSCE).Furthermore, this was extended in 1993 with the *Vienna Declaration and Plan of Action*, adopted in Vienna by the 171 States participating to the United Nations World Conference on Human Rights.[11] The first document opens the statement of CSCE's vision of "a new era of Democracy, Peace and Unity" by linking "Human Rights, Democracy and the Rule of Law" as its three pillars. It declares that human rights and fundamental freedoms "are the birthright of all human beings, are inalienable and are guaranteed by law". It thus recognizes that "their protection and promotion is the first responsibility of government" and that "respect for them is an essential safeguard against an over-mighty State". Moreover, it acknowledges that respect for the human person and the rule of law is the foundation of democracy. The second document affirms all human rights as "universal, indivisible and interdependent and interrelated". It "strongly recommends that a comprehensive programme be established within the United Nations in order to help States in the task of building and strengthening adequate national structures which have a direct impact on the overall observance of human rights and the maintenance of the rule of law".

Even beyond the distance between the formal affirmation and the actual realization of human rights, democracy and the rule of law, a counterpart of this internationalization movement, though, is that the formal bases of the rule of law concept may become somewhat diluted in this transfer from the sole legal scene to the social and political scenes as well. The risk is to end in a "fuzzy" understanding of the rule of law principle. This has been highlighted by Chevallier: "the rule of law is affirmed as a value in itself, on which no compromise can be made: encompassing multiple and fairly contradictory understandings, it appears as a swing-wing fuzzy notion; finally, its inclusion in the political discourse makes it carrying legitimating effects. The rule of law thus appears as a true myth, which scope is matched only by its inaccuracy".[12]

Guarantees are thus needed to avoid this risk, or at least to ensure some protection against it. For the realization of the rule of law, these guarantees should be both political, to protect the substance of democracy, and legal, to protect the substance of rights, and need the definition and the respect of, at the same time and in interrelation, deliberative and legal procedures.[13]

---

[10] Available at:<http://www.osce.org/item/4047.html>. The CSCE became the OSCE (Organization for Security and Co-operation in Europe) in 1994.

[11] Available at: <http://www.unhchr.ch/html/menu5/wchr.htm>.

[12] "L'État de droit est posé comme une valeur en soi, sur laquelle aucun compromis n'est possible : recouvrant des significations multiples et passablement contradictoires, il se présente comme une notion floue et à géométrie variable; enfin, son incorporation au discours politique le rend porteur d'effets de légitimation. L'État de droit apparaît ainsi comme un véritable mythe, dont la portée n'a d'égale que l'imprécision." [Chevallier 2003].

[13] As discussed by Jürgen Habermas in [Habermas 1997], showing how these principles are the necessary conditions of a legitimate use of law, even without considering any normative content.

**Challenges to the "guarantee-rights" in the information society**

While the "guarantee-rights" are a necessary part of these procedures, as constitutive elements of the rule of law, it appears that they are particularly challenged in the information society, leading not only to possible violations of these rights themselves, but to a large range of substantive human rights and freedoms, of which they are a procedural protection. This is particularly highlighted in recent national, regional and international regulation and legislation adopted or discussed in the information society sector, as shown with some examples in the following sections of this chapter.

The common nature of this legislative and regulatory trend has been to weaken the role of the judiciary power, while extending the prerogatives both of the police and of private parties, mainly the technical intermediaries or Internet Service Providers (ISPs), though other private interests have been given important powers as well in some specific cases.

On the one hand, the police and other law enforcement authorities have progressively seen their investigation powers growing, particularly in terms of interception of communications, search and seizure of data, and international cooperation by exchange of data, without the need of any court order. On the other hand, a so-called self-regulation of Internet Service Providers is strongly promoted, when not made compulsory by the legislation, and even some penalties to third parties (Internet users who subscribe to ISP services) may now be applied through contractual means granted to ISPs and other private parties.

In both cases, these increased powers are breaching the rule of law by the violation of the "guarantee-rights". However, they are being legitimized by a political discourse based at the same time on two kinds of considerations. This discourse first invokes human rights considerations, like the fight against terrorism to protect the security of persons and goods, the protection of human integrity and dignity and the protection of intellectual property. It is also based on technical and practical considerations, like the technical difficulties to enforce the law on the Internet, the need for immediate reaction – or even preventive action – where court trials are long processes, etc.

**Extending the prerogatives of police forces**

The Council of Europe (CoE) Convention on cybercrime[14] is the first intergovernmental Treaty dealing with international cooperation for investigating and prosecuting computer crimes. It is open for signature and ratification by the 46 member States of the CoE, and by non member States, some of them having actively participated to its elaboration (Canada, Japan, South Africa, the United States). Currently, 42 countries (including the four non member States) have signed the Convention, and 10 of the 38 member States signatories have ratified the Treaty and are thus bound by its provisions. Other signatories, has not yet ratified the Treaty,[15] but has implemented some of its provisions in their national legislation. This is the case in France, for instance [PHR 2004, PI-GreenNet 2003]. One Treaty section (Chapter II, section 1) is dealing with substantive criminal law issues (computer-related fraud and violations of network security, child pornography and infringements of copyright),[16] for the purpose of legislation approximation. Two other chapters,

[14] CETS N°185. Adopted in Budapest on November 23, 2001, entered into force on July 1, 2004. Available at: <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.

[15] As of April 30, 2005.

[16] The Treaty is supplemented by an additional protocol making racist and xenophobic propaganda via computer networks a criminal offence.

constituting the major part of the Convention, deal with procedural issues (respectively Chapter II, section 2, "Procedural law" and Chapter III, "International cooperation").

As described by Greg Taylor, the Treaty "attracted a storm of criticism from both civil liberties organizations as well as from computer industry organizations" since the first public draft was released in April 2000[17] [Taylor 2001].

Among the many provisions that have received strong criticisms, two of them were quite "innovative", since they created a breach of both the right against self-incrimination – thus in direct violation of the right to a fair trial – and the dual criminality requirement as a condition for mutual assistance between countries – thus violating the principle of no punishment without law. Article 19 of the Convention, dealing with search and seizure of stored computer data, aims at allowing "competent authorities" to force any person who has the knowledge of data encryption keys to provide these keys or to decrypt encrypted files. Under such obligation, a computer user may be forced to provide evidence that could allow his incrimination. Article 34 of the Convention provides with mutual assistance of parties to each other with respect to the interception of content data. This is allowed "to the extent permitted under their applicable treaties and domestic laws", although without demanding neither that the related criminal offence allows for content data interception, nor that these content data are related to a criminal offence in both countries.

Moreover, though general "conditions and safeguards" to the Convention have been added in its Article 15 after strong objections from civil liberties organizations on intermediate versions, these provisions have been found by them still "not adequate to address the significant demands and requirements for privacy-invasive techniques in the rest of the Convention".[18] This analysis was shared by the group of European Privacy Commissioners, in their opinion of March 2001,[19] which notes that safeguards and conditions are not harmonized and not required to effectively being in place. Moreover, this opinion highlights that the Convention is intended to be also signed by non-Council of Europe countries. These countries are thus not bound by the European Convention on Human Rights ("granting the right to privacy and data protection, secrecy of correspondence, fair trial, no punishment without law, freedom of expression and imposing precise conditions in clear legal texts to lawfully limit those rights") and by other European relevant instruments. These countries would then be part of an international cooperation system requiring mutual assistance as provided by the Convention, without being subject to the safeguards applicable to Council of Europe countries. This is particularly true with, e.g., the United States, one of the non-Council of Europe countries that has pushed most to have the Convention drafted and adopted. While the American Constitution indeed protects privacy in its 4th Amendment, United States privacy laws offers far less guarantees to citizens than the European legislation, as, e.g., the negotiations of *Safe Harbor* agreements between the United States and the European Union has shown [PHR 2001].
The preparatory work leading to the Council of Europe cybercrime Convention started as early as 1996, and the Convention has been adopted and opened for signature only some weeks after

[17] Most of these critics may be found at: <http://www.treatywatch.org> and at: <http://www.epic.org/privacy/intl/ccc.html>.
[18] See: http://www.treatywatch.org/Draft_27_Comments.html.
[19] EU Article 29 Data Protection Working Party Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber-crime. March 22, 2001. Available at: http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2001/wp41en.pdf.

September 11 attacks. Thus, the text doesn't contain provisions to specifically deal with the fight against terrorism, nor has it been legitimized – at least *ex ante* – by such an objective.

This is not the case of legislations and regulations adopted in many countries and regions, to specifically address the fight against terrorism, leading to important breaches in the rule of law, as controversies and strong criticism from civil liberties organizations have shown throughout the world.

Unsurprisingly, the first country that adopted such legislation was the United States, with the Patriot Act, passed in October 2001 by the US Congress. As summarized by the American Civil Liberty Union (ACLU), "while its secret search, surveillance and investigative authorities are troubling in their own right, the Patriot Act has also become a rallying point for bipartisan concern about broad erosions of fundamental checks and balances against government abuse".[20] Since the Patriot Act was passed only some days after September 11, thus under incredible emotional context, about a tenth of its provisions are temporary and should expire in 2005, unless the US Congress votes to reauthorize them or even makes them permanent. Other most problematic provisions are already permanent. Both kinds of sections violate most of the "guarantee-rights" listed in this chapter. This includes "government's ability to execute criminal search warrants (which need not involve terrorism) and seize property without telling the target for weeks or months", "allowing the FBI to seize a vast array of sensitive personal information and belongings – including medical, library and business records – using secret intelligence tools that do not require individual criminal activity. Although the records can only be seized pursuant to a court order, judges are compelled to issue these orders, making such judicial review "nothing more than a rubber stamp", "seizing a wide variety of business and financial records and in certain instances accessing the membership lists of organizations that provide even very limited Internet services", "allowing the government to demand records and content from communications providers without consent, notice or judicial review in an emergency", "Interception of 'computer trespasser' communications without a judge's assent", etc. [ACLU 2005]

At the time this chapter is being written, obviously one cannot foresee if the US Congress will reauthorize the provisions to be examined by the end of 2005, and whether it will reexamine at this occasion other, permanent, provisions of the Patriot Act, as called for by, e.g., the ACLU. However, at this step, the French case is not encouraging [PHR 2004].

The first measure taken in France after September 11 attacks have been to add new anti-terrorism provisions in a law being discussed at the time they occurred, and called the Daily Safety Law (*Loi sur la Sécurité Quotidienne*, or LSQ), enacted on November 15, 2001. It includes provisions on data retention and provides for a government access to cryptography keys. While said to be a direct response to September 11, these provisions have been extracted from the draft Law on the Information Society, introduced on June 13, 2001, *i.e.* prior to September 11, 2001, by the government and purporting to implement the EU E-Commerce Directive (2000/31/EC). With the LSQ, Internet Service Providers (ISPs) are required to store log files on all their customers' activities for up to one year. Moreover, the government has access to private encryption keys, import and export of encryption software are restricted, and strict sanctions are imposed for using cryptographic techniques to commit a crime. Many civil liberties groups opposed the LSQ because

[20] For details of the Patriot Act provisions and how they are breaching even minimal requirements of the rule of law, see ACLU main USA Patriot Act webpage at: <http://www.aclu.org/patriot>.

it heavily curtails human rights, was adopted hurriedly in defiance of regular legislative procedure, and under the pretense of the fight against terrorism. These so-called anti-terrorism provisions of the LSQ were initially valid only until December 2003, and were supposed to be subject to revision by the French Parliament at that time. As a matter of fact, this limited duration has been one of the main arguments to justify that the French Constitutional Council has not examined the compliance of this law with the French Constitution.. Socialist Senator Michel Dreyfus-Schmitt even declared that "we may hope to be back to the legality of the Republic, to call a spade a spade, after December 31, 2003 or even before this deadline",[21] de facto recognizing that these provisions were not even legal. However, before this deadline was reached, another Law called the Internal Safety Law (*Loi sur la sécurité intérieure* or LSI) was adopted on February 13, 2003, which has made LSQ so-called anti-terrorism provisions permanent. At the same time, the LSI has also authorized the immediate access by law enforcement authorities to the computer data of telecommunications operators, including Internet access providers, as well as of almost any public or private institute, organization or company. The second important measure in the LSI authorizes the search without warrant of any information system, provided that the data is accessible through a network to which the computer being searched with a warrant is connected. If the data is stored in a computer located in a foreign country, its access remains subject to applicable international agreements. The French Constitutional Council found these provisions valid, and the LSI was thus enacted on March 18, 2003.

The European Union itself has not escaped the "fight against terrorism" legitimating effect and the trend to adopt measures constituting a breach in the rule of law. It has even done this in a domain where the European Union has had for long the most advanced legislation with respect to other countries. Such legislation includes the protection of privacy and anonymity through the confidentiality of communications provided, inter alia, by the EU Directive 97/66/EC of December 15, 1997 on the processing of personal data and the protection of privacy in the telecommunication sector.[22] In addition to the general obligation put on telecommunication operators to erase or make anonymous traffic data upon termination of a call, this Directive imposed to Member States the obligation to ensure by law the confidentiality of communications. The Directive indeed prohibits any kind of interception or surveillance of communications except when legally authorized, "when such restriction constitutes a necessary measure to safeguard national security, defense, public security, the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the telecommunications system". The revision of this Directive, at first to extend its scope to any kind of electronic communications services and to implement EU internal market competition principles in the telecommunication sector, has led the European Union to abandon its well established principle of forbidding any systematic surveillance of communications. Instead, it has authorized the systematic mandatory data retention of all communications of EU

[21] "Il est vrai que le 31 décembre 2003, c'est loin, et que nous pouvons espérer revenir à la légalité républicaine, pour appeler les choses par leur nom, bien plus tôt". Michel Dreyfus-Schmitt, declaration at the French Senate session of October 17, 2001. See verbatim at: <http://www.senat.fr/seances/s200110/s20011017/s20011017_mono.html>.

[22] Available at: <http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31997L0066&model=guichett>.

citizens by Member States, despite the opposition of civil liberties organizations[23] and of a mass movement of European citizens,[24] and even despite the opinion of the group of EU data protection Commissioners. The Commissioners found that the proposal "would undermine the fundamental rights to privacy, data protection, freedom of expression, liberty and presumption of innocence", thus causing a shift in the burden of the proof in criminal cases (for a comprehensive story and analysis of this EU reversal and the role of European and non European actors, see [Marzouki 2002]).

Examples provided above are only illustrating some of the first steps of a continuous movement that we are seeing in Europe and in the United States, as well as in the rest of the world. This movement undermines protections of due process through extended prerogatives given to police forces and weakens the role of the judicial power, if only by default of requirement of a judge's assent to these kind of police investigations. However, this trend is also worsened by the extension of prerogatives of private parties.

**Extending the prerogatives of ISPs and other private parties**

Discussing how globalization may affect the law, Benoît Frydman identifies five main features of a new model of global governance: (1) a shift from institutional regulation to economic regulation; (2) a correlative shift from public regulators to private actors; (3) a shift from primary substantive rules to secondary procedural rules; (4) the increasing involvement of technical devices to implement regulations; and (5) a rhetoric emphasis put on basic human rights and fundamental liberties [Frydman 2004]. This model, which the author applies to systems apparently as different as on the one hand global warming and tradable pollution permits and on the other hand to Internet content co-regulation, seems a perfect description of Internet governance regimes and mechanisms that can be observed in other domains as well, including privacy and personal data protection [Marzouki & Méadel 2004].

An increasing implementation of this model has been occurring for almost a decade, since Internet use has been growing in the large public, making public communications at almost anyone's reach, while practical problems are indeed posed for civil or penal law enforcement, with among these problems exacerbated conflicts of rights and, obviously, conflicts of jurisdictions. This situation has led to new modalities of censorship [Marzouki 2003], where censorship is exercised either by private actors and specially Internet Service Providers or by technical artifacts implemented either in software, hardware or even Internet infrastructure itself [Lessig 1999]. How this situation leads to violations of fundamental substantive rights, starting from the right to freedom of expression, has been extensively documented in the literature, and is also discussed in other chapters of this book. However, possible violations of the "guarantee rights" identified in this chapter is seldom addressed in this context, although many adopted national and regional regulations include procedural measures which tend to affect these constitutive elements of the rule of law.

Prior to detailing this kind of procedural measures and how they may violate "guarantee rights", it appears necessary to discuss how the right to a fair trial apply in the context of civil rights and obligations. The extension of the prerogatives of ISPs and other private parties, examined in this

[23] See e.g. the letter sent by a large coalition of NGOs to the President of European Parliament, available at: <http://www.gilc.org/cox_en.html> and other actions documented at: <http://www.epic.org/privacy/intl/data_retention.html>.

[24] In less than one week, more than 17.000 EU citizens signed a petition against the proposal

section, indeed mostly relates to situations falling within the scope of civil law issues. Recalling the most important jurisprudence[25] of the European Court of Human Rights in relation to the civil aspect of Article 6 of the European Convention on Human Rights, Susan Schiavetta highlights the right of access to the court as integral part of the right to a fair trail. As she concludes: "Seeing that the rule of law would be rendered superfluous if there was no actual access to the courts, it was thought that the ability to gain access had to be an intrinsic part of Article 6. The lack of explicit reference to the right of access was merely illustrative of the fact that such a right had been entrenched in society for so long that there was no need to guarantee it further. Indeed, the ability to submit a civil claim to court is internationally recognized as a fundamental principle of law, and as such the Convention does not just presuppose the existence of courts but also the existence of the right to access courts in civil matters as without this right no civil court could begin to operate" [Schiavetta 2004]. This breach of the right of access to a court is the main violation of the right to a fair trial that can be observed in the following three groups of procedural measures extending the prerogatives of ISPs and other private parties, particularly when this extension is enforced by law.

A first group of such procedural measures deals with the limitation of ISPs liability for unlawful content they may be hosting, while authored by one of their subscribers, provided that some conditions are respected. This is the case in the European Union, with the adoption in 2000 of the E-commerce Directive. One of its provisions states that an ISP may not be held liable if either he does not have actual knowledge of illegal activity or content he is hosting or, when having such knowledge, he complies with the so-called "notice and take down" procedure by "acting expeditiously to remove or to disable access to the content". In the United States, a similar provision, though restricted to copyright infringements, applies with the Digital Millenium Copyright Act (DMCA), adopted in 1998. Regarding other kinds of infringements, the US Communication Decency Act adopted in 1996 provides that ISP are exempted from civil liability for content they host or they give access to. However, a specific provision called "the Good Samaritan provision" allows ISPs to take voluntary actions "in good faith to restrict access to or availability of material that the provider (…) considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected" [Frydman & Rorive 2002]. To summarize their practical effect, these kinds of so-called self-regulatory or co-regulatory measures allow private sector actors to remove content they host, or block content they give access to, or breach the privacy of their subscribers, or violate the protection of their personal data, upon the sole requests of third parties notifying controversial or allegedly illegal content or action. Since this decision is taken without any court decision confirming that this content or action is indeed unlawful, this may cause indiscriminate private censorship, leading to freedom of expression and privacy infringements and resulting in some cases in a breach of the principle of no punishment without law. Moreover, except with the DMCA where a "notice and put back procedure" can be issued by the author of the content to be removed so that the case can be settled by the parties without any decision to be made by the ISP, the only solution remaining for the author of the removed content is to file himself a complaint. The burden of the proof rests then to him.

A second group of procedural measures relates to the use of contractual regulations either through ISPs code of conducts or specific subscription clauses. France provides one example of the first case. Three French ministers, representatives of the music industry, and major ISPs and telecom operators signed a charter in July 2004. This charter builds on the French implementation of the E-

[25] Golder v. United Kingdom, A 18 (1975), para 35.

commerce Directive which implements the notice and takes down procedure, and the revised French privacy and data protection Act which allows royalties collection societies representing intellectual property right holders to create files with telecommunication traffic data of supposed copyright infringers using peer-to-peer networks. By signing this charter, ISPs commit to terminate contracts of their subscribers whose IP addresses have been identified by representatives of right holders. A judicial order is indeed needed for contract termination following this charter. However, this order is not the result of a normal court case respecting a contradictory procedure where each party are being heard by a judge, but rather a simple ordinance signed by a judge upon presentation of a motivated request. Consequently, there is here a breach in the right to a fair trial and the right to an effective remedy as well [Marzouki 2005].

A third category of procedural measures limiting the recourses to the judicial power is the increasing promotion of alternative dispute resolution (ADR) mechanisms, especially when implemented in on-line form (e-ADR). Susan Schiavetta provides an extensive discussion on the relationship between e-ADR and the right to a fair trial as provided by Article 6 of ECHR and in relation with the jurisprudence of the European Court of Human Rights [Schiavetta 2004]. She analyses, depending on the mandatory or voluntary character of the e-ADR mechanism, the requirements made by the European Court in order for e-ADR to comply with the right to a fair trial. These requirements are not necessarily met when the substance itself of the dispute deals with Internet content or the designation of Internet content. Examples of such cases are provided by the global and mandatory "Uniform Dispute Resolution Procedure" (UDRP) set up by ICANN, the unique Internet domain names management organism, a private party registered under California law. When a dispute over a domain name arises, the complainant – in most cases a trademark holder – may file a complaint under the UDRP procedure, so that an arbitration occurs. This process leads to a decision which may be that the domain name is given back from the defendant to the complainant, or to an enforcement procedure executed by the concerned registrar (an ISP whose role is to host the domain name). In [Mueller 2004], it is analyzed how this procedure leads to an arbitration forum shopping phenomenon, which in many cases has a biasing effect on the result of the procedure to the benefit of the complainant. Moreover, it also results in the expansion of intellectual property rights (especially trademarks) to the detriment of others (e.g. freedom of expression). This shows in the end that the UDRP procedure is far from meeting the requirements imposed for the respect of the right to a fair trial and the right to an effective remedy.

In addition to these three main categories of procedural measures extending the prerogatives of ISPs and other private parties, another major problem of law enforcement relates with the issue of competence of jurisdictions. As recalled in [Frydman 2004], "the classical rule of jurisdiction allow any State to interfere with any data posted on the Internet, as soon as these data can be accessed from a computer located in its territory". This obviously poses a central problem with respect to the inherent borderless feature of the Internet and at the same time the fact that different countries have different substantive legislation. A court decision in one country may thus find guilty a person of a criminal offence, and require execution of the corresponding penalty in this person's country, while the legislation of this person's country recognizes the act as perfectly legal. A well-known and over documented example of such a problem is the French Yahoo case [Frydman & Rorive 2002]. A – non binding – document by the Council of Europe has, for the first time ever, tried to address the problem while respecting the principle of no punishment without law. This is made by recommending to Member States "to consider whether there is a need to develop further international legal frameworks on jurisdiction to ensure that the right to no punishment without law

is respected in a digital environment".[26] However, it will certainly take a long time before such a political statement becomes binding international law.

**Conclusion**

As tentatively shown in this chapter, we are facing a heavy trend to weaken the role of the judiciary power, while extending the prerogatives both of the police and of private parties. Being solely based on procedural modifications of the law, the impact of this movement on the substance of fundamental rights may not immediately appear as obvious. Provided that the substantive rights themselves are not directly modified, these changes may still seem acceptable to many observers. However, since the "guarantee-rights" are procedural means to protect, defend and recover the "substantive rights", human rights defenders should understand that, as soon as the "guarantee-rights" are challenged, "substantive rights" are *de facto* endangered.

This tendency is the result of a globalized world, more and more ruled by economic regulation and the market forces, and where States are more and more leaving their sovereign prerogatives into the hand of private parties, promoting so-called self-regulation and co-regulation procedures in the name of efficiency. These contractual procedures, mainly involving private actors, and also sometimes public actors, apply to a subject who is not even a party in the contract: the citizen. This is particularly shown by the "Notice and take down" procedure. At the same time, States are increasing their surveillance and monitoring powers over citizens: in the name of a war against terrorism, and with the pretension of increasing our security, human rights, the rule of law and democracy are being violated, thus best realizing the objectives of the enemies of democracy.

In his analysis of how globalization affects the law, Benoît Frydman identifies two traditional ways to tackle legal issues involving international aspects: "the first one are the rules of jurisdiction [...], the second one is for the international community [...] to agree on common rules and standards." [Frydman 2004]. Although some cases, like the French Yahoo case, have shown that the first way has not yet been completely abandoned, explorations of the second way have already started.

Legislation approximation has been occurring at the European Union level, and this article has shown how, when dealing with the information society sector, this process is challenging the "guarantee rights" by many aspects. However, the European Union case is special in that it constitutes a coherent regional Union of States, with its own institutional system, rules and legal order.

The first real attempt of international agreement between sovereign States is thus the Council of Europe Convention on cybercrime. In this case too, we have shown that the "guarantee-rights" have been challenged.

The second attempt has been the World Summit on the Information Society (WSIS). Human rights defenders have seen WSIS as "an important opportunity to carry the human rights agenda forward",

---

[26] Council of Europe, Multidisciplinary Ad Hoc Committee of Experts on the Information Society (CAHSI). *Draft political statement on the principles and guidelines for ensuring respect for human rights and the rule of law in the information society*, approved by the CAHSI on April 7, 2005. Available at: <http://www.coe.int/t/e/integrated_projects/democracy/02_Activities/00_Declaration_on_Information_Society>

as declared by the WSIS Civil Society Human Rights Caucus at the Geneva phase of the Summit.[27] Aiming "to actually translate human rights principles to the context of the information society", the Caucus task has rather "become defending the formal commitment to previously reached international consensus, that is, preventing complete backtracking on human rights". After WSIS' second phase completion, the challenge of bringing forward the actual implementation of human rights standards has clearly not been met. As numerous cases show, the main human rights problems today do not relate to lack of formal commitment, but rather to lack of effective implementation of human rights. The first international attempt to translate human rights in the context of the information society has thus been squandered [Marzouki & Joergensen 2005].

Any future attempt to tackle the globalization issue and its impact on information society legislation would face the same failure, unless it starts by recognizing that procedural means to protect universally recognized human rights and fundamental freedoms, known as the "guarantee-rights", do have their precise translation in the information society, and should be protected as such. The first and foremost protection resides in strengthening the judiciary power, instead of weakening it.

**Bibliography**

ACLU, American Civil Liberty Union, *Patriot Act Sunsets*, New York, March 2005, available at: <http://www.aclu.org/sunsets>.

Chevallier, Jacques, *L'État de droit* (4th edition), Paris, Monchrestien (Clefs), 2003.

Chevallier, Jacques (dir.), "L'État de droit", *Problèmes politiques et sociaux* n° 898, La Documentation Française, Paris, March 2004.

Frydman, Benoît, "Coregulation: a Possible Legal Model for Global Governance", in *About Globalisation, Views on the trajectory of mondialisation* (dir. Bart de Schutter and Johan Pas), Brussels University Press, 2004.

Frydman, Benoît, and Rorive, Isabelle, "Regulating Internet Content through Intermediaries in Europe and the USA", in *Zeischrift für Rechtssoziologie*, vol. 23 n° 1, Max Planck Institute, 2002, p. 41-59.

Habermas, Jürgen, *Droit et démocratie. Entre faits et normes*, Paris, Gallimard (Nrf Essais), 1997.

Holt, James C., *Magna Carta*, Cambridge, Cambridge University Press, 1992 (revised second edition).

ISHR, International Service for Human Rights, Compilation of International and Regional Instruments for the Protection of Human Rights Defenders, Geneva, 2002, available at:

[27] WSIS CS Human Rights Caucus press release, December 7th, 2003. Available at: <http://www.iris.sgdg.org/actions/smsi/hr-wsis/hris-pr-071203-en.html>.

<http://www.ishr.ch/about%20ISHR/HRDO/Publications/Human%20Rights%20Defenders%20Series/Compilation/CompilationContents.htm>.

Jakubowicz, Karol, "Human Rights in the Information Society: A Preliminary Overview", Working paper prepared for the Council of Europe Preparatory Group on Human Rights, the Rule of Law in the Information Society (IP1(2004)47(web)), Strasbourg, September 2004, available at: <http://www.coe.int/t/e/integrated_projects/democracy/02_Activities/00_CAHSI/IP1%282004%2947_Jakub.asp>.

Lessig, Lawrence, *Code and Other Laws of Cyberspace*, New York, Basic Books, 1999.

Lochak, Danièle, *Les droits de l'homme*, Paris, La Découverte (Repères), 2002.

Marzouki, Meryem, "Petite histoire de la Directive européenne sur la vie privée et les communications électroniques ou le revirement de l'Europe", in *Terminal*, n° 88 (special issue *Fichiers et libertés: le cybercontrôle 25 ans après*), Paris, L'Harmattan, Winter 2002 - Spring 2003, p. 61-83.

Marzouki, Meryem, "Nouvelles modalités de la censure: le cas d'Internet en France", *Le temps des médias – Revue d'histoire*, n° 1, Paris, Nouveau-Monde Éditions, Paris, Autumn 2003, p.148-161.

Marzouki, Meryem, "Informatique et Internet: de l'État de droit à l'arbitraire", in *L'état des droits de l'Homme en France,* édition 2005 (dir. Ligue des droits de l'homme), Paris, La Découverte, 2005.

Marzouki, Meryem, and Joergensen, Rikke Frank, "A Human Rights Assessment of the World Summit on the Information Society", in Information Technologies and International Development, Vol. 1, Issues 3-4 (Special issue The World Summit in Reflection: A Deliberative Dialogue on the WSIS), MIT Press, Summer 2004, p.86-88.

Marzouki, Meryem, and Méadel, Cécile, "Gouvernance technique et gouvernement politique d'Internet: enjeux et questions de recherche", Proceedings of the 14th SFSIC National Congress on Information and Communication Sciences. Béziers, June 2004.

Mockle, Daniel, "Mondialisation et État de droit", in *Les Cahiers de Droit*, vol. 41 n° 2, Laval University, March 2000, p. 237-288.

Mueller, Milton, *Ruling the Root: Internet Governance and the Taming of Cyberspace*, Cambridge, MIT Press, 2002.

Electronic Privacy Information Center and Privacy International, "Privacy & Human Rights", Washington DC, EPIC, 2001, available at: <http://www.privacyinternational.org>.

Electronic Privacy Information Center and Privacy International, "Privacy & Human Rights", Washington DC, EPIC, 2004, available at: <http://www.privacyinternational.org>.

Privacy International and GreenNet Education Trust, "Silenced", an international report on censorship and control of the Internet, London, 2003, available at: <http://www.privacyinternational.org>.

Schiavetta, Susan, "The Relationship Between e-ADR and Article 6 of the European Convention of Human Rights pursuant to the Case Law of the European Court of Human Rights", in *The Journal of Information, Law and Technology* (JILT), vol. 2004 n° 1, April 2004. Available at: <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2004_1/schiavetta>.

Taylor, Graig, "The Council of Europe Cybercrime Convention. A civil liberties perspective", Adelaide, Electronic Frontier Australia, 2001, available at: <http://www.efa.org.au/Publish/coe_paper.html>.