

XXIIIrd International Conference of Data Protection Commissioners
Paris, 24th - 26th September 2001

**SUMMARY OF THE PAPER READ BY MARCO CAPPATO, EUROPEAN DEPUTY
ON THE " BONINO LIST " AND RAPPORTEUR TO THE EUROPEAN PARLIAMENT
ON THE PROTECTION OF PRIVACY IN ELECTRONIC COMMUNICATIONS**

INTRODUCTION

In the Klass Judgement dated 1978, the European Court of Human Rights wrote :

" 49. ... the Court notes that the national legislator enjoys a certain discretionary power (in the choice of the methods used by surveillance systems). Nevertheless, the Court makes it clear that this does not give the member States unlimited latitude in imposing secret surveillance methods on the people who are subject to their jurisdiction. Conscious of the danger inherent in such a law of undermining or even destroying democracy on the pretext of defending it, it confirms that they may not take just any measures they think fit in the name of the fight against espionage or terrorism. "

These words express the risks that our society, our States and our citizens currently run and the limits which a law-abiding State may not exceed. The ferocious and bloody terrorist attacks which struck the United States on 11th September last have encouraged some people to demand " exceptional " laws. In Italy, we have good knowledge of the " exceptional " laws on organised crime and terrorism which are rooted firmly in the penal code (which is the code we inherited from Fascism) and which have also been exported to other countries.

Many people repeatedly say nowadays that we have to sacrifice some of our liberty to gain increased security and that in a time of insecurity exceptional measures are needed. This does not upset me when this concerns controls at airports or when going through customs, however I am opposed to proposals from the State which aim to install permanent systems of access to the private life of citizens.

THE EUROPEAN UNION

The proposed directive from the European Commission on the protection of privacy in electronic communication systems - which modifies a directive dated 1997 on the same subject in the light of new technological developments and as part of a drive to liberalise the telecommunications sector - is currently being examined by the European Parliament and the Council. Certain Ministers of Telecommunications, encouraged by their colleagues in the Home Office and Police forces, want to modify the directive in that part which imposes the deletion of data relating to telephone traffic (the number making the call, the number called, the duration of the communication and the time the communication started and ended, etc.) and the localising of a mobile

phone once the processing of this data for invoicing has been completed. Certain governments within the Council wish to introduce these modifications in order to be able to impose on communications service providers the duty to retain this data for longer periods which may extend up to 7 years, in order to enable police forces, following legal authorisation, to search for the data required to track down criminals and to use it as evidence.

On this point, it should be remembered that this " external " communication data is often treated in the same way as the contents of the communication itself, as Italian case law, for example, has done ; the Italian Supreme Court in 1998 judged that traffic data cannot be used as evidence in a trial without the authorisation of the legal authorities. Therefore the retention of this data - which is one of the phases of processing - whether it is carried out by the State or by the service provider, and since it can be assimilated to the recording of the content of a conversation, must be considered as an interception of the communication. The idea circulating within the Council would therefore aim to achieve the installation of a wide ranging surveillance system.

There is a second consideration to be taken into account, an economic one : the obligation of retaining data on traffic for seven years would represent a significant cost for service providers and this would have economic consequences for subscribers and users. For example, this factor has scuppered the plans of the government of the United Kingdom to establish a State data bank.

Although the Council is moving toward the strengthening of cyber surveillance, the Commission on Liberties and Citizen's Rights unanimously supported my amendments which aimed to introduce into the directive an explicit reference to the jurisprudence of the European Court of Human Rights. The approved text noted :

(Art. 15, para.1) : " The Member States may take legislative measures with the aim of limiting the effect of the rights and obligations provided for in Articles 5 and 6, Article 8, paragraphs 1 to 4, and Article 9 of this directive when this limitation constitutes, ***in a democratic society***, a measure which is necessary, ***appropriate, proportional and limited in time*** to safeguard the security of the State, its defence, public safety, the prevention, search for, detection and prosecution of penal infringements or the unauthorised use of the electronic communications system, as provided for in Article 13, paragraph 1, of the directive 95/46/CE. ***These measures must be totally exceptional, based on a specific law which is understandable by the general public and authorised by the legal or competent authorities in specific cases. By virtue of the European Convention on Human Rights and in accordance with the judgements handed down by the European Court of Human Rights, any form of general or exploratory electronic surveillance carried out on a wide scale is forbidden*** ".

Following this vote, my Report was sent back to the commission after a vote in plenary session which was highly controversial, in particular on the question of the opt-in or opt-out, on unsolicited electronic commercial communications. As a result, the proposals

of the European Parliament on the protection of private life will have to be discussed once again in the months to come.

Personally, I am going to maintain my position, and not only with regard to a question of fundamentals but also one of method, which affects all of the decisions which the European Union is in the process of taking. On subjects as sensitive as this, we cannot accept a method that is fundamentally undemocratic in the European Union, in particular in connection with the question of cooperation between police forces and legal procedures. The Council discusses and takes decisions in secret. Europol, Schengen, Enfpol and Eurojust are outside the control of any democratic and legal body. Following the terrorist attack in the USA, any resistance to the strengthening of these instruments appears to have been overcome, in particular nearly everybody seems to agree with Europol's operational mandate but the question of the power of Parliament and of the Court has not been raised.

CYBER SECURITY OR CYBER DEMOCRACY : WHICH HAS PRIORITY ?

Obviously, after what has taken place in the United States, all pronouncements are centred on the use of computers by criminal organisations and States. The request for citizens' security to be improved cannot remain unanswered. The route which, for the moment, we have decided to take is that of strengthening the mechanisms of State controls. However, if we are able to accept a new balance between liberty and security, we certainly cannot abandon our principles and the fundamental liberties which characterise democratic and law abiding States in the name of security. In particular, we must oppose all those who take advantage of the situation to impose, like real jackals after power, repressive and even violent policies (even the declarations issued by Putin, who draws a parallel between the violence suffered by the USA and that which Russia "may be suffering" in Chechnya, where in reality he has imported war and terror).

CONSIDERATIONS AND PROPOSALS

* Secret service specialists are almost unanimous in emphasising that the limits of " intelligence " mainly lie in a strategy that is too oriented toward work at a distance and technology, especially the interception of data, and too little based on work carried out in the field with flesh and blood agents. The reason for this strategy is only too easily understood. It takes account of the human and economic costs of direct action. If this strategy on its own has failed, it is perhaps necessary to support it with other measures, with priority given to work in the field.

* Organised criminals are not going to stop when faced with security systems designed to control the general public ; they have the means to use sophisticated systems. On the other hand, we cannot accept that the person monitored, the " enemy ", becomes a simple citizen who surfs on the Net or who makes a telephone call.

* The systems for protecting private life, such as cryptology, may be very useful not only for criminals but also for protecting ourselves from criminals.

* We must design and produce a democratic counter-offensive to disseminate knowledge together with the instruments to help citizens to exercise their power. It is not only a question of protecting citizens (privacy), or fighting criminals (cyber crime), but also and above all of strengthening citizens through new technologies :

- on line democracy : the " on line " transmission of all the public events in our democracies ; the possibility of carrying out all types of " public " acts via the Internet (this is what the draft laws based on popular initiatives are asking for and for which Italian radicals are in the process of gathering signatures)
- the dissemination of information : Radio " Voice of Europe " ; to fight the generators of propaganda with counter-information.
- to overcome censorship, the filters that block the network ; freedom of expression must be included as a condition in international agreements.

Marco Cappato