



New Technical Means of Surveillance and
the Protection of Fundamental Rights -
Challenges for the European Judiciaries

Vienna, June 19th 2009
Justizpalast/Palace of Justice

Legal Restrictions – Surveillance and Fundamental Rights

Giovanni Buttarelli

Assistant European Data Protection Supervisor

Introduction

This conference takes place just after a significant event at European level. Last week, the European Commission issued an important Communication to the European Parliament and the Council on an area of freedom, security and justice serving the citizen ('Stockholm-communication'): three key values to be reinforced within a Europe that is based upon the rule of law and the constitutional traditions of the Member States.

The declared aim of the Stockholm-communication is to give a central place to citizens and their rights (pt 2.1). The Communication affirms that *"Respect for the individual and for human dignity, referred to in the Charter, is a core value in the area of freedom, security and justice. In this area without internal borders citizens can move freely and enjoy their rights fully"*.

Nevertheless, the task of reconciling those values is not an easy one.

We are living in a digital age where new technologies, profoundly innovative, are intensely growing day by day and where surveillance in a modern sense (not only through video cameras) is playing an increasing role.

Our countries present more and more new elements of a surveillance society where everyday life is significantly monitored for different and sometimes unclear purposes.

I will make some comments about the growing requests and expectations of law enforcement bodies to use personal data, about the increasing possibilities of information use, about the impact of certain technological developments and the relevant need to conceive modern and effective means for protecting individuals.

The growing needs to use information

Focusing again at European level we can see that the legislative EU agenda of recent years was dominated by initiatives for new legal instruments relating to information.

I could quote tens of proposals and relevant outcomes which are intended to facilitate the storage, exchange and access of information for the fight against crime and terrorism, for an efficient control of the external borders of the European Union but also more in general to ensure security.

Examples of these instruments are well known. I just mention, among an impressive list:

- the 2006 Data Retention directive which asks for the retention of the communications data of all European citizens;
- the Council Decision on Prüm and its implementing decision, leading to the compulsory storage and exchange of DNA and fingerprinting data between the authorities of the Member States;
- the new legal frameworks for Europol and Eurojust, with additional possibilities for data use and exchange by these bodies;
- the proposal for an EU system to use passenger data (EU PNR), which will require airlines to transfer personal data of all passengers to authorities of the Member States;
- two decisions on the exchange of criminal records between the Member States;
- the Decision giving law enforcement access to the Visa Information System;
- the legal framework for SIS II.

All these legislative initiatives are motivated by the presumed, unavoidable need to use more information. Quite often since 9/11 the fight against terrorism lies at the basis of these measures.

The focus of the EU on information and personal data might appear logical, since the institutions of the EU do not have the capacity to directly guarantee security themselves. There is no European police with executive powers; the EU can not instruct the Member States to combat specific crimes and the European Courts do not have the powers to give direct legal protection to individuals.

The EU therefore continues on focusing on measures that are intended to enable the competent authorities of the Member States to fight against crime, using an increased amount of information including personal data which sometimes is deeply excessive.

There are indeed circumstances when it is legitimate and necessary to sacrifice privacy and other fundamental rights to a certain degree, in the interest of security. Our society must be able to defend itself in the best way against threats.

However, the burden of proof must always be on those who claim that such sacrifices are necessary and the proposed measures are all effective instruments to protect society.

We should not trade away fundamental rights, if this is only for an illusion of greater security or if simply useful for "just in case". We risk sleepwalking into a surveillance-society, step-by-step and without realizing all consequences: into our society where fundamental rights and freedoms will in practice be greatly and permanently diminished.

The growing possibilities to use information

This brings me to the growing possibilities to use information.

Recent developments among information and communication technologies are sometimes considered as an independent reason for increasing exchange of and access to information for the safeguarding of security. ICT gives law enforcement bodies important new possibilities to become more effective and use new proactive strategies, based on available information and the combination of information.

It is beyond doubt that these bodies should profit from new technologies. However, any legislative, judicial or administrative instrument allowing the massive or intelligent use of information by law enforcement authorities should be based on a specific, deliberate and transparent choice of the legislator, and in sensitive cases on the basis of a public debate.

Interoperability is an important notion in this context. The Commission seems now to argue that this is a technical rather than a legal or political concept. This explanation can be questioned. It is based on the assumption that the choice of technology is a neutral one and that it is up to those using the technology to decide the conditions under which use is allowed.

However, this assumption ignores the fact that information tends to be used if it exists. We have seen this with the decision giving law enforcement access to the Visa Information System, a data base with a purpose that has nothing to do with law enforcement. The Commission is now also preparing a proposal for access to Eurodac, the EU system of fingerprints in the area of asylum.

Examples of surveillance technologies

I think it is useful to become a bit more specific at this point and give a few examples of technologies that could affect individuals and their fundamental rights.

A first one is represented by modern video-surveillance technology.

Video-surveillance systems are becoming more and more sophisticated and powerful.

There is a little doubt that we are faced with an extensive use of closed circuit television (CCTV) surveillance in private and semi-public spaces, particularly in the transport and retail sectors.

New initiatives are in place following the UK's example of deploying open street CCTV for the purposes of crime prevention.

One can argue that CCTVs are just cameras coupled by a cable to a display monitor which only facilitates the human observation of the daily life, but interesting decisions coming from the Venice Commission underline their added value and demonstrate that it is necessary to understand their impact on our societies.

Videosurveillance techniques initially focussed (especially starting from the '70s) on the monitoring of road traffic or else on the prevention of thefts and robberies in banks and shops selling luxury items.

In the subsequent years surveillance techniques were especially refined in respect of the workplace, in the transportation sector –in particular in subways and in nearby areas– as well as within certain public buildings (in order to prevent vandalism) and in recreational areas.

Surveillance techniques have subsequently been developing uninterruptedly and have been applied to the most diverse sectors.

In the transportation sector, there has been a continued increase in the number of controlled roads –both motorways and highways– with a view to the monitoring of traffic, misdemeanours (even by means of infrared devices) and, more recently, the access to town centres – both big and small.

Video surveillance devices have been widely installed in banking institutions, stadiums and sports facilities, petrol stations, taxi services, health care centres, museums and cathedrals, for the security of domestic units and residential districts, taxi services and in public places designed for promoting tourist activities.

Indeed, in many urban cities it is difficult to find a place which is not extensively monitored.

Modern systems capture and record digital images that are easily copied and distributed. The images can be instantaneously broadcast to a multitude of recipients or posted on the Internet with the help of today's and tomorrow's powerful digital communication networks.

As a result, intelligent and interconnected systems are better able to match images against a database of images or track moving targets (objects or persons) in large areas. They are also getting better at automatically identifying pre-defined, "suspicious" behaviour.

New integration tools offer the possibility to combine in a comprehensive manner a growing number of information gathered by a greater diversity of surveillance technologies. One can think of a combination of mobile phone interception and location, CCTV with license plate recognition facility, parking tickets and log files available online: an analysis of a torrent of information produced by ubiquitous surveillance technologies, with a risk of growing discrepancies between suggested scenarios and the reality of facts.

The need for protection

Growing use of personal data leads - under the rule of law! - to a growing need for protection. A balance is needed.

In a surveillance society protection is a serious concern. I use again the example of CCTV.

The growing use of surveillance techniques by an increasing number of highly patronized shops might result into a "function creep", facilitating the use of images for purposes not foreseen and specified initially, for instance the assessment of customer habits and behaviour with regard to the arrangement of the products on sale. In this specific sector, surveillance systems (especially video surveillance systems) became a valuable tool for commercial purposes even though they had been initially (or seemingly) deployed for the prevention of thefts and robberies; in turn, this made it possible to rationalize business resources both within a given shop (e.g., by determining the number of tills to be opened in accordance with the time of day and the monitoring of entrances) and from a more general standpoint (e.g., by devising "shopping routes" that could be found more stimulating by consumers).

Being watched changes the way we behave. Indeed, when watched, many of us might censor our speech and our behaviour. This is certainly the case with widespread or continuous surveillance. Knowing that every move and gesture is monitored by a camera may have a psychological impact and change behaviours. This constitutes an interference with our privacy.

There is a risk for the freedom of expression: CCTV may discourage legitimate behaviour such as political protests supporting unpopular causes. Participants traditionally had the right to anonymously participate in a

peaceful assembly, free of risk of identification and repercussions. This is fundamentally changing!

The fact of “being seen without seeing” may influence a person’s conduct and activity. On the one hand, hidden filming and/or control devices do not promote openness for citizens; on the other hand, cameras and other devices that are known to have been installed at a given location may lead to “submissive” behaviour on the citizens’ part.

Liberty of movement: modern CCTV systems equipped with facial recognition and/or dynamic-preventive surveillance software in large, interconnected systems can track movements of people in vast areas. One should actually argue that the freedom of movement means the freedom to move not only in a physical sense, but also in a more fundamental sense –that is to say, the freedom to move without having inevitably to leave continued and/or frequent traces of one’s movement for the benefit of permanent “optic informers”.

The right to be free from discrimination: CCTV operators may tend to discriminately target surveillance towards ethnic minorities, teenagers, the homeless, and all non-conformist groups of people perceived as a "risk".

There are increasing opportunities both for security breaches and misuse: the recordings may fall into the wrong hands or may be used by the lawful recipients for unlawful purposes.

Based on the technical development of these systems, it has progressively become possible to transmit images to “control centers”, to associate images and sounds, to introduce “intelligent systems” for assessment and intervention.

Surveillance systems can be equipped or associated with software for automated image retrieval, allowing the recognition of persons by means of

techniques for the targeting of suspected offenders – for instance, based on automatic facial recognition techniques (facial mapping software applications).

It is increasingly feasible to issue various types of alarm (including the signalling to watchmen) regarding persons suspected either on account of specific descriptions or based on behavioural patterns that are automatically classified as “abnormal” by the software (e.g., in a parking place or at the entrance of a stadium).

This points to the possible identification of alleged misbehaviour based either on the outward appearance (physical features, clothing, skin colour) or on actions and events that are regarded as especially interesting (sudden movements, smoke, opening of doors).

Could we say that all these are proportionate solutions to our contemporary problems and that everything is necessary and appropriate ?

Indeed, surveillance systems may have positive effects in terms of security; however, there is no uniformity in the extent to which this effect can be regarded as positive. In a few cases there has undoubtedly been a decrease in the number of criminal offences in public places; in other cases this surveillance has proved ineffective or caused criminals to move to other nearby areas, or else it has simply allowed obtaining evidence against the persons filmed. Finally, there is the risk that surveillance is implemented to an excessive extent as a handy way to cope with basic flaws in organizational and/or law enforcement matters rather than in order to meet actual requirements.

If compliance with the proportionality principle is not ensured, the number of public and private areas under surveillance might increase exponentially in the next few years: the final outcome would be a society

placing excessive restrictions on personal freedom. In other words, surveillance should be focussed on areas that are really at risk.

There can be no doubt as to the definite need in future for a more selective approach in the use of surveillance systems: the public as a whole should not suffer excessive limitations on account of the need to prevent the misbehaviour of a minority.

The scope of discussion should therefore be expanded by going beyond the issue of the beneficial effects on security for persons and property: it would be more appropriate to also evaluate the effects on citizens' freedom and conduct.

In other words, in addition to considering the extent to which surveillance causes a breach of privacy, one should evaluate the effects resulting from the widespread use of surveillance as regards citizens' freedom of movement and behaviour.

Citizens may thus be turned into information "subjects", without respecting the right to informational self-determination.

Surveillance more generally

These arguments are also relevant in connection with the more general notion of surveillance, which is wide-ranging by nature and goes well beyond the control via video equipment. This notion includes the control of phone and computerized communications as well as of the circulation of content. It may even apply to the distance control of specific users of a service (see, for instance, the location of mobile phones) or else of persons in connection with a judicial action (this is the case with the use of electronic bracelets).

Indeed, the surveillance concept could refer to *"any activity operated by technical means, consisting of monitoring, collecting and/or recording, on a non-*

occasional basis, personal data concerning one or more individuals and relating to their behaviour, movements, communications and utilization of computerized and/or electronic devices".

A clear example is represented by the emergence of cloud computing and its related remote services. Although you might need a judicial warrant to gain access to the family pc in a home, in some countries this might not be the case if certain software installed in a pc or information stored before "at home" is now held or processed outside home by a central server. Technology will offer enormous facilities in terms of surveillance as almost all the user activities will be available "externally" or "online".

We should wonder whether the effective fight against crime requires downsizing rights and fundamental freedoms of citizens that are not concerned by investigations and inquiries carried out by public bodies.

We need to evaluate the specific need for implementing investigation techniques that impinge not only on terrorists', but on millions of people's private lives -whilst these people are in no way involved in criminal activities.

It is possible to make a more balanced reasoning. We should reject the equation more security = less privacy and start from the point that privacy is not a hindrance to security.

Indeed, one thing is the emergency related to veritable terrorist activities at a given time in history, especially if large-scale activities are at stake just like those that took place in New York, Washington, London and Madrid, whilst a totally different thing are the requirements typically made by each law enforcement body in prosecuting -under ordinary circumstances, therefore within the framework of their standard investigations- offences

such as child pornography, cybercrime, xenophobic conduct, money laundering, sometimes with a massive collection of data on-line.

There is also a risk of re-introducing in some countries forms of the so-called "Rasterfahndung", i.e. the massive data tracking activity that had already been implemented in the '70s against the RAF. This approach is based on matching data in accordance with a set of criteria allowing possible criminal profiles to be defined –such as the fact of paying water and power bills cash instead of via a bank draft, or delaying payments, or losing one's passport– as well as on considering "abnormal" circumstances that are regarded as requiring more in-depth analysis. In this way, non-suspected persons are screened progressively.

Subscribers' names, power/water/gas/telephone consumptions – both standard and not -, payment arrangements (bank drafts, cash, etc.) are undergoing a blanket analysis as regards Muslim foreigners. Huge amounts of data are analysed and subsequently stored in respect of persons who – though possibly not meant to be always identified – will certainly be identifiable following this analysis.

Last December, Vice President Barrot mentioned in an EU Parliament session the taking of digital fingerprints in nomad camps in Italy, in order to point out to the recent European and national initiatives oriented to re-establish the full respect of Community law and fundamental rights.

Other references can be made (apart from the PNR issues) to the creation of no-fly lists, related to people who are not permitted to board a commercial aircraft for travel in or out of a country), as well to the unlawful, hidden and massive collection of web page addresses by some Internet access providers, to new legislation introducing the obligation to provide Internet users with unambiguous IP addresses.

Truly democratic societies must commit themselves to this fight, but there are conditions to be respected.

Proportionality criteria have to be respected.

We must act wisely: if the measures we have planned potentially produce negative effects on fundamental rights, we must limit ourselves to those measures that are not merely useful or desirable, but actually meet imperative social requirements – as also ruled by the European Court of Human Rights.

We must consider the long-term impact of the measures and initiatives we take.

In our societies, we should start discussing open-mindedly, to the widest possible extent, the initiatives aimed at fighting crime so as to assess all their concrete consequences in terms of fundamental rights and freedoms.

We should refrain from obscure, incomplete provisions and give priority to easily accessible, foreseeable measures in terms of their scope and manner of application.

We should manage, once again, to distinguish anti-terrorism measures from those with a much wider scope of application – such as ID cards, or the wide-scale implementation of biometrics, or the generic definition of “computer crimes” which allows for interpretations that are not in line with rule of law principles (see the recently enacted CoE cybercrime convention).

What is the sense of requiring biometric devices to screen frequent flyers, when a quick glance is all that is necessary for us travelling pigeons – or victims of frequent travels, as you like – to recognise each other in airport halls and waiting rooms?

If biometric data are required for identification, can we be 100% certain that no other technique is available to achieve secure identification?

We should rather try to carefully consider whether less privacy-intrusive approaches are available to establish facts and responsibilities, before introducing new measures to fight terrorism.

We should ask the competent authorities and the private entities concerned by these measures – especially in the telecommunications sector – to assess their proportionality compared to the nature and seriousness of the criminal offences, so as to avoid duplicate databases.

If, then, it is enough for certain data to be accessible online, there is no need to authorise other entities to set up separate data banks.

Too many online access points reduce the security of information systems.

We should also consider that databases brimming over with information collected to be used “just in case” are far from effective and full of information “noise”.

We should abstain from all types of blanket surveillance and lay down safeguards against possible arbitrary initiatives by public authorities.

Investigation activities: evidence and electronic media

In this perspective, the implementation of the Budapest Convention on cybercrime represents another key example.

The Convention does not apply only to cybercrime, as it addresses the implementing procedures and mechanisms in respect of various criminal investigation activities (inspections, searches, seizure of correspondence and other items, custody, urgent inquiries, etc.) related to other types of crime – i.e. “conventional” criminal offences – whenever the evidence to be gathered is to be found on and/or with the help of electronic media.

The Convention envisages various mechanisms of co-operation and mutual assistance, also for extradition purposes. They apply not only to the criminal offences *“related to computer systems and data”*, but also to *“the collection of evidence in electronic form”* of any criminal offence. This might concern a considerable number of cases, since the offences in question are punished by deprivation of liberty for a maximum of at least one year.

Given this framework, the criminal investigations carried out in the individual countries –including the investigations arising out of international co-operation requests under the Convention– might ultimately result in the collection and exchange of a considerable amount of personal data (including telephone and Internet traffic data) that need not be related directly to cybercrime – or that might be related to fully lawful activities.

The Convention only partially takes account of the objections and suggestions put forward by the European DPAs in terms of necessity, adequacy and proportionality.

Assistance measures should provide for the adequate protection of fundamental human rights – in particular those laid down in the Human Rights Convention, whose article 8 refers to the right to privacy. Additionally, they must ensure compliance with *“the principle of proportionality”*.

The application of the principle of proportionality is set forth by the Convention as a mandatory requirement in view of the proper application of the Convention itself.

Hence, it is necessary for this principle to be included (if this is not already the case) and developed appropriately in domestic legislation. To that end, each of the relevant pieces of legislation regulating investigations and preparatory work in connection with criminal proceedings should contain an ad-hoc provision whereby investigational and procedural activities will have

to be handled by judicial and/or police authorities in accordance with a proportional, selective approach – that is to say, by having regard to the data and information that are relevant and not excessive in respect of the investigations in progress, and by applying equally proportionate mechanisms. Alternatively, one might envisage a single general rule to be included in the Act ratifying the Convention and subsequently incorporated into criminal procedural law.

The “proportionality” clauses in question should also apply to other investigational activities mentioned in the Convention, irrespective of whether they are already regulated under domestic law – e.g. as regards Italy, to the interception of communications and conversations, in particular “new generation” tapping such as the one applied to VoIP.

Should it prove impossible to ensure that the principle of proportionality is explicitly mentioned in the legal instruments regulating investigations, it is unquestionably appropriate to raise the awareness of the competent investigational bodies in order to ensure that the principle of proportionality referred to in the Convention is always respected in practice during the investigations, also in connection with websites, blogs, social networks, chat and forums.

Concerning the impact of investigational activities on third parties' rights, I believe that the domestic legislation of each country should also include a provision implementing a similar principle that is laid down in article 15 of the Convention – whereby the impact of the investigational procedures upon the rights and legitimate interests of third parties should be considered. There is little doubt that the use of computerised means – which might ultimately be the subject of a seizure order – makes it easier to process a huge amount of personal data also related to other parties; this requires an especially selective approach in carrying out the investigations, also in order

to avoid affecting the rights and interests vested in individuals that have nothing to do with the facts being investigated.

Finally, concerning the freezing of traffic data, the 2001 Convention does not contain provisions that require electronic communications service providers to systematically retain traffic.

Indeed, the Convention only allows the temporary preservation of specific computer data, including traffic data, that is already in service providers' possession or control (this is the so-called data "freezing"), also in view of international co-operation. This measure is applicable if it is necessary for the competent authorities to have the data at their disposal and there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

The "freezing" of data is especially appropriate in legal systems that do not allow large-scale traffic data retention (like those implementing directive 2006/24/EC) – or else allow such retention for a very limited period only.

Any measure related to this issue should be evaluated carefully in the light of purpose limitation and proportionality principles, given that the relevant legislation would also apply to non-billing data, as well as in accordance with a selective approach. Account should be taken, additionally, of the provisions made in the Convention (Article 15(2), Article 16(1) and Article 29) with regard to data retention conditions and periods. As for EU countries, reference should also be made to the safeguards laid down in the European traffic data retention directive.

The legal recognition of protection

Our legal traditions recognise data protection and privacy as fundamental rights. I just point at the European Convention on Human Rights, the EU Charter of Fundamental Rights, the EC-Treaty and the

Constitutions of a number of Member States. The best-known legislative instrument on data protection is, of course, Directive 95/46.

All the new legal instruments of the EU on the use of information - I mentioned them earlier - must respect principles of data protection, in order to fulfil the conditions of Article 6(1) of the Treaty of the European Union.

On top of that, in the third pillar Article 30(1)(b) TEU provides that common action in the field of police cooperation relating to the collection (etc.) of information is "subject to appropriate provisions on the protection of personal data".

Recital (3) of the new Council Framework Decision on data protection (2008/977/JHA) announces common standards, contributing to the efficiency of police and judicial cooperation, as well as its legitimacy and compliance with fundamental rights.

These are just examples of an elaborate framework.

The balance which is needed between information use and data protection is possibly best illustrated by the important and recent judgment in *S. and Marper v. the United Kingdom*.

In this case, the European Court of Human Rights held that the storage of fingerprint and DNA information by the authorities of the UK violates Article 8 ECHR. The system allowed the indefinite retention of fingerprint and DNA material of any person of any age accused of any - even very minor - recordable offences.

The Court also mentioned the risk of stigmatisation, stemming from the fact that certain persons that have not been convicted of any offence were treated in the same way as convicted persons.

Technology and the Commission Communication of 10 June 2009

I started with a look at the 'Stockholm-communication' of the Commission and I return to this topic to end my presentation. I will not analyse the Communication at this stage - it is new and the EDPS will deliver an opinion in the coming weeks. However, it is good to point at the directions in which the Commission is thinking at the moment.

In my view, this Communication shows a high ambition to deal with the issue of balance between surveillance and protection. It addresses technology in several manners.

1. Technological developments and better use of technological means, allowing for surveillance of the citizen.
2. Technological developments in relation to fundamental rights, in particular data protection, as a necessary condition in the Area of Justice, Freedom and Security.
3. Technology as a tool for better judicial cooperation.

The use of technological means:

- A target is: mobilising the necessary technological tools, for instance by information security, interoperability with existing and future European systems, research efforts based on real needs of users (4.1.3 of the Communication).
- The Communication aims at expanding on the European Criminal Records Information System (ECRIS), with data of third country nationals (4.2.2).
- The development of SIS II and VIS will be finalised and an electronic system for recording entry to and exit from Member

States' territory will be established alongside registered traveller programmes (4.2.3.2).

- A better approach towards cybercrime and cyber attack is announced.
- The use of the internet for terrorist purposes must be subject to greater surveillance (4.3.2).

Data protection, as a necessary condition:

- Appropriate new technologies can ensure compliance with data protection (2.3 of the Communication)
- The Union must establish a comprehensive personal data protection scheme covering all areas of EU competence.
- The introduction of a European certification scheme for 'privacy-aware' technologies, products and services must be examined. 'Privacy-aware' technologies are usually known as privacy-by-design.
- Data protection requires strong international cooperation. The Union must contribute to the development and promotion of international standards in this area.

Technology will also be used as a tool for better judicial cooperation: eJustice is presented as providing citizens with access to justice. It consists of a portal with information, videoconferences as part of the legal procedure, the possibility of on-line procedures and the interconnection of registers (3.4.1). Exchanges between professionals will take place through the Justice Forum.

I thank you for your attention and apologise that I had to limit myself and leave out the most exciting legal development for data protection in the EU: Hopefully, we can soon work under the Lisbon Treaty. This Treaty will

give us a better framework to reconcile freedom, security and justice as key values that form an integral part of the European model of society.

It is a mistake to picture privacy as a hindrance to the effective fight against terrorism, or even as the lamb to be sacrificed.

As advocated in the recent Report issued by the French Senate's Commission on Laws Report on the 3rd of June, we need to develop modern, adequate and sustainable solutions to deal with the specific challenges of our digital age.