EDPS Workshop on Video-surveillance within Community institutions and bodies

Brussels, 30 September 2009

Welcome address: Fundamental rights at stake

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor

Dear Colleagues, Ladies and Gentlemen,

It is my pleasure to welcome you at this workshop on video-surveillance within the European institutions and bodies.

Our goal here today is not only to collect constructive feedback from you, to be used to improve the draft Guidelines, but also to increase our cooperation in an area - like video-surveillance within Community institutions - which needs to be substantially revaluated in the light of data protection principles.

I will make just a few preliminary remarks on video-surveillance and its relationship with fundamental rights. We are dealing with a fast-developing area which, at first sight, might appear very technical and reserved exclusively for IT or security management. However, in reality, video-surveillance involves sensitive and strategic issues considering that a number of liberties and rights are at stake.

I am not here to celebrate the abstract value of fundamental rights compared with the needs of security and good administration. However, we cannot deal with these issues - as seems to be

the attitude reflected in certain comments received - on the basis that this is a territory in the full ownership of security and IT choices.

We all know that video-surveillance has become a popular tool to tackle security issues. It also has an increasing presence within the European Community institutions and bodies who increase their use of this technology to help ensure the security of their buildings, the safety of staff and visitors, as well as to protect property and information located on their premises.

Despite its popularity and potential benefits, however, video-surveillance also poses serious concerns as regards to privacy and other fundamental rights and freedoms such as the privacy at the workplace, the liberty of movement, the right to be free from discrimination, the freedom of expression and the freedom of peaceful assembly - rights we cherish and all too often take for granted in Europe.

For instance, one should actually argue whether the freedom of movement (which is referred to in many constitutional charters as well as in Article 2 of Additional Protocol no. 4 to the Human Rights Convention) 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".

Indeed, video-surveillance systems are fast becoming ubiquitous. They are also becoming more and more sophisticated and powerful. 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 even on the Internet with the help of today's and tomorrow's powerful digital communication networks.

The digital records holding continuous, detailed information may also be conveniently stored, searched and indexed for infinite replay and analysis. The likelihood of images being retained for further data mining is increasing due to its technical feasibility. Intelligent and interconnected systems are better and better able to match images against a database of images or track moving targets (objects or persons) in large areas.

In certain cases they are also getting increasingly good at automatically identifying pre-defined, "suspicious" behaviour. Indeed, there are areas where today or in the near future

automated, dynamic-preventive surveillance is about to replace conventional static surveillance.

The cameras themselves are also becoming more powerful and more sophisticated. Pan-tilt-and-zoom ("PTZ") cameras can pan and zoom in on their targets further and further away. Infra-red cameras, heat recognition devices and other special-use cameras can now capture images in the dark, see through walls and search under our clothing.

Surveillance specialists in digital imaging research centres around the world are continuously working on making video-surveillance more and more intelligent with the aim of achieving improved efficiency by automation.

These and other new features of video-surveillance, along with the increasing ubiquity of the technology itself, offer permanently increasing and very real 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. If the recordings are retained for a long period of time or sent to a multitude of recipients, there is an increased risk of "function creep", that is, an increased opportunity that the images may be used for purposes not initially foreseen and specified.

The risks of video-surveillance, however, go beyond the instances when actual abuse or misuse happens. One can say that being watched sometimes changes the way we behave. Indeed, when watched, most of us censor our speech and our behaviour. In case of widespread or continuous surveillance knowing that our every move and gesture is monitored by the cameras may have a psychological influence as we might need to constantly adjust our behaviour to the expectations of those who are watching us.

According to the jurisprudence of the European Court of Human Rights this constitutes an intrusion into our privacy, which should be lawful, justified and proportionate.

Furthermore, video-surveillance also has its social costs. It may not only deter criminal activities but also all other legitimate forms of non-conformist behaviour. This is an especially relevant concern at the workplace where people should have what is often called "reasonable expectation of privacy".

We must also assess the possible effects on political protests, demonstrations and other forms of protected speech held in the vicinity of the buildings of the Institutions and thus potentially in the area of coverage of their video-surveillance systems. An important assumption when exercising the right to peaceful assembly in a democratic society is the reassurance that in principle (apart from well justified derogations to be analysed case-by-case) one can take to the streets anonymously, without leaving an extensive record.

Surveillance systems may have positive effects in terms of security. However, there is no uniform agreement on whether and to which extent this effect is indeed positive. In a few cases there has been undoubtedly a decrease in the number of criminal offences in public places; in other cases this surveillance has proved ineffective, caused criminals merely to move to other nearby areas, or else it has simply allowed obtaining evidence against the persons filmed.

There are circumstances when it is legitimate and necessary to sacrifice some degree of privacy and other fundamental rights in the interest of security. However, the burden of proof must always be on those who claim that such a sacrifice is necessary. Indeed, we should not trade away fundamental rights for an illusion of greater security.

As to proportionality, one should refrain from simply laying down the principle that it is sufficient if surveillance is related to "lawful" purposes based on – often too generic – legislation which might be construed so as to include not only breaches of criminal law, but also breaches of administrative/civil/disciplinary laws and other nondescript offences. Surveillance should be focussed on areas that are really at risk, for example, public events that can reasonably be expected to give rise to incidents and more serious crimes. Otherwise, we are sleepwalking into a surveillance-society, step-by-step and without realizing the consequences: into a society where our fundamental rights and freedoms will be greatly and permanently diminished.

Additionally, it should be noted that the openness requirement is sometimes complied with merely by informing the public about the fact that cameras or other control devices have been installed and are in operation: data subjects are “compelled” to provide personal data (often consisting in images) and no information is given as to their use, even though the data or images are included in data files or are used for identification purposes. Data subjects may

thus be turned into information “subjects”, without respecting the right to information self-determination.

In conclusion, we see the need for a definitely more selective approach to 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 today and in other fora 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.