Strasbourg, 14 February 2007

CDL(2007)012

Study No. 404 / 2006

Engl. only

EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW

(VENICE COMMISSION)

SURVEILLANCE IN PUBLIC PLACES AND PROTECTION OF PERSONAL DATA

by

Mr Giovanni BUTTARELLI[1]
(Expert, Italy)

[1] Secretary General, Garante per la protezione dei dati personali.

** This document will not be distributed at the meeting. Please bring this copy.*
*** This document has been classified restricted at the date of issue. Unless theVenice Commission decides otherwise, it will be declassified a year after its issue according to the rules set up in Resolution CM/Res(2001)6 on access to Council of Europe documents.*

Distinguishing Features Compared to Other Types of Surveillance

1. Standard Human Surveillance/Observation vs. Video Surveillance[2]

In public places at large – other than places that are only open to the public – one can easily become *the focus of the attention* by the other individuals present in those places as well as being observed – at times scrutinised – in terms of one's conduct.

Several legal systems afford protection to individuals in case they are filmed and if sound and images possibly violating their dignity, modesty, honour, reputation, or their portrait, image and/or privacy rights are likely to be *circulated*, as well as if those images are or may be circulated for promotional or advertising purposes.

Whilst individuals have a *reduced privacy expectation* in public places, it may not be argued that in public places one has no reasonable expectation of respect for one's private sphere.[3]

In terms of safeguards, it is necessary to consider the difference between observing individuals at a given location by standard physical means – like security staff performing possibly continuous controls in a public place – and the audio/video recording performed with automated means even if the recorded sound and image data are not stored (e.g. in the case of CCTV, Closed Circuit Television).

The fundamental rights and freedoms of individuals deserve special attention and, if necessary, protection also if the data are not stored – whether systematically or not – at the time images and/or sound are displayed on monitors, irrespective of whether one or more operators are always and continuously in charge of those monitors.

Indeed, audio/video surveillance (hereinafter, "surveillance") brings about a certain added value to control – which produces effects on fundamental rights and freedoms and mandates a prior impact assessment.

Whenever surveillance - rather than merely control - activities are in place, the ***visibility*** of the individual as such may be different, or downright enhanced.

Thanks to the new automated techniques, in particular digital technology – and one should be capable to be forward-looking – surveillance may actually allow detecting *events, details, traits that are invisible, or not easily visible, to the naked human eye*; only think of filming systems capable to detect fake beard or whiskers. This kind of detection may be enabled from the start, because of the filming resolution and/or viewing angle, or thanks to the use of night-vision eyepieces or freeze-frame devices, or else at a later stage via the processing of filmed images – e.g. by zooming in, blowing out, scanning.

Additionally, the quality of current surveillance systems, even where no data recording is performed, is such as to *enhance the scope of vision and resolution* to an unquestionably greater degree than may ever be available to the human eye – partly thanks to the use of fixed and/or pan/tilt cameras. Finally, the possibility for the same image to be *reproduced on several monitors* that can be viewed by several individuals simultaneously increases the opportunity for

---

[2] This paper only considers the questions raised, which are addressed in a concise manner as per the relevant request.

[3] In some cases, domestic laws may prohibit filming activities in certain places, or else afford protection to natural persons by having regard to the right not to be filmed and/or observed (consider, e.g., claims against private detectives that are shadowing someone without video recording them), irrespective of whether sound and image data are captured to pursue private purposes or anyhow for no derogatory or detrimental purposes.

keeping under control events, facts, and behaviours that might otherwise escape an on-the-spot observer's attention.

Ultimately, an individual that may not be identified or identifiable directly on the basis of the images captured through surveillance might be identified more easily if those images were matched with other items of information held by the observer – whether captured on the spot (e.g. a car plate) or elsewhere.

Under another respect, *observation as such* is turned into something different - indeed it becomes qualitatively superior.

Even where no data is recorded, a single individual in charge of a monitor on which images are displayed is capable to *simultaneously control* images coming from several devices possibly placed in different locations. The opportunities for pervasive, unrelenting supervision over individuals and places are thereby enhanced.

In the case of on-the-spot controls, the monitored individuals often manage to descry the existence of those controls in real time – in some cases, they also manage to detect who is performing such controls. Conversely, CCTV equipment – regardless of the availability of an information notice – may *impair the appreciation of the controller's existence and identity*.

This accounts for the obligation to provide – as set out in many national data protection laws - (summary) information notices, possibly via ad-hoc panels. If transparency is not ensured, it is easier to carry out controls without the data subjects' being aware of them – partly because *filming cameras are easy to disguise*, either because of their very small size or because they can be inserted into other items that are standard fixtures of public places such as lamplights.

Moreover, surveillance is usually carried out in a steadier fashion compared to other controls that might be more occasional and/or irregular in nature. Surveillance allows *remote access to the data*, and in some cases the data may be disclosed directly to several individuals – e.g. if the images filmed by a webcam are disseminated on the Internet in real time.

Finally, the impact caused by a surveillance system may be considerable also under other respects. Even where no data is recorded, a "static" surveillance system can be coupled with dynamic-preventive control devices via software based on facial recognition and/or human behaviour analysis. A system might issue sound or visual alerts based on the real-time recognition of facial traits – possibly belonging to model individuals or else to specific individuals already included in the system as "data shadows" – or else of conduct that is classed as "abnormal".[4] Other systems allow starting data recording via a simple function, and this recording is both easier and of higher quality compared to the recording that can be done if necessary on the occasion of standard controls.

Thus, the electronic eye is different from the human eye, as shown by the advanced tests carried out in some European countries on *helmet cams* to be made available to law enforcement agencies.

[4] An instance of surveillance system controlling an individual's movements without recording them is represented by certain types of electronic bracelet; here, recorded alerts are sent out exclusively if certain boundaries are crossed over.

2. Personal Data Protection

Irrespective of the conclusion one may draw as to whether surveillance produces a greater or smaller impact compared to human on-the-spot controls, one should emphasize that surveillance entails, at the very least, a processing operation in respect of personal data – i.e. their *collection*.

This operation may be followed by the recording of those data and one or more additional processing operations. The data might also be collected and disseminated in real time, like in the case of webcams or the dissemination of routinely filmed images of spectators in a football stadium, without being recorded; however, these activities do impact on the rights of the persons concerned.

This is why *surveillance falls in any case within the scope of application of Convention 108/1981*, the Recommendations issued by the Council of Europe on the protection of personal data, and several domestic laws implementing, inter alia, EU directives.

The above holds true insofar as the data arising out of sound and images concerns individuals that are or can be identified by way of the connection with other information – such as spoken words, static or dynamic images, or other sound data.

To establish whether an individual is identifiable, account should be taken of *all the means that can be reasonably used by the data controllers* and/or other parties to that purpose.

Thus, the fact that a data is merely collected, for instance via CCTV, does not rule out application of the safeguards arising out of the legislation referred to above. However, one may envisage different solutions applying to the processing operations performed after data collection – providing such *solutions are justified and reasonable*.

The regulatory framework concerning data protection, which includes article 8 of the Charter of Fundamental Rights of the EU, is aimed at ensuring that data is processed by respecting not only private life, but also all fundamental rights and freedoms. In some countries, as well as in the draft European Constitution, such rights also include the "*right to the protection of personal data*" – meaning the right to respect for the rules of the game, regardless of whether a given processing operation is in breach of confidentiality.

The interests to be protected, as also pointed out in the Opinion no. 4/2004 by the Article 29 Working Party[5], include the freedom of movement of individuals – which is also safeguarded by article 2 of Additional Protocol no. 4 of the ECHR as well as by article 45 of the Charter of Fundamental Rights of the EU. Freedom of movement does not mean simply that one must be free to move in the physical space; in fact, it means that one must *be free to move without inevitably leaving continuous and/or frequent traces* of their movements for the benefit of systems enabling permanent "optical observation and/or grassing out".

This freedom is affected, for instance, by surveillance entailing control over whole urban areas.

Being seen without seeing may condition the way a person behaves and moves.

Effects may be produced on personal conduct in public places. Where a citizen is observed, or is not certain as to whether he or she is being observed, he or she may ultimately behave in a more "conformist" manner. It is by no chance that a citizen's right to raise a claim against

[5] Document WP89, no. 4/2004, adopted on 11 February 2004 (www.europa.eu.int/privacy).

allegedly non-operating cameras has been recognised, and the conditioning effects produced by a fake camera have also been highlighted.[6]

Regardless of their knowingly or intentionally getting exposed to observation, citizens become more and more the subject of observation and master their sphere of *informational self-determination* to an increasingly reduced degree.

This is why with data protection one has to carry out the prior assessment not only of ethical, political and social implications, but also of the *actual need for surveillance*.

According to data protection rules, the very installation of a surveillance system is unlawful if other types of control allow attaining the purposes to be achieved without making use of personal data.

The insufficiency and/or non-feasibility of other measures must be assessed very carefully. If traffic in certain urban areas or on certain highway segments is to be controlled remotely with a view to taking the appropriate measures, it might not be necessary to use images related to identifiable individuals. A different conclusion might be drawn if the system in question were intended to detect violations of regulations on pedestrianised and/or restricted access areas.

Once the need for this kind of information has been established, one has to address the operational issue concerning *proportionality of the processing that is performed in concrete*. The data to be processed must be relevant and not excessive to the specific case – e.g. only car plate numbers, and no images of the cockpit should be filmed; the filming arrangements must also be proportionate in terms e.g. of visual angle, zooming, etc. .

This entails the need to ensure respect for the *purpose limitation* principle, i.e. a data may only be collected if the purposes of the collection were defined in advance and such purposes are lawful, may be pursued legally by the entities seeking to achieve them[7], and have been *duly made known* to the citizens concerned (e.g. via notices sent to public authorities, or the use of ad-hoc information notices).

To conclude, and without referring specifically to other components of the data protection framework (mechanisms to exercise access rights; notification of the processing; security measures; etc.), it is hopefully understandable why national data protection authorities urge the competent institutions to look at surveillance in a *global perspective* – by avoiding the informational avidity of individual bodies, which might trivialize surveillance and thereby reduce its deterring effects, and also deprive data subjects of the safeguards they are entitled to.

---

[6] In a decision issued by the Italian data protection authority following the complaint lodged by a citizen who claimed he was being controlled by cameras, which proved to be fake upon the inspection carried out by the authority.

[7] For instance, administrative offices of local municipalities have installed surveillance systems that are useful per se; however, such systems may only be deployed by law enforcement authorities as they are meant to facilitate the detection and prevention of crime.