Humanistische Union

Consultation of the Art. 29 Data Protection Working Party on Video Surveillance

Opinion of the Working Group on Video Surveillance and Civil Rights

Experiencing video surveillance almost every day, we welcome the initiative taken by the Article 29 Data Protection Working Party to address the issue at a European level. As a network of concerned citizens and interested researchers we are grateful for the opportunity to help the efforts to develop a "general viewpoint" on how to prevent "unjustified restrictions in the citizens' rights and fundamental freedoms" in face of the rapid proliferation of CCTV, Intranet and Internet cameras that accompanies a rising culture of risk, suspicion and control.

In Germany hundreds of thousands cameras monitor every day life in a growing number of publicly accessible spaces - many of them nearly covert and without signage. Police forces in around 20 cities operate open-street CCTV systems at public areas said to be "crime hotspots".. Moreover, the police observe demonstrations and other crowds by mobile means, and covert cameras are deployed for criminal investigation purposes. There is clear trend towards interconnection of already existing camera systems. Public-private partnerships blur the line between state and corporate surveillance. Most of the recently installed systems operate on a digital basis, and first major pilot projects with automatic facial or licence plate recognition are underway at border points and airports.

In total, nearly 40 acts regulate without effectively limiting the use of video surveillance in Germany. Among others 16 state police acts, two federal police acts, the code of criminal procedure, the federal data protection act and 16 state data protection acts govern the deployment of video surveillance in different ways depending on who is the data controller and what type of monitored location. This may serve as to illustrate the difficulties of adopting a "systematic and harmonised approach".

The use of video surveillance is representing a peculiar social technique with exceptional consequences which barely seem to be met by common data protection laws. In contrast to many other forms of data processing that require the informed consent of the data subject, video surveillance allows to collect, store and process personal data covertly and without interaction between the controller and the data subject . The only way to opt out of this form of data processing is to avoid locations under surveillance. Clearly the right of the data subjects to object to being filmed as laid down in Article 14 of the Directive cannot be applied effectively. Moreover, the more or less opaque character of the collection, storage and processing of personal data by the means of video surveillance threatens to undermine the ability of the observed to make an informed and autonomous decision on the acceptance or avoidance of such data processing by video surveillance. The mere existence of a camera - even if notified - does hardly tell the relevant details. Whether it is a dummy camera, a single camera system without storage capacity, or a camera of a large and sophisticated system additionally linked to third parties remains unknown to the citizens who happen to be affected in large quantities and for no apparent reason but broadly alleged prevention purposes. Thus, we see the relation of information that the observers hold on the observed and vice versa - which in fact is an asymmetric relation of power - as crucial for the systematic assessment and regulation of video surveillance.

Having said this, we would like to point out the following issues.

- Since data controllers cannot assume informed consent of the data subjects per se the employment of video surveillance in public and publicly accessible space should only be allowed for a limited set of clearly defined purposes. Art. 6b and Art. 7 should of Directive 95/46/EC should help to prevent both the exhaustive spread of video surveillance systems and the expandable mutability that characterises their use at the moment.

- Pictures in a way seem to be more open to interpretation by the individual controller. Therefore the regulatory approach must also address problems of this "openness" coming with pictures which also seem to undermine the principle of purpose specification. In order to ensure both compliance with Art. 6b and Art. 7 and the proportionality of video surveillance which is a socio-technical rather than simply a technical device the operators of video surveillance systems, in particular control room staff, must be trained and managed in an appropriate manner. This may serve as to limit the possible discriminating use and misleading conclusions drawn from picture materials.

- The commandment of information should be enhanced as a balance weight against the asymmetric relationship of vision between the data controllers and the data subjects. In line with Art. 10 and Art. 11 data subjects should not only be informed about the operation of video surveillance, the identity of the data controller and its purpose but also about the core features of systems such as storage of footage or possible linkages to third parties.

- Given the definition of personal data as "any information relating to an identified or identifiable natural person" by Art. 2 it should be clarified if and how the oral exchange of information drawn from the processing of image data is touched by the Directive. Such practices are evident for technical and social networks of video surveillance systems and their operators for instance within police-private-partnerships. If not addressed, this problem could easily lead to an arbitrary practice of networks informally exchanging information referring to identifiable persons.. This problem in a way seem to have been met by German laws through specific data controller obligations of keeping gathered knowledge on single persons secret.

- Finally, we wish to address the following issues going beyond the scope of the Directive but which, however, are closely related to it.

- Privatisation and securitisation are not just catchword. Although the Directive does not apply to video surveillance carried out by public crime control and national security authorities, we observe - as mentioned above - that the lines between the work and the specific tasks of these public bodies and other private data controllers where the Directive is wholly applicable are increasingly blurring. Thus, these hybrid areas of surveillance activities need increased attention and eventually regulation. We expect the Working party therefore to promote an understanding of the Data Protection Directive which strengthens its decisive meaning and impact as the common aquis also within the remaining third and second pillar of the European Union. The current discussion of a growing "European space of freedom, security and rule of law" (Constitutional Convention draft papers) should consequently be enriched by stressing the legal achievements of the EU in its first pillar activities.

- To support the assessment of the proportionality of video surveillance in general and the deployment of advanced applications in particular, professional but independent evaluations of their effectiveness in terms of declared purposes and other possible impacts and consequences, especially with respect to the basic prerequisites of open and democratic societies are necessary.

- Last but not least, the wide gap between the provisions of the Directive and the current reality in the practices and use of video surveillance show that the Directive is an important but rather weak

framework if not completed by an efficient regime of control and penalties.

Signatories for the Working Group

1. Ralf Bendrath

   Political scientist, University of Bremen

2. Peter Bittner

   Computer professional, Vice Chairman Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.

3. Dr. Thilo Weichert

   Lawyer, as Chairman on behalf of Deutsche Vereinigung für Datenschutz e.V.

4. Leon Hempel

   Research assistant, Technical University Berlin

5. Francisco Klauser

   Geographer, University of Fribourg, Switzerland

6. Nils Leopold

   Lawyer, Managing Director Humanistische Union e.V.

7. Dr. Helmut Pollähne

   Lawyer, University of Bremen

8. Eric Töpfer

   Political scientist, Technical University Berlin

9. Prof. Dr. Uwe-Jens Walter

   Sociologist, Technical University Berlin
