ARTICLE 29 Data Protection Working Party

00039/07/EN
WP129

Opinion 1/2007 on the Green Paper on Detection Technologies in the Work of Law Enforcement, Customs and other Security Authorities

Adopted on 9 January 2007

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS
WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 (1)(a) and (3) of that Directive and 15(3) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002,

having regard to its Rules of Procedure, and in particular Articles 12 and 14 thereof,

has adopted the following Opinion:

1. Background

The European Commission has adopted its Green Paper on Detection Technologies in the Work of Law Enforcement, Customs and Other Security Authorities (COM (2006) 474) on 1 September 2006 (the "Green Paper").

The aim of the Green Paper is to stimulate the discussion in the area of detection technologies at the European level and gather *"thought-provoking answers and concrete suggestions"* towards *"strengthening the common approach towards detection technologies"* to be construed in the *"broadest sense"*. The Article 29 Working Party, along with other parties, was invited to participate in the consultation process.

The replies to the questions raised in the Green Paper as well as other comments made will determine concrete steps and actions that could be subsequently taken. Furthermore, depending on priorities identified in the course of the public consultation, specific steps could be taken as soon as possible. If stakeholders show their interest, a task force delivering actions on specific subjects could be created. Such a task force could consist of representatives from various Members States authorities and experts from the private sector.

The Article 29 Working Party welcomes the fact that the Commission in its Green Paper has taken into account that policies relating to detection and associated technologies have to comply in full with the existing legal framework, including data protection principles and wishes to contribute to the discussion on the Green Paper as follows.

2. General comments

The Article 29 Working Party finds it extremely difficult to make detailed comments and offer more detailed observations at this point, as the issues outlined in the Green Paper are at a very general level. It would be preferable and more useful to be invited to comment at a later stage in greater detail, e. g. when draft versions of the studies proposed in the Green Paper become available and concrete steps will be known.

Nevertheless, the Article 29 Working Party supports the idea of facilitating a dialogue between government agencies and industry with respect to legal requirements and especially to data protection aspects, and, more specifically, to take into account right from the beginning the minimisation of the processing of personal data when planning and developing respective applications of detection systems[1].

The Working Party notes that the development of detection technologies provides the means of developing surveillance, and surveillance on an unprecedented scale. In this respect, the Working Party deems it timely to recall that the "surveillance society" was the theme of the International Conference of Data Protection and Privacy Commissioners[2], where the surveillance issue was largely discussed from privacy and data protection perspective. The Working Party wants to quote a part of the communiqué adopted at the close of the conference as it represents the major concerns:

"Surveillance activities can be well-intentioned and bring benefits. So far the expansion of these activities has developed in relatively benign and piecemeal ways in democratic societies - not because governments or businesses necessarily wish to intrude into the lives of individuals in an unwarranted way. Some of these activities are necessary or desirable in principle - for example, to fight terrorism and serious crime, to improve entitlement and access to public services, and to improve healthcare. But unseen, uncontrolled or excessive surveillance activities also pose risks that go much further than just affecting privacy. They can foster a climate of suspicion and undermine trust. The collection and use of vast amounts of personal information by public and private organisations leads to decisions which directly influence peoples' lives. By classifying and profiling automatically or arbitrarily, they can stigmatise in ways which create risks for individuals and affect their access to services. There is particularly an increasing risk of social exclusion."

In the context of analysing the Green Paper, the Working Party wishes to express its concern that the definition of detection technologies in the Green Paper is very wide-ranging, while this is a sector where precision and specification play a key role. However, this is probably due, at least in part, to the structure of the Green Paper as such. In this same general perspective, it should probably be re-affirmed from the onset that not everything that is technically feasible is also socially and politically acceptable, ethically admissible and legally allowable.

Therefore, further discussions and works on the detection technologies should include and take into consideration all necessary privacy and data protection rules and guarantees provided for by the European data protection legislation, such as the Council's of Europe European Convention for Human Rights and Fundamental freedoms[3] and the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108), the Data protection directive and the ePrivacy directive.

---

[1] See a Closing communiqué from the 28th International Conference on Data Protection and Privacy Commissioners, 2-3 November 2006, London, United Kingdom: http://ico.crl.uk.com/files/FinalConf.pdf "*A systematic use of impact assessments should be adopted. Such assessments would include but be wider than privacy impact assessments, identifying social impact and opportunities for minimising undesirable consequences for individuals and society.*

[2] The 28th International Conference on Data Protection and Privacy Commissioners, 2-3 November 2006, London, United Kingdom: http://ico.crl.uk.com

[3] It should also be pointed out that Council of Europe's Convention on Human Rights is applicable in this context, and its principles have been specified further in Recommendation R(87)15 on the processing of personal data for police purposes. In particular, Article 1(2) of the mentioned Recommendation provides that "*new technical means for data processing may only be introduced if all reasonable measures have been taken to ensure that their use complies with the spirit of existing data protection legislation"* as well as envisaging the possibility of prior checking by the supervisory authority.

In the opinion of the Article 29 Working Party, it is also crucial for further evaluation to clearly distinguish different types of detection technologies (i.e. CCTV, RFID tags, biometrics, etc.) in order to match appropriate data protection solutions to each of them separately. Moreover, a clear determination of the purposes of data processing (collecting, capture, storage and retention, recording and further use, etc.) is the key issue while establishing such surveillance systems and related data processing rules. Then, it will allow data protection authorities to determine whether the collected data are adequate, relevant and not excessive in relation to those purposes. Such analysis is necessary in order to check whether detection technologies in a particular situation are not privacy intrusive or whether intended purposes could have been achieved by other, less invasive means.

3. Specific Comments related to various chapters

Introduction

The Article 29 Working Party especially welcomes the reference (p. 5 and 6) to the need that *"the design, manufacture and use of detection technologies and associated technologies, together with legislation or other measures aiming to regulate or promote them, must fully comply with fundamental rights as provided for in the EU Charter of Fundamental Rights and the European Conventions on Human Rights"* and that *"particular attention must be paid to compliance with the protection of personal data and the right to private life"*. This statement is the appropriate starting point for contributions from the Article 29 Working Party. A reference can be made, in this connection, to the various documents adopted by the Working Party, highlighting that any public measure imposing limitations on fundamental rights must be expressly set out in a law and must be necessary, in a democratic society, to protect a substantial public interest (see, in particular, the WP's Opinion 10/2001 on the need for a balanced approach in the fight against terrorism[4]).

The Working Party also underlines the obligation to respect the principle of proportionality in relation to any measure restricting the fundamental right to privacy as required by Article 8 of the Convention on Human Rights and the relevant case-law. This implies inter alia, the obligation to demonstrate that any measure taken corresponds to an "imperative social need". Measures which are simply "useful" or "wished" may not restrict the fundamental rights and freedoms.

However, recognising this entails several consequences that would not appear to have been taken fully into account while drafting the Green Paper, especially with regards to the list of proposals/questions. This applies, in particular, to the need for ensuring that the project-designing phase of any detection tool incorporates data protection principles, with due regard to the specific purposes for which a given tool is to be used.

An additional consideration is related to the equation that is seemingly made in the document between "terrorism" and "other forms of crime" (see p. 4 and elsewhere). The Article 29 Working Party wishes to underline that the concept of terrorism should be defined very clearly and, in any case, the two concepts should be kept separate as they have to do with different requirements also in terms of security and detection technology and the relevant research efforts.

Having said this, the suggestions and remarks below focus on issues that are especially relevant from a privacy and data protection-oriented perspective:

[4] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp53en.pdf

I. Standardisation and Security Research

The Article 29 Working Party considers that in developing technical standards ensuring that personal data processing complies with applicable laws should be paramount in terms of research and subsequent studies. This is an area where the active co-operation of data protection authorities could and should be sought. Furthermore, the Working Party wishes to emphasise that compliance with the data minimization principle is fundamental to that end. Solutions should be sought that would require the processing of as little personal data as possible. Whenever feasible, technologies that would reach a desired goal even without the processing of any personal data at all should be preferred. This should be included as a key requirement into any future research and development activity in the field of detection technologies. Minimization of the processing of personal data should also be part of the exploration of best practices as set out in part III.1. of the Green Paper.

Concerning a security research, the ESRAB report mentioned in the Green Paper provides interesting clues on future research in this sector. The Article 29 Working Party is of the opinion that it is significant that one of the key findings of the report is that *"respect for privacy and civil liberties should be the programme's guiding principle"* and fully supports this statement.

The Article 29 Working Party would certainly be interested in *"identifying and exchanging best practices in the use and handling of data and information…to comply in full with the relevant legislation and rules"*. It has to be pointed out that, in this connection, the rules established at both the European level as well as at national level will have to be taken into account.

II. Needs and Solutions

Technological Needs and Solutions

It should be clarified how the mentioned Europe-wide searchable list/database containing specific areas of needs and solutions offered by the private sector is going to work. The Working Party wants to underline that proper safeguards must be in place to ensure that any decisions on inclusion of the available solutions are made in a fully transparent manner.

Portable and mobile solutions/Interoperability of systems

The Article 29 Working Party is very much in favour of contributing to clarification of what is meant by the Commission in referring to "legal and other constraints" for interoperability of systems across the EU. The Working Party shares the considerations made by the EDPS in his comments[5] on the Commission's Communication on interoperability of European databases – namely, that interoperability has significant legal implications, since *"it is obvious that making access to or exchange of data technically feasible becomes, in many cases, a powerful drive for de facto acceding or exchanging these data"*; that *"different kinds of interoperability (common use of large scale IT systems, merging databases, expand possibilities of accessing or exchanging data…) require different safeguards and conditions"*; and that *"interoperability of systems must be implemented with due respect for data protection principles and in particular the purpose limitation principle"*. However, this is not to be perceived as a "constraint" but rather as the sensible way for dealing in advance with fundamental issues.

The Working Party wishes to be involved in any related initiatives at EU level.

[5] http://www.edps.europa.eu/legislation/Comments/06-03-10_Comments_interoperability_EN.pdf

Integration of information and improved data analysis

It should be clarified that improved data analysis should not mean unrestricted data matching and navigation among different databases. Data minimisation and purpose specification should be built into data analysis systems (as "a priori" conditions for integrating information). The Working Party wants to refer to activities and guidelines developed in connection with Europol's analysis files as a possible model for ensuring compliance with data protection principles in this area.

III. Use and Certification of Equipment and Tools

Use of data- and text-mining tools

The Article 29 Working Party strongly supports the emphasis on compliance with fundamental rights and data protection principles, in particular the need for such compliance to be "built-in" detection tools.

Whilst the Working Party might support the "sharing of best practices" and information on the use of data and text-mining tools, it is of the opinion that the reference to *"pare capacity available in Member States and European bodies to help Member States that do not possess this technology to work on their documents"* is to be further clarified. It should be clearly pointed out, in this regard, that any use of the tools in question must be grounded on the appropriate legal basis. Clarification is also needed as to the meaning of a *"European or regional centre for data and text mining"*, which should not consist merely in a sort of "clearinghouse" of techniques for data extraction.

The Article 29 Working Party regrets that no reference is made to the need for including data protection compliance in the best practices for data and text mining, except for mere sharing of best practices and information. The Working Party is of the opinion that any such best practices should among other safeguards include mandatory training in data protection for involved parties.

An assessment of the potential contribution of the data mining tool on the fight against terrorism will be useful as this tool might not be the only one targeted for such a threat. Other tools with less privacy invasive impact shall always be given priority over tools using a huge amount of personal data.

As far as the confidentiality of communication is concerned, the Article 29 Working Party wishes to recall the application of the ePrivacy directive. Furthermore, Working Party's Opinion 2/2006 on privacy issues related to the provision of email screening services[6] and the case law of the European Court of Human Rights related to the interception of (tele)communication[7]

The Working Party also wants to recall its Opinion 3/99[8] on Public sector information and the protection of personal data Contribution to the consultation initiated by the European Commission in its Green Paper entitled "Public sector information: a key resource for Europe" COM (1998) 585, where it stated that *"The computerisation of data and the possibility of carrying out full-text searches creates an unlimited number of ways of querying and sorting information, with Internet dissemination increasing the risk of collection for improper purposes. Furthermore, computerisation has made it much easier to combine publicly available data from different sources,*

[6] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp118_en.pdf

[7] e.g. ECHR, *Klass v. Germany*, 6 September 1978, ECHR, *Malone v. France*, 2 August 1984, *Kruslin v. France*, 24 April 1990, *Huvig v. France*, 24 April 1990, *A v. France*, 23 November 1993, *Halford v. United Kingdom*, 25 June 1997, *Kopp v. Switzerland*, 25 March 1998, *Amann c. Switzerland*, 16 February 2000

[8] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1999/wp20en.pdf

so that a profile of the situation or behaviour of individuals can be obtained. In addition, particular attention should be paid to the fact that making personal data available to the public serves to fuel the new techniques of data warehousing and data mining. Using these techniques, data can be collected without any advance specification of the purpose, and it is only at the stage of actual usage that the various purposes are defined. So all of the technological possibilities with regard to data usage need to be considered".

Testing and certifying the quality of equipment and tools
It might be argued that the "network of national certifying authorities" could be a workable solution; however it should involve data protection authorities and experts in the field as well.

IV. Studies

The suggested lines of action can be shared; however, a privacy impact assessment should also be carried out in respect of any detection technology that is developed in order to evaluate its necessity and have a clear-cut idea of its impact in terms of costs, both societal and financial.

In the context of data protection, the Working Party agrees that some of the studies identified in section IV (3) legal provisions regulating the use of specific detection technology; (4) practical use of specific detection technology; (5) legal framework governing the use of personal detection (including surveillance) across the EU, and (6) levels of acceptance of personal detection (including surveillance and use of biometrics) across the EU – would be useful and very welcome.

V. Implementation of Results of Consultation

The Article 29 Working Party is of the opinion that it would be important to contribute to the follow-up work related to the consultation. An action plan could be therefore helpful in this regard.

4. Conclusion

The Article 29 Working Party welcomed the opportunity to be invited to comment on the Green Paper on Detection Technologies and be involved in the consultation process. However as the Green Paper is couched in rather vague terms, talking very broadly about "detection technologies" in general, it is, at this stage, very difficult to provide deep legal analysis on detection technologies from privacy and data protection point of view.

While the formulation of best practices can be helpful in providing a bridge between legislation such as Data protection and ePrivacy directives and the application of technology, best practices can only be considered in the light of fairly concrete examples, where the particular consequences of using a particular technology can be examined. It is worth noting, however, that wherever detection technologies involve the collection or processing of personal data *("any information relating to an identified or identifiable natural person"*) and insofar as their use is governed by Community law, it will be regulated by the Data protection directive.

In order to sum up, several basic principles can be identified from the Directive:

(i) The purpose of collecting personal data should be carefully specified at the outset, and the data should not be processed further in a way that is incompatible with that purpose;

(ii) Technologies in themselves do not necessarily present a problem but the collection and use of personal data must be fair. This means that people should be made aware of their operation (for example, in the already well-established case of closed circuit television surveillance), of the data that is collected and of its use;

(iii) No personal data that is irrelevant to the purpose for which it is needed should be collected, and personal data should not be retained for longer than it is needed; more importance than hitherto should be attached to the development of technologies which detect materials rather than persons.

The Working Party reserves the possibility to comment on further work in this field as it evolves.

For the Working Party
The Chairman
Peter Schaar