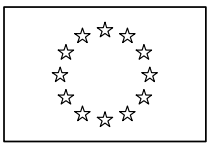

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 1.9.2006
COM(2006) 474 final

GREEN PAPER

on detection technologies in the work of law enforcement, customs and other security authorities

(presented by the Commission)

TABLE OF CONTENTS

GREEN PAPER

on detection technologies in the work of law enforcement, customs and other security authorities

(Text with EEA relevance)

INTRODUCTION

Security is a cornerstone of Commission policy. Combating crime and terrorism is a crucial dimension of security policy. The Commission set out its counter-terrorism policy in its "*Communication on Prevention, preparedness and response to terrorist attacks" of October 2004*. This Communication highlights *Public-Private Security Dialogue* as a tool for private and public sectors to engage in a meaningful dialogue on Europe's security needs. *The Hague Programme: strengthening freedom, security and justice in the European Union* adopted by the European Council in November 2004, which constitutes at present the political programme of the Union on Justice and Home Affairs, also highlights the importance of public-private interaction in the fight against organised crime and terrorism. This Green Paper aims to provide the ingredients for initiating such dialogue within the field of detection technologies.

Detection technologies are increasingly used in the daily work of security authorities to fight terrorism and other forms of crime. Detection technologies are widely used to protect passengers when boarding aeroplanes and sports fans when watching their favourite sports events, and to detect dangerous substances in the air, water or food. Security authorities also use these technologies to protect our borders and check goods entering the territory of the European Union. Moreover, detection technologies are essential for guarding private property and critical infrastructure. This Green Paper aims to find out what role the Union could play in order to foster detection technologies in the service of the security of its citizens. On the other hand, detection technologies are inherently intrusive into privacy or can pose a challenge to freedoms and rights. Therefore, each time when considering improvement and use of detection technologies, this aspect and the fundamental question of what the limitations of their intrusiveness should be, will have to be carefully analysed. The Commission intends to contribute to both issues with this initiative.

The Commission organised a conference[1] – *Public-Private Security Dialogue: Detection Technologies and Associated Technologies in the Fight against Terrorism* – in Brussels on 28-29 November 2005. The participation of over a hundred representatives both from major European business and industry associations and from the public sector attested to the interest of stakeholders in pursuing a policy in this area. The public sector was represented by members of law enforcement, customs and other security authorities.

The role of Europe, in areas such as security research or standardisation, is clearly established. Although considerable work has been achieved in certain areas in close cooperation with the

[1] For further background information, see part I of the Annex.

Member States, industry and other interested parties, there is still room for an enhanced European policy on detection technologies as such. With respect to aviation security, both Regulations (EC) No 2320/2002 and No 622/2003[2] contain detailed requirements as regards the performance of the screening equipment to be used and the methodology. In this field, standards and test protocols have been established in close cooperation with the European Civil Aviation Conference, which regroups experts from the appropriate authorities of the Member States and other European States. In addition, the Commission is regularly in close contact with the industry and other stake holders concerned (Stakeholders Advisory Group on Aviation Security – SAGAS Group).

In view of strengthening the common approach towards detection technologies the Commission took this initiative to further enhance interaction between public and private sectors in an effort to focus investment on standardisation, research, certification and interoperability of detection systems and to transform research results into useful and applicable tools. A virtuous circle has to be established in which the private sector is guided in its research effort and expenditure by a public sector that knows what it wants and what the private sector can offer. This should help to develop an advanced market in detection products and security solutions, which in turn should lead to greater availability of products and services at lower cost.

Common action and better coordination and information exchange between everyone involved in Europe are essential if this aim is to be reached. Needs have to be defined better and both technologically and economically viable solutions brought to the surface. This Green Paper certainly does **not aim to overlap with other activities either at national or European level**. The Commission does not wish to reinvent the wheel but to find out more about existing good approaches and practices, and to support them and spread them across the Union.

The Commission is keen for this Green Paper to generate as many thought-provoking answers and concrete suggestions on steps ahead as possible. **Extensive participation by Member States, the private sector and other relevant stakeholders is therefore indispensable**. The Commission is, however, aware of confidentiality requirements in both the public and the private sectors, both for security and for commercial reasons. Therefore, respondents are asked to indicate any answers that are too sensitive to be shared and to suggest an alternative approach to take account of such concerns.

Policies relating to detection and associated technologies have to comply in full with the existing legal framework, including the EU Charter of Fundamental Rights, the European Convention on Human Rights and data protection principles and rules as laid down in Directive 95/46/EC. In this context, the Commission stresses 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 Convention on Human Rights. Particular attention must be paid to compliance with the protection of personal data and the right to private life. Indeed, as the use of detection technologies will usually mean an intrusion of the fundamental rights to private life and protection of personal data, any

[2] Regulation (EC) No 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security, O.J. L355 of 30.12.2002, p. 1 and Commission Regulation (EC) No 622/2003 of 4 April 2003 laying down measures for the implementation of the common basic standards on aviation security, O.J. L89 of 5.4.2003, p. 9

intrusion of fundamental rights has to be in compliance with the European Convention on Fundamental Rights; in particular, it must be in accordance with the law and necessary in a democratic society to protect an important public interest and must be in proportion to the public interest pursued.

I. STANDARDISATION AND SECURITY RESEARCH

1. STANDARDISATION

An enormous range of technological possibilities exists in areas concerning detection and associated technologies and the work of the security authorities. Therefore, minimum standards are required. However, given this range the process of standardisation must be prioritised, which is only possible if there is sufficient interaction between the public sector (needs) and the private sector (solutions). At European level, this interaction is considered to be insufficient by both public and private sectors. Furthermore, numerous positive activities are developing at both national and European levels. However, a general overview of what is happening is missing, and this is needed to avoid duplication and improve prioritisation. It is evident, that for security reasons, the development of standards cannot be openly discussed. The discussion will therefore concentrate mainly on the question to which extent common standards may be desirable.

The use and handling of data and information collected by detection tools, for example as evidence in court proceedings, are also closely related to standardisation. The relevant authorities could benefit from identification and exchange of best practice on the subject. Creating technical standards to ensure that the data collected complies with the requirements of law for the use of such data in court proceedings should also be considered.[3]

Questions

Are common standards needed in detection and related technologies used in the work of security authorities? What standards do you consider to be a priority?

What standards lack financial support in the pre-standardisation phase?

To avoid any duplication and to improve transparency, would a regularly updated list/handbook/searchable database of past, ongoing and planned standardisation efforts in detection and closely related technological fields at national and European level be useful?

Would you be interested in identifying and exchanging best practice in the use and handling of data and information collected by detection tools in an effort to comply in full with the relevant legislation and rules governing the use of evidence in court proceedings?

What would be the best way of identifying and exchanging these practices?

2. SECURITY RESEARCH

Security research is another area which is essential for the development of new security solutions and products for the Member States' security authorities. In this context, the role of the European Security Research Advisory Board (ESRAB) must be highlighted. The ESRAB adopts a global and broad perspective in this area and advises the Commission on the content

[3] For the legal provisions governing the exchange of personal data, see part II of the Annex.

and implementation of the research to be performed, together with mechanisms to monitor relevant developments in other programmes.

A number of security research activities are ongoing at European level and in the Member States. However, there is no mechanism for aggregating and disseminating information on previous, current and proposed security research at European, national and ultimately private sector level. Such a mechanism could ensure that scarce resources are not wasted on duplication and overlapping projects. Furthermore, if considered necessary, a separate mechanism for disseminating classified security research activities could be designed, ensuring that only those who are entitled to access the information can do so.

After more than a year of work, ESRAB is finalising its report which will be published in September 2006. The report identifies around 120 security capabilities and 100 key technologies which need further research and development at EU level, while a series of other technologies are or will be dealt with at national level.

Questions

How should information on security research in Europe be disseminated in order to promote competitiveness while avoiding waste of scarce resources?

II. NEEDS AND SOLUTIONS

1. TECHNOLOGICAL NEEDS AND SOLUTIONS

Good, effective and usable solutions and products can be developed only if the producers of these solutions and products have sufficient information regarding the real needs of the end-users. However, at European level there seems to be a need for better interaction between those who need technological solutions (i.e. the relevant security authorities) and those offering them. Any such interaction should also attempt to identify what the short-, medium- and long-term needs are. On the other hand, those providing solutions should also indicate the timescale for when the solutions will be available.

Furthermore, in the dialogue between producers and users more fundamental questions relating to the nature of our societies and the role of the detection technologies should be asked and addressed. Such a debate is also important in the view of preserving the values and nature of our societies.

Questions

Are you interested in a broader debate on the role of detection technologies and the influence their use potentially has on European societies?

In what specific areas do the relevant security authorities require technological improvements? Please specify the level of priority in relation to specific needs?

Is there a gap between requirements for detection capabilities and the technology currently on offer on the market? What are possible solutions to these gaps?

In what specific areas does the private sector already offer, or plan to offer technological solutions? Please state the timescale for when such solutions would be available, and cost-effective?

Would it be helpful and useful to create a Europe-wide searchable list/database containing specific areas of needs of the relevant security authorities, and at the same time solutions offered by the private sector?

If not, what other solutions would you propose in order to improve the information flow between those who need technological solutions and those who offer them?

1.1 Versatile solutions

Today's threats, from crime or terrorism, are diverse, constantly changing and present in different forms and at different levels in different situations. Therefore they require different levels of protection and response at different times, i.e. versatile solutions.

Question

For what existing tools and equipment could the applicability and effectiveness be improved by enhancing their versatility?

What new versatile tools and equipment are needed?

1.2 Portable and mobile solutions

The nature of the threat from terrorism and crime is not only changing with time, it is also becoming increasingly mobile. Hence, security authorities require portable solutions. Such solutions can improve cost-effectiveness and be readily transferred from one location to another where they are most needed, as it is simply not feasible to cover every entry point or point of concern with the same level of security. Furthermore, portable and mobile solutions may offer new operational approaches.

Question

What existing tools and equipment could be better and more effectively used in the work of the relevant security authorities if they were mobile and portable?

What new portable and mobile tools and equipment are needed?

2. INTEROPERABILITY OF SYSTEMS[4]

The EU Member States and their relevant authorities already have a number of systems to help in the fight against crime and terrorism. However, these systems are often not able to communicate with each other. This may impede the common efforts in the fight against crime and terrorism at national and European levels. On the other hand, systems need to comply with existing legal frameworks and other guidelines (e.g. data protection, intrusiveness of detection systems).

Question

What systems need improved interoperability?

Would a study on legal and other constraints for interoperability of systems across the EU be useful to identify limitations?

3. INTEGRATION OF INFORMATION FROM DIFFERENT DETECTION TECHNOLOGIES AND IMPROVED DATA ANALYSIS

The integration of data from different detection technologies into a single data analysis system may make detection systems more effective. Any measure adopted in this respect has to comply with data protection rules.

[4] Systems other than information systems should also be considered.

Question

In what areas do you believe that the integration of information from different detection technologies would improve overall performance?

In what areas are improved data analysis techniques required?

III. USE AND CERTIFICATION OF EQUIPMENT AND TOOLS

1. BEST PRACTICE AND THE USE OF EXISTING TOOLS AND EQUIPMENT

Completely new technological solutions are not always required to deal with existing or new threats in an efficient manner. Public budgets often cannot afford them. Hence, attention should also be paid to how existing and previously purchased tools can be put to more efficient use or upgraded. This can be a cost effective way to improve effectiveness, increase reliability and reduce the number of false alarms.

A mechanism for sharing experience on such issues among the authorities in different Member States is lacking. For example, information could be shared about improvements obtained through changes in operating procedure or cost-effective upgrades.

Questions

What would be the best way of identifying and sharing best practice in this field?

Identification of best practice

Would it be through peer evaluation or questionnaires sent to the Member States?

Dissemination of best practice

Would it be through a secure and searchable database or through meetings and seminars?

Can you suggest any other options on how best to identify and disseminate best practice in this field?

If an upgrade of a tool or equipment was considered necessary and no authority in other Member States would have performed such an upgrade, would consultation with the private sector on the subject be acceptable?

2. IDENTIFICATION AND DISSEMINATION OF BEST PRACTICE AND THE USE OF NEW TOOLS AND EQUIPMENT

National authorities can also benefit in their work from a system which would facilitate the exchange of information on the use of new tools and equipment, and enable them to learn from each other and build on the experience of others. Such exchanges of information, experience and best practice on tools and equipment could help the authorities to identify equipment to address their particular needs.

In addition to this, the trial of new or experimental equipment could be promoted through co-financing from the Community budget and/or by the private sector. Wider testing of new and experimental equipment could help European industry to transform security research into effective and competitive products.

Questions

What would be the best way of identifying and sharing information and best practice in this field?

Identification of best practice

Would it be through peer evaluation or questionnaires sent to the Member States?

Dissemination of information and best practice

Would it be through a secure and searchable database or through restricted meetings and seminars?

Have you any other suggestions for how to identify best practice in this field and disseminate them effectively?

Experimental and new tools

Are you interested in the trial of new or experimental tools and equipment?

If yes/no, please explain

Would partial financing of trials of new or experimental tools and equipment by the Community and/or the private sector be of interest?

3. USE OF DATA- AND TEXT-MINING TOOLS

National and European security authorities are facing a constant increase in the volume of documentation and information they have to process. To address this challenge more efficiently, modern software tools for data and text mining exist. This technology can help to extract relevant information from huge numbers of documents. For example it is possible to intelligently filter text and documents to aid navigation (clustering of documents), for auto-categorisation (channelling and prioritising document flow within investigation teams) and code utilisation validity checking. The objectives are:

- fast overview of key entities in document collections;
- pre-processing for targeted document search;
- content-based classification of documents to help focus further analyses;
- automated information analysis across various sources.

The potential of these modern tools is not sufficiently exploited across the Member States. However, while promoting use of these technologies, it has to be very carefully considered that their use in certain applications, for example monitoring of e-mails, is in itself an intrusion of citizens' fundamental right to privacy. E-mails are correspondence and, as such, they are covered by the right to confidentiality of communication laid down in the European Convention on Human Rights. The use of any techniques for data and text mining must therefore be in accordance with the law, be necessary in a democratic society to protect an

important public interest and be proportionate to the public interest pursued. Support for compliance with fundamental rights and data protection principles should be inherent in such tools and their use. Finally, these activities will be carried out under the control and supervision of relevant public authorities.

Questions

Awareness raising exercise

Would Member States and the relevant European bodies be interested in sharing best practice and in the potential benefits arising from the use of data- and text-mining tools?

Would Member States authorities using this technology be willing to share experience with their peers?

Would restricted seminars on the subject organised by the Member States, Europol or OLAF be useful?

Enhancement of the EU capacity for data and text mining

Would a centre of excellence at European level accessible to all Member States and their relevant authorities help to tap the potential of these tools in practice?

If not, what other options would you suggest to maximise the potential of these tools?

Identification and dissemination of best practice

Would a peer evaluation or a questionnaire sent to the Member States be useful in identifying best practice in the use of these tools?

If not, what other approaches would you suggest to identify best practice in this area?

Enhancement of the regional capacity for data and text mining

Would there be any spare capacity available in Member States and European bodies to help Member States that do not possess this technology to work on their documents?

If there were no such spare capacity or only a limited capacity, would an EU-funded increase of capacity in Member States or at the European level be useful and practical?

Would Member States that lack sufficient data and text-mining capacity consider using the tools of other bodies, if made available?

Would it be possible to create European or regional centres for data and text mining which several Member States and their authorities could use for data and text mining?

Do existing data and text mining tools sufficiently deal with the various languages within Europe?

Are there adequate tools to support authorities dealing with foreign language text and documents?

Other

If you disagree with any of the options suggested above, how would you address the concerns raised by this point?

5. TESTING AND CERTIFYING THE QUALITY OF EQUIPMENT AND TOOLS

The market already offers a number of detection products. However, very often it is difficult to identify what tools and products are the best or at least meet certain minimum requirements. An EU-wide system of certifying good quality tools and benchmarking them, designed to simplify the process of establishing which of the tools or equipment can meet the particular needs of a particular authority, could address this deficit. This may make it easier for national authorities to decide what equipment and tools to purchase. It might also help authorities to make optimum use of scarce resources.

A network of *national* certifying authorities sharing experience and knowledge could be established to address this lack of a system determining the quality of tools. These authorities would also agree on standards for benchmarking and certifying good quality technological solutions. This type of certification could not only be used to help national authorities to determine whether a tool is good or not, but also to advertise European solutions in other markets. It is evident, that for security reasons, the development of test protocols cannot be openly discussed.

Question

Would creating a network of national certifying authorities sharing experience and knowledge, along with a system of quality certification and benchmarking, be useful?

If not, what other solution would you suggest to address the problem raised?

Would common standards for certifying and benchmarking be helpful?

If not, how would you ensure transparency of this process and usability of the results across the EU?

IV. STUDIES[5]

The participants at the conference identified several topics which require further studies. Hence, the Commission proposes to conduct studies on:

(1) technology and the protection of mass events;

(2) obstacles to cooperation and information-sharing among forensic laboratories and security research institutes;

(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;

(6) levels of acceptance of personal detection (including surveillance and use of biometrics) across the EU.

In general, the aim of the studies is to use them as an instrument to enhance the knowledge of the relevant stakeholders and to ensure compliance with the existing legal frameworks when preparing or using detection technologies. In other cases, the studies could be used to consider policy options and options for further practical steps.

Question

Would you be interested in receiving studies on these topics based on the background information outlined in the Annex?

If not, please specify reasons and suggest alternatives of how to address the concerns raised.

[5] For a further description of the ideas behind the need for these studies, see part III of the Annex.

V. IMPLEMENTATION OF RESULTS OF CONSULTATION

1. ENHANCED SPECIFIC PUBLIC PRIVATE DIALOGUE ON DETECTION AND ASSOCIATED TECHNOLOGIES

This Green Paper reflects a number of possible activities which can help to improve public-private interaction in the field of detection technologies, and thus help security authorities of the Member States to have access to the best available tools, solutions and best practice. On the other hand, these activities can help the private sector to focus its investment and match the needs of the public sector. It is obvious, however, that this requires intensive cooperation between public and private sectors. Hence, there is a need for an enhanced specific public private dialogue in this area. This could be done in different ways, inter alia, through the establishment of a specific body or the setting up of a specific group in the framework of horizontal public private partnership exercises related to security which should be launched in the close future.

The aim of this activity would not be to compete with existing bodies, but rather to address gaps in the interaction between public and private sectors involving the relevant security authorities at European level. Nor should it be a permanent body; it would have clearly defined objectives but when these are achieved it would cease to exist. It would serve as a forum for experts from both public and private sectors, helping to address the issues raised in this document or new challenges which may surface in the course of the implementation of results from the public consultation on this document.

On the other hand, it is clear that a number of possible actions proposed in this document would require activity on the part of the Member States without the involvement of the private sector. Moreover, the definition of the tasks of such cooperation would be subject to agreement between both public and private sectors, and thus through their membership Member States would be able to influence its role and focus. It would also have to address the issue of sharing confidential information between public and private sectors, although it should be underlined that the public sector is not the sole repository of sensitive information.

Question

Would a tool such as an enhanced specific public private dialogue on detection and associated technologies be helpful in implementing the results of the public consultation on this paper?

If yes, would you agree with the above suggestions or do you have different ideas?

If not, what other mechanisms would you suggest to follow up the results of the public consultation of this document?

Would you be interested in contributing to its work or directly participating in it?

2. ACTION PLAN

At national and European level action plans have proved to be a successful tool for overseeing action in complex areas such as the fight against terrorism or crime. Both the conference and this document have raised numerous questions in relation to detection and related technologies in the work of the relevant security authorities. To monitor progress in this field, and to set objectives, an Action Plan based on the replies to these questions and, if necessary, on further consultations could be drawn up.

Question
Would an action plan be a useful tool for implementing the measures identified in the replies to this document?

Concluding remark

The responses to this document should be sent electronically by 10 January 2007 to the following e-mail address: **JLS-D1-Detection@ec.europa.eu**. All responses from both public and private sectors will be published on the Commission's internet site unless respondents explicitly state that they wish to keep particular information confidential.

ANNEX

I. BACKGROUND INFORMATION ON THE PREPARATION OF THE GREEN PAPER

This Green Paper is based on the results of the conference and raises themes and issues that featured prominently in the discussions (e.g. standardisation, security research, improvement of technological solutions, protection of privacy, the legal framework and other guidelines by which technologies have to abide, etc.). Over one hundred participants from business, industry and the public sector engaged in the debate. The public sector was represented by the members of law enforcement, customs and other security authorities, by the Commission and by representatives of the Member States. The title of the conference suggests that it focused on the fight against terrorism. However, it became clear from the outset that a broader security approach was inevitable if important security concerns were not to be omitted. This broad approach was reaffirmed by the December 2005 Council decision to base European critical infrastructure protection on an 'all hazards' approach. Moreover, the conference took a holistic approach by bringing together stakeholders from different areas of expertise to discuss the following topics:

- Detection technologies in the protection of infrastructure
- Personal detection technologies and biometrics
- Detection of explosives and chemical, biological, radiological and nuclear (CBRN) substances.

All themes focused on the work of law enforcement, security and customs authorities. This approach enabled the conference to identify numerous areas of common concern for both public and private sectors (e.g. interaction between solution-providers and those who need solutions in the public sector). This is reflected throughout the document.

Definition of detection technologies and relevant categories

For the purposes of the consultation, the term 'detection technology' is used in the broadest sense. Detection technologies can be "in situ" or external and probably the more sophisticated means to deal with some of the security challenges in various scenarios are when integrated into the complex system (such as transport system). A detection technology can be almost anything used to detect something in a security or safety context, with the focus on law enforcement, customs or security authority. It is possible to identify several categories[6] which, if taken into consideration when responding to the questions outlined in this document, may help to sharpen the answers:

- Hand-held detectors
- Detection portals
- Surveillance solutions

[6] This is a non-exhaustive list of categories.

- Detection of biometrics
- Data- and text-mining tools
- Other software-based detection tools, etc.

Furthermore, respondents should also consider associated technologies when replying to the questions, as technologies which help humans to make sense of the data collected by the detectors are also important for effective solutions. Technology is needed to integrate solutions and to make systems interoperable. Despite having highlighted these categories, respondents should not feel constrained by them, and are encouraged to go beyond them.

II. STANDARDISATION AND THE EXCHANGE OF PERSONAL DATA

The Commission points out that, in terms of handling personal data, Directive 95/46/EC already provides the legal framework for exchange of information containing personal data in respect of activities relating to the "first pillar". As regards exchange of information as part of judicial and criminal cooperation, and under the principle of availability, the Commission has tabled a legislative proposal, which is under discussion.

III. STUDIES

1. Protection of mass events

Every year EU Member States organise several public mass events of national, European, but also of international importance. In today's security environment the costs of security for such events may take up a substantial part of their budgets. All Member States could benefit from a common approach to this problem.

To prepare the ground for eventual steps to be taken in this area, the Commission proposes to organise a study on the protection of mass events. The study would analyse what security tools, equipment and expertise applied in the protection of mass events are transferable from one event/site to another. The study would also consider the practicality and implications of Community-owned equipment, of Community-shared equipment, of developing a business model for services provided by the private sector or of a combination of all three approaches. This part of the study should determine which solution:

- is the most cost-effective and flexible enough to fit diverse needs of Member States;
- can ensure access to this solution by all Member States together with appropriate sharing of the costs by the Member States.

When the results of the study are ready, the Commission would consider further steps in this area in conjunction with the Member States and other relevant stakeholders.

2. Cooperation and information-sharing among forensic laboratories and security research institutes

The participants in the conference highlighted the fact that legal and other obstacles exist at national level which prevent effective cooperation and information-sharing among national forensic institutes at European level. Therefore, the Commission suggests conducting a study on the subject. This study could also address options for remedying the situation.

A similar concern was raised regarding cooperation and information exchange among security research institutes. A separate study addressing this issue could also be conducted.

3. Law and specific detection technology

Law enforcement, customs and other security authorities are often scrutinised for whether they comply with applicable legal standards. Even if the technology as such is not in breach of legal standards, the manner of its use may raise concerns. Accordingly, identifying the legal framework governing the use of, and setting limits for, technological solutions could help to raise greater awareness in both public and private sectors and facilitate compliance with existing standards. The private sector could also benefit from such a study when proposing and designing technological solutions and services for the public sector.

4. Specific detection technology and its practical use

Similarly, guidance and best practice in the use of technologies, particularly detection technologies, must take into account how users of these technologies actually use such tools in practice, and how they act in relation to persons subject to detection. A specific technology as such may not breach legal standards, but its real world use by an operator may raise concerns. In addition, the development of new technologies or the changing use of existing technologies may result in situations where a law regulating their use does not exist. Alternatively a particular use of a technology may not be in breach of the law, but it may run counter to best practice or codes of conducts developed to supplement legal provisions. Knowledge of regulations (instruments) in this area might provide guidance on whether they comply with the legal framework (in particular fundamental rights and data protection) and on what is acceptable or not in a situation where legal provisions have not been developed.

5. Personal detection technologies and biometrics

Personal detection (including surveillance) and biometrics are issues which affect individuals directly, and therefore a sensitive political debate is ongoing on the use of these tools for the purposes of improving security in Europe. The Commission suggests that a study should be undertaken to identify the legal framework governing personal detection technology and biometrics. This study would analyse the legal systems of the Member States and the EU and thereby establish what existing rules govern personal detection and biometrics. A study of this kind is particularly important when making technological solutions proposed by the private sector compliant with the law. In simple terms, it would help the private sector to understand the legal and other constraints on technological solutions they develop.

Special studies could also be drawn up on the levels of acceptance of surveillance and biometrics by the population in individual Member States and in the EU. The methodology of these studies would have to ensure that there is no confusion between the two subjects – surveillance and biometrics. Such studies could help the EU and national governments to deploy adequate communication strategies on these issues. In general, both studies would further contribute to the political debate in Europe on these important matters.