EU2009.CZ

České předsednictví
v Radě EU

Czech Presidency
of the Council of the EU

Présidence tchèque
du Conseil de l'UE

2009

Informal Council of Ministers for Home Affairs

Prague, 15 January 2009

Modern Technologies and Security

Concern for man himself and his fate must always form the chief interest of all technical endeavors.

Albert Einstein

Introduction

Rapid development of modern, especially information and communication technologies is one of the key elements of contemporary society and one of the essential factors of its progress. An effective and efficient application of modern technologies will play important role in the economic, social and knowledge development of the EU. However, clear positive effects of modern technologies have a reverse side as well, since they may become subject of abuse. This development implies serious challenges for authorities responsible for security in the Member States and in the EU as a whole, while at the same time, they have to continuously improve their mutual cooperation to be able to efficiently fight cross-border crime. With regard to the single internal market, especially the free movement of persons, goods and capital and the ongoing removal of barriers on the European level, the greatest challenge for these agencies consist in their cooperation within the EU. We need the EU to be able to appropriately respond to technological development, to continue monitoring and evaluating the ongoing development in all its areas, having the possibility of examining and employing new tools of technical progress and information technologies.

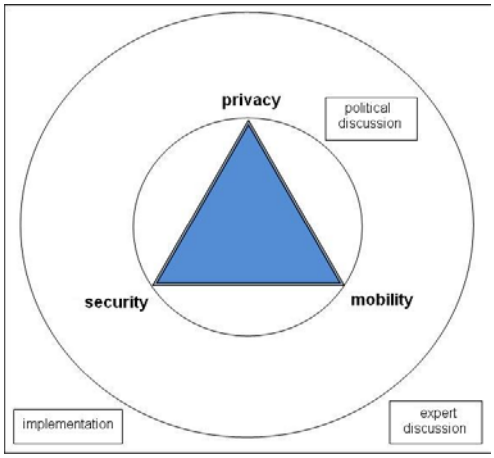
Despite the efforts of the Commission[1] and the Member States and the unquestionable progress in creating a systematic approach in this area[2], it is necessary to admit that the current activities focused on strengthening European cooperation in the area of internal security and criminal justice have not achieved the desired standard from the systematic viewpoint. The most urgent risk which we face today is the fragmentation, overlapping and the vagueness of individual instruments and mechanisms of cooperation. The agreed principles and general approaches are only seldom projected into concrete instruments we jointly prepare. This concerns support instruments (information systems and information technologies) as well, which require continuous analysis and harmonization (synergy and interoperability). The technical aspect also deserves attention, since the expanding use of modern technologies brings about the need to reflect on their current use and to consider ways of coordination of their application.

[1] Such as the Communication on improved effectiveness, enhanced interoperability and synergy among European databases in the area of Justice and Home Affairs (151222/05 CATS 82)
[2] The Proposal for Council Conclusions on the definition of a policy for a coherent approach to the development of information technology (10699/05 CRIMORG 112) can serve as an example of specific directives.

The pressure to adapt to the new technologies as well as the need to exchange information in various forms will only grow. Therefore, the time has come to pause on an overall concept allowing the Justice and Home Affairs Council to adopt a long-term and systematic approach, which will take into account the aspect of operative efficiency as well as the European values.

Where do we find ourselves at present?

Working with information will constitute the core of everyday work of security agencies. Police and other security agencies will be confronted with the need to understand new types of information (biometric data, DNA profiles, PNR etc.) and with the task to efficiently obtain and process this information. At the same time, the use of modern information technologies must be accompanied by adequate measures preventing the abuse of obtained information and by respecting the protection of personal data.



Taking into account the need for a political reaction to – to a certain degree justified – fear of our citizens of **losing privacy**, the discussion has recently focused on the more general issue of finding a **balance between the protection of privacy, security and the free movement of persons**. Recent reflections on this subject led in the conclusion of the Future Group[3], confirming the importance of this issue which should represent the main task in the area of home affairs. Careful maintenance of this balance should result in preservation of a "European model" responsible for efficient decision-making within the home affairs area.

European citizens expect guaranteeing their security as a basis of free decision-making, accompanied by a high level of privacy protection. Therefore, it is important to consider **synergic and complex relations within the triangle of these values**. Without sufficient security, most EU citizens wouldn't travel; yet without the possibility to process personal data, states would intensify controls in their territory etc. Naturally, there are also bilateral relations between the values, as has been demonstrated by discussions on the possibilities of abuse of thirds countries nationals' right of residence in Member States. One-sided promotion of one value can produce unintended consequences leading

[3] Future Group report, June 2008, Executive summary paragraph 4, report paragraphs 17, 28-32, 132, 153.

to a distortion of the delicate balance of the "triangle" and hence to an overall setback. Therefore, **the relation between security, privacy and mobility should not be understood as a zero-sum game, but as a demanding challenge to be examined in detail at the expert level and requiring responsible political decision-making.**

The current development of information society brings a number of new types of data which can be used by security agencies. These technologies, developed for legitimate purposes by the private sector allow as well the collection of extremely detailed information, for instance, on the movement of a certain object and thus on a behavior of a person using that object. Similarly negative consequences can be incurred by the analysis of digital records of various transactions. Another ethical challenge is presented by the **automated prioritization of cases** mechanisms (when providing services, etc.) which raises questions such as whether and when a similar mechanisms should be used by security agencies. Ensuring the most efficient use of information and communication technologies naturally causes not only practical difficulties, but also raises general questions of proportionality and limits of security agencies' powers.

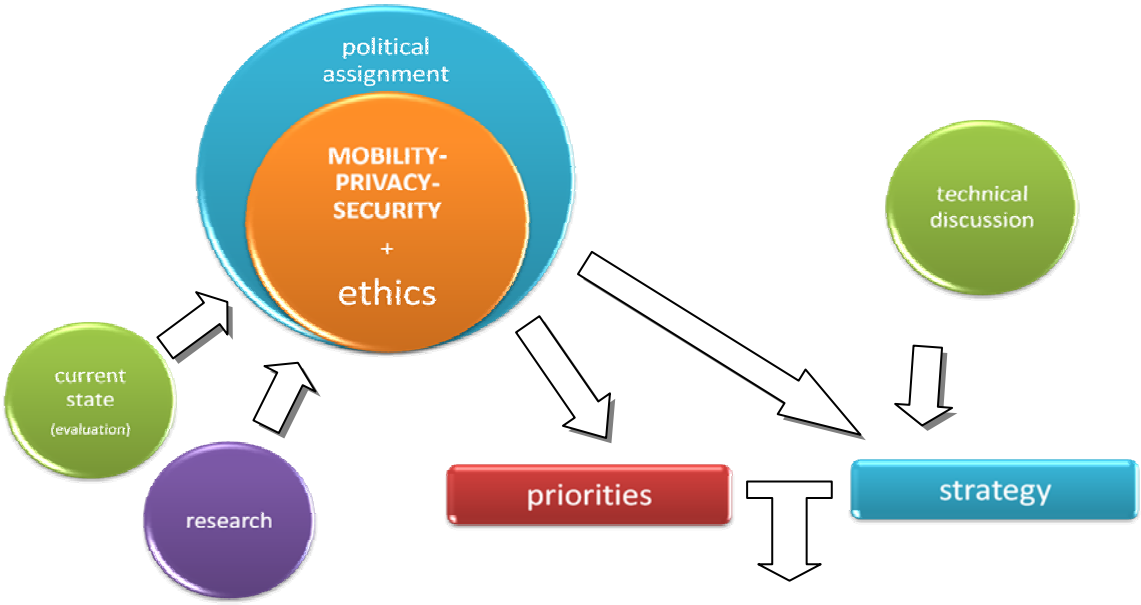
However, these technologies, which are often perceived only as a tool for intruding into citizens' privacy, may be used for an automatic limitation of the types of data to which state institutions will have access - so-called **"privacy-enhancing technologies".** Expansion of these technologies is supported by institutions and organizations dealing with personal data protection. It also represents (e.g. as regards encryption algorithms) a specific challenge for security agencies, which must face the abuse of modern technologies by criminals. The importance of an ethical dimension for ensuring security ("infoethics") will ever increase along with technological development. **Since many specific types of cooperation are and will be common to all EU Member States, it is important to hold a discussion about related ethical questions.**

The Justice and Home Affairs Council, along with the Commission, play a key role in this area. They should have the right tools to be able to face, for instance, duplicities or ageing of certain instruments. **The EU should have tools to support systematic solutions of specific types of cooperation in order to be able to improve the efficiency, proportionality and quality of specific tools and mechanisms of joint action in the area of Justice and Home Affairs.**

Although the area of Justice and Home Affairs is specific, it is neither possible nor desirable, to isolate it from other areas with which it forms a common frame of the

European citizens' lives. Since modern technologies permeate the entire spectrum of areas and issues, even specific proposals prepared by the JHA Council may have serious consequences for the internal market, for the life of some European regions, etc. **Consequently, future action in the use of modern technologies for security purposes must be kept in line with the activities of the EU as a whole.**

The need to reflect on, and to methodically manage the future development in the area of security technologies is a challenge of which the EU has been aware for a long time and the Member States along with the Commission have therefore come up with a number of initiatives[4] of how to support and promote a systematic approach to the use of modern technologies by security agencies, especially in the area of exchange and processing of information. Our work has already been reflecting certain driving principles, such as the principle of availability, which states that law enforcement agencies of one Member State should have direct access to the same information in another Member State as the agencies of that state; or the principle of convergence[5], which brings a systematic emphasis on real operative communication and cooperation of all institutions.



[4] For example, the Report by the Friends of the Presidency on the implementation of the principle of availability (e.g. 13558/05 CRIMORG 112).
[5] Council Conclusions on the principle of convergence and the structuring of internal security (14069/08).

How do we proceed from here?

The EU needs to develop information exchange tools and mechanisms for using security technologies in a rational way. The current fragmentation and vagueness of the different initiatives has on the one hand enabled the rapid implementation of some crucial cooperation mechanisms with a clear added value; on the other hand, it brings the risk of overlaps and insufficient interconnection of individual instruments.

An essential assumption of anchoring the systematic approach is a thorough evaluation of the current state of exploitation of modern information and security technologies in the area of Justice and Home Affairs and an expert discussion about the conditions and modalities of future development. The Presidency is therefore putting forward a proposal for charging preparatory bodies of the Council with the following missions:

A – ensure by mid-2009 the preparation of a description of the current state in the area of information exchange and other means of using security technologies within the EU.

These bodies should, with significant support from the Commission, the General Secretariat of the Council, as well as agencies making use of the relevant information systems, constitute a catalogue of information which flow through specific systems and describe this flow in each of the systems at least in general terms. This effort should encompass all information systems in the area of Justice and Home Affairs.

B – prepare the criteria for an evaluation of the proposed or existing systems, which could eventually be used for preparing a general strategy.

With regard to the current political discussions within the Justice and Home Affairs Council, these bodies should focus on identification of the main factors that could serve as a basis for defining the form of future systems for information processing and exchange. These criteria could also serve as a basis for an "information-technological impact assessment" for every new proposal.

Should the preparatory bodies be charged with the above-mentioned missions? Should they have any other tasks?

The Presidency suggests that the following basic general aspects be included among the individual criteria:

- *a balance between **privacy, mobility and security***

The freedom of movement in a Europe without barriers represents one of the main positive effects of European integration, despite the fact that, in some cases, it brings challenges to law enforcement agencies. Representatives of personal data protection institutions should therefore also take part in the working group.

- ***the ethical dimension** of using a specific technology for security purposes*

In some cases, using modern technologies for security purposes can be especially problematic from a moral point of view. Besides including the ethical dimension among the relevant criteria, it is pertinent to **also consider the creation of an advisory group of experts**[6] with a wide, representative participation and a mandate to advise on appropriate solutions and warn against undesired directions in the context of the development of information and security technologies ("Group on Infoethics").

- *support of **development and sharing of modern security tools***

It is relevant to consider the creation of a "signal group" or a "signal network", which would **search for specific "emerging" technological applications** and ways of their efficient use in the area of security. At the same time, this group or network would focus on specific applications, which make use of aforementioned technologies that are already being used by the private sector. This group should not create any strategy, but should serve to exchange best practices with regard to technologies already in use, which would be brought to a wider expert attention in the EU. The group would also represent a technically oriented detector of other relevant directions of the short-term development as well as a filter for non-prospective solutions.

- *cooperation with **research institutions and the private sector***

The possibility to use the advantages offered by cooperation with the private sector and results of research institutions, be it research programs financed by the EU or independent research of Member States could be included among the criteria.

[6] An alternative possibility would be to use, in cooperation with the Commission, the services of the already established European Group on Ethics in Sciences and New Technologies, which advises the Commission on ethical questions.

- *criteria* ***facilitating the preparation and the implementation of new instruments***

It is presumable that, apart from these general criteria, the expert working group will provide a number of additional criteria and factors. Another source of useful knowledge will be without doubt provided by successful solutions proven in practice, or, eventually, reactions to procedures that have revealed themselves as problematic[7].

However, the preparation of criteria and of the entire systematic approach **should not** prevent the continuation of work on initiated projects, or on initiatives with an apparent added value for the EU.

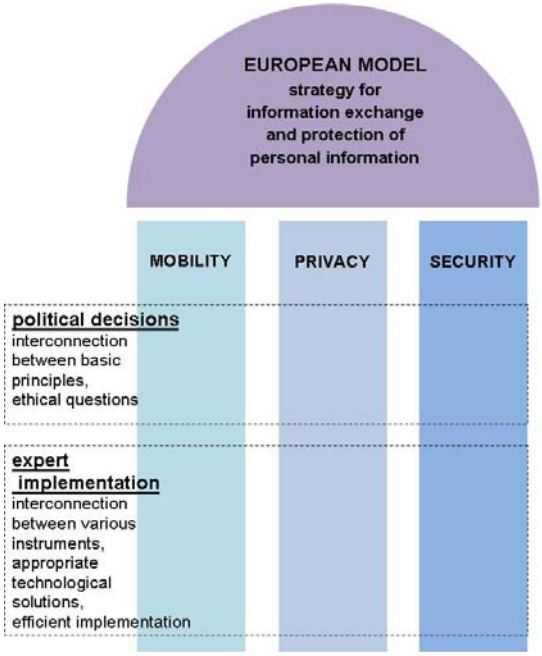
Should work on the identification and definition of relevant criteria be an important part of the preparation of the future systematic approach to creating information systems in the security area? Are the proposed criteria relevant? Should the subsequent discussion concerning various criteria be held not only at the political but also at the expert level?
Should the work on particular new initiatives which do not represent an essential added value in practice, be postponed until their evaluation according to the relevant criteria?

Further action

In case there is at least a framework consensus between Member States on the approach proposed above, discussions within the expert working group should provide a sound basis for the next step, which could consists in the preparation of a European model of comprehensive strategy for the information exchange and personal data protection. Such a strategy does not need to cover the entire area of security technologies. Since processing information is the core of police work, it would without doubt be an important step towards directing further development of cooperation between law enforcement agencies in accordance with requirements placed before us by the reality of a united Europe. This strategy should support and keep the European model of balance between security, privacy and mobility and should ensure an efficient, effective and rational

[7] Criteria that could assure a smoother preparation, especially where complex systems and instruments are concerned, could include realistic and technically feasible planning; harmonization of the technical parameters of solutions; securing of sufficient security; a project management system equipped with alternative solutions and monitoring mechanisms, which would respond to emerging problems.

expenditure of EU resources and those of the Member States to support better police and judicial cooperation in combating crime and ensuring security.



Approaching the use of modern technologies in a systematic fashion, especially in the area of information exchange and processing, is an important challenge for the years ahead. Cooperation between law enforcement agencies cannot lag behind modern forms of crime. New and existing instruments and mechanisms should be precisely described and efficiently coordinated so as to bring about an optimal employment of all resources, the elimination of redundant duplications and the identification of priorities for a future development of cooperation. This is the only way we can guarantee that in the 21st Century the European internal security architecture will stand up to its duties.