EUROPEAN PARLIAMENT

DIRECTORATE GENERAL INTERNAL POLICIES OF THE UNION

BRIEFING NOTE

Policy Department C
Citizens' Rights and Constitutional Affairs

INTERDEPENDENCE OF THE VARIOUS INITIATIVES AND LEGISLATIVE PROPOSALS IN THE FIELDS OF COUNTER-TERRORISM AND POLICE COOPERATION AT THE EUROPEAN LEVEL

CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS

OCTOBER 2007
PE 393.257

EN

PARLAMENTO EUROPEO EVROPSKÝ PARLAMENT EUROPA-PARLAMENTET
EUROPÄISCHES PARLAMENT EUROOPA PARLAMENT ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ EUROPEAN PARLIAMENT
PARLEMENT EUROPÉEN PARLAMENTO EUROPEO EIROPAS PARLAMENTS
EUROPOS PARLAMENTAS EURÓPAI PARLAMENT IL-PARLAMENT EWROPEW EUROPEES PARLEMENT
PARLAMENT EUROPEJSKI PARLAMENTO EUROPEU EURÓPSKY PARLAMENT
EVROPSKI PARLAMENT EUROOPAN PARLAMENTTI EUROPAPARLAMENTET

Directorate-General Internal Policies
Policy Department C
Citizens Rights and Constitutional Affairs

INTERDEPENDENCE OF THE VARIOUS INITIATIVES AND LEGISLATIVE PROPOSALS IN THE FIELDS OF COUNTER-TERRORISM AND POLICE COOPERATION AT THE EUROPEAN LEVEL

BRIEFING NOTE

Abstract:
The note reviews the development and the interdependence of the various initiatives and legislative proposals in the fields of counter-terrorism and police cooperation at the European level. It will be demonstrated that a vast majority of these measures involve the collection and exchange of personal data. The challenges of this approach to the protection of fundamental rights, in particular privacy and data protection, will be highlighted.

The note covers a wide range of issues such as money laundering and terrorist financing, Europol, databases and their interoperability, the principle of availability of information, the rules to improve police cooperation (Schengen and Title VI), the Prüm Decision and data protection.

One could says that the EU counter-terrorism and police co-operation measures are based largely on the gathering and exchange of personal data. This may lead to maximisation of surveillance via the collection of a wide range of personal data and thus pose significant challenges to privacy and data protection. This is true in particular in the light of the fragmentation of the EU data protection framework applying to the various databases and forms of information exchange.

PE 393.257

This note was requested by The European Parliament's committee on Civil Liberties, Justice and Home Affairs.

This paper is published in the following languages: EN, FR.

Authors: **Valsamis Mitsilegas and Anneliese Baldaccini, Centre d'Etudes sur les Conflits, Paris**

Manuscript completed in October 2007

Copies can be obtained through:
M. Alessandro Davoli
Tel: +32 2 2832207
Fax: +32 2 2832365
E-mail: alessandro.davoli@europarl.europa.eu

Informations on DG Ipol publications:
http://www.ipolnet.ep.parl.union.eu/ipolnet/cms

Brussels, European Parliament

The opinions expressed in this document are the sole responsibility of the author and do not necessarily represent the official position of the European Parliament.

BRIEFING NOTE

Interdependence of the various initiatives and legislative proposals in the fields of counter-terrorism and police cooperation at the European level

Valsamis Mitsilegas and Anneliese Baldaccini
September 2007

The note will review the development and the interdependence of the various initiatives and legislative proposals in the fields of counter-terrorism and police cooperation at the European level. It will be demonstrated that a vast majority of these measures involve the collection and exchange of personal data. The challenges of this approach to the protection of fundamental rights, in particular privacy and data protection, will be highlighted.

Money laundering and terrorist financing

The objective of countering terrorist finance has been central in efforts to amend EU anti-money laundering legislation. The third money laundering Directive, adopted in 2005, was the outcome of such efforts.[1] Along with money laundering, the Directive now also prohibits 'terrorist financing'. The definition of terrorist financing is similar, but not identical to that found in the UN 1999 Convention, and terrorism is formulated in accordance with the relevant EU Framework Decision.[2] Another interesting addition, that may have criminal law repercussions, is the Directive requirement that Member States protect employees who report suspicions of money laundering or terrorist financing from being exposed to threats or hostile action. The nature and means of such protection are left unspecified, and the broader issue is whether the Community has competence to impose this obligation, which may lead to the inclusion of such employees in protection schemes under national criminal justice systems, in a first pillar instrument.[3]

Moreover, in order to further align the Community framework with developments within the framework of the Financial Action Task Force (FATF), a number of changes have been introduced by the third money laundering Directive in the field of customer identification and due diligence. Chapter II of the Directive is now entitled

[1] [2005] OJ L 309/15.
[2] Article 1(4). Terrorist financing is defined as 'the provision or collection of funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism'.
[3] See Article 27 of the Directive. Recital 32 in the Preamble implicitly recognises the potential impact on national systems by stating that 'although the Directive cannot interfere with Member States' judicial procedures, this is a crucial issue for the effectiveness of the anti-money laundering and anti-terrorist financing system'.

'customer due diligence' and comprises no less than 15 Articles.[4] The provision on customer identification has been expanded to introduce various levels of diligence, which may range from simplified due diligence[5] to enhanced due diligence, in particular when cross-frontier correspondent banking with third countries, transactions with politically exposed persons, or the use of shell banks is involved.[6]. This is primarily achieved by the use of the principle of due diligence 'on a risk-sensitive basis'.[7] This is in compliance with the new FATF approach embraced in 2003, and may be a useful principle in ensuring that the institutions and professions concerned are not unnecessarily overburdened with obligations.[8]

While the new provisions introduced by the third money laundering Directive may contribute towards a more efficient fight against money laundering and terrorist finance, there are a number of issues that need to be addressed in the implementation of this measure. The first issue concerns the applicability of the money laundering criminalisation model to terrorist finance. There is a fundamental difference in the two phenomena. While the laundering of money involves proceeds of crime, terrorist finance may involve perfectly legitimate funds, which are then used *ex post* to fund terrorism. Moreover, while money laundering involves usually significant sums of money, terrorist finance may involve only small sums, whose detection may necessitate different mechanisms of action. There may be a tension between extending the regulatory network to cover the monitoring of non-financial institutions (such as charities) for anti-money laundering and terrorist finance purposes and the need to ensure the smooth functioning of such bodies and the facilitation of the global flow of funds by alternative methods to the banking system.[9]

The Directive also consolidates the extension of reporting duties to the legal profession and, as said above, introduces changes to customer due diligence, by emphasising a 'risk-based' approach and drawing attention to specific transactions such as those involving the so-called 'politically exposed persons'. However, as with terrorist finance, a number of these issues have not been defined precisely in the Directive. Rather, on a number of occasions, decisions on definitions in and amendments to the Directive will not be taken under the ordinary legislative procedure under which the Directive was adopted (co-decision between the European Parliament and the Council), but by a 'comitology' committee chaired by the Commission and consisting of representatives of Member States. This would result in practice in minimal parliamentary scrutiny at both the European and national level. Article 40 of the Directive calls for adoption under this procedure by the Commission and the Committee on the Prevention of Money Laundering and Terrorist Finance established by Article 41, of a number of measures in order to take account of technical developments in the field. These include in particular clarifications of the technical aspects of definitions of concepts such as beneficial ownership, politically

[4] Articles 6-19 of the Directive.
[5] Articles 11-12.
[6] Article 13.
[7] Articles 8(2), 11(2), 13(1).
[8] This approach is also reflected in the chapter on performance by third parties (Articles 14-19). Article 14 allows Member States to permit institutions and persons covered by the Directive to rely on third parties to meet the requirements of customer due diligence under certain conditions.
[9] The FATF-led focus on monitoring of cash movements is also reflected in the Regulation of 26 October 2005 on controls of cash entering or leaving the Community. OJ L309, 21 November 2005, p.9.

exposed persons, business relationship, and shell bank. These concepts are central to the delimitation of the duties set out by the Directive in applying the FATF standards, and their definition may have significant implications for the liability of the institutions and persons involved, but also for the fundamental rights of the individuals concerned (such as politically exposed persons).[10]

Europol

At the end of 2006, the Justice and Home Affairs Council agreed that the Europol Convention should be replaced by a Council Decision.[11] A few days later, the Commission tabled such a draft Decision.[12] Along with the change in the legal basis of Europol, the proposal introduced a number of changes in the organisation's mandate and powers. With regard to the Europol's tasks regarding databases and information collection, analysis and exchange, the proposal extends the reach of Europol to information and intelligence forwarded by third countries 'or other public or private entities'.[13] The potential extension of Europol's role with regard personal data is also evident in Article 10 of the Commission draft, which mentions the possibility of the establishment by Europol of a system for processing of personal data other than its current Information System.[14] The same provision expressly calls upon Europol to ensure the interoperability of its data processing systems with the data processing systems in the Member States and in particular with the processing systems of EC or EU bodies such as the European Borders Agency (Frontex), the European Central bank, the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), the European Anti-Fraud Office (OLAF), Eurojust and the European Police College (CEPOL).[15] Moreover, access to the Europol Information System will no longer be limited to national units, but will be extended to other authorities designated as such by Member States (however only on a hit/no hit basis).[16] The mandate of Europol will include 'serious crime', including terrorism.[17]

If adopted as such the proposals will introduce significant changes in the mandate of Europol with regard to its handling of personal data. The Commission proposal signifies the end to the basic principle underlying the work of Europol, namely that the main channel of co-operation is between Europol and central national police units – according to the proposals, other national authorities could have access to Europol databases, while Europol can also work with the private sector. At the same time, the exchange of data between Europol and other EC/EU bodies is boosted by the express reference of the proposal to 'interoperability' of their databases. These developments – indicative of the trend towards maximising the exchange of personal data in the EU-

[10] See the 'comitology' Commission Directive o2006/70/EC which inter alia contains provisions on the definition of politically exposed persons and technical criteria for simplified due diligence procedure (OJ L214, 4 August 2006, p.29).
[11] Justice and Home Affairs Council of 4-5 December 2006, doc. 15801/06 (Presse 341), pp.20-21.
[12] *Proposal for a Council Decision establishing the European Police Office (EUROPOL)*, COM (2006) 817 final, Brussels 20 December 2006.
[13] Article 5(1)(a).
[14] Article 10(3).
[15] Articles 10(5) and 22.
[16] Article 13(6).
[17] Articles 3 and 4 of the proposal, which seem to distinguish between the objective and the competence of Europol.

have been criticised by EU data protection authorities. The European Data Protection Supervisor (EDPS) noted that the principle of interoperability reverses the current approach of the Europol Convention, which in Article 6(2) strictly prohibits the linking between Europol Information System to other automated processing systems and opposes the view that interoperability should be treated merely as a technical concept.[18] This view is shared by the Europol Joint Supervisory Body, which notes that technical interoperability does not mean that data may actually be exchanged without legal provisions in place.[19]

These developments, along with the more general debate regarding the nature of Europol and whether it should obtain a more 'operational' role, highlight the need for enhanced monitoring of the operations and data collection and exchange from this body.

Databases and their interoperability

The establishment and development of EU databases and the achievement of their interoperability have been key elements of the EU counter-terrorism Strategy in recent years. This has been reflected in the European Council Declaration of 25 March 2004, on combating terrorism, which called for the enhancement of the interoperability between EU databases and the creation of 'synergies' between existing and future information systems (such as SIS II, VIS and EURODAC) 'in order to exploit their added value within their respective legal and technical frameworks in the prevention and fight against terrorism.' The European Council also stressed the need to link measures monitoring movement with counter-terrorism.

Interoperability appeared again prominently in a Commission Communication examining potential use of databases in AFSJ.[20] According to the Commission, the purpose of the Communication is to highlight how, beyond their present purposes, databases 'can more effectively support the policies linked to the free movement of persons and serve the objective of combating terrorism and serious crime'. The Communication also provides a definition of 'interoperability', which is the 'ability of IT systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge'. According to the Commission, interoperability is a technical rather than a legal/political concept.

The extensive use of interoperability as envisaged by the European Council and the Commission causes a number of concerns touching upon both the protection of fundamental rights and issues of democratic control and accountability. The various new and developing EU databases were constructed to serve very diverse purposes, ranging from the facilitation of the assessment of visa and asylum applications (VIS and EURODAC respectively) to police co-operation and counter-terrorism (aspects of SIS, the Europol database) – and contain quite diverse categories of data. Interoperability of these different databases – especially if it is justified under the blanket need to combat terrorism – challenges data protection safeguards based on

[18] *Opinion of the European Data Protection Supervisor on the proposal for a Council Decision establishing the European Police Office*, 16 February 2007, points 21 and 22 respectively.
[19] *Opinion of the Joint Supervisory Body of Europol with respect to the proposal for a Council Decision establishing the European Police Office*, Opinion 07/07, 5 March 2007, p.11.
[20] See the Commission Communication on interoperability, COM (2005) 597 final, 24 November 2005.

purpose limitation regarding access and use of personal data included therein. Protection of personal data may be particularly weakened in the light of the fragmentation of data protection related to the various EU databases. The latter are created under different legal bases (first and third pillar) and are governed by different data protection regimes. These are very fragmented in the third pillar, where specific rules and specific supervision arrangements apply to specific bodies holding databases (such as Europol and Eurojust), with no general, across the board, standards or supervision. The need to adopt EU legislation to provide uniform and adequate protection of sensitive personal data in the third pillar is discussed further below.

In the light of these challenges to privacy, attempts to enhance the interoperability of databases must be closely examined. The Commission's approach that interoperability is merely a 'technical' rather than a legal/political concept disregards the far-reaching consequences the principle may have for the protection of fundamental rights and may lead to shielding the relevant developments from full transparency and scrutiny.

Availability of information

Along with creating EU databases and enhancing their interoperability, another aspect of the recent EU counter-terrorism Strategy has been the move to facilitate the exchange of information between national law enforcement authorities. The key mechanism to achieve this goal is deemed to be the "principle of availability". This was central to the Hague Programme, which defined it as meaning that 'throughout the Union, a law enforcement officer in one Member State who needs information in order to perform his duties can obtain this from another Member State and that the law enforcement agency in the other Member State which holds this information will make it available for the stated purpose, taking into account the requirement for ongoing investigations in that State'.

The Commission tabled a proposal on the principle of availability in 2005.[21] It envisaged: the provision of information to 'equivalent' authorities of other Member States almost exclusively on a 'need to know basis'; the exchange of information taking place on the basis of standard, pro-forma documents, becoming thus quasi-automated; as a safeguard, requesting police authorities cannot ask for information to be obtained – with or without coercive measures – by the requested authority solely for the purposes of cooperation – but information already lawfully collected by the requested authority by coercive measures may be provided (even though these measures may not be lawful in the requesting State – something that would potentially infringe national constitutional provisions through the 'back door'); and authorities that can benefit from the principle of availability will be defined by a 'comitology' Committee. The proposal has not been adopted but elements of it have been taken forward by the Prum Treaty (see below).

The principle of availability is reminiscent to a considerable degree of the principle of mutual recognition in criminal matters. Cooperation is facilitated on the basis of the recognition of *national* standards and legal systems, and authorities are requested to cooperate with their counterparts in other Member States on the basis of trust, without asking too many questions regarding the purpose of the request or the use of the

[21] (COM(2005) 490 final, 12 October 2005.

information provided in the legal and policy system of the requesting state. In the light of the considerable differences between the national law enforcement and counterterrorism systems in Member States, the blanket application of availability may lead to considerable legal uncertainty and a legitimacy and transparency deficit.

Rules to improve police cooperation: Schengen and Title VI

Rules to improve law enforcement cooperation were first set out in the Schengen Convention. The Schengen police cooperation measures provide for mutual assistance and direct information exchange between police services, cross-border surveillance and pursuit of suspects, improved communication links and information exchange via central law enforcement agencies.

Cross-border surveillance and hot pursuit

In July 2005 the Commission submitted a draft council decision on the improvement of police cooperation between Member States, especially at the internal borders and amending the Schengen Convention (doc 5284/06).[22] The proposed Decision further develops the Schengen Convention in respect of operational cross-border police cooperation as requested by the Hague Programme. Moreover, it follows on from Declaration on combating terrorism of 29 March 2004, which had instructed the Council to examine measures in the area of 'cross-border hot pursuit' and called for further development of the legislative framework. The proposed amendments to the Schengen Convention concern the extension of the hot pursuit provisions (Article 41) to include, amongst others, pursuit by sea, waterway or air, as well as across land borders. Amendments to Article 40 would extend the possibility to carry out cross-border surveillance, particularly with respect to non-suspects who might assist in tracing or identifying suspects. While data protection would comply with the relevant legal provisions laid down in Title VI of the Schengen Convention, it would be important to ascertain whether these adequately adress the privacy implications of the extension of police powers to cross-border surveillance of non-suspects.

Negotiations on this dossier were last held under the Austrian Presidency but were discontinued because of the difficulty in reaching agreement among Member States. There is no indication that negotiations will resume under the current Presidency.

Information exchange

Information sharing is a vital tool for the detection and investigation of crimes and key to better cooperation between Member States' law enforcement authorities. Rules governing the exchange of information were first laid down by the Schengen Convention. Article 39 of the Schengen Convention stipulates that Member States undertake to ensure that police authorities shall assist each other to prevent and detect criminal offences. The request for assistance must be exchanged via central bodies reponsible for police cooperation, unless the urgency of the matter justifies that requests are exchanged directly between the competent police authorities. Article 46 gives police authorities the right to exchange information which may be important in

[22] COM(2005) 317 final, 18 July 2005.

helping to prevent crime and threats to public order with another Member State on their own initiative, without being asked.

Title VI of the TEU

Title VI of the Treaty of the European Union requires Member States to further develop police cooperation, including through the collection, analysis and exchange of law enforcement information (Article 30(1)(b)). Importantly, this Article also establishes that European rules on the processing and exchange of police information must be subject to appropriate provisions on data protection.

There have been a number of information sharing dossiers under Title VI. These include:

- the Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities (the Swedish initiative).[23] This Framework Decision overhauls the general legal and operational conditions for the exchange of law enforcement data provided for in the Schengen Convention in its Articles 39 and 46 by setting up an enhanced mutual assistance procedure. It seeks to advance cooperation by laying down an obligation to provide information, subject to limited grounds for refusal, within specific time limits. However, according to the Commission's own evaluation, the initiative does not eliminate the unpredictability that is inherent to the application of rules alien to the requesting authorities.[24] Furthermore, it is conceived to improve situations where the requesting law enforcement officer knows that a given Member State holds certain data, which is not often the case.

- The draft Framework Decision on the exchange of information under the principle of availability (see above). This proposal intends to eliminate the current unpredictability by combining mutual recognition and equivalent access. It makes certain types of existing information that are available to competent authorities of the Member State, available to authorities with equivalent competences of other Member States or of Europol. To that end it lays down the obligation to notify whether certain types of information are available in electronic databases, and whether or not they are directly accessible to competent authorities via online access. It furthermore lays down the obligation of creating data indexes for online consultation as regards information that is not accessible online. This proposal has been sidelined in favour of the model offered by the Prüm Treaty, now to be incorporated into EU law.

- The draft Council Decision on the stepping up of cross-border cooperation (the Prüm Decision).[25] This Decision will speed up the process by which DNA, fingerprints and vehicle registration data is shared for law enforcement purposes. Member States' authorities are granted online access to one another's databases to search or compare data on a hit/no hit basis. In the case of a hit the next step is to seek related personal data from the Member State administering the file and,

[23] [2006] OJ L 386/89.
[24] MEMO/05/367, 12 October 2005.
[25] For the latest draft see Council document 11896/07 of 17 September 2007.

where necessary, request further information through mutual assistance procedures, including (presumably) the procedure set out in the Swedish initiative. When a match is found, there is an obligation to supply further information to the requesting State's contact point. Concerns over this proposal are considered further below.

Schengen Information System

The Schengen Information System (SIS) has been operational since 1995. It is currently being developed to allow access to the new Member States and enhance its technological features.[26] One of the key aspects of the overhaul is the addition of biometric information to the SIS. SIS is currently based on alphanumeric data which allow only for two results: hit or no hit. Biometric systems, instead, are designed to search for an acceptable degree of similarity and are more effective, therefore, in linking information to persons. They will also significantly improve the possibilities for police searches. In particular, biometric data can be used both to confirm someone's identity (one-to-one search) and to identify somebody (one-to-many search). One-to-many searches transform the nature of the SIS from a database used for control purposes to one which can be used for investigative purposes, enabling so-called 'fishing expeditions' in which people registered in the database will form a suspect population. Data protection authorities have warned that the use of biometrics as a unique means of identification can have serious consequences for those who are wrongly identified, given the tendency of authorities to overestimate the reliability of biometrics.[27] The European Parliament, which had co-decision power on the Regulation setting up the SIS II, also had reservations on the use of SIS to identify third country nationals on the basis of their biometric information.[28] The ensuing compromise was to subject the biometric search function in the SIS II to a Commission report on the availability and readiness of the relevant technology.[29] The expectation, however, is that biometric searches will be enabled as soon as SIS II becomes operational.[30] The haste in allowing the biometric search function is troubling in the absence of provisions on misused identity and inaccurate identification due to technological failure, let alone any provision on compensation for those who have been wrongly identified.

Similar concerns arise from the move to adopt a proposal for access by police and law enforcement agencies to Eurodac, the shared EU database which contains records and compares the fingerprint images of asylum applicants and certain categories of illegal entrant. At the Justice and Home Affairs Council meeting of 12/13 June 2007,

[26] Legislation for the establishment of the SIS II comprises: Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) [2006] OJ L381/4; Council Decision on the establishment, operation and use of the second generation Schengen Information System (SIS II), doc 14914/06. These two instruments replace Article 92-119 of the Schengen Convention. In addition, the Community adopted Regulation (EC) No 1986/2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates [2006] OJ L 381/1.

[27] See the Opinion of the European Data Protection Supervisor on the draft SIS II legislation, [2006] OJ C 91/38.

[28] See European Parliament Report, A6-0335/2006 of 13 October 2006.

[29] Article 22(c) of the SIS II Regulation and Decision.

[30] Council Conclusions on the SIS, doc 10586/07, 8 June 2007, para 15.

Ministers asked the Commission to present "as soon as possible" an amendment to the Council Regulation 2725/2000 on the establishment of Eurodac to allow for police access to the database.[31] The Conclusions stress that police access to Eurodac should be subject to strict compliance with the rules governing the protection of personal data. While it remains to be seen what detailed data protection rights will be proposed, there are wider concerns about the discriminatory impact on asylum seekers of law enforcement uses of this database which have not yet been addressed. It is to be hoped that the impact assessment promised by the Commission will address the question of whether it is acceptable to subject anyone on the Eurodac database to a greater level of surveillance than others in the population, particularly as the disproportionate criminal activity which might result from this group, as against the population as a whole, will in turn foster discrimination and reinforce wide-spread prejudices.

The Prüm Decision

The incorporation into EU law of elements of the Treaty of Prüm is an initiative which Member States believe will bring practical benefits to law enforcement cooperation. It is evident, however, that the haste in bringing provisions of the Treaty, in force only among a few Member States,[32] into the EU legal framework has not allowed full consideration of the implications of allowing automated database searches in the wider context of the EU. In this respect, the absence of an Impact Assessment is highly regrettable, as is the lack of meaningful involvement of the European Parliament which has not allowed a full debate over the costs and benefits of this measure.

The proposal was brought forward by the German Presidency on the basis of its enthusiasm for the results achieved by matching DNA profiles held in its database with those held by the Austrians. It ignores problems which are likely to arise when the same exercise is carried out among 27 Member States. Bilateral exchanges are different from exchanging automatically the DNA data among 27 Member States, all of which deploy different methods of enrolment, different legal, administrative and operational systems. The absence of a harmonised approach to the collection and retention of data means, for instance, that there will continue to be differences between the grounds on which Member States collect DNA and fingerprints, and the length of time they are allowed to retain these data under their national law. There are also questions as to the readiness of the technology to allow for a vast exchange of data, as well as the costs which Member States have to incur in setting up relevant databases where these do not currently exist.

The German Presidency has, likewise, failed to include any regulatory impact assessment or cost estimate in the Implementing Decision submitted in the last week of June.[33] There is particular concern over the fact that a large number of the

[31] Access to Eurodac by Member State police and law enforcement authorities – Council Conclusions. Available at: http://register.consilium.europa.eu/pdf/en/07/st10/st10002.en07.pdf

[32] The Treaty was signed on 27 May 2005. The seven initial contracting States are: Belgium, Germany, Spain, France, Luxembourg, the Netherlands and Austria. It entered into force in Austria and Spain on 1 November 2006 and in Germany on 23 November 2006.

[33] Draft Council Decision on the implementation of Decision 2007/ /JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (Document 11896/07) .

implementing provisions are to be contained, not in the Decision itself, but in 'a manual as stated in Article 18', which will be formulated and agreed at a later stage outside the normal procedures for Council legislation and in the absence of scrutiny by both the European and national parliaments.

In addition, the Prüm Decision complicates the already complicated patchwork of rules governing data protection in the law enforcement field at EU level. While the European Data Protection Supervisor (EDPS) believes that the relevant provision in the Decision offer in substance an appropriate protection, he points out that they are intended to build on a general framework for data protection that has not been adopted. As stated in his formal Opinions, the Prüm Decision should build on a general framework of data protection in the third pillar, and should not be adopted before the adoption of a framework on data protection guaranteeing an appropriate level of data protection.[34] In practice, however, this order has been reversed: legislation facilitating exchange of data is adopted before an adequate level of data protection is guaranteed.

Data protection

Data protection is central to measures on enhanced police cooperation – and the need to guarantee the former while improving the latter is an obligation under Article 30(1)(b) of the EU Treaty. As repeatedly highlighted by the EDPS, current data protection standards are inadequate: there is no common legal framework on the level of the EU in the area of police cooperation that meets basic criteria of consistency and effectiveness. Different rules apply for the same situations, existing EU agencies and databases have their own, fragmented regimes of data protection (with their respective joint supervisory authorities); there is further fragmentation in the light of the persistence of the pillars (the European Data Protection Supervisor is for instance responsible for the first pillar aspects of Schengen but not for the third pillar).

A proposal for a Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (third pillar) was adopted by the Commission in October 2005.[35] This proposal was based closely on Directive 95/46 which governs all processing of personal data in the fields of Community law (i.e. in the various spheres of economic and social activity commonly referred to as first pillar).[36] Member States have failed to date to found unanimous agreement on the proposal.

In March 2007, the German Presidency submitted a fresh proposal for a third pillar Data Protection Framework Decision.[37] It is a simplified version of previous proposal, with many provisions stating no more than basic principles. It is an overall weaker text, likely perhaps to get the unanimous agreement that is needed in the Council, but unlikely to provide sufficient protection to individuals and ensure the quality and reliability of the law enforcement data exchanged. The EDPS has voiced strong concerns, particularly on the following:

[34] See the Opinions on data protection and the third pillar: [2007] OJ C 139/1, [2007] OJ C 91/9, [2006] OJ C 47/27.
[35] COM(2005) 475 final, 4 October 2005.
[36] OJ L 281, 23 November 1995.
[37] Council document 7315/07, 13 March 2007.

- The exclusion of domestic data from the scope the proposal;
- Lack of any distinction between different kinds of data subjects (suspects, convicted people, victims, witnesses, etc.);
- No adequate rules governing transfer of data to and from third countries;
- No provisions addressing the risks of the use of biometric data and DNA profiles.[38]

The lack of an adequate regulatory framework for data protection in this field will become particularly acute when plans on the interoperatibility of existing and future EU databases are developed. An adequate regulatory framework is also of vital importance to address the risks brought about by the move to extend police access to first pillar databases, to allow biometric searches, and by the expanding practices of profiling. The adoption of the third pillar Framework Decision providing adequate data protection standards is a high priority. The adequacy of the current data protection systems to address issues of interoperability and use of biometrics must be addressed as a matter of priority. The issue of remedies for misuse of data must also be examined.

Conclusions

From the above overview it appears that the EU counter-terrorism and police co-operation measures are based largely on the gathering and exchange of personal data. This objective is achieved by the growing monitoring of financial transactions, the creation and development of EU databases, the attempts to link such databases, regardless of their content and purpose, and the attempts to boost the speedy and "no questions asked" exchange of information between national law enforcement authorities. These developments may lead to the maximisation of surveillance via the collection of a wide range of personal data and thus pose significant challenges to privacy and data protection. This is true in particular in the light of the fragmentation of the EU data protection framework applying to the various databases and forms of information exchange. In the light of these challenges - and the considerable challenges to transparency and democratic scrutiny that the current procedures for the adoption of third pillar legislatives instruments and the mechanisms for monitoring the EU databases -, both the issues of the protection of privacy as a constitutional value and the enhanced transparency and democratic debate, as to the future developments of counter-terrorism policy, need to be put at the heart of the debate.

[38] EDPS Opinion [2007] OJ C 139/1.