2011

Privacy and data protection in the EU-security continuum

Gloria Gonzàlez-Fuster
Paul De Hert
Serge Gutwirth

in:ex
Converging and conflicting ethical values in the internal/external security continuum in Europe
European Commission, 7th Framework Programme

CENTRE FOR EUROPEAN POLICY STUDIES
Thinking ahead for Europe

INEX Policy Brief

Privacy and Data Protection in the EU Security Continuum

Gloria González Fuster, Paul De Hert and Serge Gutwirth

No. 12 / June 2011

ABSTRACT

There is no doubt that EU measures on the automated processing of data on individuals have an impact on fundamental rights. But which fundamental rights are more deeply affected by them? And how should these rights be safeguarded to ensure the effective protection of individuals and democratic societies? This Policy Brief highlights a series of elements that are critical to addressing the legal dilemmas arising in this area and puts forward recommendations based on research undertaken for the INEX project (Work Package 2).

SEVENTH FRAMEWORK PROGRAMME

Research for this Policy Brief was conducted in the context of Work Package 2 of INEX, a three-year project on converging and conflicting ethical values in the internal/external security continuum in Europe, funded by the Security Programme of DG Enterprise of the European Commission's Seventh Framework Research Programme. The project is coordinated by PRIO, International Peace Research Institute in Oslo. For more information about the project, please visit: www.inexproject.eu

PRIO
International Peace Research Institute, Oslo

PRIVACY AND DATA PROTECTION IN THE EU SECURITY CONTINUUM

INEX POLICY BRIEF NO. 12/JUNE 2011

GLORIA GONZÁLEZ FUSTER, PAUL DE HERT AND SERGE GUTWIRTH*

Be it in the name of security, in the name of mobility control or in the name of these two "twin objectives",[1] the automated processing of data related to individuals has been and continues to be strongly promoted by the EU. The practices supported by EU institutions range from the creation of large-scale databases to store information, which can include biometric data,[2] to the adoption of legal instruments that impose the massive processing of information on the everyday activities of all individuals moving across the EU's territory, on their communications or their financial transactions. They can also involve the transfer of data to specialised EU agencies, such as Europol or Eurojust or to the 'competent authorities' of third countries, to mention a few examples.

There is no doubt that these measures have an impact on fundamental rights. But which fundamental rights are more deeply affected by them? And how should these rights be safeguarded to ensure the effective protection of individuals and democratic societies? This Policy Brief highlights a series of elements that are critical to addressing the legal dilemmas arising in this area. The paper reviews them in the light of the results of research undertaken for Work Package 2 of the INEX project,[3] under the title "Cross-border legal dilemmas of the internal/external security continuum".[4]

1. Data processing needs to comply with the requirements of the Council of Europe regarding the right to respect for private life and the EU legal framework for personal data protection. As repeatedly recalled by the European Court of Human Rights (ECtHR), storing information about persons can constitute an interference with their right to respect for private life as established by Art. 8 of the European Convention on Human Rights (ECHR). This implies that any decision to record data about individuals is only acceptable if it pursues a legitimate interest, if it is taken in accordance with the law and if it is necessary in a democratic society.

---

* Gloria González Fuster is a researcher at the Law, Science, Technology & Society (LSTS) Research Group of the Vrije Universiteit Brussel (VUB). Paul De Hert is a professor at the Tilburg Institute for Law, Technology and Society (TILT) and at the VUB, as well as a member of the VUB's LSTS. Serge Gutwirth is a professor at the VUB and chairman of the VUB's LSTS.

[1] Citing migration management and the fight against crime as "twin objectives" of border management, see European Commission, Communication on the EU Internal Security Strategy in Action: Five Steps Towards a More Secure Europe, COM(2010) 673 final, Brussels, 22 November 2010(d), p. 11.

[2] For example, this is the case for Eurodac, the not-yet operative Visa Information System (VIS) and Schengen Information System (SIS) II.

[3] More information on the INEX project, funded by the European Commission, can be found on the INEX project website (http://www.inexproject.eu/).

[4] For specific policy recommendations regarding the Schengen Information System, see Joanna Parkin, *The Intersection between the Schengen Information System and the EU Rule of Law*, INEX Policy Brief, CEPS, Brussels, 2011 (forthcoming).

Additionally, the EU legal framework foresees a series of safeguards for the processing of any data that can be legally qualified as 'personal', i.e. data that refers to identified or identifiable individuals. Since the entry into force of the Lisbon Treaty in 2009, the protection of personal data defined in such terms has been formally elevated to the status of a fundamental right in the EU. Therefore, it is now more important than ever for EU institutions to ensure that any initiative leading to the processing of personal data respects all the core elements of this emergent right, as described by Art. 8 of the EU Charter of Fundamental Rights.[5]

Yet, the current importance placed on the right to the protection of personal data should not lead to any disregard of the fact that the obligation to comply with Art. 8 of the ECHR (which is echoed in Art. 7 of the EU Charter of Fundamental Rights) remains as relevant as ever and the scope of application of this right can cover the processing of data not relating to any identified or identifiable individual, but to 'unidentifiable' people's movements, activities, behaviours or their environment. Practices that do not constitute a personal data protection issue *strictu sensu* can still represent an infringement of the right to privacy – and vice versa. *EU institutions should never limit the assessment of the impact on fundamental rights of security measures that comprise the processing of personal data to an assessment of their compliance with data protection law.*[6]

2. The mere storage of data, as well as the broadening of access to existing databases, can also have other consequences for fundamental rights and notably constitute stigmatising and discriminating measures.[7] The possible negative impact of processing data about individuals is not limited to infringements of the right to respect for private life or the right to the protection of personal data. Imposing the use of some data processing practices for some categories of individuals can have important consequences in terms of stigmatisation and discrimination of the affected individuals.

The case law of the highest European courts has highlighted such outcomes. In its judgment of the case *S. and Marper v. United Kingdom*,[8] Strasbourg's ECtHR underscored that retaining the biometric data of innocent persons in a database used for criminal identification purposes presented risks of stigmatisation, notably because individuals entitled to the presumption of innocence were being treated in the very same way as convicted persons. The Court noted that although the retention of data of an innocent person did not exactly equate with the voicing of suspicion, the innocent person's perception of not being treated as innocent could be heightened as his/her data were stored indefinitely, just like those of convicted persons.[9]

In a different context, Luxembourg's European Court of Justice (ECJ) observed (in the *Huber* judgment)[10] that the use for crime-fighting purposes of a system for processing the personal data of non-national EU citizens, in the lack of an equivalent data processing system for nationals, is

---

[5] See the Charter of Fundamental Rights of the European Union, OJ C 83, 30.3.2010, pp. 389-403.

[6] An extremely problematic case of limited assessment of a proposed measure's impact on fundamental rights with respect to its effects on personal data protection can be seen in the European Commission's *Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, COM(2011) 32 final, Brussels, 2 February 2011, pp. 8-9.

[7] On this point, see notably Gloria González Fuster, Paul De Hert, Erika Ellyne and Serge Gutwirth, *Huber, Marper and Others: Throwing new light on the shadows of suspicion*, INEX Policy Brief No. 11, CEPS, Brussels, June 2010.

[8] See the case *S. and Marper v. The United Kingdom*, Applications nos. 30562/04 and 30566/04, European Court of Human Rights, Judgment of 4 December 2008 (hereinafter, *Marper*).

[9] *Marper* § 122.

[10] Refer to Case C-524/06, *Huber v. Germany* [2008] ECR I-09705, European Court of Justice, Judgment of 16 December 2008.

contrary to the principle of non-discrimination of EU citizens. In his Conclusions for the case, Advocate General Poiares Maduro pointed out that the coexistence of different data processing practices for nationals and for non-national EU citizens cast an "unpleasant shadow" over non-national EU citizens.

Specific data processing practices can also put pressure on other fundamental rights – such as the freedom of expression and the freedom of religion, especially if they rely on religious or political characteristics as parameters or if they target particular groups or activities – as well as the principles of criminal law, including the presumption of innocence. *Therefore it is imperative that EU institutions assess the impact of security measures, taking into account the full range of fundamental rights and legal principles that could be affected.*

3. Currently, third-country nationals are particularly exposed to the negative impact of EU-supported data processing practices. Fundamental rights, such as the right to privacy and the right to the protection of personal data, are not exclusively aimed at the protection of EU citizens, but generally of 'everyone' and thus also third-country nationals. The rights of the latter, however, are especially vulnerable in the face of the persistent deployment of EU-supported data processing measures. These measures range from the creation of large-scale information systems (the so-called 'digital borders' of the EU) to the reliance on modern surveillance technologies for the control of the EU's external physical borders, and include the pressure to expand the powers of the European Agency for the Management of Operational Cooperation at the External Borders (FRONTEX). A current trend towards the progressive interconnection of the digital borders and linkage with systems of surveillance of physical borders represents a major challenge in this area.[11] In this sense, any progress towards the *interoperability* of information systems (including their possible management through a single EU agency) cannot be accepted without taking into account the consequences for the right to privacy, the core principles of data protection and the need to restrain all the negative effects of such progress. *Just as the EU institutions acknowledge that the fundamental rights of EU citizens must be placed at the centre of the development of an Area of Freedom, Security and Justice (AFSJ),*[12] *they should also explicitly place the individual's fundamental and human rights at the core of border management.*

4. Lack of privacy and data protection are too often the result of EU institutions imposing data processing practices without simultaneously substantiating the necessary safeguards. The particular dynamics of EU integration have been facilitating the proliferation of situations in which data processing measures are adopted and implemented while effective privacy and personal data protection are deferred to another time, delegated to different actors, or both postponed and handed over to another level of decision-making. And this can have dramatic consequences for the effective assurance of fundamental rights.

The problems with Directive 2006/24/EC, the Data Retention Directive,[13] can be regarded as an example of this phenomenon. Under the Data Retention Directive, telecommunication companies are required to store communication traffic data for a period of between six months

---

[11] See Gloria González Fuster and Serge Gutwirth, "When 'digital borders' meet 'surveilled geographical borders': Why the future of EU border management is a problem", in Peter Burgess and Serge Gutwirth (eds), *Security, Migration and Integration* (working title), Brussels: VUB Press, 2011 (forthcoming).

[12] See for instance, European Commission, Communication on an Area of Freedom, Security and Justice Serving the Citizen, COM(2009) 262 final, Brussels, 10 June 2009, p. 5.

[13] See Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, pp. 54-63.

and two years. The circumstances in which access to such data can be granted and the use of the retained data are not defined, but left to member states' discretion. It is precisely in this area that most of the (many) data protection concerns raised in the implementation of the Data Retention Directive have appeared.[14]

Problems referring to the implementation of the national measures taken in relation to Directive 2005/60/EC, the Third Money Laundering Directive[15] must also be mentioned. This Directive imposes on the regulated sector a duty to report to the national Financial Intelligence Unit (FIU) any transactions and activities that seem to involve funds that are the proceeds of criminal activity, in the form of reports. In the UK, these reports are entered into a database[16] that has been repeatedly criticised as not ensuring basic requirements for personal data protection. The criticism has highlighted the long retention periods for all reports – even those for which the 'suspicious' dimension of the activity or transaction has not been confirmed – and the wide access granted to different actors to their contents.[17] In different member states, data protection issues have emerged owing to the wide derogations and exemptions to standard safeguards granted in the name of the fight against terrorism, which is officially the general purpose of legislation in this area, despite the fact that the vast majority of flagged transactions and activities are unrelated to counterterrorism.

Another example of extremely risky lack of precaution on the part of EU institutions can be found in the European Commission's Communication with its latest proposal on the travel data of individuals flying to and from the EU and the use of such data for the sake of counterterrorism and the fight against serious crime.[18] In its Communication, the European Commission goes so far as to admit that the entire proposal is based on a definition of 'serious crime' that in various member states can include minor offences (which makes the proposal contrary to the principle of proportionality), only to add that these member states are entitled to exclude such minor offences from the scope of application of the transposing legislation.[19]

The European Commission adopted in 2010 a strategy for ensuring that the fundamental rights provided for in the EU Charter of Fundamental Rights become reality, and in this regard committed to remind member states where necessary of the importance of complying with the Charter when implementing EU law.[20] Yet when legal instruments that lead to data processing of a magnitude as that described are adopted, such reminders might be insufficient to guarantee that the rights to privacy and to personal data protection of individuals are satisfactorily guaranteed. *EU institutions should support data processing practices of this significance only if they meet all necessary requirements in terms of necessity and proportionality, and in such cases if they are to be deployed together with, and not while waiting for, clearly defined and adequate safeguards.*

---

[14] In three member states, the Constitutional Court has annulled the national law transposing the Directive.

[15] See Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, OJ L 309, 25.11.2005, pp. 15-36.

[16] The database is known as ELMER and is maintained by the Serious Organised Crime Agency.

[17] House of Lords European Union Committee, *Money laundering: Data protection for suspicious activity reports*, London: The Stationery Office Limited, 2011, p. 5.

[18] See European Commission (2011), op. cit.

[19] *Idem*, pp. 15-16.

[20] European Commission, Communication on a Strategy for the Effective Implementation of the Charter of Fundamental Rights by the European Union, COM(2010) 573, Brussels, 19 October 2010(b), p. 13.

5. Profiling is an exceptionally intrusive method of data processing requiring explicit justification. Profiling as a contemporary security practice is a data processing technique requiring the analysis of vast amounts data in order to identify patterns that seem to match the description of a threat, and based on the patterns elaborated through this procedure, select items or individuals.[21] It has infiltrated EU security through the fight against money laundering[22] and the use for law enforcement purposes of travel information of individuals travelling by plane. Relying on this technique to pursue security objectives has particular implications from a human rights perspective.

The Council of Europe's Committee of Ministers recently adopted a Recommendation on the protection of individuals with regard to the automatic processing of personal data in the context of profiling, which makes clear that profiling has its own risks.[23] According to this Recommendation, profiling can have a significant impact on the rights and freedoms of the persons affected because it puts them in predetermined categories, very often without their knowledge, and because the profiling technique is generally invisible and thus uncontrollable by the subject concerned. The Recommendation explicitly recognises that the impact of profiling is unaffected by whether the data originally processed refer to identified persons or are based on 'anonymous' observations, even though the Recommendation focuses on providing guidance for the processing of personal data defined as relating to an identified or identifiable individual.[24]

In any case, it is not enough for data processing practices relying on profiling to meet the requirements of data protection law regarding issues such as the duration of the storage of data, the data subject's rights in relation to the data processed or independent monitoring. *The very reliance on the technique of profiling needs to be justified as necessary in a democratic society and in accordance with law, this latter idea including obligations in terms of transparency and thus of publicity of the variables used to establish patterns and to flag individuals.*

6. Crime prevention is an interest that can justify interferences with the right to respect for private life, but when used as such it must be interpreted restrictively. Contemporary security practices, and especially those related to profiling and data mining, are marked by a trend towards prevention that in some cases appears to slide towards anticipation. Less concerned with preventing future crimes than with taking advance measures that could be useful if crimes were committed (and thus playing less a 'pre-emptive' function than a sort of 'preparatory' role), such practices can be described as following a reasoning of *radical prevention*, which encourages the adoption of measures *just in case* a crime is committed. In this regard, one can think of the storage of DNA data of innocent individuals, unsuspected of any crime, in criminal identification databases.

The link between crime-fighting and crime prevention is far from new, but its application in terms of the use of modern information technology, offering unprecedented capabilities in terms

---

[21] See Gloria González Fuster, Serge Gutwirth and Erika Ellyne, *Profiling in the European Union: A high-risk practice*, INEX Policy Brief No. 10, CEPS, Brussels, June 2010; and Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European citizen: Cross-disciplinary perspectives*, New York: Springer, 2008.

[22] See for instance Directive 2005/60/EC, op. cit.

[23] See Council of Europe, Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, adopted on 23 November 2010.

[24] This can be explained by the fact that the legal instrument serving as a reference for the Recommendation is the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 28 January 1981, European Treaty Series No. 108 (known as 'Convention 108').

of data collection, storage and processing, raises questions that need to be carefully considered. These relate to the very principles of criminal law, as well as to other rights, including the right to privacy. Although Art. 8(2) of the ECHR does mention "the prevention of disorder or crime" as one of the interests that can legitimately be invoked by states to justify an interference with the right to respect for private life, it must be taken into account that all constraints on human rights must be interpreted restrictively. Thus, "the prevention of disorder or crime" cannot be understood in this particular context as also covering cases where the link between the interference and the (strictly defined) prevention of crime is unclear or inexistent.

The ECtHR has not yet provided exact guidance on when the storage of data related to individuals should be justified in the name of crime prevention and when it should not.[25] *Nevertheless, circumscribing the role of crime prevention to democratically acceptable limits must be a priority when considering any measures that amount to an interference with the right to privacy.*

7. Public data are not freely available data. There is a trend in the security field to increasingly consider or even support the processing of so-called 'open source data'. This category of data would refer to data that are "publicly available", in the sense of "not intended for or restricted to a particular person, group or organisation", for instance by being accessible through the Internet.[26] The expression appears to have originated in the US, where the military has advocated the systematic collection, processing and analysis of information obtained through such data in response to intelligence requirements.[27]

From the US, such data are now reaching EU security intelligence.[28] In the EU legal framework, however, the notion of 'open source data' has no meaning:[29] it does not refer to any particular type of data and its use can create dangerous confusion. What is relevant from a European (legal) perspective is that the processing of any data, including data that could be regarded as 'publicly available' in the sense of 'not confidential', can potentially constitute interference with the right to respect for private life of individuals as guaranteed by Art. 8 of the ECHR, and thus is only permissible under strict conditions.

The ECtHR has made it clear that even though its name might seem to suggest otherwise, the right to respect for 'private life' as guaranteed by Art. 8 of the ECHR is not unconcerned with the respect for 'public life'. The European right to respect for private life is not about the protection of any 'private' sphere, nor 'private' communications or 'private' spaces, or even the places and acts for which one might have any 'expectations of privacy'. Additionally, all data, including 'publicly available' data, can potentially fall under data protection legislation, which defines 'personal data' solely taking into account whether the data refer to an identified or identifiable person, and thus regardless of whether the data are disclosed or undisclosed, accessible or inaccessible, private or public. *The use of the notion 'open source data' to drive*

---

[25] See Gloria González Fuster, Serge Gutwirth and Paul De Hert, *Analysis of the value dimensions of European law relevant to current and anticipated challenges of the internal/external security continuum*, INEX Deliverable D.2.2, INEX Project, Brussels, 2009, p. 8.

[26] See Ben Hayes, *Spying in a see through world: The "Open Source" intelligence industry*, Statewatch Analysis No. 119, Statewatch, London, 2011, p. 1.

[27] Ibid., p. 2.

[28] For instance, the European Commission is funding (through FP7) a project for the design of a "Versatile InfoRmation Toolkit for end-Users oriented Open-Sources explOitation (VIRTUOSO)".

[29] Yet it can conflict with other existing legal notions established in the member states. For instance, the Spanish legal framework regulates the use of data from 'publicly accessible sources' (*fuentes accessibles al público*), but explicitly limits the number of sources that can be considered as such, and the Internet is not one of them.

the processing of data related to individuals is, from a European standpoint, fundamentally misleading and thus should be avoided.

8. 'Privacy by design' is a policy notion with international appeal, yet in order to incorporate it into the EU legal framework, it needs to be carefully translated into EU legal terms. The 'privacy by design' motto is more and more present in EU policy documents.[30] It originated in Canada and has been spreading globally thanks to the support of the international community of data protection authorities and privacy commissioners.[31] It also seems to enjoy some backing from the industry.[32]

The European Commission has been considering the possibility of introducing the notion of 'privacy by design' into the upcoming legal instrument for a comprehensive EU legal framework on personal data protection, even if the Commission has not yet clearly expressed how the term can be translated into legal terms.[33] The European Data Protection Supervisor (EDPS), who has recurrently advocated promoting this notion,[34] envisages it as an element of accountability and considers that it refers to the integration of data protection and privacy from the very inception of new products, services and procedures that entail the processing of personal data.[35]

The introduction of the 'privacy by design' approach to EU legislation on personal data protection raises two crucial issues that have not yet been satisfactorily addressed:

a) *The first is the relation between the notion of privacy in 'privacy by design' and EU privacy and personal data protection.* Over recent years, the EU has progressively configured the protection of personal data as an autonomous fundamental right, different from the right to privacy. The idea of 'privacy by design' has nonetheless been developed mainly outside the EU, by non-EU data-protection authorities and privacy commissioners, as well as by multinational companies, which have conceptualised it by emphasising that it allows the embedding of something that they designate as 'privacy'

---

[30] Acknowledging the interest of the Council in 'privacy by design', see for instance the Justice and Home Affairs Council, 3071st meeting, Council conclusions on the Communication from the Commission to the European Parliament and the Council: A comprehensive approach on personal data protection in the European Union, Brussels, 24 and 25 February 2011, p. 4.

[31] See for example the Resolution on Privacy by Design, adopted by the 32nd International Conference of Data Protection and Privacy Commissioners, Jerusalem, 27-29 October 2010.

[32] See for instance, Microsoft, "Privacy by Design at Microsoft", November, Seattle, WA, 2010; the European Security Research and Innovation Forum (ESRIF) has also expressed its backing (see the *ESRIF Final Report*, ESRIF, Brussels, December 2009 p. 205).

[33] The services of the European Commission appear actually to be struggling to determine how the term 'privacy by design' should be translated into the different official languages of the EU. Taking as main reference COM(2010) 609 final (European Commission, Communication on a Comprehensive Approach on Personal Data Protection in the European Union, Brussels, 4 November 2010(c), p. 13), it is interesting to note that in some languages (such as Italian) the expression has been adopted as such and no translation has been attempted, whereas others (re)interpret the idea of 'by design' as 'from conception' (in the French and Portuguese versions, i.e. «*principe de prise en compte du respect de la vie privée dès la conception*» and "*privacidade desde a concepção*") or replace the entire concept with a reference to "embedded data protection" (in German, "*mit eingebautem Datenschutz*").

[34] See European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – "A comprehensive approach on personal data protection in the European Union", EDPS, Brussels, 14 January 2011.

[35] Ibid., p. 23.

into different practices.[36] But what kind of 'privacy' is exactly being referred to in this respect? Is it what the EU legal framework currently regards as 'privacy'[37] or the peculiar 'informational privacy' that the global 'privacy community' commonly hides under such a term?[38] If the latter option appears to be more accurate, then privacy by design might just be an unlucky term to refer to 'data protection by design'. In this case, it would be more appropriate to speak of data protection by design, since privacy covers both a broader and a narrower scope than data protection: privacy violations can occur without any violation of data protection law, and not every violation of data protection is a violation of privacy.

b) *The second is the possibility to incorporate into a legal instrument an organisational notion that is based on the idea of ensuring respect of the legal framework.* It is undisputed that those who are responsible for the processing of personal data should comply with the pertinent data protection laws. And it is certainly beneficial to encourage them to remember that they have to do so before it is too late. What could be dangerous, however, is if the legislator incorporates into mandatory rules a notion that some tend to interpret not as an invitation to embed into their own practices the requirements of privacy and personal data protection as defined by legal and judicial practice, but as an enticement to reinterpret the content of privacy in the light of their own interests. 'Privacy by design' cannot be perceived as meaning 'design your own privacy', but should focus on the search for ways to satisfactorily articulate legal requirements and non-legal practices.

EU institutions urgently need to clarify the relationship between 'privacy by design' and the EU rights to privacy and personal data protection.

9. The review of the Data Protection Directive (95/46/EC) is a major opportunity to restate the importance of personal data protection and increase its effectiveness, including with respect to cross-border data flows.

In the next few years the EU is to establish a comprehensive, personal data protection scheme that is to cover all areas of EU competence and at the same time be a driving force behind the development and promotion of international standards for personal data protection and for the conclusion of appropriate bilateral or multilateral instruments.[39] These two objectives (namely, reinforcing personal data protection within and outside EU territory) cannot be envisaged independently.

The work towards comprehensive, personal data protection in all areas of EU competence has been marked by the European Commission's publication of a Communication taking as a starting point the possible review of the Data Protection Directive (95/46/EC).[40] This Directive had originally been drafted at a time when the very possibility for EU institutions to legislate on issues touching upon the protection of fundamental rights was debated. The current challenge

---

[36] For instance, it has been asserted that "[p]rivacy by [d]esign refers to the philosophy and approach of embedding privacy into the design, operation and management of information technologies and systems, across the entire information life cycle" (Resolution on Privacy by Design, 2010, op. cit.).

[37] This is anchored in Art. 8 ECHR and Art. 7 of the EU Charter of Fundamental Rights.

[38] On the monopolisation of privacy through issues related to the automated processing of personal data, see Serge Gutwirth, *Privacy and the information age*, Oxford: Rowman & Littlefield Publishers, 2002, p. 2.

[39] See European Commission (2009), op. cit., p. 8.

[40] Refer to Directive 95/46/EC of the European Parliament and Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, pp. 31-50.

for EU institutions is to move decidedly from the provisions originating in those circumstances to a new instrument that must be fully consistent with the entry into force of the Lisbon Treaty, which formally establishes the right to the protection of personal data as an autonomous fundamental right and obliges the EU legislator to secure it across EU competences.

In this context, regulating cross-border transfers of personal data triggers a significant number of legal dilemmas. The most critical one concerns the need to establish rules on applicable law that ensure the direct applicability of the member states' data protection legislation even when personal data are processed outside the borders of the EU, as soon as there is a justified claim of applying EU law.[41] This is crucial for EU personal data protection to be effective. Existing rules on applicable law are not only complex,[42] but also unable to provide any assurance to EU citizens that EU data protection will be applicable to data processing situations brought about by their daily on-line or off-line activities. *By revising such rules, the EU legislator would not only contribute to the effectiveness of personal data protection within the EU, but would also strategically reinforce its position and credibility in the development and promotion of international standards for personal data protection and in relation to the conclusion of any international agreements regarding data protection safeguards for non-covered data transfers.*

10. The trend towards positively integrating fundamental rights into EU political discourses should not divert attention away from the reality that, at least in some cases, these rights must play a countering role. The much-criticised portrayal of security and liberty as opposing values in a zero-sum game (sometimes expressed in terms of *security vs. privacy*)[43] seems to be a thing of the past. Currently, the message coming out of EU institutions could be summarised as follows: security and fundamental rights can only coexist and develop in a series of *win–win* situations; they go "hand in hand".[44] The reliance on this kind of imagery certainly has its positive effects, such as emphasising the potentially constructive contribution to EU policies of actors that are directly concerned with fundamental rights' protection and continually involved in dialogue with the EU legislator, such as the EDPS. Nevertheless, it can also distract from the reality that fundamental rights are not always expected to push in the same direction as concerns about security and mobility control. The right to privacy and also the right to the protection of personal data, just as any other fundamental rights, by definition carry a degree of resisting strength. It might be the power to oppose certain intrusive practices, as with the right to privacy, or to impose a series of obligations on those implementing data processing measures, as with the right to the protection of personal data. Deprived of such a function of resistance, fundamental rights are ultimately transformed into mere enabling factors of the very policies that, at least in some circumstances, they are supposed to be able to transform.

---

[41] European Data Protection Supervisor (2011), op. cit., p. 25.

[42] See the Opinion of the Article 29 Data Protection Working Party (Opinion 8/2010 on applicable law, WP179), adopted on 16 December 2010, p. 5.

[43] See Gloria González Fuster, Paul De Hert and Serge Gutwirth, *State-of-the-art of the Law–Security Nexus in Europe*, INEX Deliverable D.2.1, INEX Project, Brussels, 2008, pp. 4-5.

[44] European Commission, Communication on Delivering an Area of Freedom, Security and Justice for Europe's Citizens: Action Plan Implementing the Stockholm Programme, COM(2010) 171 final, Brussels, 20 April 2010(a), p. 3.

References

European Commission (2009), Communication on an Area of Freedom, Security and Justice Serving the Citizen, COM(2009) 262 final, Brussels, 10 June.

————— (2010a), Communication on Delivering an Area of Freedom, Security and Justice for Europe's Citizens: Action Plan Implementing the Stockholm Programme, COM(2010) 171 final, Brussels, 20 April.

————— (2010b), Communication on a Strategy for the Effective Implementation of the Charter of Fundamental Rights by the European Union, COM(2010) 573, Brussels, 19 October.

————— (2010c), Communication on a Comprehensive Approach on Personal Data Protection in the European Union, COM(2010) 609 final, Brussels, 4 November.

————— (2010d), Communication on the EU Internal Security Strategy in Action: Five Steps Towards a More Secure Europe, COM(2010) 673 final, Brussels, 22 November.

————— (2011), *Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, COM(2011) 32 final, Brussels, 2 February, pp. 8-9.

European Data Protection Supervisor (EDPS) (2011), Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – "A comprehensive approach on personal data protection in the European Union", EDPS, Brussels, 14 January.

European Security Research & Innovation Forum (ESRIF) (2009), *ESRIF Final Report*, ESRIF, Brussels, December.

González Fuster, Gloria and Serge Gutwirth (2011), "When 'digital borders' meet 'surveilled geographical borders': Why the future of EU border management is a problem", in Peter Burgess and Serge Gutwirth (eds), *Security, Migration and Integration* (working title), Brussels: VUB Press, forthcoming.

González Fuster, Gloria, Paul De Hert and Serge Gutwirth (2008), *State-of-the-art of the Law–Security Nexus in Europe*, INEX Deliverable D.2.1, INEX Project, Brussels.

González Fuster, Gloria, Paul De Hert, Erika Ellyne and Serge Gutwirth (2010), *Huber, Marper and Others: Throwing new light on the shadows of suspicion*, INEX Policy Brief No. 11, CEPS, Brussels, June.

González Fuster, Gloria, Serge Gutwirth and Erika Ellyne (2010), *Profiling in the European Union: A high-risk practice*, INEX Policy Brief No. 10, CEPS, Brussels, June.

González Fuster, Gloria, Serge Gutwirth and Paul De Hert (2009), *Analysis of the value dimensions of European law relevant to current and anticipated challenges of the internal/external security continuum*, INEX Deliverable D.2.2, INEX Project, Brussels.

Gutwirth, Serge (2002), *Privacy and the information age*, Oxford: Rowman & Littlefield Publishers.

Hayes, Ben (2011), *Spying in a see through world: The "Open Source" intelligence industry*, Statewatch Analysis No. 119, Statewatch, London.

Hildebrandt, Mireille and Serge Gutwirth (eds) (2008), *Profiling the European citizen: Cross-disciplinary perspectives*, New York: Springer.

House of Lords European Union Committee (2011), *Money laundering: Data protection for suspicious activity reports*, London: The Stationery Office Limited.

Justice and Home Affairs Council (2011), 3071st meeting, Council conclusions on the Communication from the Commission to the European Parliament and the Council: A comprehensive approach on personal data protection in the European Union, Brussels, 24 and 25 February.

Microsoft (2010), "Privacy by Design at Microsoft", November, Seattle, WA.

Parkin, Joanna (2011), *The Intersection between the Schengen Information System and the EU Rule of Law*, INEX Policy Brief, CEPS, Brussels, forthcoming.