in:ex Converging and conflicting ethical values in the internal/external security continuum in Europe

European Commission, 7th Framework Programme

CEPS CENTRE FOR EUROPEAN POLICY STUDIES

Thinking ahead for Europe

INEX Policy Brief

# *Huber, Marper* and Others:

# Throwing new light on the shadows of suspicion

**Gloria González Fuster, Paul De Hert, Erika Ellyne and Serge Gutwirth**

**No. 8 / June 2010**

**ABSTRACT:** The proliferation of large-scale databases containing personal information, and the multiple uses to which they can be put can be highly problematic from the perspective of fundamental rights and freedoms. This paper discusses two landmark decisions that illustrate some of the risks linked to these developments and point to a better framing of such practices: the *Heinz Huber v. Germany* judgement, from the European Court of Justice, and the *S. and Marper v. United Kingdom* ruling, from the European Court of Human Rights. The paper synthesises the lessons to be learnt from such decisions. Additionally, it questions the impact of the logic of *pure prevention* that is being combined with other rationales in the design and management of databases.

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

# *HUBER, MARPER* AND OTHERS:

# THROWING NEW LIGHT ON THE SHADOWS OF SUSPICION

## *INEX POLICY BRIEF NO. 8 / JUNE 2010*

**GLORIA GONZÁLEZ FUSTER, PAUL DE HERT, ERIKA ELLYNE AND SERGE GUTWIRTH***

All over the European Union (EU), large-scale databases containing personal information are regularly being created, fed, expanded, altered or enriched with data of a very varied nature. Some of these information systems are the result of national policies of member states, while others are born or redesigned under the main impulse of EU institutions, notably in the so-called Area of Freedom, Security and Justice (AFSJ).[1] Access to their content tends to be widened systematically,[2] they are sometimes interconnected, and their data is often processed not only for the purpose that originally justified its collection, but also for new and unrelated purposes, transforming the databases into multi-functional, hybrid information systems.

These developments can have serious consequences for the fundamental rights and freedoms of individuals. But how should they be framed in order to counter such negative repercussions? Which requirements should be taken into account? Which questions need to be asked before decisions can be taken? Two landmark judgements, one from the European Court of Justice and

* 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. Erika Ellyne is a researcher at VUB's LSTS. Serge Gutwirth is a professor at the VUB and chairman of VUB's LSTS.

[1] Notions related to information-sharing strategies such as the 'principle of availability' and 'interoperability' have been instrumental in this sense. See, for instance: European Commission (2005a), *Proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM(2005) 490 final)*, 12.10.2005, Brussels); and European Commission (2005b), *Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs*, COM(2005) 597 final, 24.11.2005, Brussels (on this Communication, see Paul De Hert and Serge Gutwirth (2006), "Interoperability of Police Databases within the EU: An Accountable Political Choice?", *International Review of Law, Computers & Technology*, 20(1&2), pp. 21-35). See also Florian Geyer (2008), *Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice*, CEPS Research Paper No. 9, Brussels, May.

[2] See, for instance, Council Decision 2008/633/JHA of 23 June 2008, concerning access for consultation of the Visa Information System (VIS) by designated authorities of member states and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, OJ L 218, 13.08.2008, pp. 129-136. See also, commenting this general tendency: European Data Protection Supervisor (EDPS) (2009), *Opinion on the Amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No [.../...][establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], and on the Proposal for a Council Decision on requesting comparisons with EURODAC data by member states' law enforcement and Europol for law enforcement purposes*, 7 October, Brussels, p. 4.

the other from the European Court of Human Rights, help to better understand the issues at stake and delineate some essential conditions to be respected.

## 1. Huber and discrimination among EU-Citizens

The first ruling to be considered was delivered on 16 December 2008 by the European Court of Justice in the *Heinz Huber v. Germany* case.[3] The proceedings dealt with the existence in Germany of a centralised, nationwide database containing information on non-German EU citizens for the sake of applying the law relating to the right of residence, and its use by German authorities to fight crime. The register was in place even though no similar register had ever been created to store equivalent information on German citizens, so no equivalent processing of German citizens' personal data ever took place. The European Court of Justice was required to examine different questions[4] in relation to the existence of such a database and the secondary use of its content. It soon appeared that the issue of discrimination was at the very core of the case.

Indeed, the European Court of Justice concluded that the database discussed was not contrary to Community law insofar as it contained only the data necessary for the application of the residence legislation, and insofar as its centralised nature enabled such legislation to be more effectively applied.[5] However, it established that its use for crime fighting purposes had to be interpreted as the putting in place of a system of processing for personal data precluded by the principle of non-discrimination of EU-citizens.[6] In its assessment, the Court took the view that, as the fight against crime necessarily involves the prosecution of crimes and offences committed irrespective of the nationality of their perpetrators, it follows that, as regards a member state, the situation of its nationals cannot be different in relation to this objective from that of non-national EU citizens who are resident on its territory.[7]

The Advocate General appointed to the case, Poiares Maduro, had arrived at the same conclusion concerning the discriminatory nature of the processing of the registered personal

---

[3] *Huber v. Germany*, European Court of Justice, Case C-524/06, Judgement of 16 December 2008, following a request for a preliminary ruling made by the Higher Administrative Court of the federal state of North-Rhine Westphalia, in proceedings between an Austrian national resident in Germany (Mr. Huber) and the Federal Republic of Germany (hereafter, '*Huber'*). See, on this judgement: Lucioni, Carlo (2009), "Tutela dei dati personali del cittadino dell'Unione e giudizio di non discriminazione in base alla nazionalità", *Diritto pubblico comparato ed europeo*, No. 2, pp. 575-582; and D. Martin (2009), "Comments on *Förster* (Case C-158/07 of 18 November 2008), *Metock* (Case C-127/08 of 25 July 2008) and *Huber* (Case C-524/06 of 16 December 2008)", *European Journal of Migration and Law*, No. 11, pp. 95-108.

[4] Concretely, whether the storage of personal data of foreign citizens of the EU in a central register, when no equivalent storage applies for nationals, is compatible with the prohibition of discrimination of nationality against EU citizens who exercise their right to move and reside freely within the EU territory, with the prohibition of restrictions on the freedom of establishment of nationals of a Member State in the territory of another Member State, and with the requirement of necessity under Article 7(e) of the Data Protection Directive (Directive 94/46/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).

[5] The ECJ expressly stated that the storage and processing of personal data in such a register for statistical purposes could not, in any case, be considered necessary in that sense.

[6] As established by Article 12(1) of the Treaty the European Community (TEC), now Article 18(1) of the Treaty on the Functioning of the European Union (TFEU): "Within the scope of application of the Treaties, and without prejudice to any special provisions contained therein, any discrimination on grounds of nationality shall be prohibited".

[7] *Huber*, §§ 78-79.

data for the sake of crime fighting.[8] Poiares Maduro had pointed out that the coexistence of different data processing practices, one for nationals and the other for non-national EU citizens – the latter being much more strictly and systematically monitored – casts an "unpleasant shadow" over non-national EU citizens.[9] The Advocate General underlined that, although the combating of crime and threats to security can be a legitimate public policy reason qualifying rights granted by Community law, it cannot justify the difference in treatment between nationals and non-nationals that are citizens of other member states: member states cannot invoke such an aim selectively.[10]

The importance of the *Huber* judgement lies in the emphasis put on the issue of discrimination, and in particular on the indirect effects of foreseeing secondary uses of information originally stored for other purposes. It warns against the temptation, apparently regularly experienced by policy-makers, to allow for the use of any existing database or available data for the purpose of crime fighting.[11] The grounds for and limits to such initiatives are often sought in the nature of the crimes to be investigated, as if the seriousness of some crimes could justify all kinds of data processing operations. The ruling, however, recalls that these decisions need also imperatively to take into account the *shadows of suspicion* that are de facto projected by different data processing practices.

## 2. Marper and the stigmatisation of the innocent

Another crucial judgement in relation to the challenges of large-scale databases containing personal information was pronounced by the European Court of Human Rights on 4 December 2008, in the *S. and Marper* case.[12] The proceedings concerned two non-convicted individuals who wanted to have their records removed from the DNA database used for criminal identification in the United Kingdom.[13] More concretely, they asked for their fingerprints, cellular samples and DNA profiles, which had been obtained by police, to be destroyed.[14]

---

[8] Poiares Maduro (2008), *Opinion of Advocate General Poiares Maduro in Case C-524/06 (Heinz Huber v Bundesrepublik Deutschland)*, delivered on 3 April 2008.

[9] Poiares Maduro, op. cit., § 5.

[10] Poiares Maduro, op. cit., § 21. Additionally, Maduro considered that granting access to a system such as the one at issue in the proceedings to public authorities other than immigration authorities is incompatible with Article 8 of the European Convention of Human Rights (ECHR) and, therefore also with the requirements of necessity under Article 7(e) of the Data Protection Directive (ibid., § 27, § 32).

[11] See, for instance, European Commission (2005a), op. cit., p. 10.

[12] *S. and Marper v. The United Kingdom*, Applications nos. 30562/04 and 30566/04, European Court of Human Rights, Judgement of 4 December 2008 (hereafter, *'Marper'*). See, on this judgement, Daniel De Beer De Laer, Paul De Hert, Gloria González Fuster and Serge Gutwirth (2010), "Nouveaux éclairages de la notion de 'donnée personnelle' et application audacieuse du critère de proportionnalité. Cour européenne des droits de l'homme Grande Chambre S et Marper c. Royaume Uni, 4 décembre 2008", *Revue Trimestrielle des Droits de l'Homme*, No. 81, pp. 141–161; Paul De Hert and Karen Weis (2009), "Het voor onbepaalde tijd bijhouden van vingerafdrukken, celstalen en DNA profielen van vrijgesproken personen schendt het recht op eerbiediging van hun privé-leven. Noot bij E.H.R.M., 4 december 2008 (Marper)", *Vigiles: Tijdschrift voor politierecht*, 2(15), 2, pp.71–78; Gloria González Fuster (2009), "TJCE - Sentencia de 04.12.2008, S. y Marper c. Reino Unido", *Revista de Derecho Comunitario Europeo*, mayo-agosto (33), pp. 619-633.

[13] As criminal proceedings against them had ended with an acquittal or had been discontinued (*Marper*, § 3).

[14] The applicants based their application on Articles 8 and 14 of the ECHR.

In its ruling, the Court established that it is contrary to the requirements of Council of Europe's European Convention of Human Rights (ECHR)[15] to store for unlimited periods of time that type of personal information related to innocent people in a database of that nature.[16] It concluded that the blanket and indiscriminate nature of the powers granted to UK authorities constituted a disproportionate interference with the applicants' right to respect for private life, and could not be considered as necessary in a democratic society,[17] amounting therefore to a violation of Article 8 of the ECHR.[18]

One of the major lessons to be learnt from the assessment of the European Court of Human Rights in the *Marper* case is that the storage of data such as fingerprints, cellular samples and DNA profiles in a database such as the one under examination is not inconsequential, irrelevant or neutral. On the contrary, the mere storage of such information conveys by itself a risk of stigmatisation:[19] *shadows of suspicion*, one could say, are projected upon those whose data is stored in a database dedicated to criminal identification and mainly destined to the storage of data of convicted people. Therefore, the storage of such data, when related to non-convicted individuals, has to be somehow limited.[20] If conveniently limited, it could be considered in accordance with the requirements of the ECHR.

But how should the applicable limits be determined? In the *Marper* judgement, the European Court of Human Rights underlined that the core principles of data protection require the retention of data to be proportionate in relation to the purpose of collection and that they insist on the importance of foreseeing limited periods of storage.[21] Comparing such requirements with the blanket and indiscriminate nature of the power of retention granted in England and Wales, it judged this power to be a disproportionate interference with the applicants' right to respect for private life, which cannot be regarded as necessary in a democratic society and thus is a violation of Article 8 of the ECHR.

Nevertheless, the idea that the duration of the retention of data needs to be proportionate to the 'purpose of collection' triggers, in situations like the one under examination, some problematic issues that were left unclear in the ruling. These problematic issues are linked to the fact that in

---

[15] Council of Europe (1950) *European Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No. 11*, Rome, 4 November.

[16] As such storage represents an interference with the right to respect for private life established by Article 8 ECHR (*Marper*, § 77 and § 86) that cannot be judged proportionate.

[17] *Marper*, § 125.

[18] Art. 8 of the ECHR states: "(1) Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

[19] *Marper*, § 122. Moreover, the Court highlighted that the stigmatisation can be especially harmful when minors are concerned (ibid., § 124). For a discussion of the significance of the judgement in terms of warning against risks of stigmatisation, see Rocco Bellanova and Paul De Hert (2010), "Le cas S. et Marper et les données personnelles: l'horloge de la stigmatisation stoppée par un arrêt européen", *Cultures & Conflits*, No. 76, pp. 15-27.

[20] The judgement reviews different national approaches in Europe to the taking and retention of DNA information in the context of criminal proceedings, and notes that the UK is the only Council of Europe Member State expressly to permit the systematic and indefinite retention of DNA profiles and cellular samples of persons who have been acquitted or in respect of whom criminal proceedings have been discontinued.

[21] *Marper*, § 107.

databases such as the one in question the official grounds for collecting data are, as a matter of fact, not exactly the same as those pressing for as long as possible periods of storage of the data.

## 3. Possibly even better: Dealing with the preventive logic

Two strands of logic can be identified as possibly governing the collection and storage of data in databases such as the UK DNA database and in many other comparable DNA databases in Europe. These two rationales can be described as:

- a fundamentally *post-crime* logic, by virtue of which the data is collected and stored mainly in order to facilitate the identification of criminals related to already committed crimes, in the understanding that the effectiveness of this practice might *indirectly* contribute to discouraging individuals from committing crimes in the future (and deploying, thus, a diffuse *preventive* force); and
- a *purely preventive* rationale, on account of which the data is collected and stored not because of its current usefulness but in the belief that it could be *directly* useful and relevant in the future, in the context of the identification of criminals of crimes still to be committed. This logic is totally forward-looking and demands that data is stored for periods of time as long as possible.

Nowadays the two logics generally tend to operate simultaneously, although not openly, as the *purely preventive* logic is rarely recognised in its full significance. This situation triggers much confusion in relation with the criteria that determine or should determine which data need to be collected and stored and for how long they should be stored – and such confusion tends to increase the availability of data stored in a dangerous way.[22]

Typically, data are nowadays collected on grounds that seem to respond to a *post-crime* logic (for instance, the collection is made dependent on the seriousness of an already committed crime of which the individual is suspect). Once the data are no longer required under such logic (for instance, because the individual has been acquitted), the concern is: should the data be kept in the database? If core data protection principles as recalled by the European Court of Human Rights are to be taken seriously, and thus storage needs to depend on the 'purpose of collection', and if the 'purpose of collection' was the investigation of the mentioned crime, the data must then be destroyed. Unless (and herein lies the problematic part of the reasoning) it is admitted that the 'purpose of collection' was actually not to prosecute a determined crime, but to feed a database with a *purely preventive* function. In this case, storing the data for an unlimited period would be fully consistent with the 'purpose of collection'.

In practice, the coexistence of the two logics in information systems and the ambiguities surrounding them provoke highly undesirable shifts in terms of suspicion: *undesirable shadows* are projected upon those individuals whose data is stored, as they appear to have been somehow judged to be particularly inclined to be involved in future crimes, even though there is no objective reason to believe so.

In the *Marper* judgement, unfortunately, the European Court of Human Rights failed to take into consideration with enough detail the consequences of having two different rationales concurrently operating in the same database, or even the actual legitimacy of storing data on

[22] See, on the mismatch between criteria being applied and purpose of the processing, Jacobo López Barja de Quiroga (2008), "El registro único de las huellas de ADN, la protección de datos y la investigación criminal", in A. Emaldi Cirión, E. Domínguez Peco, F. Aranda Guerrero, J. López Barja de Quiroga, J. Bayo Delgado, J.A. Martín Pallín, V. Moreno Catena, J. Salom Clotet, M. Pérez Sánchez, M. García-Herraiz Rooabert, R. Martínez Martínez and R. De Cospedal García (eds), *La protección de datos en la cooperación policial y judicial*, Thomson Aranzadi, Cizur Menor, p. 291 and p. 305.

exclusively or predominantly *preventive* grounds.[23] Endorsing the statement of the UK government according to which the retention of fingerprints and DNA data pursued the legitimate purpose of crime *detection*, the Court simply added that, because such storing pursued the *detection* of crime, it also pursued the *prevention* of crime.[24] The Court actually did acknowledge that two separate logics are in place in this kind of system: the original collection of information aims at linking a particular person to a particular crime of which he or she is suspected, whereas the retention of such data aims at another, different, purpose, i.e. assisting in the identification of offenders of future crimes.[25] Thus, it conceded that the original collection responds to what can be described as a *post-crime* function, whereas further storage is governed by a *preventive* (in a wide sense) logic, but it did not enter into any discussion of why (and when) it should be considered legitimate to use for the second purpose the data collected for the first purpose.[26] By failing to do so, it left a critical question unanswered: *why* should it be considered legitimate, in a democratic society, to store the personal data of innocent individuals for the sake of preventing the committal of future, and perhaps never to be committed crimes, even when there is no particular indication that such future possible crimes will be committed, and there is no relation whatsoever between the individuals whose data is processed and the yet uncommitted crimes? This question appears to be closely linked to the issue of how the obligations of law-enforcement authorities regarding the prevention of crime must be interpreted, and how different understandings of such a preventive mission can make the European human rights framework inconveniently vulnerable.

## 4. Concluding remarks

Decisions such as the *Huber* judgement of the European Court of Justice and the *Marper* ruling of the European Court of Human Rights need to be carefully taken into account when thinking about the design and use of large-scale databases containing personal information, in order to avoid some of their negative repercussions. By clarifying issues such as the risks of discrimination and stigmatisation conveyed by certain practices of data collection and storage, they represent two prime examples of how the judiciary can provide useful instruments to ensure that advances in this area are not detrimental to the fundamental rights and freedoms of individuals. These decisions are powerful alert signs warning against the *shadows of suspicion* that data processing practices can cast upon different categories of persons. They need to be accompanied, nevertheless, with further critical questioning of current developments, and in particular of the logic of *pure prevention* that tends to infiltrate the management of information systems.

---

[23] For a discussion of the eventual need to redefine or clarify the purposes of the UK DNA database, see Human Genetics Commission (2009), *Nothing to hide, nothing to fear? Balancing individual rights and the public interest in the governance and use of the National DNA Database*, London, p. 37.

[24] "The Court agrees with the Government that the retention of fingerprint and DNA information pursues the legitimate purpose of the detection, and therefore, prevention of crime", ibid., § 100. The notion of "prevention of disorder or crime" is mentioned in Article 8(2) of the ECHR as a possible ground to justify interferences with the right to respect for private and family life, but, as any restrictions of fundamental rights shall be interpreted restrictively, it is difficult to hold that the possible scope for that notion of prevention could be interpreted in broad terms.

[25] "While the original taking of this information pursues the aim of linking a particular person to the particular crime of which he or she is suspected, its retention pursues the broader purpose of assisting in the identification of future offenders", idem.

[26] Also lamenting this missed opportunity, Sylvie Peyrou-Pistouley (2009), "L'affaire *Marper c/ Royaume-Uni*, un arrêt fondateur pour la protection des données dans l'espace de liberté, sécurité, justice de l'Union européenne", *Revue Trimestrielle de droit européen*, 5(4), p. 746.

## References


Bellanova, Rocco and Paul De Hert (2010), "Le cas S. et Marper et les données personnelles: l'horloge de la stigmatisation stoppée par un arrêt européen", *Cultures & Conflits*, No. 76, pp. 15-27.

Council of Europe (1950), *European Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No. 11*, Rome, 4 November.

De Beer De Laer, Daniel, Paul De Hert, Gloria González Fuster and Serge Gutwirth (2010), "Nouveaux éclairages de la notion de la notion de 'donnée personnelle' et application audacieuse du critère de proportionnalité. Cour européenne des droits de l'homme Grande Chambre S et Marper c. Royaume Uni, 4 décembre 2008", *Revue Trimestrielle des Droits de l'Homme*, No. 81, pp. 141-161.

De Hert, Paul and Serge Gutwirth (2006), "Interoperability of Police Databases within the EU: An Accountable Political Choice?", *International Review of Law, Computers & Technology*, 20(1&2), pp. 21-35.

De Hert, Paul and Karen Weis (2009), "Het voor onbepaalde tijd bijhouden van vingerafdrukken, celstalen en DNA profielen van vrijgesproken personen schendt het recht op eerbiediging van hun privé-leven. Noot bij E.H.R.M., 4 december 2008 (Marper)", *Vigiles: Tijdschrift voor politierecht*, 2(15), 2, pp. 71-78.

*Directive 94/46/EC of the European Parliament and Council of 24 October 1995 on 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).

European Commission (2005a), *Proposal for a Council Framework Decision on the exchange of information under the principle of availability (COM(2005) 490 final)*, 12.10.2005, Brussels.

———— (2005b), *Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs*, COM(2005) 597 final, 24.11.2005, Brussels.

European Data Protection Supervisor (EDPS) (2009), *Opinion on the Amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No [.../...][establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], and on the Proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement and Europol for law enforcement purposes*, 7 October, Brussels.

Geyer, Florian (2008), *Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice*, CEPS Research Paper No. 9, Brussels, May.

González Fuster, Gloria (2009), "3TJCE - Sentencia de 04.12.2008, S. y Marper c. Reino Unido", *Revista de Derecho Comunitario Europeo*, mayo-agosto (33), pp. 619-633.

*Heinz Huber v. Germany*, European Court of Justice, Case C-524/06, Judgement of 16 December 2008.

Human Genetics Commission (2009), *Nothing to hide, nothing to fear? Balancing individual rights and the public interest in the governance and use of the National DNA Database*, London.

López Barja de Quiroga, Jacobo (2008), “El registro único de las huellas de ADN, la protección de datos y la investigación criminal”, in A. Emaldi Cirión, E. Domínguez Peco, F. Aranda Guerrero, J. López Barja de Quiroga, J. Bayo Delgado, J.A. Martín Pallín, V. Moreno Catena, J. Salom Clotet, M. Pérez Sánchez, M. García-Herraiz Rooabert, R. Martínez Martínez and R. De Cospedal García (eds), *La protección de datos en la cooperación policial y judicial*, Thomson Aranzadi, Cizur Menor.

Lucioni, Carlo (2009), “Tutela dei dati personali del cittadino dell'Unione e giudizio di non discriminazione in base alla nazionalità”, *Diritto pubblico comparato ed europeo*, No. 2, pp. 575-582.

Martin, D. (2009), “Comments on *Förster* (Case C-158/07 of 18 November 2008), *Metock* (Case C-127/08 of 25 July 2008) and *Huber* (Case C-524/06 of 16 December 2008)”, *European Journal of Migration and Law*, No. 11, pp. 95-108.

Peyrou-Pistouley, Sylvie (2009), “L’affaire *Marper c/ Royaume-Uni*, un arrêt fondateur pour la protection des données dans l’espace de liberté, sécurité, justice de l’Union européenne”, *Revue Trimestrielle de droit européen*, 5(4), pp. 741-757.

Poiares, Maduro (2008), *Opinion of Advocate General Poiares Maduro in Case C-524/06 (Heinz Huber v Bundesrepublik Deutschland), delivered on 3 April 2008.*

*S. and Marper v. the United Kingdom*, European Court of Human Rights, Applications nos. 30562/04 and 30566/04, Judgement of 4 December 2008.

## Acronyms

AFSJ Area of Freedom, Security and Justice

ECHR European Convention of Human Rights

EU European Union

TEC Treaty the European Community

TFEU Treaty on the Functioning of the European Union

UK United Kingdom