3

Information society and data protection

Google Street View, Facebook and other social media have become part of the fabric of everyday life in the information society in recent years. In 2010, data protection concerns were raised in a number of EU Member States in relation to these developments. Moreover, national security threats continued to have an impact on airport security in 2010, which led to a heated debate at European Union (EU) level as well as in some Member States, particularly in relation to the introduction of body scanners. The protection of personal data was at the forefront of many fundamental rights debates in the EU in 2010 including in relation to new technologies and proposals concerning the reform of the EU data protection framework, taking into account the Lisbon Treaty and the Stockholm Programme.

This chapter covers developments in EU and Member State policies and practices in the area of information society and data protection in the year 2010. It sets out concerns raised by national courts with regard to the EU framework for data protection, noting in particular the question of whether the Data Retention Directive is in compliance with fundamental rights and, more generally, examining calls for reform of the framework. The chapter then deals with concerns relating to the independence, powers and resources of data protection authorities in EU Member States. Reflecting on the need for transparency in an information society, the chapter also considers the delicate balance which must be struck between data protection and the right to information. The chapter ends by reflecting on how data protection challenges were met in 2010 and how they may be met in the future in the areas of police and security cooperation, technological advances and airport security.

Key developments in the area of information society and data protection:

- new technologies raised new fundamental rights concerns and led to calls for a modernisation of EU data protection legislation;
- consensus grew that data protection forms a key concern in international agreements, especially in the case of those dealing with Personal Name Records (PNR) and Swift;
- concerns were raised at political and legal levels in relation to the rise in compulsory retention of communication data (telephone and Internet) by private companies;
- the independence of data protection authorities became an issue that was dealt with before the Court of Justice of the European Union (CJEU);
- political debate continued on the implications of the use of body scanners as security devices at airports;
- the balance between data protection concerns and the right to information emerged as a topic and was addressed before the CJEU.

3.1. Review of the current EU data protection framework

Data protection is explicitly enshrined in Article 8 of the Charter of Fundamental Rights of the European Union as a distinct fundamental right, the first international human rights instrument to have done so. The processing of personal data and the free movement of such data are also regulated by the Data Protection Directive.[1] Moreover, following the adoption of the Lisbon Treaty in December 2009, European Commission Vice-President Viviane Reding identified the protection of personal data of European citizens as a priority policy area in 2010.

1 Directive 95/46/EC, OJ 1995 L 281, pp. 31-50.

"I would like to single out (...) priority areas where I believe we need to show strongly that Europe's policy is changing with the Lisbon Treaty. First of all, we need to strengthen substantially the EU's stance in protecting the privacy of our citizens in the context of all EU policies."

Viviane Reding, European Commission Vice-President, 11 January 2010.

Rapid technological evolution and the increased exchange of data in today's information society has led to a rich debate on the review of current EU legislation governing data protection and privacy, which dates from 1995. The current data protection framework in the EU is therefore still based on the pre-Lisbon system and thus heterogeneous in its provisions and application. The European Commission took the first step in this debate by launching in 2009 a public consultation on the future legal framework for the protection of personal data in the EU.[2] In November 2010, the European Commission published in a communication its views on the protection of personal data in the EU, which highlights new challenges in this area and identifies the need to revise the data protection rules in the areas of police and judicial cooperation in criminal matters.[3] Prior to this, the European Commission issued a communication providing an overview of information management in the area of freedom, security and justice.[4] The Council of Europe also initiated in 2010 a modernisation of its data protection framework, Convention 108 on the protection of individuals with regard to automatic processing of personal data.[5] The Council of Europe is seeking to identify whether the protection framework set out by Convention 108 needs to be modified and complemented in order to better satisfy the legitimate expectation of individuals and concerned professionals with respect to data protection. To this end, the Council of Europe launched – on the occasion of the 30th anniversary of Convention 108 – a public consultation with a view to allowing all stakeholders and interested persons to make their views known. The modernisation of Convention 108 should also lead to an enhanced monitoring of the implementation of the convention.

3.2. Compliance of the Data Retention Directive with fundamental rights principles

In 2010, the European Commission announced that the 2006 Data Retention Directive, which compels telephone and Internet companies to collect data about all of their customers' communications,[6] is under review.[7] Concerns have been raised in EU Member States that the directive does not comply with fundamental rights standards. In a joint letter, dated 22 June 2010, more than 100 non-governmental organisations (NGOs) from 23 EU Member States asked the European Commissioners Cecilia Malmström, Viviane Reding and Neelie Kroes to "propose the repeal of the EU requirements regarding data retention in favour of a system of expedited preservation and targeted collection of traffic data". According to the letter, such generalised data retention puts confidential activity as well as contacts with journalists, crisis lines and business partners, for example, at risk of disclosure by way of data leaks and abuse.[8] National campaigns against the implementation of the directive took place in **Austria**, **Belgium**, **Bulgaria** and **Germany**, and gained broad media coverage. Such concerns about the gradual erosion of privacy protection were also recognised at the end of 2009 by the United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism.[9]

The debate surrounding the fundamental rights compliance of the Data Retention Directive was further fuelled by a number of rulings in EU Member States' constitutional courts. In its Decision No. 1258 of 8 October 2009, the **Romanian** Constitutional Court (*Curtea Constituțională*) declared the implementation of the directive unconstitutional.[10] In March 2010, Germany's federal Constitutional Court (*Bundesverfassungsgericht*) annulled German legislation implementing the Data Retention Directive. The Court also held that the legislation posed a serious threat to personal privacy rights.[11] Following this judgment, the German federal Commissioner on Data Protection and Freedom of Information (*Bundesbeauftragter für den Datenschutz und die Informationsfreiheit*, BfDI) asked German companies to delete all data collected under the unconstitutional statute. According to the BfDI, all companies complied with this request. In a joint resolution, the BfDI and the Data Protection Commissioners of the German states (*Länder*) called on the German federal government to support the repeal of the Data Retention Directive.[12]

"For warding off danger, it follows from the principle of proportionality that a retrieval of the telecommunications traffic data stored by way of precaution may only be permitted if there is a sufficiently evidenced concrete danger to the life, limb or freedom of a person, to the existence or the security of the Federal Government or of a Land (state) or to ward off a common danger."

German Constitutional Court, Press release, 2 March 2010

Another legal challenge was brought before the Irish High Court (*An Ard-Chúirt*) in 2006 by the non-governmental organisation, Digital Rights **Ireland** (DRI). The case challenged both the directive itself as well as its transposition into national law. In July 2008, the Irish Human Rights

2 For a summary of the replies to this consultation, see European Commission (2010a).
3 European Commission (2010b).
4 European Commission (2010c).
5 Council of Europe (2010).
6 Directive 2006/24/EC, OJ 2006 L 105, p. 54.
7 European Commission (2010d).
8 See joint letter of more than 100 NGOs of 22 June 2010, available at: www.vorratsdatenspeicherung.de/images/DRletter_Reding.pdf.
9 Scheinin, M. (2009).
10 Romania, Constitutional Court (2009).
11 Germany, Constitutional Court (2010).
12 Germany, BfDI (2010a).

Commission (*An Coimisiún ul Chearta an Duine,* IHRC) was given the permission of the court to appear as a friend of the court *(amicus curiae)* in this action. According to a press release issued by the IHRC, "[t]his case raises important issues about the extent to which laws and measures governing the monitoring of one's private life by the State in pursuit of tackling crime possess sufficient human rights safeguards".[13] In May 2010, the High Court held that DRI had standing *(locus standi)* to bring this challenge and agreed to refer the question concerning the validity of the directive to the Court of Justice of the European Union (CJEU).[14]

Promising practice

Public consultation on draft bill transposing Data Retention Directive

Between 15 November 2009 and 15 January 2010, the Austrian government carried out a public consultation on a draft bill transposing the Data Retention Directive. Public bodies, private entities and persons submitted 189 comments in total – the greatest number ever reached in a public review of draft legislation in Austria. Most of the comments criticised the duty set out in the directive to retain traffic data, location and subscriber data processed in publicly available electronic communications services or networks.

For a list of all comments received in the consultation on the draft bill, see the Austrian Parliament's website at: http://www.parlinkom.gv.at/PAKT/VHG/XXIV/ME/ME_00117/index.shtml.

Meanwhile, doubts about the fundamental rights compliance of the Data Retention Directive were also delaying its transposition in certain Member States. Although the CJEU held in July 2010 that **Austria** had violated the EU Treaty by not transposing the directive by the 15 March 2009 deadline,[15] the Austrian transposition of the directive was further delayed.[16] In the proceedings before the CJEU, Austria expressed concerns about the compliance of the directive with fundamental rights, especially Article 8 of the EU Charter of Fundamental Rights.[17] In **Sweden**, the implementation of the Data Retention Directive was also delayed due to fundamental rights concerns.

13 European Digital Rights (2008).
14 Ireland, *Digital Rights Ireland Ltd. v. Minister for Communication, Marine and Natural Resources and others*, High Court, McKechnie J., unreported, 5 May 2010.
15 CJEU, C-189/09, *Commission v. Austria*, 29 July 2010.
16 Austria, Federal Ministry of Justice (2010).
17 CJEU, C-189/09, *Commission v. Austria*, 29 July 2010.

3.3. Data protection authorities: independence, powers and resources

According to Article 28 of the Data Protection Directive, supervisory authorities must be set up in each EU Member State in order to monitor the application of the directive. The independence, powers and resources of data protection authorities in EU Member States emerged as a key concern in 2010. The FRA addressed this issue in greater detail in its report on *Data protection in the European Union: the role of National Data Protection Authorities*, which was published in May 2010.

3.3.1. Independence

In the case of *Commission v. Germany*, the CJEU dealt with the question of the independence of data protection supervisory authorities for the first time. By applying strict criteria, the CJEU held that the German data protection institutions at federal state (*Länder*) level responsible for monitoring the processing of personal data by non-public bodies were not sufficiently independent because they were subject to oversight by the state.[18] The case revolved around the interpretation of Article 28 (1) of the Data Protection Directive which requires data protection authorities to "act with complete independence in exercising the functions entrusted to them".

> *"Directive 95/46 is to be interpreted as meaning that the supervisory authorities responsible for supervising the processing of personal data outside the public sector must enjoy an independence allowing them to perform their duties free from external influence. That independence precludes not only any influence exercised by the supervised bodies, but also any directions or any other external influence, whether direct or indirect, which could call into question the performance by those authorities of their task consisting of establishing a fair balance between the protection of the right to private life and the free movement of personal data."*
>
> *CJEU, C-518/07* Commission v. Federal Republic of Germany, *9 March 2010, paragraph 30.*

In his Opinion, the Advocate General qualified the term 'independence' as relative in nature, since it is necessary that the legislator specifies the level of such independence and this remains undefined. Following this logic, the Advocate General concluded that the German data protection institutions in question were sufficiently independent even though they were subject to state oversight.[19] In contrast, the Court rejected this line of argument and stressed that the directive should be interpreted in accordance with the usual meaning of the words, thereby opting for a strict construction of 'independence'. The CJEU also pointed out that the word 'independence' is complemented by the adjective 'complete'

18 CJEU, C-518/07, *Commission v. Germany*, 9 March 2010.
19 *Ibid.*

in the directive and should therefore be understood in a broad sense.

In December 2010, the European Commission referred **Austria** to the CJEU for lack of independence of its data protection authority. Austrian data protection legislation requires the relevant authority to exercise its functions independently and not to take any instruction when performing its duties. According to the Commission, 'complete independence' is not guaranteed because the authority is integrated into the federal Chancellery, where the Chancellor has the right to be informed on all subjects concerning the daily management of the authority at all times.[20]

3.3.2. Powers

On 24 June 2010, the European Commission requested the **United Kingdom (UK)** to comply with EU law by strengthening the powers of its national data protection authority, the Information Commissioner's Office (ICO).[21] The European Commission called for the ICO to be given power to: conduct random checks for compliance with data protection law; to issue penalties; and to assess the recipient country's data protection regime before international transfers of information are made from the UK.[22] The European Commission is currently analysing the UK response to the allegations that it has raised.

FRA ACTIVITY

Comparison of Data Protection Authorities

In May 2010, the FRA published its report *Data Protection in the EU: the role of National Data Protection Authorities*. The report provides a comparative overview of the powers and independence of data protection authorities in the EU and highlights the lack of independence, powers and resources of data protection authorities in certain EU Member States.

FRA (2010), Data Protection in the EU: the role of National Data Protection Authorities – Strengthening the fundamental rights architecture in the EU II, *available at: http://fra.europa.eu/fraWebsite/research/publications/publications_en.htm.*

3.3.3. Resources

The resources of data protection authorities are crucial for their functioning as fundamental rights guardians. Nevertheless, in 2010, budgets were curtailed in many EU Member States as a result of the financial crisis. The information provided below is not directly comparable but still indicative of certain trends.

The following countries reported a significant decrease in human and/or financial resources during the reporting period: **Estonia** (12.5% decrease of financial resources for the period from 2008 to 2010), **Ireland** (in 2008, EUR 2.04 million; in 2009, EUR 1.81 million; in 2010, EUR 1.21 million), **Latvia** (in 2008, 25 staff; in 2009, 16 staff; in 2010, 19 staff; in 2008, EUR 730,984; in 2009, EUR 476,984; in 2010, EUR 381,295), **Lithuania** (reductions of staff unspecified, but wages fund reduced by 69% from LTL 2,929,000 (EUR 848,690 as of 31 December 2010) to LTL 1,886,000 (EUR 546,477), cuts of 64.6%), **Slovakia** (no change of human resources; in 2008, EUR 960,850; in 2010 EUR 728,696).

However, from 2007 to 2010, **France** and **Germany** reported a significant increase in human and financial resources.[23] A similar trend was also observed in Spain where the Spanish data protection authority (*Agencia Española de Protección de Datos*) saw the number of employees rise from 99 employees in 2007 to 155 in 2009. Its budget also increased from EUR 13.44 million for 2008 to EUR 15.32 million for 2009.[24]

Lastly, either no changes or only slight changes with regard to human and financial resources were reported during 2010 in the following countries: **Austria**, **Bulgaria**, **Cyprus**, **Finland**, **Greece**, **Hungary**, **Italy**, **Malta**, **Poland**, **Romania**, **Slovenia** and the **UK**.

3.4. Data protection and transparency in the information society

It is often the case in fundamental rights discourse that a delicate balance must be found between competing interests. In the case of data protection, this balancing act takes place when the right to the protection of personal data is pitted against the right to information. The CJEU dealt with this issue in 2010 in the context of ensuring transparency.

In June 2010, in the case of the *Commission v. Bavarian Lager*, the CJEU considered the scope of the protection of personal data in the context of access to documents of the EU institutions.[25] In that case, the European Commission had provided access to minutes of a meeting but had blanked out five names. The applicant had applied for full access to the document yet could not justify the necessity for such personal data. As a result, the CJEU upheld the European Commission's decision to refuse full access to the document.

It is also worth mentioning the Joined cases C-92/09 and C-93/09, which came before the CJEU Grand Chamber in November 2010, as here EU legislation was challenged on the basis of its compliance with fundamental rights.[26] This

20 European Commission (2010e).
21 European Commission (2010f).
22 United Kingdom, Information Commissioner's Office (2010).
23 If not otherwise stated, these data were provided by the FRA network of senior legal experts, FRALEX.
24 Spain, Agency for the Protection of Data (2008), p. 84, and (2009), p. 92.
25 CJEU, C-28/08 P, *Commission v. Bavarian Lager*, 29 June 2010.
26 CJEU, Joined cases C-92/09 and C-93/09, *Eifert, Schecke v. Land Hessen*, 9 November 2010.

case related to EU legislation on agricultural policy which requires EU Member States to ensure the annual *ex-post* publication of beneficiaries' names and the respective amounts paid under the European Agricultural Guarantee Fund (EAGF) and the European Agricultural Fund for Rural Development (EAFRD).[27] The applicants had asked the administrative court of Wiesbaden to require the German federal state (*Land*) of Hessen not to publish the data relating to them. As a result, the court in Wiesbaden referred the case to the CJEU. The CJEU stated that it is legitimate in a democratic society that taxpayers have a right to be kept informed of the use of public funds. The CJEU also held that the publication of data on a website which named the beneficiaries of EAGF and EAFRD aid and set out the precise amounts they received constitutes an interference with the right to respect for private life in general, and to the protection of their personal data, in particular. The CJEU concluded that the publication of the personal data of each and every EAGF and EAFRD aid beneficiary was not sufficiently proportionate as it was not strictly necessary to achieve the pursued aim of transparency. As a result, the CJEU declared certain provisions of Regulation No. 1290/2005 and Regulation No. 259/2008 invalid, thereby striking down EU legislation on the basis of fundamental rights concerns.

3.5. New challenges

3.5.1. Data protection, and police and security cooperation

The Lisbon Treaty abolished the previous division of the EU in three distinct pillars and extended the ordinary legislative procedure to the area of police and judicial cooperation in criminal matters. Moreover, the powers of the European Parliament have been considerably strengthened in the context of the conclusion of international agreements, which has important implications for data protection. In February 2010, the European Parliament used these new powers to withhold its consent to an interim agreement between the EU and the United States of America (US) concerning the processing and transfer of financial messaging data from the EU to the US (so-called Swift I Agreement), signed on 30 November 2009. The Parliament claimed this agreement did not offer enough protection for EU citizens' personal data.[28] On the 8 July 2010 – after the European Data Protection Supervisor (EDPS) delivered an opinion,[29] the European Parliament gave its consent to the revised agreement,[30] which was formally concluded on 13 July 2010.[31]

Fundamental rights concerns have also arisen in relation to international agreements on the exchange of PNR data. On 1 March 2010, a Belgian human rights NGO (*Ligue des Droits de L'Homme*) brought a case before the constitutional court of **Belgium** claiming that the domestic legislation of 30 November 2009, which implemented the 2007 EU-US PNR Agreement, violated data protection standards.[32] On 5 May 2010, the European Parliament adopted a resolution[33] stating that both a Privacy Impact Assessment and a proportionality test must be carried out before the finalisation of any new European legislation on the transfer of PNR data.

In September 2010, the European Commission adopted a package of proposals on the exchange of PNR data with third countries,[34] consisting of an EU external PNR strategy and recommendations for negotiating directives for new PNR agreements with Australia, Canada and the US.[35] The strategy aims to ensure a high level of data protection in the exchange of PNR data with third countries.[36]

3.5.2. Technological challenges

Fundamental rights concerns posed by new technological challenges featured prominently on the agenda of the Council of Europe during the reporting period. In 2010, the Committee of Ministers of the Council of Europe adopted a package of declarations and recommendations in this context: a declaration on the digital agenda for Europe;[37] a declaration on network neutrality;[38] a declaration on the management of the Internet protocol address resources in the public interest;[39] a declaration on enhanced participation of Member States in Internet governance matters – the Governmental Advisory Committee (GAC) of the Internet Corporation for Assigned Names and Numbers (ICANN).[40] Furthermore, the Parliamentary Assembly of the Council of Europe adopted Recommendation 1906 (2010) on rethinking creative rights for the Internet age.[41]

New technological challenges also led to fundamental rights debates in EU Member States. Google Street View is a service provided by the information technology (IT) company Google, which offers panoramic views from various positions along streets in many cities worldwide. For this purpose, Google sends specially adapted cars through cities in the EU and beyond in order to collect pictures. However, during this task the IT company had – according to Google's statement – inadvertently gathered fragments of personal data sent over unsecured Wi-Fi systems.

As a result, on 21 May 2010 the **Austrian** Data Protection Commission (*Österreichische Datenschutzkommission*, DSK) imposed a temporary ban on the collection of data through 'Google Street View' cars and initiated an investigation. By

27 Council Regulation (EC) No. 1290/2005, OJ 2007 L 322, p. 1 and Commission Regulation (EC) No. 259/2008, OJ 2008 L 76, p. 28.
28 European Parliament (2010a).
29 European Data Protection Supervisor (EDPS) (2010).
30 European Parliament (2010b).
31 Council Decision 2010/412/EU, OJ 2010 L 195, p. 3.
32 Belgium, La Ligue des droits de l'Homme (LDH).
33 European Parliament (2010c).
34 European Commission (2010g).
35 European Commission (2010h).
36 See European Union Agency for Fundamental Rights (FRA) (2008).
37 Council of Europe, Committee of Ministers (2010a).
38 Council of Europe, Committee of Ministers (2010b).
39 Council of Europe, Committee of Ministers (2010c).
40 Council of Europe, Committee of Ministers (2010e).
41 Council of Europe, Parliamentary Assembly (2010).

the end of November 2010, the temporary ban was lifted, but the investigation into the procedures of Google Street View continues.[42] Similar proceedings took place in many countries, including **Spain**,[43] **Slovenia**[44] and **Italy.**[45]

In **Germany**, the debate focused on the right to object to pictures taken by Google Street View. In August 2010, the German branch of Google agreed to accommodate individual objections, which since the end of 2010 can be lodged online,[46] against the publication of pictures of private houses and of persons in its Street View service. The Data Protection Commissioner of Hamburg (*Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit*, HmbBfDI) published an information leaflet[47] and a form[48] for submitting such objections. Moreover, the federal Commissioner on Data Protection and Freedom of Information demanded a central register for objections regarding the publication of personal data on the Internet, including services such as Google Street View.[49] The second chamber of the German federal parliament (*Bundesrat*) adopted a draft bill amending the federal Law on Data Protection (*Bundesdatenschutzgesetz*, BDSG) to ensure improved protection of personal data with regard to geographical information services on the Internet such as Google Street View.[50] In a press release on 18 August 2010, it appeared that the German federal government (*Bundesregierung*) seemed to favour wholesale reform of the online data protection law and would make a proposal in that regard.[51]

> *"Most of the 75% of Europe's youngsters who go online are enthusiastic users of social networking sites. ...However publishing personal information or pictures may lead to embarrassing or even traumatic situations. Young people do not always realize the risk that online images and videos may circulate beyond their control and knowledge."*
>
> *Viviane Reding, European Commission Vice-President, 9 February 2010.*

On 7 July 2010, the Data Protection Commissioner of Hamburg initiated an investigation against Facebook concerning the collection of e-mail and mobile phone contact data and the creation of contact profiles for marketing purposes of non-users of Facebook via address books of registered users.[52] This procedure may result in a fine and it is the first time that such a procedure has been initiated against Facebook in Europe.

The role of Facebook in election campaigns also came to the fore as a topic of discussion in **Bulgaria** in 2010. On 22 June 2010, several members of the ruling party in Bulgaria proposed provisions introducing restrictions relating to election campaigns on the Internet. The main purpose was to compare the information provided via electronic media, bloggers and social networks like Facebook and Twitter with the information provided by more traditional text, radio and television media. Ordinarily, the same rules regarding reporting of election campaigns should apply to both forms of media. In response to this proposal, opposition parties expressed their concern and declared it would constitute a violation of freedom of expression and amounted to control of the Internet.[53]

3.5.3. Body scanners

Airport security measures, in particular the use of body scanners, seemed to dominate debates about data protection in the EU in 2010. Indeed, in the aftermath of the attempt to blow up a plane with hidden explosives on a flight between Amsterdam and Detroit on 25 December 2009, the debate about various types of body scanners at airports took a more prominent position on the political agenda. This issue attracted considerable media attention and it was claimed that displaying images in which a person going through the scanner is shown naked interfered with the right to respect for private life. On 15 June 2010, the European Commission published its communication on the use of security scanners at EU airports, which argued that only a solution found at EU level would guarantee uniform application of security rules and standards. This is considered essential "to ensure both the highest level of aviation security as well as the best possible protection of EU citizens' fundamental rights and health". [54] In this context, the European Commission underlined the importance of various provisons of the EU Charter of Fundamental Rights, including human dignity (Article 1), respect for private and family life (Article 7), protection of personal data (Article 8), freedom of thought, conscience and religion (Article 10), non-discrimination (Article 21), the rights of the child (Article 24) and a high level of human health protection in the definition and implementation of all Union's policies and activities (Article 35).

A European Privacy and Data Protection Commissioners' Conference, which took place in Prague in April 2010, also addressed this issue. The Commissioners adopted a resolution stating that data protection principles and safeguards as well as privacy by design should be taken into account when considering the use of body scanners.[55]

42 Austria, Austrian Data Protection Commission.
43 Spain, Spanish Agency for Data Protection (*Agencia Española de Protección de Datos*).
44 Slovenia, Information Commissioner (*Informacijski Pooblascenec*).
45 Italy, Italian Data Protection Authority (*Garante Per la Protezione Dei Dati Personali*).
46 Germany, Commissioner on Data Protection and Freedom of Information for Hamburg (HmbBfDI) (2010a).
47 Germany, HmbBfDI (2010b).
48 See Germany, The independent federal state centre for data protection for Schleswig-Holstein (*Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein*, ULD).
49 Germany, BFDI (2010b).
50 Germany, Federal Parliament (*Bundestag*) (2010).
51 *Ibid.*, p. 15.
52 Hamburg.de (2010).
53 Bulgarian Helsinki Committee (2010).
54 European Commission (2010i).
55 European Privacy and Data Protection Commissioners (2010).

The European Court of Human Rights (ECtHR) referred to security measures at airports in *Gillan and Quinton v. United Kingdom*.[56] The case concerned the practice of police stops and searches in the UK. In this case, the UK government argued that police stops and searches do not amount to an infringement of the right to privacy because they equate to searches passengers regularly submit to at airports.[57] Rejecting this argument, the ECtHR pointed out that passengers submit to customary searches at airports voluntarily because they choose to fly knowing such searches take place, whereas such choice does not exist with regard to police stops and searches which can take place anywhere and at any time.[58] It is unclear whether this reasoning applies also to body scanners because they go beyond customary searches.

The debate surrounding body scanners and data protection concerns also arose in other EU Member States, such as **France**,[59] **Spain**[60] and **Germany**, during 2010.[61]

FRA ACTIVITY

Body scanners and fundamental rights

In July 2010, the FRA issued a discussion paper on *The use of body scanners: 10 questions and answers*. The paper identifies fundamental rights potentially affected by the use of body scanners. It further reflects on the requirements and specific considerations that should be taken into account when discussing the introduction of such technical devices at European airports. The paper also examines the conditions that should apply in order to address the concerns related to fundamental rights.The Agency presented the paper's conclusions at a hearing at the European Economic and Social Committee in January 2011.

FRA (2010), The use of body scanners: 10 questions and answers, *available at: http://fra.europa.eu/fraWebsite/research/publications/publications_en.htm.*

Outlook

New technical developments continue to shape our lives, bringing fundamental rights concerns to the fore. Facebook, Google Street View and body scanners are likely to remain on the agenda and will probably contribute to the ongoing overarching debate about the modernisation of the EU data protection framework. Against the background of the Lisbon Treaty, two issues will be central in the near future: compliance with fundamental rights standards (for example, in the context of data retention), and the possible extension of the scope of the general data protection framework to include areas of police and justice cooperation in criminal matters. This is likely to affect the way in which data protection is dealt with both inside and outside the EU. Indeed, the debate on data protection will probably continue to move towards the centre of the fundamental rights discourse in the EU in coming years.

56 European Court of Human Rights (ECtHR), *Gillan and Quinton v. United Kingdom*, No. 4158/05, 12 January 2010.
57 *Ibid.*, at paragraph 60.
58 *Ibid.*, at paragraph 60.
59 See France, National Commission on information technology and liberties (*Commission nationale de l'informatique et des libertés, CNIL*) (2010).
60 For an experts debate on the use of body scanners at airports, see the Data Protection Agency of Madrid website, available at: www.dataprotectionreview.eu/.
61 Germany, BfDI (2010a); Germany / BfDI (2010b).

References

Austria, Austria Data Protection Commission (2010) (*Österreichische Datenschutzkommission*, DSK), 'Neue Entwicklungen betreffend Google Street View?'.

Austria, Federal Ministry of Justice (*Bundesministerium für Justiz*) (2010), 'Vorratsdaten: Justizministerium prüft Vorschlag', Press release, 27 July 2010.

Austria, Telekommunikationsgesetz 2003, Änderung (117/ME), available at: www.parlinkom.gv.at/PAKT/VHG/XXIV/ME/ME_00117/index.shtml.

Belgium, La Ligue des droits de l'Homme (LDH), 'PNR, l'oeil de Washington', available at: www.liguedh.be/index.php?option=com_content&view=article&id=854:pnr--lil-dewashington&catid=110:communiques-de-presse-2010&Itemid=283.

Bulgarian Helsinki Committee (2010), ДПС е против опитите да се наложи чрез изборното законодателство контрол върху Интернет, 22 June 2010, available at: www.bghelsinki.org/index.php?module=news&lg=bg&id=3393; ГЕРБ обмисля да има или да няма контрол върху социалните мрежи, блоговете и форумите, available at: www.bghelsinki.org/index.php?module=news&lg=bg&id=3391.

Commission Regulation (EC) No. 259/2008 of 18 March 2008 laying down detailed rules for the application of Regulation No. 1290/2005 as regards the publication of information on the beneficiaries of funds deriving from the European Agricultural Guarantee Fund (EAGF) and the European Agricultural Fund for Rural Development (EAFRD), OJ 2008 L 76.

Council Decision 2010/412/EU on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, Brussels, 13 July 2010, OJ 2010 L 195.

Council Regulation (EC) No. 1290/2005 of 21 June 2005 on the financing of the common agricultural policy, OJ 2005 L 209, p. 1, as amended by Council Regulation (EC) No. 1437/2007 of 26 November 2007, OJ 2007 L 322.

Council of Europe, *Council of Europe response to privacy challenges Modernisation of Convention 108*, Position paper, 32nd International Conference of Data Protection and Privacy Commissioners, Jerusalem, 27-29 October 2010.

Council of Europe, Committee of Ministers (2010a), *Declaration of the Committee of Ministers on the Digital Agenda for Europe,* Strasbourg, 29 September 2010.

Council of Europe, Committee of Ministers (2010b), *Declaration of the Committee of Ministers on network neutrality*, Strasbourg, 29 September 2010.

Council of Europe, Committee of Ministers (2010c), *Declaration of the Committee of Ministers on the management of the Internet protocol address resources in the public interest*, Strasbourg, 29 September 2010.

Council of Europe, Committee of Ministers (2010d), *Declaration of the Committee of Ministers on enhanced participation of member states in Internet governance matters – Governmental Advisory Committee (GAC) of the Internet Corporation for Assigned Names and Numbers (ICANN),* Strasbourg, 26 May 2010.

Council of Europe, Committee of Ministers (2010e), 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, Strasbourg, 23 November 2010.

Council of Europe, Parliamentary Assembly (2010), Recommendation 1906 (2010) on rethinking creative rights for the Internet age, Strasbourg, 12 March 2010.

Court of Justice of the European Union (CJEU), C-189/09, *Commission v. Austria*, 29 July 2010.

Court of Justice of the European Union, C-518/07, *Commission v. Germany*, 9 March 2010.

Court of Justice of the European Union, C-28/08 P, *Commission v. Bavarian Lager*, 29 June 2010.

Court of Justice of the European Union, Joined cases C-92/09 and C-93/09, *Schecke and Eifert v. Land Hessen*, 9 November 2010.

Data Protection Agency of Madrid *(Agencia de Protección de Datos de la Comunidad de Madrid)*, website: www.dataprotectionreview.eu

Directive 95/46/EC of the European Parliament and of the 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 1995 L 281.

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 amending Directive 2002/58/EC, OJ 2006 L 105.

European Commission (2010a), *Summary of replies to the public consultation about the future legal framework for protecting personal data*, Brussels, 4 November 2010.

European Commission (2010b), *A comprehensive approach on personal data protection in the European Union*, COM(2010) 609 final, Brussels, 4 November 2010.

European Commission (2010c), *Overview of information management in the area of freedom, security and justice*, COM(2010) 385 final, Brussels, 20 July 2010.

European Commission (2010d), 'European Commission sets out strategy to strengthen EU data protection rules', Press release IP/10/1462, Brussels, 4 November 2010.

European Commission (2010e), 'Data Protection: Commission to refer Austria to Court for lack of independence of data protection authority', Press release IP/10/1430, Brussels, 28 October 2010.

European Commission (2010f), 'Data protection: Commission requests UK to strengthen powers of national data protection authority, as required by EU law, IP/10/811, Brussels, 24 June 2010.

European Commission (2010g), *On the global approach to transfers of Passenger Name Record (PNR) data to third countries*, COM(2010) 492, Brussels, 21 September 2010.

European Commission (2010h), 'European Commission adopts an EU external strategy on Passenger Name Record (PNR)', Press release IP/10/1150, Brussels, 21 September 2010.

European Commission (2010i), *Use of security scanners at EU airports*, COM(2010) 311, Brussels, 15 June 2010, available at: http://ec.europa.eu/transport/air/security/doc/com2010_311_security_scanners_en.pdf.

European Court of Human Rights (ECtHR), *Gillan and Quinton v. United Kingdom*, No. 4158/05, 12 January 2010.

European Data Protection Supervisor (EDPS) (2010), Opinion on a *Proposal for a Council Decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program (TFTP II)* , 22 June 2010.

European Digital Rights (2008), 'Irish Human Rights Commission added to data retention challenge', Newsletter *EDRI-gram*, No. 6.14, 16 July 2008, available at: www.edri.org/edrigram/number6.14/irish-human-rights-data-retention.

European Parliament (2010), 'SWIFT: MEPs to vote on backing or sacking EU/US data sharing deal', 5 February 2010.

European Parliament (2010b), 'EU/USA Agreement: processing and transfer of Financial Messaging Data for purposes of the Terrorist Finance Tracking Program', Procedure file, NLE/2010/0178.

European Parliament (2010c), Resolution on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada, P7_TA-PROV(2010)0144, Brussels, 5 May 2010.

European Privacy and Data Protection Commissioners (2010), *Resolution on the use of body scanners for airport security purpose adopted by the European Privacy and Data Protection*, Commissioners' Conference, Prague, 29-30 April 2010, available at: www.tietosuoja.fi/uploads/z1k164nuv.pdf.

European Union Agency for Fundamental Rights (FRA) (2008), *Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes*, Vienna, 28 October 2008.

European Union Agency for Fundamental Rights (2010), *Data Protection in the EU: the role of National Data Protection Authorities - Strengthening the fundamental rights architecture in the EU II*, Luxembourg, Publications Office of the European Union, Vienna, 7 May 2010.

European Union Agency for Fundamental Rights (2010), *The use of body scanners: 10 questions and answers*, Luxembourg, Publications Office of the European Union, Vienna, July 2010.

France, National Commission on information technology and liberties (*Commission nationale de l'informatique et des libertés*, CNIL) (2010), 'Body scanner: quel encadrement en France et en Europe', 8 June 2010.

Germany, Federal Parliament (*Bundestag*) (2010),'Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes, Publikation/Bt-Drs. 17/2765, 18 August 2010.

Germany, Constitutional Court (*Bundesverfassungsgericht*), 'Data retention unconstitutional in its present form', Press release No. 11/2010, 2 March 2010.

Germany, Federal Commissioner on Data Protection and Freedom of Information (*Bundesbeauftragter für den Datenschutz und die Informationsfreiheit*, BfDI) (2010a), 'Vorratsdatenspeicherung', Bonn.

Germany, BfDI (2010b), 'Google Street View: Schaar fordert Schaffung eines Widerspruchsregisters und Profilbildungsverbot', Press release, 18 August 2010.

Germany, BfDI (2010c), 'Diskretionszone für Körperscanner gewährleisten!', Bonn, 24 November 2010.

Germany, Commissioner on Data Protection and Freedom of Information for Hamburg (*Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit*, HmbBfDI) (2010a), 'Vorab-Widerspruch gegen Veröffentlichungen in Google Street View: So funktioniert's', Press release, Hamburg, 13 August 2010.

Germany, HmbBfDI (2010b), *Aus den Augen, aus dem Sinn … Information zur Umsetzung des Vorab-Widerspruchs gegen Abbildungen im Internetdienst Google Street View*, Hamburg, HmbBfDI.

Germany, The Independent federal state centre for data protection for Schleswig-Holstein (*Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein*, ULD), website: www.datenschutzzentrum.de/geodaten/20100310-google-streetview-musterwiderspruch.pdf.

Hamburg.de (2010), 'Bußgeldverfahren gegen Facebook wegen Speicherung der Daten Dritter', 7 July 2010.

Ireland, High Court of Ireland (*An Ard-Chúirt*), *Digital Rights Ireland Ltd. v. The Minister for Communication, Marine and Natural Resource and others*, 5 May 2010.

Italy, Italian Data Protection Authority (*Garante Per la Protezione Dei Dati Personali*), 'Excerpts From The Italian Dpa's Decision Regarding Google Streetview Information Obligations Applying To Google Inc.', Press release, 15 October 2010.

Reding V., 'Opening remarks at the European Parliament hearing in the Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE)', 11 January 2010.

Reding V., 'Think before you post! How to make social networking sites safer for children and teenagers?', Safer Internet Day Strasbourg, 9 February 2010.

Romania, Constitutional Court (*Curtea Constituțională*) (2009), Decision No. 1258 of 8 October 2009 regarding the unconstitutionality exception of the provisions of Law No. 298/2008.

Scheinin, M. (2009), *Report on the protection of the right to privacy in the fight against terrorism*, A/HRC/13/37, Human Rights Council, Office of the High Commissioner for Human Rights, 28 December 2009.

Slovenia, Information Commissioner (*Informacijski Pooblascenec*), Communication relating to Google Street View, available at: www.ip-rs.si/fileadmin/user_upload/Pdf/mnenja/0712-258-2010.pdf.

Spain, Agency for the Protection of Data (*Agencia Española de Protección de Datos*) (2008), *Annual Report 2008*, Madrid, Agencia Española de Protección de Datos.

Spain, Agency for the Protection of Data (*Agencia Española de Protección de Datos*) (2009), *Annual Report 2009*, Madrid, Agencia Española de Protección de Datos.

United Kingdom, Information Commissioner's Office (2010), 'European data protection Commission's call for the UK to strengthen the powers of its national data protection authority', London, 28 June 2010.

United Kingdom, Ministry of Justice (2010), 'Call for Evidence on the data protection legislative framework', London, 6 July 2010.

UN & CoE

28 December 2009 – UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism publishes a report on the protection of the right to privacy in the fight against terrorism

December

January

February

March

April

May

June

July

August

29 September – CoE Committee of Ministers issues declarations on the Digital Agenda for Europe, on network neutrality and on the management of the Internet protocol address resources in the public interest

September

October

23 November – CoE Committee of Ministers issues a recommendation on the protection of individuals with regard to automatic processing of personal data in the context of profiling

November

December

EU

January

February

9 March – CJEU interprets the Data Protection Directive in the *Commission v. Germany* case

March

April

May

15 June – European Commission issues a communication on the use of security scanners at EU airports.

29 June – CJEU considers the scope of the protection of data in the context of access to EU documents in the *Commission v. Bavarian Lager* case

June

20 July – European Commission issues a communication on information management in the area of freedom, security and justice

July

August

21 September – European Commission issues a communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries

September

October

4 November – European Commission issues a communication on a comprehensive approach to personal data protection in the EU

9 November – CJEU rules in the *Volker und Markus Schecke GbR, Hartmud Eifert, Land Hessen v. Bundesanstalt für Landwirtschaft und Ernährung* case that various provisions of EU secondary law are invalid due to a violation of the EU's data protection rules

November

December