Translation funded by the Justice programme of the European Union

Directorate-General of the Library, Research and Documentation

No. 1/2015

R E F L E T S

Edition focusing on personal data protection

Legal developments of interest to the European Union

* The contributions with an asterisk deal with the protection of personal data.

- - - - - - - -

- The European Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter, the "ECHR"); the European Court of Human Rights (hereinafter, the "ECtHR"); the Charter of Fundamental Rights of the European Union (hereinafter, the "Charter");
- The directive 2006/24/EC 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 the directive 2002/58/EC (hereinafter the "directive 2006/24/EC");
- The directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter, the "Directive 95/46/EC");
- The Digital Rights Ireland and Seitlinger e.a ruling (C-293/12 and C-594/12, EU:C:2014:238) (hereinafter, the "Digital Rights Ireland ruling");
- The Google Spain and Google ruling (C-131/12, EU:C:2014:317) (hereinafter, the "Google Spain ruling").

...

Preface

This edition of *Reflets* focuses on **the protection of personal data**. The recent case law of the Court on the matter reveals the presence of new legal issues, as regards the EU law, related to the use of new technologies, especially the Internet. These issues are even more interesting since the Charter, elevated to primary law, prescribes, in Article 7, a law governing the respect of privacy and family life, and in Article 8, a right to protection of personal data for every individual. Therefore, this issue of *Reflets* gives an account of the manner in which these issues are perceived with regard to the recent case law and legislation in the Member States.

For example, after the Court of Justice declared as invalid the Directive 2006/24/EC 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 the directive 2002/58/EC in the Digital Rights Ireland ruling, some Member States have either made amendments, already in force, to the national legislation transposing the directive (Finland) or initiated the process of repeal of the said law by drawing up a bill (Greece, Netherlands). In addition, the United Kingdom has adopted a new law in order to clarify the legal basis of the existing system for data retention. In Sweden, any changes with regard to legal security must be considered in accordance with a survey conducted by experts appointed by the government. Moreover, the effects of the national transposition law were suspended in Slovakia (see *Reflets No.* 2/2014, p. 46). Finally, in Slovenia, the national law transposing the aforementioned directive has lost legal effect owing to the delivery of the ruling by the Constitutional Court invalidating it (see p. 49).

The Digital Rights Ireland ruling has also resonated with the national courts (Austria, Bulgaria, Cyprus, Spain, France, Netherlands, Romania, Slovenia, Sweden). In Austria, for example, the Verfassungsgerichtshof delivered its judgement as a result of the Court ruling, thus ending a controversy that lasted several years about the retention of personal data. The national court found the regulations transposing the directive 2006/24/EC non-compliant with the requirements of proportionality (p. 19). It may also be noted that in Bulgaria, following a request from the Ombudsman, the Constitutional Court gave a ruling on the unconstitutionality of national provisions transposing the aforementioned directive.

Regarding the principles laid down in the Google Spain ruling, several national courts have applied them in their recent case laws (Germany, Belgium, Bulgaria, Spain, France, Italy, United Kingdom). In addition, two provisional orders delivered by a French court inviting requests for removing links referenced by the Google search engine in order to end a manifestly unlawful infringement may be cited. Furthermore, the Italian Court of Cassation ruled on the responsibility of the hosting site provider and, in particular, on the lack of due diligence obligation incumbent upon it (p. 36). Regarding Spain, the Audiencia Nacional delivered its judgment by specifying the criteria concerning the recognition of the right to be forgotten, in accordance with the Google Spain ruling (p. 24).

The doctrinal echoes will reflect the comments on the Digital Rights Ireland and Google Spain rulings (p. 63).

It should be recalled that the protection of personal data is a common theme addressed in the national case law referred to in *Reflets*. In this regard, two decisions from the Bundesverfassungsgericht were discussed in previous editions of *Reflets* (*nos. 2/2010 and 2/2013*). While the first decision was regarding the national court's jurisdiction to examine the national provisions transposing the directive 2006/24/EC, with regard to national fundamental rights, the second decision concerned the compatibility of the principles of the German law on the "counter-terrorism file" with the German Constitution. In the latter decision, the German high court held that it was not necessary to request the Court of Justice for a preliminary ruling to check the scope of the protection of fundamental rights of the Charter, and particularly Article 8, since the said law did not implement the Union law, within the meaning of Article 51, paragraph 1, of the Charter.

Beyond the protection of personal data, we will report, first of all, in this new edition of *Reflets,* a decision of the French Constitutional Council, delivered as part of a priority preliminary ruling on constitutionality, regarding compliance of the disqualification of French citizenship of individuals responsible for acts of terrorism with the French Constitution (p. 29). It should also be noted that a judgment of the Supreme Court of the United Kingdom by which an action directed against a law of the Scottish Parliament denying prisoners in Scottish prisons the right to vote in the referendum on the independence of Scotland was rejected (p. 47). Finally, as far as legislative matters are concerned, it should be noted that the law on the opening of marriage to homosexual couples came into force on 1 January 2015 in Luxembourg (p. 58) and that an identical law was recently adopted in Slovenia (p. 61).

We should point out that the Reflets bulletin has been temporarily available in the "What's New" section of the Court of Justice intranet, as well as, permanently, on the Curia website (www.curia.europa.eu/jcms/jcms/Jo2_7063).

The Newsletter is also available in English on the ACA website (http://www.aca-europe.eu/index.php/en/).

A. Case law

I. European and international jurisdictions

European Court of Human Rights

ECHR - Law governing the respect of privacy and family life - Collection and processing of personal health data by public authorities - Scope and terms of the discretionary power of competent authorities - Guarantees offered by the national law - Pressing social need - Absence - Violation of Article 8 of the ECHR

In its ruling of 6 June 2013, in the Avilkina et al/Russia case, the ECtHR ruled that Russia had violated Article 8 of the ECHR, in that its domestic law in no way limited the scope of the health data of the applicants, which could be collected and processed by public prosecution authorities.

The applicants, members of a religious organisation that, at that time was the subject of an official investigation into the legality of its activities, saw confidential medical information about them disclosed and subsequently processed by the Russian judicial authorities. Following an order of the said authorities requiring the reporting of all cases of refusal of blood transfusion of the members of the aforementioned organisation, the public health institutions that treated the applicants disclosed the data concerning them. Note that the possibility for the judicial authorities to demand the disclosure of confidential data without the consent of the persons concerned was provided for by national law.

The ECtHR recalled that the protection of the confidentiality of the medical data, included in the general category of personal data, is intrinsically linked to the exercise of the right to privacy under Article 8 of the ECHR. In this context, the Court highlighted the fact that the prejudice to this protection, in the interest of patients as in the interest of the community as a whole, may be necessary for the investigation of criminal offences and the protection of open courts, when it is established that these interests are of much greater importance. However, it was acknowledged that it is advisable to grant the competent national authorities certain discretion to strike a balance between the protection of open courts, on the one hand, and the protection of the interests of people who wish to see their data remain confidential, on the other hand.

However, in the present case, the Court found that the reasons given by the public authorities in support of the justification of the disclosure of confidential medical information did not meet a social pressing need. In addition, it was found that the applicants were not the subject of a criminal investigation that could justify the application of such oppressive measures by the Russian prosecutors. Moreover, the public authorities did not take the opportunity to seek the consent of the applicants on the disclosure of the medical data in question. It is thus clear from this that the efforts to strike a fair balance between the applicants' right to privacy and the objective of the open court system, were not made.

Furthermore, by examining the criteria of legitimacy of the possible interferences in the right to respect for medical data under

the domestic laws, the Court referred to its well-established case law according to which such national measures clearly describe the scope and procedures for the application of said interferences, in order to provide individuals with the adequate guarantees against the risk of misuse and arbitrary power. Moreover, these procedures must be sufficiently accessible, comprehensive and foreseeable so as to enable them to regulate their conduct.

In this case, the Court found that national laws governing the access by Russian public prosecution authorities to the medical data of individuals were expressed in fairly general terms and lent themselves to an interpretation that was very broad, and, therefore, non-compliant with the conditions mentioned above. Therefore, the Court found a violation of Article 8 of the ECHR by Russia.

In a similar context, attention must be drawn to the ruling in the case L.H./Latvia dated 29 April 2014, in which the ECtHR tried to have the applicant's medical records processed by a State agency, the applicant not having given his consent. This processing was carried out with the objective of carrying out an administrative investigation on the quality of medical care received by the applicant in public health institutions. The Latvian national law authorised, in the past, the public departments to conduct investigations and controls by collecting patient medical data, on the grounds that such measures were necessary to improve the treatment and provision of medical care.

Firstly, the ECtHR noted that the collection of said data, carried out unbeknownst to the applicant and without his consent, began seven years after the medical operation of the applicant, in the public institution in question, which called into question the actual purpose of this collection. In addition, it was observed that the jurisdiction of the public departments and, consequently, the scope of the personal data that can be collected during investigations, were described in very general terms by the internal regulations, which did not offer the applicant adequate protection against arbitrary interference. In these circumstances, the ECtHR, by observing that the respect for confidentiality of medical data is essential to ensure respect for privacy of individuals as well as to preserve a relationship of trust with the medical profession and the healthcare departments in general, found a violation of Article 8 of the ECHR by Latvia.

European Court of Human Rights, ruling dated 06.06.13, Avilkina et al/Russia (request no. 1585-1509), European Court of Human Rights, ruling dated 29.04.14, L.H./Latvia (request no. 52019/07), www.echr.coe.int

IA/34056-A
IA/34055-A

[GANI]

- - - - - -

ECHR - Law governing the respect of privacy and family life - Retention of fingerprints of persons not convicted by public authorities - Refusal to carry out their removal from the automated fingerprint file - Use of data for police purposes - Discretion of national authorities in relation to the recording and duration of data retention - Fair balance between public and private interest - Absence - Violation of Article 8 of the ECHR.

In a ruling dated 18 April 2013, M.K./France, the ECtHR ruled that France had violated Article 8 of the ECHR due to the retention of fingerprints of a person charged with a criminal offence (hereinafter the "applicant") and by the refusal of the State prosecutor to carry out their removal.

It must be noted that no action was taken for the acts of which the applicant was accused and that he was not the subject of any criminal conviction. In this context, the justification provided by the State prosecution authorities against the removal of fingerprints consisted of the guarantee of protection of the applicant against acts of third parties that may impersonate him during possible future criminal offences. The retention of fingerprints in an automated file was prescribed by domestic law with the aim of detecting and, consequently, preventing such offences.

Firstly, the ECtHR reiterated that the retention of fingerprints of an individual in an automated file by the national authorities, constitutes an interference with the right to privacy. The domestic law must have sufficient guarantees pertaining to the duration of retention, its scope as well as protection against misuse, particularly in the context of use of data for police purposes, involving their automatic processing. Thus, the ECtHR conducted a review to verify whether the reasons adduced by the national authorities to justify the interference met a social pressing need, as required in a democratic society, and whether they were sufficiently relevant to achieve the legitimate aim being pursued.

Regarding the proportionality of the national measure which sought the addition and retention of data of a larger number of people, the ECtHR noted that, even if the terms of consultation of the fingerprint file were adequately regulated by domestic law, the French Government could not justify the reason why persons who were not convicted or prosecuted were treated in the same way as persons who had committed offences as serious as organised crime or sexual assault.

This measure posed a real risk of stigmatisation for some individuals, as in this case the applicant, who was accused of minor offences but was not convicted for them. In addition, the possible success of a request for removal of fingerprints, in the interest of such people, was a "theoretical and illusory" guarantee and not a "practical and effective" guarantee. Since the principle of the presumption of innocence was not respected by France, the Court held that disputed national measures were excessive in relation to the legitimate aim being pursued. The State, in fact, exceeded its discretion in the matter by failing to strike a fair balance between the competing public and private interests at stake and, therefore, violated the applicant's right to privacy.

European Court of Human Rights, ruling dated 18.04.13, M.K./France (request no. 19522/09),www.echr.coe.int

IA/34057-A

[GANI]

- - - - - -

ECHR - Law governing the respect of privacy - Refusal to order the removal of an article available in the online archives of a newspaper and damaging the applicant's reputation - Non-violation of article 8 of the ECHR

In its Chamber judgment, delivered in the Wegrzynowski and Smolczewski/Poland case, ECtHR unanimously held that Poland had not violated Article 8 of the ECHR, in that the Polish judicial authorities refused to order the removal of an article available in the online archives of a newspaper, which damaged the applicant's reputation.

...

In this case, two lawyers complained that a newspaper article, in which it was alleged that they had made a fortune by assisting politicians for dubious business transactions, damaged their reputation. In the first civil proceedings, the Polish courts, hearing an action for defamation, had held that the article in question was not substantiated by adequate information and went against the rights of those concerned.

Subsequently, after having found that the impugned article was still available on the newspaper's website, the applicants initiated a new civil proceedings against the newspaper, in which they sought a decision ordering the removal of the article from the site. Their request was rejected on the grounds that an order for withdrawal of the article from the website would constitute censorship and be tantamount to rewriting history.

Citing Article 8 of the ECHR, the applicants complained of the rejection by the courts of their request to withdraw the impugned article from the online archives of the newspaper.

The ECtHR declared the complaint inadmissible for one of the applicants, on the grounds that he had not filed his request within the prescribed period of six months after the final decision delivered by the Polish courts.

Concerning the other applicant, the Court observed that, in the context of the first civil proceedings, the latter had not made any request concerning the presence of the article on the Internet. The courts had not thus been able to rule on this issue. Accordingly, their ruling, in the first proceedings, could not create, for the applicants, a legitimate expectation of seeing the article removed from the newspaper's website.

The ECtHR upheld the decision according to which, in the second civil proceedings, the court held that it was not the responsibility of the judicial authorities to rewrite history by ordering the withdrawal from public domain of all traces of past publications that, by final decisions handed down by the courts, have been deemed to constitute unjustified harm to the reputation of individuals.

Moreover, according to the Court, it is necessary to take into account the aspect of legitimate interest of the public in the access to public electronic archives of the media, protected by Article 10 of the ECHR concerning freedom of expression.

Accordingly, the Court held that the Polish courts had struck a fair balance between, on the one hand, the public's right of access to information, within the meaning of Article 10 of the ECHR and, on the other hand, the applicant's right to protect his reputation, guaranteed by Article 8 of the ECHR. The ECtHR held, in particular, that the total withdrawal of the impugned article from the newspaper's archives would have been disproportionate. It also noted that the applicant had not requested the inclusion in the article posted online of a reference to the ruling in his favour.

European Court of Human Rights, ruling dated 16.07.13, Wegrzynowski and Smolczewski/Poland (request no. 33846/07)
www.echr.coe.int

IA/34060-A

[NICOLLO] [GALEAAN]

- - - - -

ECHR - Law governing the respect of privacy and family life - Freedom of expression - Orders for search and seizure insufficiently defined - Violation of Articles 8 and 10 of the ECHR - Protection of journalistic sources during a search - Violation of Article 10 of the ECHR

In its Chamber judgment, the ECtHR held that Luxembourg has violated Articles 8 and 10 of the ECHR, relating respectively to the right to privacy and to the freedom of expression, in that an order for search and seizure, granted by an investigating judge, was not reasonably proportionate to its purpose and not sufficiently restricted.

On 17 December 2008, the newspaper Contacto - edited by the applicant Saint Paul Luxembourg S.A. - published an article describing the situation of families that have lost custody of their children. The author of this article cited the name of a social worker and the children who were in his care, who complained to the competent authority. Following the opening of a judicial investigation by the prosecution against the author of the article on the basis of a violation of the law on the protection of youth as well as for slander or defamation, and for order search and seizure was issued by the investigating judge at the head office of the applicant, who was the editor of the newspaper Contacto. Armed with said search order, the police seized various documents.

Citing, one the one hand, Article 8, the applicant argued that the search at the premises of the newspaper (which she owns) had resulted in home invasion and was disproportionate and, on the other hand, Article 10, the applicant alleged a violation of her freedom of expression, since the impugned measure consisted of searching for sources of the journalist and would have had an intimidating effect.

Firstly, the Court considered that the investigating judge could have taken a less intrusive measure than a search to confirm the identity of the author of the article and that the search and seizure order was not reasonably proportionate to its purpose, resulting in a violation of Article 8 of the ECHR. Secondly, the Court considered that the said order was insufficiently restricted to avoid any possible misuse by investigators, like the search for the journalist's sources for example, causing a violation of Article 10 of the ECHR.

Attention must also be drawn to another ruling pertaining to Article 10 of the ECHR, in which the ECtHR ruled against Latvia in that the Latvian investigation authorities did not sufficiently protect the journalistic sources while searching the journalist's house.
Her house was searched following a programme broadcast in February 2010, in which she had informed the public of a leak of information from the database of tax authorities relating to incomes, tax payments and wages of officials; the said information had emanated from an anonymous source.

In its Chamber judgment of 16 July 2013, the Court stated that the right of journalists to not reveal their sources cannot be considered a mere privilege, which would be granted or withdrawn depending on the lawfulness or unlawfulness of the sources, but that it must be seen as an attribute of the right to information, and be treated with utmost caution. In this case, the investigating authorities did not properly weigh the interests of the investigation against the acquisition of evidence and the public interest in the protection of freedom of expression of journalists.

The Court found that the reasons given by the domestic authorities to support the conduct of the search were neither relevant nor sufficient and did not correspond to a social pressing need. The Court found a violation of Article 10 of the ECHR.

European Court of Human Rights, ruling dated 18.04.13, Saint-Paul Luxembourg S.A./Luxembourg (request no. 26419/10)

European Court of Human Rights, ruling dated 16.07.13, Nagla/Latvia (request no. 73469/10),
www.echr.coe.int

IA/34061-A
IA/34065-A

[NICOLLO] [GALEAAN]

- - - - -

ECHR - Right not to be tried or punished twice - Tax and criminal penalties for the same offence - Double prosecution for the same offence - Tax proceedings continued despite a final judgment in the criminal proceedings declaring the accused person not guilty - Violation of Article 4 of protocol no. 7

In a ruling dated 27 November 2014, Lucky Dev/Sweden, the fifth section of the ECtHR found that Sweden had violated Article 4 of Protocol 7 of the ECHR concerning the right not to be tried or punished twice.

In June 2004, the Swedish tax authorities initiated tax proceedings against the applicant with regard to income tax and value added tax for which the applicant was liable for the year 2002, and ordered the payment of a tax increase and tax penalties against him. The applicant, who was also the subject of criminal proceedings for accounting and tax offences related to the same tax returns, challenged this decision before the courts. She was convicted of the accounting offence but acquitted for the tax offence (on grounds of absence of intent). The tax proceedings lasted nine and a half months after the date on which her acquittal became final. In her application before the ECtHR, the applicant argued, in view of the prosecution initiated against her and the decision of payment of tax penalties arising from the same facts, that she was being tried and punished twice, in violation of Article 4 of Protocol no.7.

The ECtHR held in its ruling, after reviewing a formal question on exhaustion of domestic remedies, that Article 4 of Protocol No. 7 was applicable *ratione temporis* in the case, in the light of the Zolotukhin/Russia case (ruling dated 10 February 2009, request no. 14939/03), which made the said article applicable in Swedish cases concerning tax and criminal penalties imposed for the same facts. It then ruled that the tax penalty imposed in this case was of a criminal nature and that it had been imposed on the taxpayer for the same offence (same facts: failure to declare business profits and VAT amounts, the two proceedings - tax and criminal - pertain to the same period and essentially the same amount of tax fraud) as the one that led to the introduction of the criminal action for tax fraud. However, the Court did not consider that the action for accounting fraud was pertaining to the same facts as the action for tax fraud.

Then, the ECtHR reviewed the issue of duplication of proceedings (tax penalty imposed by the tax authorities and criminal action for the same facts), and recalled that Article 4 of Protocol 7 does not cover only cases of double conviction, but also cases of double jeopardy for the same offence.

...

This provision thus also applies when the person concerned has been prosecuted in proceedings that did not result in a conviction. However, the protection comes into play only after the final decision on the same offence is delivered; Article 4 of Protocol No. 7 does not prevent the conduct of several concurrent legal proceedings before taking final decision. There would, however, be a violation if proceedings continued after the date on which the other proceedings were concluded by a final decision. However, in the Swedish case, the tax proceedings had not ended and the tax penalties that had been imposed on the applicant had not been cancelled when the criminal proceedings against the applicant were completed by a final judgment. Instead, the tax proceedings continued for another nine and a half months. There was no connection that was sufficiently close, substantial or temporal, between the two proceedings so that they could be considered as part from same set of penalties. It should be recalled that, in the cases R.T./Switzerland (decision dated 30 May 2000, request no. 31982/96), and Nilsson/Sweden (decision dated 13 December 2005, request no. 73661/01), the ECtHR held that the decisions concerning the withdrawal of a driving license were directly based on an expected or final conviction for a violation of the Highway Code, and, therefore, gave rise to no separate examination of the offence or conduct in question.

In short, according to the ECtHR, the applicant was tried "twice", owing to an offence for which she had already been acquitted by a final judgment.

European Court of Human Rights, ruling dated 27.11.14, Lucky Dev/Sweden (request no. 7356/10),

EFTA Court

www.echr.coe.int

IA/33969-A

[JON]

- - - - -

Regulation (EEC) no. 95/93 - Allocation of slots at EEA airports - Intervention of public authorities - Fast-track proceedings before the EFTA Court

By a ruling delivered on 10 December 2014, the EFTA Court responded to a request for an advisory opinion addressed by the court of first instance of Reykjavik (Iceland) on the interpretation of regulation (EEC) no. 95/93 as amended by regulation no. 793/2004 determining the common rules for the allocation of slots at airports of the Community.

Icelandair and Wow air are air carriers providing regular air services to and from Iceland. The second is a new entrant. Isavia is the company managing the Icelandic international airport of Keflavík, which is a coordinated airport under the provisions of the regulation in question.

In November 2013, following a complaint by the company Wow air, the Icelandic competition authority considered that the procedure for allocating slots for takeoffs and landings at Keflavik airport were having a negative impact on competition. It then ordered the company Isavia to grant certain slots to Wow air for the flight schedule period of the summer

season of 2014, and to adopt the guidelines sent to the coordinator. In February 2014, the Appeals Chamber on competition annulled this decision, by considering that it should not have been addressed to the company but to the coordinator of the Isavia airport, who is the only one responsible for slot allocation under an independent power.

Wow Air challenged this decision of the Appeals Chamber before the court of first instance of Reykjavik, which questioned the EFTA Court on the status of the airport coordinator and the possibilities of intervention by public authorities in the allocation of slots on the basis of competition law.

The use of fast-track proceedings was decided by the President of the Court owing to the exceptional urgency presented by this case because of the special geographical situation of Iceland - Keflavík is the only international airport in the country - and the significant resulting economic sensitivity. This is the first use of fast-track proceedings.

On the one hand, the Court held that Regulation No. 95/93 requires the EEA States to ensure the appointment of a qualified airport coordinator, who must be independent by law and in fact and have a functional separation from any other party involved. From the moment these conditions are met, the EEA States have discretionary power to determine the status of the coordinator.

On the other hand, the Court considered that the complaint proceedings outlined in Article 11, paragraph 1, of regulation no. 95/93 as amended by regulation no. 793/2004 are not mandatory and cannot undermine the power of the competition authority to require the transfer of slots between air carriers and govern the manner of their allocation under national legislation or that of the EEA in matters of competition. Thus, the complaints relating to the allocations to of slots and based on considerations under the competition law may be submitted directly to the national competition authorities.

Although this regulation has rarely been invoked before the Court of Justice of the EU, the Commission has recently introduced infringement proceedings against Portugal concerning the independence of the coordinators (case C-205/14).

EFTA Court: Wow Air ehf./Icelandic competition authority, Isavia ohf. and Icelandair ehf., case E-18/14 dated 10.12.14, www.eftacourt.int

IA/34066-A

[SIMONFL]

II. National courts

1. Member states

Germany

Protection of individuals with regard to processing of personal data - Processing of personal data - "Autocomplete" function of a search engine - Damage to the honour and rights of personality by false factual allegations - Obligation of control and prevention incumbent on the operator of a search engine – Scope

Hearing an application for an injunction and damages, the Bundesgerichtshof

ruled, in a judgment dated 14 May 2013, on the responsibility of the operator of a search engine vis à vis violations of personality rights caused by the "Autocomplete" feature of a search bar. The application was made by a contractor to prevent his name from being associated, due to the automatic suggestion of certain search terms ("predictions"), to the term "Scientology" and to fraudulent activities, to the extent that the applicant was in fact involved in neither the said sect nor in such activities.

In this context, the Bundesgerichtshof considered that a violation of honour may result, in principle, from the "Autocomplete" function when the users of a search engine tend to presume the existence of an actual relation between the words inserted in the search bar and the "predictions". However, the finding of a violation of personality rights requires, according to the German judges, a balancing of those rights with the fundamental rights to free expression and economic freedom of the operator of the search engine. In this case, the Bundesgerichtshof was led to conclude the existence of a violation of personality rights of the applicant, since the "Autocomplete" suggestions in question would be tantamount to false factual allegations.

However, the Bundesgerichtshof specified that the tort liability of the operator of the search engine was subject to the further condition that measures likely to prevent the automatic display of the terms violating the personality rights may reasonably be required of it. In this regard, the German courts held that the role of the operator of a search engine with an "Autocomplete" feature does cannot be likened to that of a provider of a referencing service, since the latter, under Article 14 of Directive 2000/31/EC on electronic commerce, is exempt, as regards purely passive storage of information, from liability for the stored information. The programming and operation of an "Autocomplete" function constitute active intervention that falls, in principle, within the liability of the operator. However, according to the Bundesgerichtshof, the latter can be reasonably held responsible only for the failure of implementation of appropriate mechanisms for control and prevention of false factual allegations. However, this obligation of control cannot imply a general duty of verification of "Autocomplete" suggestions, but would manifest itself only when the operator having been informed of a misrepresentation caused by these suggestions, would nonetheless fail to stop it.

To the extent that the courts had not established all the facts necessary for determining if the conditions, thus defined, seeking to establish the liability of the operator of the search engine, were met, the Bundesgerichtshof referred the case to the Oberlandesgericht (Higher Regional Court) of Cologne. In a judgment of 8 April 2014, it accepted, on the basis of the legal guidance provided by the Bundesgerichtshof, the request for injunction and dismissed the request for damages, since a sufficiently serious violation of personality rights of the applicant was lacking.

In contrast to what the Court of Justice clarified in the Google Spain ruling, in respect of the liability of the operator of a search engine for the personal data displayed in the

list of results, the Bundesgerichtshof did not address the issue of the "Autocomplete" feature from the perspective of the right to protection of data, but has exclusively engaged in striking a balance between the different competing fundamental rights involved. Since the case before the Bundesgerichtshof referred to false factual allegations, it did not involve, for the applicant, being granted a "right to be forgotten". In this context, it will be noted, however, that this right, established by the Court in the Google Spain ruling cited above, has now been applied by several German courts, including the Landgericht (Regional Court) in Heidelberg which, in a judgment dated 9 December 2014, responds to a request to remove some links from a list of results, by supporting the interpretation recommended by the Court.

Bundesgerichtshof, ruling dated 14.05.13, VI ZR 269/12, www.bundesgerichtshof.de

Oberlandesgericht Köln, ruling dated 08.04.14, 15 U 199/11, www.olg-koeln.nrw.de

Landgericht Heidelberg, ruling dated 09.12.14, 2 O 162/13, www.landgericht-heidelberg.de /

IA/34115-A
IA/34120-A
IA/34116-A

[BBER]

- - - - -

Fundamental rights - Respect for private life - Right to digital self-determination - Balancing public interest in the fight against tax evasion - Purchase by the State of data media containing banking details of alleged tax evaders, obtained by confidential informant - Usage of these data for purposes of criminal investigation - Admissibility – Conditions

Hearing a constitutional appeal aimed at escrowing documents, particularly an index card of a Luxembourg bank and a request for registration in the shares register, the Constitutional Court of the state of Rhineland-Palatinate (Verfassungsgerichtshof of Rheinland-Pfalz) enquired, in a ruling dated 24 February 2014, into the impact of the fact that the suspected tax evasion justifying the investigation was based on the bank data acquired by the tax authorities from a private person based abroad. The ruling in question falls within the context of a debate about several cases of acquisition of data media ("Tax data - CDs") containing information on bank accounts held in Switzerland and Liechtenstein by alleged tax evaders. Since 2006, these measures have allowed the tax authorities to recover taxes amounting to an estimated several billion Euros.

In the present case, the applicant argued that the data obtained must not be used for purposes of criminal investigation, since their disclosure constituted an infringement of business secrets, which the authorities may have encouraged by following a practice of acquisition of media containing data relevant to the fight against tax evasion. According to the applicant, given the personal nature of the data involved, selling them for such purposes was inconsistent with the principle of legality, the "right to digital self-determination" (Recht auf informationelle Selbstbestimmung) and the protection of respect for private life.

However, the state concerned held, on the one hand, that the use of the data in question for the purpose of commercial transactions did not damage the core of the right to privacy and did

not thus benefit from absolute protection. On the other hand, according to the state, the public authorities were not responsible for a possible offence committed by the seller of said data and were entitled, as part of their investigative mandate, to take the opportunity to acquire the data representing a volume of tax evasion of around 500 million euros. The Verfassungsgerichtshof Rheinland-Pfalz dismissed the constitutional appeal against the judgments of the specialised courts confirming the validity of the investigative measures based on the bank data in question, by ruling, in accordance with a decision given in the context of another dispute by the Bundesverfassungsgericht (the federal Constitutional Court, order of 9 October 2010, 2 BvR 2101/09), that the fundamental rights of the applicant and, in particular, his rights to digital self-determination, to inviolability of the home and to a fair trial, had not been violated. While the use of bank data was, according to the Verfassungsgerichtshof, an interference in the right to digital self-determination, a balancing of this right against public interest in the fight against tax evasion led the Constitutional Courts to conclude that the measures in question which met the requirements arising from the principle of proportionality were justified. Specifically, they felt that since the information in question did not fall within the "core of private sphere" (Kernbereich persönlicher Lebens-gestaltung) but within the "economic sphere" of the applicant, the use of these data for purposes of criminal investigation need not necessarily, under the principle of legality, be substantiated by a specific legal base.

With respect to the fact that the data provider had evidently obtained said data illegally, the Verfassungsgerichtshof held that the applicant's right to a fair trial had not been violated, since the informant's actions were performed at his own initiative and were thus not attributable to the State. In these circumstances, the constitutional courts left the question of possible culpability of the State agents involved in the transaction incomplete, stating that this culpability was not, in any event, established with certainty. However, the Verfassungsgerichtshof also ruled that the acquisition of data media for purposes of criminal prosecution was admissible only insofar as the public authorities do not systematically encourage the committing of crimes. In this regard, the criminal courts will be required in the future, to determine whether, owing to the volume and frequency of bank data purchases, the theft of these bank data by private individuals should be attributed to law enforcement authorities who have encouraged it.

Verfassungsgerichtshof Rheinland-Pfalz, ruling dated 24.02.14, VGH B 26/13, www.mjv.rlp.de/Gerichte/Verfassungsgerichtshof/

IA/34113-A

[BBER]

- - - - -

**** Briefs (Germany)***

In a ruling dated 3 July 2014, the Bundesgerichtshof ruled on the admissibility of the retention by an Internet access provider of dynamic "Internet Protocol" (IP) addresses. The IP addresses of this type are allocated to users every time they connect to the Internet, for the purposes of communication with their local servers for the duration of use.

...

The storage of these data, for seven days, is intended to prevent “denial of service attacks" preventing proper operation of the service. In these circumstances, the Bundesgerichthof judged that the storage practise was permitted with regard to the German enacting terms transposing article 15 of the directive 2002/58/EC concerning processing of personal information and protection of private life in the domain of electronic communication. A different interpretation would not be imposed, particularly under the judgment of the Court in the Digital Rights Ireland case. In this regard, the German courts noted that, in this case, the retention of dynamic IP addresses was not intended, contrary to what the aforementioned directive indicated, for the provision of such data for the purpose of criminal prosecution and detection by the national law enforcement authorities, but exclusively for the maintenance of proper functioning of Internet access services by the access provider. Furthermore, the data in question have been stored only for seven days, which is a lot less than the minimum retention period of six months, provided for in Directive 2006/24/EC. For these reasons, the Bundesgerichtshof concluded that the practice of data retention in question was compatible with the Union law, without it being necessary to submit a preliminary question to the Court of Justice. On an ancillary basis, the case was an opportunity for the Bundesgerichtshof to note that it considers the dynamic IP addresses as traffic data within the meaning of Article 6 of Directive 2002/58/EC.

Bundesgerichtshof, ruling dated 03.07.14, III ZR 391/13, www.bundesgerichtshof.de

IA/34114-A

[BBER]

- - - - -

In a ruling dated 23 September 2014, the Bundesgerichtshof made clarifications with regard to the balancing of the right to protection of personal data with the interest of the operator of an online assessment portal, consisting of making information available to users. Hearing a request seeking to delete an assessment profile of a gynaecologist, the latter being aggrieved because of the diffusion, against his will, of objective information and assessments concerning his medical activities, the German courts ruled that the processing of personal data for the operation of such a portal falls within the scope of Article 29 of the law of data protection. (Bundesdatenschutzgesetz). This provision focuses, in particular, on the collection and storage of such data as part of a commercial activity, such as that of advertising agencies or intelligence companies, requiring their transmission to the public. Taking into account, on the one hand, the professional freedom and freedom of communication of the operator of the assessment portal and, on the other hand, the applicant’s right to “digital self-determination” (Recht auf informationelle Selbstbestimmung), the Bundesgerichtshof held that the online assessments can have a significant impact on the social and professional status of a physician. In this regard, the Bundesgerichtshof observe d in particular, referring to the judgment of the Court in the Google Spain case, that such information is easily accessible to all Internet users who search for details using the name of the physician concerned. Nevertheless, the German courts have concluded that the interference in the right to digital self-determination was not sufficiently serious to prevail over the interests of the operator of the portal. To the extent that the

applicant would be entitled, where appropriate, to request the removal of false factual allegations and abusive assessments, he is obligated to accept the maintenance of his profile.

Bundesgerichtshof, ruling dated 23.09.14, VI ZR 358/13, www.bundesgerichtshof.de

IA/34117-A

[BBER]

Austria

Retention of data generated or processed in connection with the provision of publicly available electronic communications services - Directive 2006/24/EC - Interference - National legislation non-compliant with the requirement of proportionality

The Verfassungsgerichtshof (Constitutional Court, hereinafter the "VfGH") ended in June 2014, a controversy that lasted several years on the protection of personal data, by ruling that the laws transposing the Directive 2006/24/EC did not meet the requirements of the fundamental right to data protection.

The VfGH took this decision following the Digital Rights Ireland ruling, in which the latter had found, at the request of the VfGH and the High Court (Ireland), the Directive 2006/24/EC to be invalid. In that decision, the Court recalled that the said directive aims to ensure the availability of data for the prevention, investigation, detection and prosecution of serious crimes, including those linked to organised crime and terrorism. Thus, the directive provides that the providers of communications services must retain the traffic data, the location data and the related data necessary to identify the subscriber or the user. On the contrary, it does not authorise the retention of the content of the communication and information consulted. The Court of Justice thus formed the opinion that these data, taken together, are likely to provide very precise information on the privacy of persons whose data are retained. This data includes habits of daily life, places of residence, travel, activities performed, social relationships and social circles frequented.

Several appeals, seeking the annulment of certain provisions of the Telekommunikationsgesetz (law on telecommunications), the Sicherheitspolizeigesetz (law on the security police) and the Strafprozessordnung (law on criminal procedure) introduced for the purpose of the transposition of Directive 2006/24/EC, were responsible for the request for a preliminary ruling of the VfGH. The applicants considered, in particular, that the impugned provisions violated the fundamental right of individuals to the protection of their data.

In its judgment in consideration, the VfGH emphasised, first, that data retained were thus used for the detection of thefts and situations of harassment. However, the data was never used for the detection of crimes related to terrorism. It explained further that the fundamental right to data protection is indispensable for the proper functioning of a democratic society, in order to ensure the communication in a confidential manner. The VfGH particularly criticised the fact than the transposition laws did not have adequate safeguards to protect personal data against abuse. It stressed that these laws did not have any obligation to install an independent body to monitor the use of data and that the right of an individual to request the removal of data is not safeguarded.

The VfGH admitted, however, that data retention could be justified for the purposes of the fight against serious crimes in cases where the provisions governing the retention would meet the stringent requirements of data protection of the Charter and the Austrian law on data protection. Given the magnitude and seriousness of the interference with the fundamental rights, these provisions must in particular limit access by national authorities to data and their subsequent use for purposes of prevention, detection or criminal prosecution of offences considered as sufficiently serious to justify such interference.

In light of the foregoing, the VfGH decided to repeal the national provisions in question.

Verfassungsgerichtshof, ruling dated 27.06.14, G 47/2012-49, G 59/2012-38, G 62/2012-46, G 70/2012-40 and G 71/2012-36,www.vfgh.gv.at/cms/vfgh-site/attachments/1/5/8/CH0006/CMS1409900579500/vds_schriftliche_entscheidung.pdf

QP/07784-P1

[KAUFMSV]

Belgium

Protection of individuals with regard to processing of personal data - Respect for privacy and family life - Freedom of expression - Balancing these two fundamental rights - Posting of archives of a daily online - Right to be forgotten of a person having been the subject of a news article - Non-contractual liability of the daily editor*

In its ruling dated 25 September 2014, the Liège Court of Appeal was called upon to settle a dispute between a doctor who caused, when drunk, a serious road accident in 1994, and a daily that had implemented since 2008, free access on its website to all of its articles published since 1989, including the electronic version of an article from the time of the accident caused by the doctor and stating the facts of that accident, for which the doctor had been convicted in criminal proceedings. The name of the doctor, who was the subject of a rehabilitation decision in 2006, was explicitly mentioned therein.

Considering himself disadvantaged by this online post, which allowed, by way of a request initiated using his first and last names, not only through the search engine available on the newspaper's website, but also through other search engines such as Google, dissemination of the article concerning him, the doctor requested the anonymisation of that article. Since he did not receive any positive response to his request, the doctor brought an action before the civil courts, based on an alleged tort liability of the editor of the daily under Article 1382 of the Civil Code.

After having reiterated that the parties to the proceedings were each entitled to fundamental rights of equal value, i.e., freedom of expression for the daily, and the right to respect for private and family life for the doctor, the appeal court emphasised that the right to digital oblivion was established by the Court of Justice in its Google Spain ruling. In light of these observations, the Appeal Court, by balancing the different protected interests, ruled that, by refusing, in the specific context of the case and without reasonable cause, to accept the doctor's request for anonymisation, although this request was part of a legitimate claim of right to be

forgotten, and did not constitute a disproportionate
interference in the freedom of expression of the press, the editor was at fault within the meaning of Article 1382 of the Civil Code and caused prejudice to the doctor. The editor was therefore ordered to ensure the anonymisation of the electronic version of the article in question, and to pay a symbolic euro to the doctor, as non-pecuniary damage.

Liège Court of Appeal, ruling dated 25.09.14, 2013/GR/393, Nieuw Juridisch Weekblad 2015, p. 26,
www://jure.juridat.just.fgov.be/JuridatSearchCombined/?lang=fr

IA/34207-A

[EBN]

Bulgaria

Protection of individuals with regard to the processing of personal data - Directive 95/46/EC, Articles 2 and 6 - Internet search engines - Processing of data on websites - Search, indexing and storing of such data - Liability of individuals owning websites, when processing personal data

In a ruling dated 2 July 2014, the Administrative Court of Sofia - grad ruled on the liability of the persons owning websites, when processing personal data, referring to the Directive 95/46/EC. The facts, in this case, are very similar to the facts of the Google Spain ruling.

In this case, the applicant, Mr B, as a private bailiff, appealed against the decision of the personal data protection commission accepting the claim of an individual, Ts. B., who alleged that the entry of his name in the "Google" search engine in 2013, presented, in the list of first results, a link that redirected the user to the digital page of the Chamber of private bailiffs concerning a notice of real estate auction, which contained personal data and data relating to his wife, their names and their national identification numbers (EGN), and the characteristics of the building in question.

In his complaint, Ts. B. contacted the personal data protection commission as the control authority to order Google to remove this information from the Internet, insofar as the said auction had ended in 2010, and the mention of it was now completely irrelevant.

In its reasons, the personal data protection commission noted that, given the sensitivity of the information contained on this webpage on the private details of this person, and the fact that it was first published three years ago, the person concerned is entitled to have this information disassociated from his name through such a list and that, therefore, the data controller had not implemented the appropriate technical and organisational measures to protect the personal data of the person concerned and had thus allowed easy and unauthorised access to the personal data in question.

By its judgment of 2 July 2014, the Administrative Court of Sofia - grad upheld the decision of the personal data protection commission based on Article 23, paragraph 1, of the law on the protection of personal data, transposing Article 6, paragraph 1, d) of the Directive 95/46 / EC which states that: "... all the reasonable steps must be taken so that the inaccurate or incomplete data, with regard to the purposes for which they were collected or for which they are further processed, are erased or rectified...".

In its judgment, the court held that, in respect of a situation like the one at issue, the announcement specifying the name and national identification number of that person was not necessary for the real estate auction since the aim of the announcement consisted of the possibility of ensuring access to information relating to the individualisation of the building in question and the conditions of its public sale. Therefore, the publication of the applicant's personal data was beyond these objectives. Similarly, the national court pointed out that it was the responsibility of the private bailiff to perform periodic checks on the announcements relating to the enforcement cases that were already closed and to remove them, if applicable. There non-performance of this obligation is an offence for which criminal and administrative liability may be engaged.

It should be noted that the obligation to publish announcements relating to the real estate auctions on the Internet is provided for in the Code of Civil Procedure. This publication is legally justified and is designed to give maximum publicity to the auction in order to ensure the participation of as many bidders as possible.

The emphasis, in this judgment, is more on the volume of data to be published and the duration of such publication on the Internet. Regardless of the liability of the private bailiff in this case, the question that arises is that of the liability of the Chamber of Private Bailiffs, which publishes on its web page, announcements of all private bailiffs, relating to auctions. In this regard, the national court found that the Chamber of Private Bailiffs may also be regarded as the "controller" of the data, as defined in Article 2 d) of Directive 95/46/EC and has an obligation to control the content of the publications as well as the duration of the publication. The said Chamber may not change the content of the existing publications, but can however ensure that they are not available on the Internet, in case of non-compatibility with the law on protection of personal data or delete the data already published in the event of termination of the executive proceedings.

Note that this ruling, which has not been the subject of an appeal before the Supreme administrative court, is thus, final.

Administrativen sad - Sofia grad, ruling dated 02.07.14, No. 4516, www://domino.admincourtsofia.bg/BCAP/ADMC/WebData.nsf/ActsByCaseNo/2AC49528A331DB0EC2257D0A00444F06/$FILE/temp4182363986111113945O1E98D51A734C2257D0A003B43E4.pdf

IA/33646-A

[NTOD]

**** Brief (Bulgaria)***

In a judgment of 7 February 2013, the Supreme administrative court upheld the judgment of the Administrative Court of Sofia - Grad on the issue of a fair balance between freedom of expression and provision of information and the processing of personal data for journalistic purposes.

In the case in the main proceedings, it refers to the publication, in its entirety, on the Internet, of the charge sheet of an individual.

There Supreme administrative court as well as the Administrative Court of Sofia - grad note that the processing of personal data is, in principle, permitted in public interest and for journalistic purposes, but must however respect the principle of reciprocity of data, under Article 2, paragraph 2, point 3 of the law on protection of personal data.

Therefore, the administrative high court decided that the relevant persons responsible for the publications should remove some of the applicant's personal data, such as the identification number and age, since mentioning them does not seem relevant in view of the legitimate objectives pursued. The information relating to the name of the person must be regarded as sufficient for the purpose of his identification by the public, which would justify the journalistic purpose in this case.

The Supreme administrative court finally ruled that the publication of additional data could encourage the misuse of such information.

Varhoven administrativen sad, ruling dated 07.02.13, no. 1811, www://www.sac.government.bg/court22.nsf/d6397429a99ee2afc225661e00383a86/f4378614df7ecdc6c2257b08002ccd35?OpenDocument

IA/33647-A

[NTOD]

Cyprus

Retention of data generated or processed in connection with the provision of publicly available electronic communications services - Directive 2006/24/EC - Request for investigative measure concerning an IP address - Nature of an IP address as personal data - Effect of the Digital Rights Ireland ruling on national legislation

In the Isaias judgment dated 7 July 2014, the Supreme Court had occasion to rule on the nature of an IP address as personal data and on the issue of the effect of the Digital Rights Ireland judgment on the Cypriot law on the retention of telecommunications data for the purpose of investigating serious crimes, a law that transposed Directive 2006/24/EC.

The subject matter of the case was a request for an investigation of the telecommunications data as part of criminal proceedings. The case concerned a complaint filed by a user of the social network Facebook, on the grounds that his profile was hacked; the said hacking involved a change of his name to a vulgar name as well as the addition of an explicit photo depicting the latter. The victim, with the help of an acquaintance, who is a computer specialist, was able to track the IP address of the offender, and, thereafter, filed a complaint with the police providing it with the information collected on the IP address. After a request for an investigation pursuant to the Cypriot procedure, the police obtained from the telecommunications operator the information relating to the offender and arrested the perpetrator and his father, as owners of the IP address.

Following a certiorari request by the defendants, the trial judge quashed the request for investigation, which allowed the police to obtain information about the defendants via their IP address, by noting that an IP address can be described as personal data, which therefore falls within the category of confidential communication, in the same way as a telephone number.

Following this interpretation, the trial judge considered that the police should have obtained a warrant, allowing it to use the information collected by the victim.

As part of the appeal of the trial decision before the Supreme Court by the prosecuting attorney of the Republic, the Supreme Court, on the one hand, accepted the first ground of appeal**,** in that the trial judge was wrong in concluding that the request for investigation was based on an incorrect legal basis.

On the other hand, by ruling on the merits, the Supreme Court noted that it is only from the time when the service provider transfers the data of the IP address user that the said address can be considered personal data. Moreover, the Supreme Court found that the trial decision had not properly applied the Cypriot case law, particularly the Siamisis/Police ruling, (2011) A.A.Δ. 308, in which the Supreme Court had drawn a distinction between a public and private IP address, in the context of the acquisition by the police of personal data related to a private IP address without first obtaining a request for an investigative measure. Thus, the Supreme Court concluded that the police had in this case, followed the standard procedure, and that the request for investigation was enough. The Supreme Court also noted that the validity of the request for investigation was not affected by the Digital Rights Ireland ruling, invalidating the Directive 2006/24/EC, on the ground that the Cypriot law transposing it remained in force as domestic law.

It should be noted that, according to the dissenting judges, the police had an obligation to follow the procedure of a warrant application at the time of receipt of the complaint from the victim. More fundamentally, the dissenting judges felt that the Digital Rights Ireland ruling led to the invalidity of the Cypriot law and, therefore, the invalidity of the system allowing the police to access telecommunications data. According to them, it would not be appropriate to accept the request in question given the invalidity of the mechanism used for data retention by data providers. Accordingly, the dissenting judges, following the approach of the trial judge of quashing the request for investigation, would have dismissed the appeal.

Supreme court, second instance, ruling dated 07.07.14, no. 402/2012, Majority decision:
www.cylaw.org/cgi-bin/open.pl?file=apofaseis/aad/meros_1/2014/1-201407-402-12maj.htm&qstring=402%20w/1%202012
Dissenting opinion:
www.cylaw.org/cgi-bin/open.pl?file=apofaseis/aad/meros_1/2014/1-201407-402-12minor.htm&qstring=402%20w/1%202012

IA/34051-A

[LOIZOMI]

Spain

Protection of individuals with regard to the processing of personal data - Directive 95/46/EC - Information obtained from the name of an individual- Right to be forgotten on the Internet

In its ruling dated 29 December 2014, the Audiencia Nacional established the criteria relating to the recognition of the right to be forgotten, as a result of the Google Spain ruling.

The administrative dispute chamber of the Audiencia Nacional thus recognised, in accordance with the said ruling of the

...

Court of Justice, the right to request the removal from the list of results displayed after a search performed using a person's name, links to web pages published by third parties and containing personal information.

Firstly, the Audiencia Nacional held that the operation of a search engine must be classified as "processing" of personal data and the operator must be held responsible for this processing.

Secondly, when the search using this search engine is performed using the name of an individual, it is likely to significantly affect the fundamental rights to respect for privacy and protection of personal data. For this reason, this search cannot be justified by the economic interest of the operator of such an engine. A balance must be sought between the legitimate interest of internet users in the information and the fundamental rights of the person established in Articles 7 and 8 of the Charter.

Thirdly, the Audiencia noted that the person requesting the removal of the data, must indicate to the Spanish agency for data protection that the search was carried out using his name and the data obtained, and that the processing of personal data was "performed as part of advertising and business activities" of the operator responsible, on the territory of a Member State.

All this information must allow, according to the Audiencia Nacional, the particular circumstances of the person concerned to be taken into consideration to find the right balance between the rights and the competing interests involved, in which it is necessary to take into account the importance of the rights of that person and the compliance with the case law established by the Court of justice, so as to prevent the processing performed by the operator responsible from targeting these data.

Audiencia Nacional, ruling dated 29.12.14, no. 5211/2014,
www.poderjudicial.es

QP/07480-P1

[NUNEZMA]

- - - - -

Retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks - Directive 2006/24/EC - Declaration of invalidity - national transposition law

This ruling delivered by the Audiencia Provincial de Gerona is part of an action brought against the trial judge's refusal to allow the police to use the means of obtaining data, established by law 25/2007 transposing Directive 2006/24/EC, in order to obtain of information on the use of SIM cards contained in a stolen mobile phone, through mobile telephone companies.

The Audiencia Provincial de Gerona has taken account of the Digital Rights Ireland ruling in its interpretation of the law 25/2007. Firstly, this court observed that the Digital Rights Ireland ruling rendered Directive 2006/24/EC invalid on grounds that are not applicable to the law 25/2007 transposing the directive in Spanish law, to the extent that, if the ruling cited above finds a lack of requirement of judicial control prior to obtaining the data, the law 25/2007 requires a prior judicial authorisation in order to guarantee the principles of necessity and proportionality.

...

Nevertheless, the Court of Justice found that the said ruling imposed a limitation of cases in which data can be transferred and retained, for example, cases of serious crimes, insofar as an interference with a fundamental right would be justified only in these cases.

Following the ruling of the Court of Justice, the Audiencia Provincial de Gerona held that the authorisation for obtaining and retaining data as established by law 25/2007 should be issued only in the event of serious offences. The Audiencia Provincial stressed that the Spanish courts are bound by the case law of the Court of Justice, and that, although the Spanish legislature should have amended the national laws to conform to the requirements of the aforementioned ruling, the national courts must interpret the law in accordance with this case law.

Finally, the Audiencia Provincial de Gerona found that the theft of a mobile phone was not a serious enough offence to warrant obtaining of data through mobile phone companies.

Audiencia Provincial de Gerona, ruling dated 13.06.14, no. 304/2014, *www.poderjudicial.es*

IA/33963-A

[NUNEZMA] [GARCIAL]

Protection of individuals with regard to processing of personal data - Unauthorised recording of personal data in a debtor register accessible to the public - Right to honour

The Supreme Court, as part of an appeal, found an illegitimate interference with the right to honour owing to the unauthorised recording of personal data in a publicly available debtor register on the basis of the Organic Law 15/1999 on the protection of personal data.

In the present case, the applicants had concluded a service contract with a private security company, which included a contractual clause whereby such users undertook to use the said service for a minimum of twenty-four months and that gave the company, in the case of a termination of the contract before its term ended, the right to claim the amounts due until the actual expiry of the contract. Following the non-payment of the amount claimed by the company, the latter had unilaterally decided to register the applicants in a public debtor register.

In that judgment, the Supreme Court recalled its case law on the violation of the right to honour when personal data are recorded in such a medium, by examining the consequences of this registration from the point of view of the individual and in terms of the social context. In this case law, the effective dissemination of data is not a necessary condition for the finding of such a violation. If such dissemination has already taken place, where appropriate, the economic consequences of such violation shall be compensated as moral or pecuniary damages (see also STS 284/2009 of 24 April 2009).

Furthermore, referring to the regulation of the Union relating to the protection of personal data as well as the national laws, the Supreme Court noted that, in consideration of a breach of the right to honour, because of a registration like the one in this case, it must be verified that the data subject to processing are authentic, accurate and updated.

...

Tribunal Supremo, ruling dated 19.11.14, no. 2208/2013,
www.poderjudicial.es

IA/33964-A

[NUNEZMA]

**** Briefs (Spain)***

The Supreme Court ruled, in its judgment of 8 October 2014, and considering the declaration of invalidity of the Directive 2006/24/EC in the Digital Rights Ireland ruling, that the national investigating judges who grant authorisations for the interception of communication between individuals must assess the compliance of this interception with the rights enshrined in Articles 7 and 8 of the Charter, interpreted in the light of the principle of proportionality.

In this regard, the Supreme Court emphasised that the principle of proportionality must be interpreted in a strict manner and, therefore, phone tapping should be limited to cases of suspected offences regarded as being serious.

The case concerned persons belonging to an organised crime group that acquired tobacco illegally in cooperation with the Guardia Civil (military status security force) to subsequently distribute it. Phone tapping was authorised to stop these activities. The parties involved appealed against this phone tapping on the basis of Article 18 of the Constitution, establishing the right to confidentiality of communication.

However, the Supreme Court dismissed the applicants' appeal, considering that such tapping was justified in view of the seriousness of the offences.

Tribunal Supremo, ruling dated 08.10.14, no. 646/2014,
www.poderjudicial.es

IA/33962-A

[GARCIAL]

- - - - -

The Spanish Supreme Court made a sudden change in the case law relating to actions for protection of community trademarks, in order to harmonise the protection granted to the proprietor of the trademark in the regulations of all the Member states.

Traditionally, the Court Supreme required that the condition of prior introduction of the action for declaration of invalidity of the trademark registered later be met for the infringement action to be declared admissible.

However in the Fédération Cynologique Internationale ruling (C-561/11, EU:C:2013:91), the Court of Justice held, by interpreting Article 9, paragraph 1, of the regulation (EC) no. 207/2009, that the exclusive right of the proprietor of a Community trade mark to prevent all third parties from using signs identical or similar to its mark in the course of trade, extends to third party proprietors of a later Community trademark, without it being necessary that the nullity of the latter be declared beforehand.

Following this ruling, the Supreme Court stated that the proprietor of a previously registered trademark has the right to prohibit the use by any third party of a later

...

registered mark, without having to first obtain a declaration of nullity of the latter.

Tribunal supremo, ruling dated 14.10.14, www.poderjudicial.es

IA/33965-A

[NUNEZMA]

**** Brief (Estonia)***

In a ruling dated 15 January 2015, the Supreme Court ruled on the rights of a local authority relating to the organisation of waste collection in its territory.

In this case, the issue concerned the right of local authorities to provide, through a procurement contract, a predetermined facility for transportation of waste that is the subject of the said request. In particular, the local authorities of Surju, Tori, Paikuse, Tahkuranna and Sindi, as the contracting authority, designated for the transportation of waste a facility whose only operators were two local authorities - the Paikuse commune and the city of Pärnu. The Supreme Court, contrary to the court of appeal, accepted the request of the local authorities, considering that such a point in the specification did not violate the rights from the company in charge of the transportation of waste.

The Supreme Court explained that by initiating a procurement contract in the field of waste management, the contracting authority can provide a facility where waste is to be transported, taking into account all relevant considerations, including the waste hierarchy as provided in Article 4 of the Directive 2008/98/EC on waste and the principle of proximity laid down in Article 16 of that directive. Based on the case law of the Court of Justice, the Estonian high court reiterated that the movement of waste could be limited in order to ensure the protection of the environment (Ragn-Sells AS ruling, C-292/12, EU:C:2013:820) and that it should therefore be eliminated as near as possible to their place of production, so as to limit their transportation as much as possible (Commission/Federal Republic of Germany ruling, C-17/09, EU:C:2010:33).

Supreme Court, ruling dated 15.01.15, no. 3-3-1-68-14, www.riigikohus.ee/?id=11&tekst=222576874

IA/33977-A

[PIIRRAG]

France

Protection of individuals with regard to the processing of personal data - Directive 95/46/EC - Right of access of the person concerned to the personal data and the right to object to their processing - Right to request the removal of links to web pages from the list of results

By two interlocutory orders delivered in 2014, the Paris regional court accepted the requests for removal of links referenced by the search engine Google in order to end a manifestly unlawful infringement.

Firstly, in the case at the origin of an interlocutory order delivered on 16 September 2014, the applicants called into question the fact that at the time of searches performed using their surnames, the list of results obtained from the search engine referred to links comprising remarks that were deemed defamatory to them by a judgment of the criminal court of Grasse delivered on 13 March 2014.

...

To substantiate their request for delisting, the applicants invoked the law of 6 August 2004, transposing Directive 95/46/EC and the Google Spain ruling. In the case that was submitted before the Paris regional court, the company Google France challenged the admissibility of the request arguing, on the one hand, that the company is only involved in providing marketing and demonstration services to clients that use advertising services and, on the other hand, that it is outside the scope of the editorial activity or operation of websites managed by Google Inc., based in the United States. In this regard, the judge in chambers, referring to the Google Spain ruling, noted that Google France is a 100% subsidiary of Google Inc., whose business activity ensures the financing of the search engine, which means that the activities of Google France and Google Inc. are inextricably linked. Accordingly, the applicants are admissible in their claim against Google France, to the effect that the company carries out the necessary procedures to end the condemned violations. Therefore, the judge in chambers, noting that the remarks whose withdrawal was requested had been definitively deemed defamatory, considered that the request for delisting was well-founded, and ordered Google France to remove the impugned referenced links. This injunction was accompanied by a periodic payment of a penalty amounting to 1,000 euros per day of delay and the interim relief judge refused to limit it to only Google.fr links on the grounds that the defendant had not established the impossibility of logging in from French territory using other search engine endings.

Secondly, in the case at the origin of the order of 19 December 2014, the applicant, convicted in 2006, had made a request for delisting on the grounds that the operation of the search engine using his full name referred to sites indicating this conviction such that it interfered with his search for employment. Noting that the criminal conviction was delivered more than eight years ago and given the lack of mention of this conviction in bulletin no.3 of the criminal records, whose content is determined by the law establishing the conditions under which third parties may obtain information about the criminal status of persons, the judge in chambers considered that the applicant justifies the compelling and legitimate grounds prevailing over the right to information. Accordingly, the request for delisting was found to be justified. Unlike the case above, the court ordered Google Inc., and not Google France, to delist or remove links referring to the conviction of the applicant.

Paris regional court, interlocutory order dated 16.09.14, n° 14/55975,

IA/33649-A

Paris regional court, interlocutory order dated 19.12.14, n° 14/59124,

IA/33650-A

[WAGNELO]

- - - - -

European citizenship - Forfeiture of nationality of perpetrators of terrorist acts - Jurisdiction of the Constitutional Council to pass a preliminary ruling under the question prioritaire de constitutionnalité [priority preliminary ruling on constitutionality] (QPC)

In a decision dated 23 January 2015, the Constitutional Council, hearing a priority preliminary ruling on constitutionality concerning the compliance with the Constitution of the provisions of the Civil

Code regarding forfeiture of nationality of naturalised French persons perpetrating terrorism, considered that the said provisions were not unconstitutional and that it was not within its jurisdiction to pass a preliminary question to the EU Court of Justice to assess the compliance of these provisions with the principles of equality and non-discrimination enshrined in Articles 20 and 21 of the Charter and Article 18 of the TFEU.

Mr Ahmed S. acquired French nationality in 2002 while retaining his Moroccan nationality. He was convicted in 2013 on charges of participation in a criminal association for the preparation of an act of terrorism. By the decree of 28 May 2014, he was stripped of his French nationality under 1° of Article 25 and Article 25-1 of the Civil Code. He challenged this decision before the Council of State. The latter referred a priority preliminary ruling on constitutionality to the Constitutional Council.

At first, the Constitutional Council rejected the applicant's claim seeking to refer a preliminary question to the Court of Justice. The Constitutional Court then forwarded a preliminary ruling in the Jeremy F. case (decision no. 2013-314 QPC of 14 June 2013). However, the problem was different: "this matter involved knowing whether the lack of remedy under the criminal procedure code against the authorisation to extend the effects of the European Arrest Warrant (EAW) was a necessary consequence of the framework decision on the EAW. If [...] this lack of remedy resulted from the European acts, its compliance with the Constitution was ensured by the letter of Article 88-2 of the Constitution. [...] However, if [...] the lack of remedy could not find its source in these acts, it was incumbent upon the Constitutional Council to review it with regard to the constitutional requirements." (Constitutional Council, comment from the Mr Ahmed S. decision). In the Jeremy F. case, the interpretation given by the Court of Justice (see F. ruling, C-168/13 PPU, EU:C:2013:358) was thus a prerequisite for the exercise of constitutional review. However, in the Ahmed S. case, the Council sought its well-established case law (see decision no. 2009-605 DC of 12 May 2010) consisting of declaring that it did not have jurisdiction in the context of priority preliminary questions on constitutionality to examine the compatibility of national law with EU law and thus to refer a preliminary question to the Court of Justice. In this regard, the Council recalled that the review of complaints alleging violation of EU law and transmission of preliminary questions fall within the jurisdiction of the administrative and judicial courts.

Based on the merits, the Constitutional Council considered that the provisions in question were not contrary to the rights and freedoms guaranteed by the Constitution.

The facts of this case may be closer to those at the origin of the Rottmann judgment (C-135/08, EU:C:2010:104) in which the Court of Justice held that, if the definition of conditions of acquisition and forfeiture of nationality falls within the jurisdiction of each Member State, the latter must comply with EU law when the exercise of that jurisdiction affects the rights conferred and protected by the legal system of the Union, especially those arising from European citizenship. Mr Rottmann, an Austrian national, had subsequently obtained German nationality, which resulted in him forfeiting his original nationality. The German authorities had then ordered the withdrawal of the naturalisation on the basis of the fraudulent conduct of the applicant. There was thus a risk of statelessness and consequent forfeiture of the status of European citizen.

...

In the Ahmed S. case, if there is no risk of statelessness, the forfeiture of French nationality is likely to lead to loss of rights arising from European citizenship.

Constitutional Council, decision dated 23.01.15, Ahmed S., QPC 2014-439, www.conseil-constitutionnel.fr/

IA/33654-A

[SIMONFL]

**** Briefs (France)***

Three days after the delivery of the Digital Rights Ireland ruling, which it, however, did not refer to in its decision of 11 April 2014, the Council of State partially annulled decree no. 2011-1447 establishing a system for automated processing of personal data. That decree had introduced a provision in the criminal procedure code providing for the retention of personal data for five years from the end of the sentence or detention order that a person was subject to.

The Council of State thus held that the retention of data relating to persons who are not the subject of any sentence or detention order has no connection with the purposes of the automated processing of personal data, which is primarily intended to facilitate the management and implementation of measures for the application of sentences, probation and integration. According to the Council of State, the retention of these data being neither appropriate nor necessary to achieve the objectives that this automated processing seeks, the decree in question is partially deemed unlawful.

Therefore, the Council of State ordered the Prime Minister to consider, within a reasonable time period, a new decree amending the provision in question in order to provide for the removal of data relating to persons who are not the subject of any sentence or detention order.

Council of State, sub-sections 9 and 10 combined, decision of 11.04.14, no. 355624, www.legifrance.gouv.fr

IA/33648-A

[CZUBIAN]

- - - - -

Three individuals, opposed to a fourth individual who had posted information about them on his blog, referred the matter to the Court of cassation. The fourth individual had also released on the same blog, a direct reference indicating abuse and defamation that they had made about him. He had, moreover, introduced their full names as meta-tags in the source code of his web pages, thus guiding the users in searches pertaining to them. The three applicants in the appeal argued that the defendant engaged in the unauthorised use of their personal data, which constituted an infringement of their privacy. They therefore demanded that this unauthorised use be stopped, but their request was rejected by the Court of Appeal of Paris. Before the Court of Cassation, the applicants tried to argue, by analogy with the Trademark Law, that the use of their surnames in bad faith constituted an infringement of personality rights.

The Court of Cassation upheld the contested judgment according to which the choice of the name of an individual as a keyword for easy referencing by internet search engines of pages that support does not constitute a fault when it is not associated with any other personal data and becomes personal, where appropriate, only when the content of the page to which this keyword is associated is reprehensible.

...

Court of cassation (1st civil chamber), ruling dated 10.09.14, appeal no. 13-12464, www://legifrance.gouv.fr/

IA/33652-A

[ANBD]

- - - - -

In an order of 9 December 2014, the Council of State annulled an order of the judge in chambers rejecting the request of an applicant with Cameroonian nationality having sole parental authority over her daughter of three years, a Spanish national, seeking to suspend a prefectural decision opposing her with a denial of residence permit coupled with an obligation to leave French territory (OQTF).

The French authorities had considered that the applicant justified neither the resources required nor coverage by an appropriate health insurance, allowing her to benefit, as a mother of a minor citizen of the Union, from the provisions of Article 7 of the Directive 2004/38/EC on the right of EU citizens and their family members to move and reside and move freely within the territory of member States, and from the interpretation of the Court of Justice relating thereto.

Under Article 20 of the TFEU and four judgments of the EU Court of Justice (Baumbast, C-413/99, EU:C:2002:493; Zhu and Chen, C-200/02, EU:C:2004:639; Ruiz Zambrano, C-34/09, EU:C:2011:124 and Alokpa Moudoulou and C-86/12, EU:C:2013:645), the Council of State observed that the applicant was employed in a job conferring her stable resources and that, if she was receiving medical aid from the State, this was due to the fact that the lack of residence permit did not allow her to benefit from the compulsory health insurance for which she and her employer were paying their social security contributions. In these circumstances, the applicant and her daughter could not be regarded as imposing an unreasonable burden on French government finances.

The Council of State then considered that the prefectural decision was a serious and manifestly illegal infringement of fundamental freedoms, in this case those that the legal system of the Union attaches to the status of a citizen of the Union, justifying that it has accepted the request for liberty injunction of the applicant.

Council of State, summary judgement, order of 09.12.14, no. 386029, www://legifrance.gouv.fr/

IA/33651-A

[SIMONFL]

- - - - -

In this case, the brandy producers appealed in cassation against the conviction pronounced by the Bordeaux Court of Appeal against them for having carried out direct maceration of wood chips in alcohol for the preparation of cognac.

The Court of cassation upheld the contested judgment in which, to establish the offences of deception and counterfeiting, the appeal judges held, first, that Regulation (EC) no. 110/2008, which defines brandies and spirits, does not prohibit traditional methods. The court of appeal said that the decrees of 15 May 1936 and 13 January 1938 and Decree No. 2009-1146 of 21 September 2009 repealing them, define the appellations of cognac. It then reiterated that only the traditional practice of aromatisation by addition of oak chip infusions in distilled water is known and no other practice is authorised.

...

Therefore, the infusion of chips in a product other than distilled water constitutes a tampering of the beverage. The defendants were fined for counterfeiting of food, drinks, drugs or agricultural products and deception based on the nature, substantial quality, origin or the quantity of goods and usurpation of the appellation of origin.

Court of cassation (criminal division), ruling dated 18.11.14, appeal no. 13-86660, 5752,
www://legifrance.gouv.fr/

IA/33653-A

[ANBD]

**** Briefs (Greece)***

In its ruling dated 26 June 2013, the Areios Pagos (Greek Supreme Court, hereinafter the "AP") examined the conditions for lawful processing of personal data.

The case concerned the collection and, subsequently, the disclosure, by the defendant party, of documents containing personal information about the applicant to the special council for public service, responsible for the evaluation of applications of state officials for the post of head of department of the Ministry of Economy, a procedure for which the applicant and defendant were candidates. These documents were pertaining to the sentence to imprisonment delivered against the applicant for a minor offence and to the various confidential reports concerning his professional misconduct. The purpose of the use of these documents was to weaken the application of the applicant and to thus give the defendant a competitive advantage during the evaluation procedure.

According to the AP, notwithstanding the availability of the documents in question in the archives of the Ministry of Economy, the common employment office of the disputing parties, the documents must not be excluded from the protection granted to personal data, in view of their confidential and sensitive content. In addition, the AP also considered that the processing of data in this case was neither dictated by the need for proper selection of the best candidate nor justified by the need to fulfil a legitimate predominant interest of the defendant. The lawful data processing conditions were, however, not complied with in that no prior authorisation was given by either the person concerned or by the National Data Protection Authority. Thus, the AP found that the unlawful disclosure of such data violated the personality rights, right to self-determination and right to protection of privacy and professional life of the applicant.

Areios Pagos, Politiko Tmima A1, ruling dated 26.06.13, no. 1355/2013, www://lawdb.intrasoftnet.com.nomos2.han3.ad.curia.europa.eu/nomos/3_nomologia.p hp (NOMOS database),

IA/34053-A

[GANI]

- - - - -

The ruling of 9 April 2013 of the Areios Pagos (Greek Supreme Court, hereinafter the "AP"), concerned the collection by the applicants, members of the board of directors of an association, of various documents concerning the activity of the defendant, a former director of the association, as part of its exchanges with public departments. The 42 documents collected were written by the defendant and consisted of complaints, claims, letters, reports and other official documents as well as several judicial and extrajudicial documents directly targeting the applicants.

...

The applicants requested psychometric assessment by an expert psychologist with the aim of characterising the mental state of the defendant before the court. The said assessment was carried out on the basis of information contained in those documents, which pointed to a psychopathological profile of the defendant.

In this case, the AP focused its deliberation on the concept of "information" as personal data. However, it was considered that the documents collected were incorrectly qualified as a "set of sensitive information" by the judgment of the Court of Appeal, which decided the case on the merits. Instead, they should have been regarded as administrative documents, in accordance with the national law, in that they corresponded to the prosecution of the defendant. However, the applicants could legitimately go through and keep these documents, to the extent that their content concerned them personally and could jeopardise their interests. In addition, the AP considered that the scientific opinion of the expert psychologist, which does not constitute a disclosure to third parties of any sensitive information known to him and is a mere expression of opinion of a person with specialised knowledge, cannot be considered or protected as personal data of the defendant.

Areios Pagos, Politiko Tmima B2, ruling dated 09.04.13, no. 637/2013, www://lawdb.intrasoftnet.com.nomos2.han3.ad.curia.europa.eu/nomos/3_nomologia.php (NOMOS database),

IA/34054-A

[GANI]

Hungary

Fundamental rights - Freedom of expression and information - Information society - Internet - Lack of moderation - Responsibility of the Internet content provider vis à vis the comments appearing on the website

Under the order of 27 May 2014 of the Constitutional Court, the website content provider is responsible for the content of the reactions of reader to an article on the website.

In the case at issue, a statement posted on a website resulted in a considerable number of reactions from readers. The site content provider immediately removed the reactions that seemed illegal, since they seemed to violate the rights of reputation of certain individuals. However, following appeals of the aggrieved persons, the civil courts of first and second instance and the Supreme Court established the tort liability of the content provider for violation of the rights of reputation of these individuals.

An association of content providers filed an appeal before the Constitutional Court challenging the restriction of freedom of opinion and thought, and freedom of the press. It stressed that the final civil judgment would make it impossible to operate websites on which users can respond via comments not subject to moderation.

The Constitutional Court was therefore invited to decide on the question of whether the site content provider is responsible with regard to the insertion of an unlawful comment by a reader even if it is unaware of the identity of the latter.

By rejecting the appeal, the Constitutional Court answered this question in the affirmative.

...

According to the court, although the responsibility of providers restricts the freedom of the press, this restriction is justified and proportionate. According to the Court, the provider's responsibility is justified since, in most cases, the perpetrator of the unlawful comment cannot be identified. It added that if we accept the provider's responsibility for comments subject to moderation - which is the case here - there is no reason to apply more favourable rules to the providers who are not in charge of moderation. The provider is thus held responsible in both cases, but the penalties imposed must be proportionate and may therefore differ from case to case. The Constitutional Court nevertheless refrained from pronouncing the proportionate sanction that could be applied in such cases.

According to two judges, who expressed partially different points of view, the appropriate penalty for such violation of individual rights is the so-called "notice and take down", which involves the immediate removal of the illegal comment.

Alkotmánybíróság, order of 27.05.14, no 19/2014. (V. 30.) AB, www.mkab.hu/letoltesek/abk_2014_17_alairt.pdf

IA/33961-A

[VARGAZS]

On 24 February 2015, the Supreme Court unanimously rejected an appeal by the mother a child, who was a member of the travelling community in Ireland, against the practice of admission to a school of Catholic boys funded by the State. The issue to be settled in that case was whether the practice of admission to the school, which, in accordance with its Christian ethics and mission, consists of give preferential access to candidates whose father or brother have already attended the school or who can claim a close family relationship with the school, constitutes indirect discrimination under Irish regulations relating to the principle of equality (the Equal Status Act 2000 as amended by the Equality Act 2004).

The main argument, in the context of a controversial historical situation of deprivation of the members of this community in terms of education, was that the admission rules giving preferential treatment to a student whose father has already attended the school ("the parental rule") is indirect discrimination against members of the travelling community, since this condition works against a community that was traditionally not educated.

The High Court, in the capacity of the lower court, had ruled that the "parental rule" in question did not have an indirect discriminatory effect, since it applies to any candidate who is not the son of a former student.

The Supreme Court quashed the judgment of the High Court, noting that under the relevant national laws, indirect an discrimination assumes the existence of a "particular disadvantage" which must be established by the applicant on the basis of statistical data concerning the practice of admission of children from the travelling community over a number years, while taking into account the admission practice reserved for other groups of comparison throughout the geographical area covered by the school's activities. The Supreme Court considered that the statistics produced by the applicant were insufficient to establish the existence of indirect discrimination.

It should be noted that, by establishing its "particular disadvantage" test, the Supreme Court did not refer to the extensive case law of the Court of Justice relating to indirect discrimination or that of the ECtHR.

It should finally be noted that in the United Kingdom, in the O'Leary and others / Allied Domecq Inns Ltd and others case, the travelling community was considered a racial group defined by reference to ethnic origin within the meaning of the relevant legislation (Race Relations Act 1976).

Supreme Court, ruling dated 24.02.15, Stokes / Christian Brothers High School Clonmel & anor, [2015] IESC 13, www.courts.ie

IA/33430-A

[CARRKEI]

Italy

Protection of individuals with regard to the processing of personal data - Responsibility of the hosting site provider - Obligation of due diligence of the website content – Absence

By the ruling of 17 December 2013, the Italian Court of Cassation ruled on the responsibility of the hosting site provider and, in particular, on the lack of due diligence obligation incumbent upon it.

A matter was referred to the Court of cassation by the Attorney General of the Republic, following the reformation of a trial judgment that found a lack of control by the management of Google Italy of the content of a video loaded on "Google video".

The core of the decision concerns two notions: first, that of "controller", taken from the definition contained in the privacy code that reorganised matters particularly based on directives 95/46/EC and 2002/58/EC on "privacy and electronic communications". Second, that of the "hosting site provider" under the legislative decree no. 70/2003 transposing Directive 2000/31/EC on electronic commerce. In this regard, the Court noted, firstly, that the controller is the one who determines the objectives, methods of processing and the instruments to achieve it and, secondly, that the hosting site provider provides a service for storing the information supplied by the recipient of the service. It follows from the interpretation of the concept of controller that the control of stored data is not incumbent upon the service provider.

The notion of hosting site provider corresponds, according to the Court of Cassation, to the one established by the working group comprising representatives of the data protection authorities of the States members. According to this group, the controller of the data uploaded to a hosting site is the user who processes such data for his own purposes. He is, therefore, solely responsible in case of violations of the rules on data protection. In its judgment, the Supreme Court makes a reference to the case law of the Court of Justice and, in particular, the Google Spain and Google France and Google judgments (C-236/08 to C-238/08 , EU:C:2010:159). Regarding the first case, the Court of Cassation has, by relying on the conclusions of the Advocate General,

considered that the Internet search engine provider becomes responsible for the processing when it can exert direct influence on the structure of the search index, for example, by favouring or not favouring the search of a particular site. Regarding the combined Google France and Google cases cited above, the Court of cassation endorsed the position of the Court of Justice according to which, the provider of a referencing service on the Internet, when it has not played an active role that is likely to give it knowledge or control of the stored data, cannot be held liable in respect of the data that it has stored at the request of an advertiser, unless, after having known the unlawful nature of these data or the advertiser's activities, it failed to act expeditiously to remove or disable access to the said data.

According to the Court of Cassation, the principles can be applied to the present case since the role of Google Italia srl was limited to providing a platform on which users can load their videos for which they are solely responsible. Therefore, it excluded the existence of an obligation of control of the provider because of the nature of mere "hosting" of the service, and a criminal liability with regard to the unlawful processing of data stored by users on a video platform available on the Internet.

Criminal Court of Cassation, sez. III, ruling dated 17.12.13, no. 5107,
www.dejure.it

IA/34059-A

[GLA]

**** Brief (Italy)***

The Italian Constitutional Court declared as contrary to Articles 2 and 3 of the Constitution - respectively concerning the respect for fundamental rights and the principle of equality - the seventh paragraph of Article 28 of Law No. 184/83, regarding access to information identifying the biological parents, as replaced by Article 177, paragraph 2 of legislative decree no. 196/2003 (Code of protection of personal data, hereinafter "the Code"), since it provides no procedure allowing the judicial authority, which is referred the matter by the child not recognised at birth, to ask the biological mother, who has not consented to be named in the birth certificate, if she wishes to maintain her anonymity.

According to this law, if the biological mother decides to give birth anonymously, the child unrecognised at birth does not have the option of knowing his mother's name. Article 93 of the code states that the person concerned can access only the information contained in the medical records of birth which does not identify the biological mother. Access to all information, including the identity of the mother, is possible only after a period of one hundred years after the birth.

The Constitutional Court, confirming its case law on anonymous births, reiterated that it aims to protect the life and health of the mother and child during pregnancy and childbirth, and intends to meet a public health objective, which is to ensure birth in the appropriate health conditions, while respecting the mother's decision for anonymity.

However, referring to the case law of the ECtHR, more specifically to the Godelli / Italy case (judgment of 25 September 2012, request no. 33783/09) and the Odièvre/France case (ruling dated 13 February 2013, request no. 42326/98), the Constitutional Court observed that, although the decision for anonymity entails the definitive surrender of parental authority,

it should not, in principle, imply an irreversible and definitive surrender of "natural parenthood".

In this regard, the Constitutional Court also stressed that the child's right to know its origins is an important element in the constitutional system of protection of the individual.

Therefore, the Court, not calling into question the principle of anonymous birth, declared the unconstitutionality of Article 28 of the aforementioned law, that it considered "excessively rigid" as regards the irreversibility of the secret, and asked the legislature to provide for a procedure whereby the court, hearing the person concerned, can ask the biological mother if she wishes to maintain her anonymity.

Constitutional court, ruling dated 18.11.13, no. 278,
www.cortecostituzionale.it

IA/34058-A

[RUFFOSA]

Latvia

**** Brief***

By a request filed before the Constitutional Court, the Supreme Court of Latvia asked a question on the compatibility of the provisions of Decree No. 331 of the Council of Ministers relating to the amount and the method of calculation of insurance compensation for moral damage caused to persons, with Article 15, paragraph 1, sub-paragraph 1, of the law on the mandatory insurance for civil liability of owners of land vehicles, and with Article 92, third paragraph of the Constitution that provides for the right to an adequate compensation (see also *Reflets No. 1/2014*).

In a judgment of 29 December 2014, the Constitutional Court ruled on that request, added to another application on the same subject, introduced by a private company that had invoked the incompatibility of the provisions of Decree No. 331 with Article 105 of the Constitution relating to the right to property. The Constitutional Court declared, inter alia, several provisions of Decree No. 331 as incompatible with Article 15, paragraph 1, sub-paragraph 1 of the law and certain provisions of the same decree as incompatible with article 105 of the Constitution. In contrast, the Constitutional Court found no incompatibility with Article 92 of the Constitution.

The Constitutional Court held, referring to the Commission/Denmark judgment (C-143/83, EU:C:1985:34), that the Member States are obligated to ensure the precise transposition of provisions of the directives, which must be done in clear and precise manner in order to enable a proper understanding of rights and obligations.

Furthermore, this obligation must not be interpreted strictly as applying it only to the legislator. Thus, according to the Constitutional Court, in the event that the legislator has delegated the resolution of certain issues to the executive authority, the latter has the obligation of ensuring the full transposition of the provisions of the directives in the Latvian legal arsenal. Otherwise, it would not be possible to achieve the objectives sought by the directives.
Latvijas Republikas Satversmes tiesa, ruling dated 29.12.14, no. 2014-06-03,
www.satv.tiesa.gov.lv/upload/spriedums_2014_06_03.pdf

IA/33966-A [BORKOMA]

...

Netherlands

Protection of individuals with regard to the processing of personal data - Directive 95/46/EC - Scope of application - Automated personal data set that is not a personal data file - Inclusion

In its judgment of 16 July 2014, relating to the interpretation of Directive 95/46/EC, the Dutch Council of State held that article 3 of the Directive, read in the light of recitals 15 and 27, must be interpreted as meaning that the automated processing of personal data falls within the scope of application of the Directive, unlike the non-automated processing of personal data, where all such data cannot be considered a personal data file.

In the present case, the applicant, a former employee of the municipality of Zevenaar, had requested access to his personal file, which was refused by the Board of the mayor and aldermen of that municipality. This involved, in particular, documents drawn up by city officials, including letters and reports of discussions conducted.

At trial, it was found that access to the said documents had been rightly denied, in that the digital documents in question did not constitute a personal data file, within the meaning of the national legislation and article 2 c) of the aforementioned directive, to the extent that these documents were not a structured set of personal data.

The Council of State noted that the aforementioned directive aims to differentiate automated processing of personal data from non-automated processing of the said data.

Therefore, as regards the automated processing of personal data, it is irrelevant whether the data in question constitute or not a file within the meaning of Directive 95/46/EC.

It is important to note in this regard that the Council of State will, thus, against its own judgment of 30 January 2013, in which it had held that the "file condition" applied not only to non-automated processing of personal data but also to automated processing of the data.

Raad van State, ruling dated16.07.14, 201304235/1/A3,
www.rechtspraak.nl
ECLI:NL:RVS:2014:2594,

IA/34205-A

[SJN] [DEBRUGU]

**** Brief (Netherlands)***

In its judgment of 27 May 2014, as part of a criminal case, the Amsterdam Court of Appeal ruled that the declaration of invalidity of directive 2006/24/EC, pronounced by the Court of Justice in the Digital Rights Ireland case, did not imply the automatic revocation of the Dutch legislation transposing the directive. Since the Dutch legislation is based on Article 87 of the Constitution, according to which a bill becomes law after its adoption by the States General and its ratification by the King, the argument that renders the said Dutch legislation invalid, following the judgment of the Court of Justice, is factually incorrect, according to the Court of Appeal.

It is interesting to note that, in the opinion of 17 July 2014, the Council of State came to the same conclusion as the Amsterdam Court of Appeal.

...

Following the Digital Rights Ireland ruling, the Dutch minister for Security and Justice had asked the Council of State to rule, by way of opinion, on the consequences of this Court ruling on the relevant Dutch legislation transposing the directive. However, the Council of State concluded, referring to Article 51 of the Charter, that the said Dutch legislation is contrary to Articles 7 and 8 of the Charter.

Nevertheless, the Dutch legislator will have to examine to what extent the judgment of the Court of Justice involves modifying said national legislation. It should be noted in this respect that the bill amending the relevant Dutch legislation is dated 17 November 2014. One proposal is to limit the possibility of accessing the data from telephony for a period of twelve months for serious offences subject to an eight-year prison term at least. For other offences for which remand is warranted, access to such data is limited to six months. Furthermore, it is proposed that the prosecutor may order such access only in case of prior authorisation from the investigating judge.

Finally, it should be added that even in a very recent judgment in a civil case, the interim relief judge of the trial court of The Hague declared the Dutch legislation transposing Directive 2006/24/EC as unenforceable for breach of Articles 7 and 8 of the Charter, given that the violation of the right to privacy and protection of personal data is not reduced to what is strictly necessary.

Gerechtshof Amsterdam, ruling dated 27.05.14 23-005230-12,
www.rechtspraak.nl
ECLI:NL:GHAMS:2014:2028

IA/34206-A

Rechtbank Den Haag, voorzieningenrechter, ruling dated 11.03.15, C/09/480009,
www.rechtspraak.nl
ECLI:NL:RBDHA:2015:2498

IA/34208-A

[SJN] [DEBRUGU]

Poland

Retention of data generated or processed in connection with the provision of publicly available electronic communications services - Directive 2006/24/EC - Respect for privacy - Use by State authorities of the data retained by telecommunications operators - Absence of independent control of the supply of data, the obligation of destruction of irrelevant or prohibited documents as procedural acts - Incompatibility with the Constitution

In its judgment of 30 July 2014, the Trybunal Konstytucyjny (Constitutional Court) ruled on the compatibility with the Polish Constitution of certain legislative provisions relating to the use of personal data transferred by telecommunications operators to State authorities and departments responsible for fiscal control and security.

The proceedings before the Constitutional Court were initiated by requests for constitutional review by the Ombudsman and the Attorney General. The said request did not cover national provisions relating to the
obligation of telecommunications operators with regard to data retention, being a direct transposition of Directive 2006/24/EC, and declared invalid by the Digital Rights Ireland ruling.

In this regard, the Constitutional Court expressly found that it was not bound by that judgment of the Court in these proceedings, provided that the provisions in question did not constitute a transposition of directive 2006/24/EC. It nevertheless felt it necessary to take the judgment into consideration, in this case, as a "background of the decision", given the functional correlation between the impugned provisions and directive 2006/24/EC, and the degree of protection of the right to privacy under the Charter.

The Constitutional Court examined the provisions in question, mainly in the light of Articles 47, 49 and 51 of the Constitution enshrining the respect for fundamental rights related to the respect for privacy and communication and protection of personal data. On the one hand, it reiterated that the said rights are guaranteed both constitutionally and internationally and that their limitation may be invoked only in exceptional cases. On the other hand, it stressed that the obligation for State authorities to create conditions for citizens to enjoy freedoms and associated rights also involves, among others, the need to ensure the security of citizens, independence of the State, and the proper functioning of the administration. This results in the need to provide State authorities with the means that allow them to ensure effective execution of their tasks, including those offered by modern technology.

After an in-depth analysis of the national provisions in question, the Constitutional Court deemed them to be unconstitutional, as long as they did not include certain rules pertaining to the transfer of data and their subsequent processing by the State authorities. Firstly, the Constitutional Court deemed as unconstitutional the omission of rules providing for independent monitoring of the transfer of data by telecommunications operators to State departments. Then, it deemed as unconstitutional the lack of guarantee of immediate destruction of the material containing information covered by professional secrecy, excluded as evidence, according to the procedural rules in the absence of a decision of the court of competent jurisdiction. Finally, it deemed as unconstitutional the lack of obligation of destruction of the material that has no relevance to the proceedings at issue. In essence, it appears from the judgment that, by way of the said omissions, the right balance between the need to transfer information enabling State departments to perform their tasks and the need to ensure the protection of constitutional rights of citizens, has not been achieved by the national legislator.

Given the damage that the immediate effect of its judgment would cause, particularly to the fight against crime, the Constitutional Court ruled that the provisions in question shall remain in force for a period of 18 months following the promulgation of the ruling in the Official Journal.

Trybunał Konstytucyjny, ruling dated 30.07.14, K 23/11,
http://otk.trybunal.gov.pl/orzeczenia/ezd/sprawa_lista_plikow.asp?syg=K%2023/11

IA/33974-A

[PBK] [JURAGAD]

**** Briefs (Poland)***

In a judgment of 21 August 2013, the Naczelny Sąd Administracyjny (Supreme Administrative Court, hereinafter "NSA") interpreted, among others, Article 18,

paragraph 6, of the Polish law on the provision of electronic communications services, the article transposing Article 4 of Directive 2006/24/EC.

The dispute concerned the request of a company to the Inspector General for personal data protection and the decision of thus authority ordering the provider of electronic communications services to transfer personal data of writers of comments on an Internet forum, on the grounds of violation of the right to image of the said company. The provider of electronic communications services submitted the matter to a voivodship administrative court, which annulled the decision of the Inspector General accepting the request, by concluding that only State authorities are allowed to request the transfer of such data. That decision was challenged in an appeal in cassation brought before the NSA.

Referring to the Bonnier Audio AB and Others ruling (C-461/10, EU:C:2012:219), the NSA noted that the provisions of EU law are not opposed to prescriptive national rules that allow ordering of the transfer of personal data to an individual, which are indispensable for the protection of his interests in civil court proceedings. The onus, however, in on the administrative authorities to weigh, taking into account the special circumstances of the case, the right to protection of personal data, on the one hand, and the right to dignity, honour, reputation or the image of a company, on the other.

Naczelny Sąd Administracyjny, ruling dated 21.08.13, I OSK 1666/12,
http://orzeczenia.nsa.gov.pl/doc/2650539008

IA/33975-A

[PBK] [JURAGAD]

- - - - -

In a judgment of 13 February 2014, the Naczelny Sąd Administracyjny (Supreme Administrative Court, hereinafter "NSA") commented on the relation between the obligation for an employer to ensure the protection of personal data of its employees and the respect for the right to privacy of the latter.

The main proceedings concerned the appeal by an employee to the Inspector General for personal data protection concerning the legality of a system for monitoring and recording connections established by employees between the internal network of the establishment of the employer and external networks.

In its judgment, the NSA concluded that the system in question is indeed an employee monitoring system. Although the protection of personal data held by the controller is subject to the obligations of the latter and the system for monitoring connections is in principle intended for the protection of personal data, the employees should be informed of its existence and the rules governing its operation. By invoking Article 8 of the ECHR and the Lynette Copland/United Kingdom case (judgment of the ECtHR of 3 April 2007, request no. 62617/00), the NSA found that the failure of an employer to fulfil its obligation to inform the employees of the existence of the system in question constitutes a violation of the right to respect for privacy. In addition, such monitoring should also comply with the provisions of the law on the protection of personal data transposing directive 95/46/EC.

Naczelny Sąd Administracyjny, ruling dated 13.02.14, I OSK 2436/12,

...

http://orzeczenia.nsa.gov.pl/doc/A2B1C2D069

IA/33976-A

[PBK] [JURAGAD]

Portugal

Protection of individuals with regard to processing of personal data - Respect for privacy - National legislation prohibiting the use of remote electronic surveillance means at the workplace to monitor the work performance of employees - Installation of GPS technology on board heavy vehicles carrying dangerous substances - Non-violation

By its judgment of 13 November 2013, the Supremo Tribunal from Justiça (Supreme Court) had to rule on the issues of whether GPS technology ("Global Positioning System", hereinafter "GPS") constitutes a "means for remote monitoring" at the workplace within the meaning of the Labour Code and whether the use, by an employer, of this technology in a truck carrying dangerous substances violates the rights to the protection of personal data and privacy of an employee.

This judgment originated from an application for review introduced by a fuel transport company that had dismissed a worker, who was the driver of a truck carrying dangerous goods, on the grounds that he had on several occasions during work time not taken the route planned for the transport of these goods.

In support of its application, the company argued, in particular, that the GPS cannot be considered as a means for remote monitoring intended to monitor the work performance of workers. Rather, it would correspond to a technological means for comprehensive monitoring that can help remotely track, during transit, the vehicles and the goods that they carry, in particular dangerous goods, and thus, ensure the safety of people and goods. Moreover, according to the applicant, the installation of this technology had been imposed on it owing to the highly flammable nature of the goods transported and therefore would not require the prior authorisation of the National Commission for Data Protection.

Called upon to deliver a final judgement, the Supreme Court ruled that it follows from the systematic and teleological interpretation of the relevant provision of the Labour Code that the concept of "remote monitoring means" rather comprises the technology of capturing images and sounds to identify people and their behaviour. Therefore, according to the high court, the GPS cannot be considered as a means for remote monitoring at the workplace intended for monitoring work performance, in that this technology does not allow the monitoring of behaviour of drivers of vehicles but only to know their physical location in real time.

Regarding the question of whether the use of the information contained in the GPS is a violation of personality rights of the workers and, in particular, an interference with the right to respect for privacy, the Supreme Court held that, given the objectives pursued and the various legitimate interests at stake, the use by the employer of the information contained in the GPS did not violate the respect for privacy of the workers.

In this case, the information obtained was used only to prove that the driver had not followed the route map established by the employer and not to determine what he was doing in the different places he visited during working hours.

Following this judgment, the National Commission for Data Protection said that the interpretative framework of national legislation in this area must be reviewed owing to the rapidly evolving geo-tracking technologies, in particular the increase in accuracy and the new functionalities of these technologies. Consequently, it approved in October 2014, a decision applicable to the processing of personal data collected in the context of work relations through the use of geo-tracking technologies. Through the latter, it set, among others, the conditions, purposes of the data processing and limitations applicable to the use by employers of information collected through geo-tracking technologies in vehicles.

Supremo Tribunal de Justiça, ruling dated 13.11.13, available on:
www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/e32eab3444364cb980257c2300331c47?OpenDocument

IA/33973-A

[MHC]

Czech Republic

**** Brief***

In a judgment of 22 October 2014, the extended chamber of the Nejvyšší správní soud (Supreme Administrative Court) reiterated the case law according to which the information on beneficiaries of public funds, which the public authorities have an obligation to disclose at the request of the people concerned, also includes the information pertaining to salaries and remuneration of employees of these authorities. According to the Nejvyšší správní soud, the wording of the impugned provision of the law on free access to information clearly specifies the information to be disclosed (first name, last name, date of birth, commune of residence of the beneficiary and the amount, the purpose and the conditions for granting the public funds), leaving the required authorities no discretion in this regard. Thus, it is not for the responsibility of these authorities to strike a balance, in each specific case, between public interest justifying the disclosure of the information in question and the interest of the employee concerned in the protection of his privacy. The conflict between these two interests has been resolved by the legislator even in favour of the right to information.

The Nejvyšší správní soud noted the importance of the interest of an effective public control of the management of public expenditure, which governs the disclosure of such information. It is only in exceptional cases that the obligation of disclosure must be excluded under the principle of proportionality. According to the extended chamber, the infringement of the rights of the employee concerned is disproportionate only when the two following cumulative conditions are met: first, where the employee concerned is involved only indirectly and marginally in the activities of the public authority in question and, second, when there is no concrete doubt on the reasonableness of the public expenditure related to the salary and remuneration of this person.

It should be noted that the Nejvyšší správní soud examined the conformity of the provision in question with Articles 7 and 8

of the Charter insofar as the disclosure of such data constitutes a processing of personal data and, as such, is governed by Union law. It concluded that the impugned national provision meets the requirement of foreseeability and proportionality in relation to the objectives pursued.

Nejvyšší správní soud, ruling dated 22.10.14,
8 As 55/2012-62,
www.nssoud.cz

IA/33972-A

[KUSTEDI]

Romania

Retention of data generated or processed in connection with the provision of publicly available electronic communications services - Directive 2006/24/EC - Respect for privacy - National legislation transposing this directive - Unconstitutionality

In its judgment no. 440 of 8 July 2014, the Constitutional Court declared the unconstitutionality of law no. 82/2012 concerning the retention of data generated or processed by providers of public networks of electronic communications and by providers of electronic communications services intended for the public. This law ensures the transposition of directive 2006/24/EC into a national law.

While substantiating its decision by the reasoning of the Court of Justice in the Digital Rights Ireland ruling, the Constitutional Court found that the law infringes Articles 26, 28 and 30 of the Constitution guaranteeing the right to respect for privacy, the confidentiality of correspondence and the freedom of expression.

To arrive at this conclusion, the Constitutional Court made a distinction between data retention, which it does not consider to constitute interference, and access to said data.

Regarding the latter, the Court criticised the lack of adequate safeguards in the said law to ensure respect for the aforementioned fundamental rights. It particularly highlighted the vagueness of the terms used by the law, the absence of an effective control mechanism for the activity of the electronic communications services providers, as well as the possibility for some institutions to access data outside judicial authorisation.

The Court clarified the effects of its judgment by pointing out that the data already stored on the basis of law no. 82/2012 could no longer be processed.

It expressly incorporated its decision in a European context by referring to the decisions delivered by other high courts, i.e. the German Constitutional Court, the Czech Constitutional Court and the Bulgarian Supreme Administrative Court.

This ruling of the Constitutional Court is also part of extensive disputes regarding constitutionality of personal data, which commenced in October 2009, when a first transposition law for Directive 2006/24/EC was declared unconstitutional.

Beyond its scope from a strictly legal standpoint, the decision of 8 July 2014 marks the will to effectively protect fundamental rights in the particularly sensitive area of privacy. It sets out the requirements in this regard and is thus a benchmark in the process of filling the existing legislative void. These requirements do not appear to have been observed by the new bill on cyber security,

which too was recently declared unconstitutional by the decision of the Constitutional Court of 21 January 2015.

Constitutional Court, ruling no. 440 dated 08.07.14, www.ccr.ro/ccrSearch/MainSearch/SearchForm.aspx

IA/33967-A

[CLU]

United Kingdom

Protection of individuals with regard to the processing of personal data - Directive 95/46/EC - Responsibility of a search engine - Applicability of Articles 13 and 15 of Directive 2000/31/EC - Effect of the invocation of fundamental rights

Following the Google Spain ruling, Max Mosley, former President of the Fédération Internationale de l'Automobile, submitted a new complaint before the United Kingdom courts to support his efforts of preventing access, by Internet, images and video footage showing him in a compromising position.

In 2008, the High Court had granted him compensatory damages amounting to 60,000 pounds (about 83,500 euros) and an injunction prohibiting the publisher of the newspaper News of the World from republishing said images and video footage.

It turned out that, despite the applicant's efforts to block the sites hosting these images, a number of images still remained or reappeared.

On 15 January 2015, the High Court dismissed the request for removal of the new complaint of Mr Mosley, introduced by the defendant Google Inc. Although a judgment on the merits was not yet delivered, the decision of the High Court raises several interesting questions regarding the liability of search engines with regard to data protection.

In its request for removal, Google argued that Article 13 of Directive 2000/31/EC, relating to certain legal aspects of services of the information society, and in particular electronic commerce, in the internal market, states that service providers such as search engines, are not liable for the form of storage, i.e. "caching", provided in particular that the provider does not modify the information. Google also argued that Article 15 of the Directive provides that Member States must not impose on service providers a general obligation of monitoring of information that they transmit or store, or of active search for facts or circumstances indicating illegal activity. In addition, Google argued that Directive 2000/31/EC does not apply to processing of personal data.

The High Court decided that, by reducing the images in the form from thumbnails, Google has not modified them. As regards the interaction between the directive 2000/31/EC and directive 95/46/EC, the High Court observed that the two directives must be interpreted in the same manner and, if possible, applied together. In support of this finding, it cited the Parquet de Milan/Drummond judgment, dated 12 December 2013, of the Italian Supreme Court, which was of the same opinion.

At the same time, in the Vidal-Hall/Google case, which was an action for damages against Google for anxiety and mental anguish caused to the applicants by the monitoring and synthesis of data relating to their use of the Internet through the browser Safari, performed without their consent, the High Court observed that the concept of "damage" for the purposes of the regime for protection

of data includes non-pecuniary damage and that, in any event, in the absence of a possibility of collecting such damages under the law on data protection, the applicant could possibly collect them under Article 8 of the law of 1998 relating to human rights and the right to respect for privacy. At the appeal stage, a hearing before the Court of Appeal was scheduled on 8 December 2014; however, a decision has still not been delivered.

Regarding the claim for damages in the Mosley case, the High Court decided to delay the judgment until the Court of Appeal ruled on the appeal in that case.

The need to provide compensation for morale damage when the personal data are inappropriately used was raised in a reasoned opinion of the Commission in the United Kingdom in 2010.

High Court, ruling dated 15.01.15, Mosley / Google Inc, [2015] EWHC 59 (QB),
High Court, ruling dated 16.01.14, Vidal-Hall /Google Inc, [2014] EWHC 13 (QB), www.bailii.org

IA/34305-A
IA/34306-A

[HANLEVI]

**** Briefs (United Kingdom)***

On 17 December 2014, the Supreme Court rejected an appeal against a law of the Scottish Parliament denying prisoners in Scottish prisons the right to vote in the referendum on the independence of Scotland. The applicants, two men convicted of serious offences, had raised, in support of their applications, different pleas alleging infringements of the ECHR, the Union law and international law. Rejecting these pleas, the Supreme Court held that Article 3 of Protocol 1 of the ECHR does not apply to referenda and that a more extensive right to vote does not follow from Article 10 of the ECHR. As regards the EU law, the Supreme Court recalled that, as is clear from the Chester and McGeoch judgment *(Reflets No.*3/2013, p. 48-49), it does not confer any right to vote. In terms of international law, as long as the International Covenant on Civil and Political Rights has not been incorporated into domestic law, the applicants could not claim a right to vote on the basis of Article 25. Finally, with regard to common law, the Supreme Court held that the law has not evolved to a point where it recognises a right to universal and equal suffrage for which any derogation must be provided for by law and in proportion to the objective pursued.

It should be noted that, by the decision of 10 February 2015 in the case Mc Hugh et al / United Kingdom case (application no. 51987 and 1014 other requests), the ECtHR upheld its Hirst case law and found a violation by the United Kingdom of Article 3, Protocol 1 of the ECHR.

Supreme Court, ruling dated 17.12.14, Moohan and another v Lord Advocate [2014] UKSC 67,
www.bailii.org

IA/34302-A

[PE] [DANNRAN]

In a judgment of 14 November 2014, the High Court dismissed the action involving the decision of the British government to exercise the option afforded by protocol no. 36 annexed to the EU treaty and TEEC of taking part in 35 of the acts adopted before the entry into force of the Lisbon Treaty in the area of police and legal cooperation in criminal matters, including that relating to the European arrest warrant.

...

According to the applicant, the treasurer of the Eurosceptic party UKIP, which had challenged the decision to ratify the Lisbon Treaty *(Reflets no.* 3/2008, p. 34), the exercise of such a right would be subject to the prior organisation of a referendum, in accordance with the European Union Act 2011 *(Reflets no. 2/2011*, p. 42-43), since the reinstatement of the European arrest warrant would result in the UK's participation in the European prosecution. In addition, the applicant had claimed a violation of the principle of protection of legitimate expectations, in that the impugned decision had not been subject to parliamentary vote. Rejecting these arguments, the High Court found that the obligation to hold a referendum, as stipulated in the 2011 act, did not apply to the impugned decision. Similarly, there were no legitimate expectations to be protected and, even assuming that this was the case, the High Court cannot encroach on the parliamentary prerogatives.

High Court (Queen's Bench Division, Administrative Court), ruling dated 14.11.14, Wheeler v Prime Minister and Secretary of State for the Home Department, [2014] EWHC 3815 (Admin),
www.bailii.org

IA/34303-A

[PE]

In a judgment of 15 December 2014, the Court of Appeal annulled, for violation of Article 47 of the Charter and Articles 6 and 8 of the ECHR, the guidelines issued by the Minister of Justice on access to legal aid in civil matters. These guidelines specified the notion of "exceptional case funding" (ECF), introduced by a law in 2012 and which allows on an exceptional basis the payment of legal costs relating to civil cases, which do fall within the scope of application of the legal aid system. In this regard, the guidelines provided that the legal aid under the ECF would be granted only in rare cases where a refusal to grant legal aid constituted a clear violation of the ECHR or EU law. The text of the document also contained erroneous references to the case law of the ECtHR, including the finding that nothing obligated the United Kingdom to grant legal aid.

Recalling the case law of the ECtHR (see, for example, Airey/Ireland, judgment of 9 October 1979, Application No. 6289/73), the Court of Appeal stressed that the crucial issue concerning the granting of aid under the ECF is whether a party that is not represented by a counsel would have the option of presenting its case effectively and fairly. In this respect, the availability of legal assistance cannot be limited to extreme cases. Consequently, the Court of Appeal annulled these guidelines.

Court of Appeal (Civil Division), ruling dated 15.12.14, R (on the application of Gudanaviciene and others) v Director of Legal Aid Casework and Lord Chancellor [2014] EWCA Civ 1622,
www.bailii.org

IA/34304-A

[PE]

In a judgment of 10 December 2014, the Supreme Court decided not to follow the reasoning of the ECtHR in the James, Wells and Lee / United Kingdom case (judgment of 8 September 2012, requests nos. 25119/09, 57715/09 and 57877/09). In that decision, the ECtHR concluded that, even though indefinite detention is admissible in cases where a government justifies the said detention solely by the risk posed by offenders to

society, it must, however, take account of the need to work towards their rehabilitation; it therefore concluded that between the expiry of the minimum sentence and the implementation of measures enabling them to follow appropriate rehabilitation courses, detention is arbitrary and therefore unlawful within the meaning of Article 5, paragraph 1 of the ECHR.

In the Haney case, the Supreme Court held that Article 5, paragraphs 1 and 4 of the ECHR, does not provide for the obligation to provide prisoners a reasonable opportunity to advance their rehabilitation and release, but rather the right to liberty and safety guaranteed by Article 5 of the ECHR, which imposes an implicit auxiliary obligation for the Minister of Justice to facilitate the rehabilitation and release of prisoners. The Supreme Court held that, in violation of Article 5 of the ECHR, the period before the transfer of a prisoner to an open prison and before the start of the sex offender treatment programme of another prisoner denied them the opportunity to prove that they no longer pose a risk to society. However, the Supreme Court concluded that such a period, as regards the two other prisoners, did not constitute a violation of Article 5 of the ECHR, due to the fact that they had followed other programmes, giving them the opportunity to provide the necessary evidence. Thus, the Supreme Court held that the appropriate remedy was to award damages, and not to release the prisoners.

Supreme Court, ruling dated 10.12.14, R (on the application of Haney, Kaiyam, Massey) v Secretary of State for Justice, [2014] UKSC 66,
www.bailii.org

IA/34307-A

[HANLEVI] [DANNRAN]

Slovenia

Retention of data generated or processed in connection with the provision of publicly available electronic communications services - Directive 2006/24/EC - Respect for privacy - National legislation ensuring the transposition of this directive - Violation of the principle of proportionality

In its judgment of 3 July 2014, the Constitutional Court ruled on the compatibility of the Slovenian legislation transposing Directive 2006/24/EC with the rights to protection of privacy and personal data as well the principle of proportionality, enshrined in the Constitution.

The impugned provisions of the Slovenian law on electronic communications provided for the retention of data enabling, in particular, to know the person with whom a subscriber or a registered user communicated and by what means, and to determine the duration of the communication and the location from which it took place.

First, the Constitutional Court assessed the legitimacy of the objectives pursued by the impugned provisions along with their adequacy. In this regard, while reiterating that the objectives listed in the impugned provisions, i.e. the protection of national security, defence and public security and the prevention, investigation, detection and prosecution of criminal offences constitute legitimate objectives, it then examined the adequacy of the impugned provisions. By accepting the Slovenian government's statement according to which the use of retained personal data significantly contributes to the

...

collection of proof intended to prove the evidence against a person, it considered that the retention and subsequent use of personal data is an appropriate measure for the prevention, investigation, detection and prosecution of criminal offences.

Secondly, the Constitutional Court assessed the necessity of the impugned measures, i.e. whether the legislator could have achieved the objective sought by less restrictive means. On the one hand, by observing that the impugned provisions provide for preventive and non-selective collection of personal data regarding all the individuals using electronic communication, it considered that these data, taken together, may allow drawing very precise conclusions regarding the privacy of individuals whose data has been stored.
Furthermore, it is possible that the said data is used by unauthorised persons or for illegitimate purposes. In such conditions, the impugned provisions are constitutive of a clear interference with fundamental rights.

On the other hand, the Constitutional Court reiterated that the retention period of the data in question is also a relevant factor in the context of the assessment of the need for the impugned measures. In particular, a retention period in excess of what is necessary to achieve the objective in question is contrary to the principle of proportionality. In this regard, the impugned provisions are silent as to the reasons that led the legislator to define the data retention period, which makes them contrary to the principle of proportionality. This is particularly so due to the fact that that the legislator did not limit data retention, under the impugned provisions, to the prevention, research, detection and prosecution of criminal offences, but provided for it in a general manner as regards all people using electronic communication.

Therefore, the Constitutional Court held that, by having failed to carefully define the circumstances delimiting data retention to what is strictly necessary to achieve the objective sought, the legislature clearly violated the right to protection of personal data. Therefore, it was held that the impugned provisions were contrary to the right to protection of personal data provided for in Article 38 of the Constitution, and annulled them in their entirety.

However, the Constitutional Court reiterated that, despite the annulment of the impugned provisions and directive 2006/24/EC, the member States have the right to adopt, in accordance with Article 15 of Directive 2002/58/EC, the aforementioned data retention measures for the protection of national security, defence and public security and for the prevention, investigation, detection and prosecution of criminal offences when such restriction is necessary, appropriate and proportionate within a democratic society. Such measures that may be adopted in the future by the national legislator must be examined in the light of the principle of proportionality, as long as they constitute a limitation of fundamental rights. Such a restriction is permissible only if it is a necessary, appropriate and proportionate measure within a democratic society.

Ustavno sodišče Republike Slovenije, decision dated 03.07.14, U-I-65/13-19, www://.us-rs.si

IA/33970-A

[SAS]

...

Sweden

Retention of data generated or processed in connection with the provision of publicly available electronic communications services - Directive 2006/24/EC - Respect for privacy - Limitations - Proportionality – Admissibility

Two cases were brought before the Swedish courts, following the Digital Rights Ireland ruling. In a judgment of 13 October 2014 (Tele 2 Sverige AB/Post-och telestyrelsen, case no. 14891-14), the Administrative court of first instance of Stockholm arrived at the same conclusion as that presented in the report of the two experts put in charge by the Swedish government of analysing the consequences of the Digital Rights Ireland ruling, by following the same reasoning as the one of the said analytical report. The administrative court found that the interference with the protected rights, caused by the data retention, reflects an objective of general interest, and that the Swedish provisions governing access to data are compatible with the EU law and the ECHR.

The judgment is currently under appeal before administrative Court of Appeal of Stockholm (Case No. 7380-14).

A second case (No. 27349-14) for the same purpose is currently pending before the administrative court of first instance of Stockholm.

Förvaltningsrätten i Stockholm, ruling dated 13.10.14, case no. 14891-14, www.forvaltningsrattenistockholm.domstol.se/Domstolar/lansrattenistockholm/Pressmeddelande/14891-14.pdf

IA/33971-A

[JON]

(As for the report of the aforementioned experts, see the Swedish contribution in the part titled "National legislation").

**** Brief (Sweden)***

In a judgment of 17 December 2014, the Högsta förvaltningsdomstolen (Supreme Administrative Court, hereinafter the "HFD") interpreted the Swedish regulations on the competences of health professionals in accordance with the Union law concerning the recognition of degrees and certificates. In the case resulting in that judgment, a Danish physician who not only received his medical degree in Denmark on 1 July 1999, but also received a medical degree in Sweden on 3 February 2009, had undertaken a specialisation in Sweden. On 17 March 2010, this physician asked the Socialstyrelsen (competent authority in the matter) for a specialist doctor certification in urology. The Socialstyrelsen rejected the request stating that the Swedish legislation providing for the criteria for obtaining that certification had been amended on 1 July 2006. Therefore, the applicant was obligated to fulfil the requirements of the new legislation, in contradiction with the documentation that he had. The said certification could be granted under the old regulations to the doctors who graduated before 1 July 2006, but only to doctors who had a Swedish degree. Finally, even if the new regulations allow the acquisition of the certification requested for specific reasons, in this case, they were lacking, according to the Socialstyrelsen.

The HFD, having considered that the case discussed pertained to issues of the Union law, referred in particular to Article 45 of the TFEU and the directives 2005/36/EC on the recognition of professional qualifications and 93/16/EEC facilitating the free

movement of doctors and the mutual recognition of their degrees, certificates and other qualifications. After finding that the applicant in question did not have a specialist medical certification issued by another Member State of the Union, and that he was therefore obligated to fulfil the conditions provided by the new Swedish regulations to obtain one, it confirmed the opinion of the Socialstyrelsen, according to which, as per the relevant Swedish regulations, a doctor seeking a specialist medical certification under the old requirements had to be in possession of a Swedish medical degree, before the adoption of the new regulations in July 2006, a condition that formally prevented him from obtaining such a certification under the criteria in force prior to that date.

The HFD then concluded that the applicant, in view of his Danish medical degree, obtained on 1 July 1999, was entitled, according to the automatic recognition rules provided for in the aforementioned directives, to obtain a Swedish diploma and that the applicant, regarding the possibility of an application for the certification in question, considered as per the old regulations, shall be treated the same way as those who received a Swedish degree before 1 July 2006. However, since the said regulation does not allow this possibility, the HFD decided that the certification in question be granted on the basis of special reasons, in order to interpret the Swedish regulations in conformity with EU law.

Högsta förvaltningsdomstolen, ruling dated 17.12.14, case no. 2924-13,

www.hogstaforvaltningsdomstolen.se/Doms tolar/regeringsratten/Avg%C3%B6randen/2014/December/2924-13.pdf

IA/33968-A

[JON]

2. Other countries

United States

Laws on stored communication - Search warrant - Obligation to provide the content of an email account stored on a server located in Ireland - Admissibility - Lack of importance of the data storage location

In December 2013, the District Court of New York, hereinafter the "District Court", issued pursuant to Article 2703 (a) of the American Stored Communications Act, a "search warrant" ordering Microsoft to provide it with the contents of a personal email account of a client, stored in a server located in Dublin (Ireland). Under the said law, the prosecutor may ask an ISP to provide emails of its clients by injunction.

In April 2014, the said court rejected Microsoft's argument that the district courts have no authority to issue warrants for search and seizure of property outside the territorial limits of the United States.

In this regard, the District Court stressed that a distinction must be made between conventional "physical property" and "electronic property". The new kind of property is actually "just a block composed of digits from zero to one, stored somewhere on someone else's computer" and is accessible on "an electronic device that ignores geographical boundaries".

In this context, the district court said that the search warrant in question is not a conventional warrant, but rather a hybrid order: part search warrant and part summons, in that it is presented to the ISP

...

in possession of the information. A summons orders the recipient to produce information in its possession, custody or control, regardless of the location of that information.

According to the district court, even if a search warrant is applied to the information stored in servers abroad, the actual search will take place only on the US territory, so that the warrant does not violate the principle of prohibition of extraterritorial application of US law. In this regard, the district court also mentioned the legislative history of Article 108 of the Patriot Act, regarding search warrants for electronic evidence, and a report of the legislative committee in charge of reviewing this act, which indicates that it explicitly considers the storage location of electronic information as the head office of the ISP. Therefore, an American ISP may nevertheless be required to provide electronic information stored abroad.

In July 2014, the same court, by order, dismissed Microsoft's application for revocation of the decision of April 2014 concerning the provision of electronic information stored abroad on the basis of the search warrant. Moreover, according to that court, the decision relating to the rejection of the request for cancellation of the search warrant in question did not constitute a final and challengeable act.

Following this decision, Microsoft and the federal government signed before that court a declaration indicating contempt of court on the part of Microsoft for failure to comply with the order of July 2014, without this act entailing the adoption of penalties against Microsoft.

Therefore, Microsoft was able to appeal against that order before the Court of Appeal (United States Court of Appeals for the Second Circuit).

United States District Court, Southern District of New York, Order of 25.04.14, *www.documentcloud.org/documents/1149373-in-re-matter-of-warrant.html*

IA/34062-A

United States District Court, Southern District of New York, Order of 29.08.14, *www://fr.scribd.com/doc/238413669/Microsoft-Warrant-Ruling*

IA/34063-A

United States District Court, Southern District of New York, Order of 08.09.14, *www://ia801402.us.archive.org/28/items/gov.uscourts.nysd.427456/gov.uscourts.nysd.427456.92.0.pdf*

IA/34064-A

[SAS]

Russia

Other countries - Russia - Restrictive measures concerning products originating in the Union - Legality of said measures

By its decision of 11 November 2014, the Supreme Court of the Russian Federation rejected the appeal of a Russian fish processing company by which the latter requested the partial annulment of economic sanctions adopted by the Russian government, on agricultural products from

the United States, the Union European, Canada, Australia and Norway. As a reminder, these economic sanctions were adopted in response to sanctions against the Russian Federation related to the crisis in Ukraine. In support of its action, the applicant company relied on means relating to the contradiction of the impugned sanctions with the provisions of the decree of the President of the Russian Federation on the special economic measures to ensure the security of the Russian Federation and with the State policy on the development of small and medium enterprises. It also cited the price inflation in the country, induced by these sanctions.

The Supreme Court, by referring to the federal law on special economic sanctions, considered that, by adopting economic sanctions concerning defined agricultural products for a period of one year, the Russian government, based on the decision of the President of Russia, had respected the law and the framework of its powers. According to the Supreme Court, the judiciary is not competent to re-evaluate the need to adopt the impugned measures, since the adoption of such measures falls within the exclusive jurisdiction of State bodies.

Supreme Court of the Russian Federation, decision of 11.11.14, 14-1124, www.supcourt.ru/stor_pdf.php?id=622762

IA/34052-A

[BORKOMA]

Switzerland

Fundamental rights - Law governing the respect of privacy and family life - Article 8 of the ECHR - Swiss cantonal regulations establishing measures for preventive observation, secret preventive search and undercover investigation as well as automatic surveillance of closed platforms on the Internet - Principle of proportionality – Violation

By two judgments of 1 October 2014, the Swiss Federal Court annulled several cantonal provisions establishing police measures of secret investigation to prevent or identify, irrespective of the existence of serious grounds for suspicion, future offences. This case involved, on the one hand, measures of preventive observation, from preventive secret searches and undercover investigation and, on the other hand, automatic surveillance of closed platforms on the Internet.

Noting that these measures constitute an interference with the right to respect for privacy and family life, i.e. the right to protection of privacy and the confidentiality of correspondence, guaranteed by the Swiss Constitution and by Article 8, paragraph 1 of the ECHR, the federal court found a violation of the principle of proportionality in the two procedures. It noted that the national provisions at issue disproportionately interfered with the said rights in that they did not guarantee adequate legal protection to the persons concerned.

Concerning the three investigative measures at issue, the Federal Court noted in particular that, in the field of data protection, the right to self-determination regarding personal information ensures that the individual remains in principle the owner of the data concerning him, regardless of the actual degree of sensitivity of the information involved.

To prevent any misuse in the context of the measures at issue, the federal court ruled that the principle of proportionality requires judicial authorisation prior to the adoption of such measures, that the persons concerned are, in principle, informed after their implementation and that these same people have a right to appeal. As for the automatic surveillance of closed platforms on the Internet, the Federal Court found that such a measure requires the existence of serious threats, judicial authorisation prior to its adoption as well as specific remedies.

Since the cantonal provisions in question do not meet the conditions thus indicated, the federal court pronounced their revocation.

Federal Court, rulings of 1 October 2014, 1C_653/2012 and 1C_518/2013, www.bger.ch

IA/34118-A
IA/34119-A

[KAUFMSV]

B. Practice of international organisations

World Trade Organization

WTO - GATT 1994 - Agreement on import licensing procedures - Measures affecting the import of goods

At its meeting of 26 January 2015, the dispute settlement body adopted the report of the appellate body, relating to certain measures adopted by Argentina concerning the import of goods. On 25 May 2012, the European Union sought the initiation of consultations with Argentina regarding these measures. Since a suitable solution has not been found in the context of its consultations, the dispute settlement body established on 31 May 2013, a special group in charge of reviewing this dispute, in accordance with Article 9:1 of the memorandum on dispute settlement.

As for the measures challenged by the European Union, the First was a procedure related to the affidavit prior to import required for the majority of imports of goods to Argentina (hereinafter the "DJAI" measure). The second impugned measure concerned the obligation for economic operators, as a condition of import or to obtain certain benefits in Argentina, of one or more trade-related requirements (hereinafter the "TRR" measure). The impugned measures focused, for example, on compensating the value of imports by a value of exports that is at least equivalent, on limiting imports (in volume or value), investing in Argentina as well as refraining from repatriating profits.

The European Union filed a complaint against the said Argentinean measures, arguing that they were inconsistent with the provisions of the GATT and the agreement on import licenses. Regarding the DJAI measure, the European Union asked the special group to note that this measure constitutes a restriction that is incompatible with Article XI:1 of the GATT, which prohibits quantitative restrictions and with Article X:3 a) of the GATT, which cites the procedure of publication and enforcement of trade regulations. Furthermore, the European Union argued that the procedure of the DJAI measure is applied in a manner that is inconsistent with the provisions of the agreement on import licensing procedures, in that Argentina has not promptly published the information concerning the implementation of the DJAI procedure in the manner prescribed by this agreement,

and Argentina has not followed the notification procedure laid down by that agreement. With regard to the TRR measure, the complainant also alleged that this had a limiting effect on the ability of traders to import and, therefore, constituted a violation of Article III:4 of the GATT (which prohibits regulatory discrimination of imported products by according them less favourable treatment than the treatment accorded to similar domestic products), Article X:1 of the GATT (in that Argentina had not promptly published the measure, thereby preventing governments and traders to become acquainted), and Article XI:1 of the GATT.

For its part, Argentina asked the special group to reject the request of the European Union in its entirety. Concerning the DJAI measure, Argentina argued that it was a customs formality covered by Article VIII of the GATT (regulating the fees and formalities regarding imports and exports) and that, therefore, was not within the scope of Article XI of the GATT or the agreement on import licenses. For the TRR measure, Argentina argued that, firstly, the complaint was inadmissible because it was not made in the request for consultations and, secondly, it only concerned a limited number of individual traders involved in a limited number of sectors, for which the application is neither general nor prospective. Since it was not a unique and comprehensive measure, it did not fall, according to Argentina, within the scope of the GATT.

In its report of 22 August 2014, the special group concluded that the DJAI and TRR measures were inconsistent with Article XI:1 of the GATT, and that the TRR measure was inconsistent with Article III:4 of the GATT. The special group refrained from making findings regarding the procedure relating to the DJAI measure and the allegations concerning Article X of the GATT and the agreement on import licensing.

On 26 September 2014, Argentina notified the dispute settlement body of its decision to appeal to the appellate body, whose report was released on 15 January 2015. The appellate body upheld the special group's findings on the applicability of Article XI:1 of the GATT and the incompatibility of the DJAI measure with it. It also concluded that the TRR measure was a unique measure applied systematically and consistently and, thus, upheld the finding of the special group according to which the TRR measure was incompatible with the said articles of the GATT.

Report of the WTO Appellate Body, adopted on 26.01.15, case DS438, *www.wto.org/*

[LOIZOMI]

C. National legislations

Finland

The Digital Rights Ireland ruling and the Finnish code for the information society

The Digital Rights Ireland ruling, annulling the Directive 2006/24/EC, was delivered at a particularly favourable time with regard to the assessment of its impact on Finnish legislation. On that date, the Parliament was studying a major proposal for reform and overhaul of the entire legislation on electronic communication in a new information society code. This overhaul involved inserting

national provisions transposing the said directive in chapter 19. Thus, the Parliament had the opportunity to examine the consequences of the ruling and, if necessary, amend the national legislation accordingly.

The constitutional committee of the Parliament, which plays an important role in regulating the constitutionality of Finnish laws, examined the bill. In its opinion, it observed that chapter 19 of the draft, pertaining to the retention of data relating to electronic communication, includes, in substance, the existing legislative provisions, which transposed directive 2006/24/EC.

This committee, however, reiterated that the annulment of the directive does not mean that national legislation cannot pertain to the annulled directive, but that legislation cannot be based on this directive or refer to its provisions. In this context it is necessary to assess the national legislation in the light not only of the national provisions on fundamental rights, but also of Articles 7 and 8 of the Charter, and to rely in particular on the Court's observations in the Digital Rights Ireland ruling cited above; the national legislation has to meet the requirements expressed in this ruling.

Regarding the extent of the data collected, the constitutional committee observed that, although it would certainly be preferable to limit the sphere of individuals whose data are stored, such a limitation would be difficult to implement in practice and would require careful preparation. However, to comply with the said judgment of the Court and in particular the requirements arising from the principle of proportionality, other means may be considered.

In its detailed analysis of the provisions proposed by the bill, the said committee felt that, as regards the data to be retained, it is preferable to replace the reference to Article 5 of the directive made in Article 157 of the bill with a detailed list of data to be retained. In this regard, it should be limited only to data necessary for the purpose of searches, detection and prosecution of serious crimes.

Regarding data access, the constitutional committee noted with satisfaction that, in the bill, the use of data is reserved only for the detection and prosecution of well-defined crimes and that access to data is, moreover, restricted to the authorities whose access is prescribed by law.

With regard to the data retention period, according to the bill, it covers a period of twelve months. In this regard, the constitutional committee proposed that this retention period is determined according to the objective pursued and, where appropriate, phased, without however exceeding twelve months.

Following the opinion of the commission, the committee on transport and communication handling the case, in its report, analysed the need to maintain the provisions of chapter 19 in the national legislation, notwithstanding the annulment of directive 2006/24/EC. It considered this justified with regard to criminal investigations and to ensure the security of citizens. It also acted on the recommendations of the constitutional committee and listed in detail the data retained, by restricting them to the data related to mobile telephony, Internet telephony and Internet access. The retention periods of these data were respectively staggered at twelve, six and nine months.

In addition, the duty of retention was limited to companies designated by the Ministry of Interior. In addition, the parliamentary committee appended a declaration to the adoption of the law, requiring the creation of a working group to examine in depth the issues related to data retention.

The Parliament adopted the information society code (917/2014) as amended by the committee on transport and communication as well as the declaration. The code entered into force on 1 January 2015.

**** Brief (Greece)***

Law no. 3917/2011 of 21 February 2011 transposed directive 2006/24/EC in Greek law. By way of a ministerial decision of 21 July 2014, the Greek legislator started the procedure of repeal or amendment of the said national legislation, in the light of the Digital Rights Ireland ruling, by creating a special legislative committee responsible for drafting a bill on the matter.

Although the deadline for the preparatory legislative work was set at 31 December 2014, there is no information yet about the progress of the bill.

Law no. 3917 of 21.02.11, (Official Journal A' 22 of 21.02.11), *www.et.gr/index.php/2013-01-28-14-06-23/2013-01-29-08-13-13*

Ministerial decision no. 57148 of 08.07.14, (Official Journal B' 1963 of 21.07.14), *www.et.gr/index.php/2013-01-28-14-06-23/2013-01-29-08-13-13*

[GANI]

**** Brief (Hungary)***

In the summer of 2014, the Hungarian legislature introduced a new special tax on advertising revenue. The law on advertising tax applies, in addition to electronic press products, including print and online, to outdoor advertising and online advertising. It is payable not only by companies that are established in Hungary, but also by the companies that provide services in Hungarian while paying their taxes abroad. If the advertising entity does not pay its taxes on advertising revenues, the tax due must be paid, in certain conditions, by the entity that ordered the advertising service. The applicable rate of the special tax is progressive.

2014. évi XXII. törvénya reklámadóról (Law on the tax on advertising)

[VARGAZS]

Luxembourg

Law providing for marriage reform

The Luxembourg parliament voted on 18 June 2014 for a law on the right of homosexual couples to marriage. This law, which came into force on 1 January 2015, places homosexual couples on an equal footing with heterosexual couples. Marriage reform is part of the government's determination to create a society without discrimination. It focuses on the opening of marriage to same-sex couples, who were hitherto excluded from this form of union. Homosexual couples now have right to marry. In addition, the simple and full adoption is also open for these couples. Homosexual couples therefore have the same rights as heterosexual couples. Luxembourg, which in 2004 had recognised the right to civil union for homosexual couples, is the 11th European

country to recognise homosexual marriage, after the Netherlands, Belgium, Spain, Sweden, Norway, Portugal, Iceland, Denmark, France and Great Britain.

It is observed that this marriage reform is not limited to according the right of marriage to same-sex couples, but aims at a comprehensive reform of Title V of Book 1 of the Civil Code, titled "Marriage".

Law of 04.07.14 establishing reform of Title V .- of Book 1 of the Civil Code of "Marriage", Memorial, 17.07.14, no. 214, p. 1798,
www.legilux.public.lu

[IDU]

Czech Republic

Retention and transmission of traffic data and location data

Following the repeal by the Ústavní soud (Constitutional Court), on 22 March 2011, of the national provisions transposing directive 2006/24/EC (see *Reflets no.1/2011, p.* 30), a new law came into force on 1 October 2012, that aims to remedy the unconstitutional elements raised by the constitutional court. As a reminder, the Ústavní soud had repealed certain provisions of the law on electronic communication and its enforcement regulations by ruling that they went far beyond the framework provided by Directive 2006/24/EC as regards the volume and nature of the information to be retained. According to the Ústavní soud, the said provisions were a disproportionate interference with the right to privacy (right to digital self-determination) and did not constitute an effective safeguard against abuse and arbitrariness. The Ústavní soud criticised in particular the impugned regulation for neither limiting the purpose of the transmission of data nor specifying the competent authorities to which the data were likely being transmitted nor identifying the texts serving as a legal basis for such jurisdiction.

The new law amends the law on electronic communication, the criminal procedure code and other acts. With regard to the law on electronic communication, the new text states the obligation for operators to secure and protect traffic data and location data. It also limits the data retention period to six months (previous provisions provided for a period of 6 to 12 months). It also provides an exhaustive list of the authorities with jurisdiction to request for the transmission of these data and the legal basis of that jurisdiction. It should be noted that the obligation to transmit data is not limited only to criminal proceedings. The data may also be required by the police in some cases outside the criminal proceedings, by the intelligence services as part of their activities, or by the Česká národní banka (Czech National Bank) as part of its capital market surveillance duty.

As regards the Criminal Procedure Code, the amendments made by the new law govern, in particular, the request for data transmission by the criminal justice bodies. The request is limited to intentional crimes, punishable by a custodial sentence of a maximum period of more than three years and other crimes, listed exhaustively.

Zákon č. 273/2012 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a některé další zákony,

www://aplikace.mvcr.cz/sbirka-zakonu/

[KUSTEDI]

United Kingdom

Data Retention and Investigatory Powers Act

On 17 July 2014, a new law on data retention and investigative powers, namely the Data Retention and Investigatory Powers Act 2014 (hereinafter the "DRIP Act 2014") came into force, in response to the Digital Rights Ireland ruling.

The DRIP Act 2014 thus replaces the Data Retention (EC Directive) Regulations 2009, which transposed Directive 2006/24/EC, and amends the Regulation of Investigatory Powers Act 2000, i.e. the 2000 law on regulation of investigatory powers (hereinafter the "RIPA 2000").

Among the amendments introduced by this new law, it provides in particular for a maximum data retention period of 12 months, instead of the fixed 12 months, under the previous legislation. However, as regards the data on telecommunications and their interception, it broadens the concept of "telecommunications services" of the RIPA 2000, to include the services provided by the Internet, such as Webmail. It also confirms the extraterritorial effect of the provisions of the RIPA 2000, which had been challenged by companies established outside the United Kingdom and providing services to customers in that State.

Although the explanatory notes accompanying the DRIP Act 2014 confirm that this new law seeks to respond to the Digital Rights Ireland ruling cited above, they also claim that the previous legislation transposing directive 2006/24/EC had already addressed the issues raised in that ruling. Owing to the invalidity of that directive, which was declared in that ruling, the government wanted to provide a clear legal basis with regard to data retention in the United Kingdom. As a result, the DRIP Act 2014 was the subject of expedited parliamentary scrutiny.

The decision to submit the bill to such a procedure was heavily criticised, as was the DRIP Act 2014 itself. More specifically, Liberty (also known as the "National Council for Civil Liberties") argued that the DRIP Act 2014 is contrary to Article 8 of the ECHR and Articles 7 and 8 of the Charter. In particular, Liberty claims that the communication data can give access to personal information relating to the private life of a person, that the data access system adopted is not adequately secure and that the condition of serious criminal offence of is an essential criterion for systematic data retention.

It should be noted that, on 8 December 2014, the High Court gave its authorisation allowing Liberty and other applicants to apply for a judicial review of the DRIP Act 2014.

Data Retention and Investigatory Powers Act 2014,
www.legislation.gov.uk

[HANLEVI]

- - - - -

Amendment of the enforcement procedure for European arrest warrants

In order to remedy the perceived flaws in the European arrest warrant system, the British Parliament voted for an amendment to the law transposing the framework decision 2002/584/JAI to solve

two issues, namely the issuance of an arrest warrant before making a decision to indict or for minor offences. The new law received royal assent on 13 March 2014.

According to the amended law, it is now up to the Member State requesting the surrender of a person to prove that a decision of indictment or prosecution has been taken in respect thereof. When no decision has been made, the surrender of a person can only be ordered if this situation is due solely to the absence of the State representative making the request for surrender. This amendment aims to avoid situations in which persons who surrender on the basis of a European arrest warrant are remanded in custody pending a decision in their regard. This was the case of Andrew Symeou, who spent 10 months in custody in Greece, followed by 9 more months of bail before finally being acquitted.

Hence, the national courts must now monitor the proportionality of the requests for surrender, taking into account three criteria, namely, the severity of the offence for which the surrender of a person is sought, the sentence likely to be given in case of conviction and whether this sentence would constitute a less coercive measure than the surrender of the person sought.

Anti-social Behaviour, Crime and Policing Act 2014,
www.legislation.gov.uk

[PE]

Slovenia

Law amending the law on marriage and family relations

The Slovenian Parliament adopted, on 3 March 2015, a law amending the regulations on marriage and family relations authorising marriage between persons of the same sex. According to this text, marriage is now defined as "the lifelong union of two people regardless of their gender". This law must now be enacted by the President to enter into force.

As can be seen from the preparatory work, the new law addresses the issue of compliance with the Constitution of the previous version that allowed in this regard discriminatory treatment of persons of the same sex. According this version, the registered partnerships involving same-sex individuals received were entitled only to the rights specifically listed in the law on registered partnership involving individuals of the same sex. However, such differential treatment on the basis of gender and sexual orientation was not, as is clear from the preparatory work, in line with the principle of equal treatment stipulated in Article 14 of the Constitution.

Under the new law, any discrimination between, on the one hand, married individuals of the same sex and, on the other hand, married individuals of opposite sex was removed, since the former now enjoy the same rights as the latter.

It should be recalled that a popular initiative is underway to collect signatures for the organisation of a referendum on the new law. In Slovenia, a referendum on the enforcement of a law can be organised provided on the condition that 40,000

signatures are collected. However, the Constitutional Court, ruling on an application, may prohibit a referendum if it considers that a possible rejection of a new law by popular vote would be unconstitutional.

Zakon spremembah in dopolnitvah zakona o zakonski zvezi in družinskih razmerjih (ZZZDR-D),
www.dz-rs.si

[SAS]

Sweden

The Digital Rights Ireland ruling annulling the Directive 2006/24/EC had aroused strong reactions in Sweden and some Swedish providers of publicly available public communication networks or electroni c communication services had decided not to retain information and delete those already stored. Therefore, access by law enforcement officials to such information has been restricted.

Given this situation, the Swedish government appointed two experts to analyse the implications of the aforementioned judgment on the relevant Swedish legislation. The experts' report was presented in June 2014 after a general review of Swedish legislation, in the light of the EU law, the ECHR and the case law of the ECtHR.

During this review, the experts found that, in both the Swedish legislation as well as the EU law, data retention is performed in a general manner, thus reflecting a legitimate interest at the origin of the obligation to retain data, and that the said obligation, in its Swedish form, goes even beyond the obligation under the law of the Union, notably in that it includes an obligation to retain data relating to telephone calls that do not get through. In addition, this national legislation is stricter than Directive 2006/24/EC, since it limits access to such data to meet the requirements of proportionality laid down by the Court in the judgment in question. According to the analysis, it is the fact of having a large storage requirement combined with poorly defined access rules that is not acceptable and that has led the Court to annul the directive.

The two experts then found that, even if the Court of Justice, in its judgment, annulled Directive 2006/24, and that this judgment therefore has retroactive effect, it does not automatically render the Swedish law unenforceable, and that, if there is no longer an obligation of data retention under the Directive, the Member States nevertheless have the right to maintain the obligation for providers to retain data, provided that Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the sector of electronic communications is complied with. They also stressed that it is not the same general nature of the data retention obligation under Directive 2006/24/EC that was challenged by the Court, but the fact that the methods of retention and processing of data was not proportionate in all cases.

The experts identified four points, in the Court judgment, in which it has criticised Directive 2006/24/EC. These four points, focusing on the general nature of the obligation of data storage, the absence of limits as regards data access, the data retention period and, finally, the safety and protection of stored data, were then discussed in light of the Swedish legislation applicable in the matter, thus verifying its proportionality.

...

The report concludes that the national legislation appears to meet the requirements defined by the Court in its judgment, but a few possible changes with regard to legal security must, however, be considered as regards the retention obligation for certain categories of data, the monitoring of transfer requests for traffic data of subscribers, the independent control of data transfer requests during the investigation phase of criminal proceedings and a possible prohibition of data retention outside the European Union.

Uppdrag med anledning av EU-domstolens dom om datalagringsdirektivet ; Ju2014/3010/P.

[JON]

D. Doctrinal echoes

Protection of personal data - Articles 7 and 8 of the charter of fundamental rights of the European Union - Directive 2006/24/EC - Retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks - Invalidity - Directive 95/46/EC - Protection of individuals with regard to the processing of personal data and the free movement of data - "Right to be forgotten" - Comments on the rulings of the Digital Rights Ireland Court and Seitlinger et al (C-293/12 and C-594/12) and Google Spain and Google (C-131/12)

In two judgments of the Grand Chamber of 8 April 2014 in the joined cases Digital Rights Ireland and Seitlinger and Others, and of 13 May 2014 in the Google Spain case, the Court of Justice ruled on the different aspects of the protection of personal data. In light of articles 7 and 8 of the Charter of Fundamental Rights of the European Union concerning, respectively, the respect for private and family life and the protection of personal data, it found that Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks was invalid and recognised the obligation of the operator of an Internet search engine to remove, under certain conditions, the name of a person from the list of results.

The high number of doctrinal comments on these judgments have identified their common importance to the field of data protection and the role of the Court[1]. In addition, some aspects specific to each ruling were the subject of special attention.

Digital Rights Ireland, Google Spain and the right to protection of personal data

According to Kühling, "with a one-two punch, the ECJ has accomplished nothing less than re-establishing the 'reign of data protection law"[2]. Granger and Irion note that "[t]aken together, the Digital Rights Ireland and Spain Google rulings confirm

[1] See, for example, HESS, B., and MARIOTTINI, C.M. (eds.), "Protecting Privacy in Private International and Procedural Law and by Data Protection – European and American Developments", Nomos Ashgate 2015.

[2] KÜHLING, J., "Rückkehr des Rechts: Verpflichtung von „Google & Co." zu Datenschutz", *Europäische Zeitschrift für Wirtschaftsrecht*, 2014, p. 527-532, p. 527.

that the high standards of privacy and data protection are applicable to the public and private sectors of the European Union in the Big Data era".[3] Similarly, Spiecker gen. Dohmann considers that the two judgments of the Court set out a framework for the processing of personal data, reinforcing the importance of European law for the protection of personal data: "zwei spektakuläre Entscheidungen vom April [entwickeln] einenneuen, unmittelbar verbindlichen Rahmen zum Umgang mit Daten durch Private und Behörden. [Damit] steht das europäische […] Datenschutzrecht […] vor erheblichem Bedeutungszuwachs."[4]

In fact, a vast majority of the doctrine considers that the scope of the two judgments extends beyond the case. Concerning the Digital Rights Ireland ruling, Boehm and Cole discern the will of the Court to identify the general principles applicable to the right to data protection: […] ist die Intention des Gerichtshofs zu erkennen, grundsätzliche Rechtsprinzipien im Bereich des Datenschutzes aufzustellen, die weit über den behandelten Sachverhalt hinausgehen und in den kommenden Jahren eine wichtige Rolle spielen werden."[5] Concerning the scope of the Google Spain ruling, Kuner also stresses that "[t]he accomplishment of the judgment is to clarify the application of EU data protection law to the Internet"[6]. Similarly, Briem considers that this ruling ensures the protection of privacy and personal data on the Internet: "Dieses Urteil gibt dem Internet jenes Maß an Schutz der Privatsphäre und der personenbezogenen Daten zurück, das lange fehlte. Eine gedeihliche Weiterentwicklung der Gesellschaft erfordert, dass diese Grundrechte auch und gerade im digitalen Raum respektiert werden."[7]

Many commentators have noted the importance that the Court has given to fundamental rights in the area of protection of personal data. Concerning the application of the Charter in the Digital Rights Ireland ruling, Granger and Irion "do not suggest that the Court of justice is purposely establishing a hierarchy of rights in the Charter […]. Still, it seems to afford certain rights, including the right to privacy, a particular status"[8]. Jacqué notes "the fundamental importance that [the Court] attributes to privacy and protection of personal data. [...] [T]he Court gradually clarifies the scope of the Charter, but highlights in particular the equilibria to be established in cases of conflicts between fundamental rights and the analysis of

[3] GRANGER, M-P, and IRION, K., "The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection", *European Law Review* 6/2014, p. 835-850, p. 850.

[4] SPIECKER GEN. DÖHMANN, I., *Juristenzeitung*, 22/2014, p. 1109-1113, p. 1109.

[5] BOEHM, F., and COLE, M.D., "Vorratsdatenspeicherung und (k)ein Ende?", *Multimedia und Recht,* 2014, p. 569-570, p. 569.

[6] KUNER, C., "The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges", September 15, 2014, Studies of the Max Planck Institute Luxembourg for International, European and Regulatory Procedural Law, Nomos / Brill 2015, available on SSRN, http://ssrn.com/abstract=2496060, p. 28.

[7] BRIEM, S., "Datenschutzrechtliche Verantwortung des Suchmaschinenbetreibers - Löschung personenbezogener Daten aus der Suchergebnisliste ("Recht auf Vergessenwerden")", *Medien und Recht International*, 2014, p. 7-17, p. 16

[8] GRANGER, M-P, and IRION, K., cit. supra note 3, p. 846.

restrictions [to these rights]. All rights are not equally fundamental and protection of privacy, with which the protection of personal data is associated, is among the rights that are the subject of the strictest control"[9].

In addition, some authors have commented on the importance given to the ECHR in the weighting of the fundamental rights at stake in the Google Spain ruling. In this regard, Marino regrets that "the Court of Justice completely abandons the ECHR and the case law of the ECtHR, since it now follows the Charter internally"[10]. However, Van Den Bulck observes that in its decision, "[t]he Court refers [...] without saying so explicitly, to the criteria applied by the European Court of Human Rights to manage the conflicts between the fundamental right to freedom of expression and the fundamental right to privacy"[11].

The Court of *justice and fundamental rights*

The issue of the impact of the two decisions on the role of the Court in the area of protection of personal data and in the interpretation of fundamental rights has been the subject of many doctrinal comments. Thus, Koutrakos and Nic Shuibhne consider that "[t]he Court of Justice has assumed the role of the ultimate protector of the right to privacy of EU citizens"[12]. Spiecker gen. Dohmann highlights the importance of the two rulings for the entire structure of European law, with the Court endorsing the role of constitutional jurisdiction incumbent upon it under the Lisbon treaties and the Charter of fundamental rights: "Institutionell sendet die Entscheidung zur Vorratsdatenspeicherung gemeinsam mit der Google Spain-Entscheidung ein Fanfarensignal an die europäische Rechtsstruktur. Der EuGH definiert sich und seine Rolle neu. Er verlässt seine bisherige Rolle als Motor der europäischen Einigung vorrangig zum Wohle des Binnenmarktes und etabliert sich erstmals prägnant als ein europäisches Verfassungsgericht, das in wesentlichen Bereichen Grundrechte der Bürger schützt. [Er] nimmt […] endlich die Rolle an, die ihm die Verträge von Lissabon und die Integration der Grundrechte-Charta schon lange zugedacht haben und die in der Konsequenz der Weiterentwicklung der EU zu einer politischen Union steht. [Damit] agiert der EuGH als ein Grundrechte schützendes Verfassungsgericht."[13]

Several authors have questioned the relation between the Court and the European legislator in the area of fundamental rights. In this regard, Granger and Irion note that

[9] JACQUÉ, J.P., "Protection of personal data, Internet and conflicts between fundamental rights before the Court of Justice", *Quarterly review of European law*, 3/2014, p. 283-288, p. 283; see also NOLTE, N., "Das Recht auf Vergessenwerden - mehr als nur ein Hype?", *Neue juristische Wochenschrift,* 2014, p. 2238-2242, p. 2238.

[10] MARINO, L., "A 'right to digital oblivion' established by the ECJ", *La Semaine Juridique Edition Générale,* No. 26, June 30, 2014, p 768; see also infra note 35.

[11] VAN DEN BULCK, P., "Google Spain ruling: extent of the right to be forgotten", *Journal de droit européen,* 2014, no. 211, p. 289-290, p. 290.

[12] KOUTRAKOS, P., and NIC SHUIBHNE, N., "To strive, to seek, to Google, to forget", *European Law Review*, 2014, p. 293-294, p. 294.

[13] SPIECKER GEN. DÖHMANN, I., cit. supra note 4, p. 1110; see also ROßNAGEL, A., "Neue Maßstäbe für den Datenschutz in Europa - Folgerungen aus dem EuGH-Urteil zur Vorratsdatenspeicherung", *Multimedia und Recht,* 2014, p. 372-377, p. 377.

"[the Court's] usual technique was to "pass" laws […] and then to instruct Member States to use their discretionary powers to implement the measure in a manner compatible with EU human rights standards. In contrast, in Digital Rights Ireland, the Court of Justice shifts the responsibility to protect human rights onto the EU legislator. […] In this redefined constitutional context, human rights would eventually supersede the internal market as the core aim of the integration project, and the Court would slowly reinvent itself, evolving from the engine of integration into a proper constitutional court […]."[14] As regards the control exercised by the Court in the Digital Rights Ireland ruling, Aubert, Broussy and Cassagnabère find: "Out goes therefore, in terms from fundamental rights at least, the traditional Community case law according to which the Court keeps its control restricted only to the manifest error of assessment in the legislative choices of the EU legislator when intervening in a field requires it to make political, economic and social choices, and in which it is called upon to undertake complex assessments."[15] In their review of the Google Spain ruling, Martial-Braz and Rochfeld felt that this decision is "[s]ubversive also because the Court of Justice, with this decision as with others settles a debate that the cautious European legislator does not resolve to confront and leads a sort of putsch based on fundamentalisation of rights"[16].

Finally, some authors comment on the division of jurisdictions between the Union and the Member States in matters relating to the protection of fundamental rights in the field of data retention. Thus, Classen believes that the Court would have recognised the jurisdictions of the European Union legislator based on fundamental rights: "Zweifel weckt das Urteil aber vor allem aus kompetenzrechtlicher Perspektive. […] Vorliegend wird im Ergebnis das gleich mehrfach postulierte Verbot, aus Grundrechten Kompetenzen abzuleiten […] unterlaufen."[17] In this regard, commenting on the refusal of the Court to recognise the possibility for Member States to ensure respect for fundamental rights under the Directive 2006/24/EC, Spiecker gen. Döhmann believes that there is a need to limit the jurisdiction of the Court as long as Member States provide protection that is equivalent to the Charter: "Möglicherweise wird es […] einer weiteren ‚Solange'-Entscheidung bedürfen, dieses Mal allerdings von Seiten des EuGH."[18]

The objective of Directive 2006/24/EC

Several authors have expressed reservations about the purpose on the basis of which the Court assessed the

[14] GRANGER, M-P., and IRION, K., cit. supra note 3, p. 850; see also KÜHLING, J., "Der Fall der Vorratsdatenspeicherungsrichtlinie und der Aufstieg des EuGH zum Grundrechtsgericht", *Neue Zeitschrift für Verwaltungsrecht*, 2014, p. 681-685, p. 684.

[15] AUBERT, M., BROUSSY, E., CASSAGNABÈRE, H., "Vie privée et protection des données personnelles - Moteur de recherche et «droit à l'oubli»" (Privacy and protection of personal data - Search engine and the 'right to be forgotten'), *Actualité Juridique. Administrative law,* 2014, p. 1147-1149, p. 1149.

[16] MARTIAL-BRAZ, N., and ROCHFELD, J., "Les moteurs de recherche, maîtres ou esclaves du droit à l'oubli numérique ? (Search engines, master or slave of the right to digital oblivion?), Act II: Le droit à l'oubli numérique, l'éléphant et la vie privée" (The right to digital oblivion, the elephant and privacy), *Recueil Dalloz*, 2014, p. 1481.

[17] CLASSEN, C. D., "Datenschutz ja - aber wie?", *Europarecht,* 2014, p. 441-445, p. 445.

[18] SPIECKER GEN. DÖHMANN, I., cit. supra note 4, p. 1111.

proportionality of Directive 2006/24/EC. For Lynskey, performing such an assessment "in light of [the Directive's] 'material objective' - crime prevention - rather than its stated objective – market harmonisation […] sits uncomfortably with the Court's finding in Ireland v Council. […][T]he most disappointing element of the judgment […] is that it does not query the appropriateness of data retention as a tool to fight serious crime"[19]. In the Ireland/Parliament and the Council ruling (C-301/06, EU:C:2009:68), the Court had held that the Directive 2006/24/EC has been validly adopted on the basis of Article 95 EC on measures that are intended for the establishment and operation of the internal market. Vaciago submits that "[p]erhaps, when considering the Data Retention Directive […] the CJEU had the accessibility of […] data for secret intelligence services like the NSA in the back of the mind"[20]. In any event, Lynskey believes that "[g]iven the prominence of this issue in both the EU and the US in the post-PRISM period, empirical evidence is needed to justify this claim [of data retention as an appropriate tool]"[21]. In the same vein, Granger and Irion note that "the fact that the Court of Justice assessed the proportionality of the interference with the rights to privacy and data protection under the Charter only by reference to the "unofficial" security objective of the Directive is puzzling. Had it been keen to "save" the Directive once again, choosing the security objective would have served that purpose well; it is, quite obviously, easier to justify serious intrusion into privacy based on security grounds than on market objectives [...] The Court's framing of the Directive as a security measure [...] enables the Court to develop a strong precedential basis for stricter human rights scrutiny of security policies, even when adopted under the ordinary (supranational) legislative process. By marginalising the internal market objective, the Court retains the option of applying different standards of review for market-related measures"[22].

The practical consequences of the Digital Rights Ireland ruling on data retention

Many authors have questioned the impact of the Digital Rights Ireland ruling on the legal situation within the EU and Member States. Aubert, Broussy and Cassagnabère note that "as a result of invalidity [...] of the directive of 2006, the Union law now rests, until the adoption of a new text, on the previous directive 2002/58/EC [that] already foresaw the possibility for States to retain data for security purposes [...] Given the bridge created by this provision with fundamental rights, there is no doubt that the approach taken by the Digital Rights ruling is also within the ambit of the 2002 directive"[23]. Furthermore, Boehm and Cole observe that many existing data retention instruments at the EU level would also be contrary to the principles established in the Digital Rights ruling: "Weitreichende Auswirkungen hat das Urteil aber auch auf Datensammlungsinstrumente auf EU- Ebene, wobei zahlreiche dieser Maßnahmen

[19] LYNSKEY, O., "Joined Cases C-293/12 and 594/12 Digital Rights Ireland and Seitlinger and Others: The Good, the Bad and the Ugly", *European Law blog*, http://europeanlawblog.eu/?p=2289

[20] VACIAGO, G., "The Invalidation of the Data Retention Directive", *Computer und Recht* 2014 p. 65-69, p. 69.

[21] LYNSKEY, O., cit. supra note 19.

[22] GRANGER M-P. and IRION K., cit. supra note 3, p. 846 et s.

[23] AUBERT, M., BROUSSY, E., and CASSAGNABÈRE, H., cit. supra note 15, p. 1150.

eindeutig in Konflikt mit den im Urteil aufgestellten Grundsätzen stehen."[24]

As for the situation in the Member States, Jacqué believes that "[i]f the "retention" directive violates fundamental rights, it seems that the national measures enforcing them also violate them [...] are contrary to EU law. [...] There is thus a risk of embrittlement of the prosecution on the basis of evidence obtained by means of data retention and the adoption of a new directive is urgently needed"[25]. Cassart and Henrotte also concede that the Digital Rights ruling "will inspire [...] different the supreme courts hearing annulment appeals against transposition laws [and] will undoubtedly be of paramount importance in other Member States by validating the arguments of civil society, which had objected to this Directive"[26]. Concerning the downstream impact on the private sector, Rauhofer and Mac Síthigh feel that "[f]or EU citizens and businesses, in particular the communications service providers that were directly affected by the now invalid retention requirement, this is likely to mean a sustained period of legal uncertainty as the various institutions both at EU and at Member State level come to an agreement on how [the] substantive and procedural issues raised by the ECJ's decision should be resolved"[27]. As for private actors in other countries, Vaciago notes that it is "likely that American providers will not change their policies which were already in place prior to the arrival of the Data Retention Directive, but it cannot be ruled out that this decision may lead them to adopt a much "colder" attitude with regards to collaborating with European law courts"[28]. Regarding the future system for data retention, the doctrinal reactions seem mixed. While Otto and Seitlinger believe that the Digital Rights Ireland judgment has sounded the death knell for data retention performed without suspicion or distinction[29], authors like Simitis regret that the Court accepts the possibility of such a system without questioning its legitimacy as such: "Der EuGH mag grundlegende Gesichtspunkte ebenso wie sekundäre Probleme exakt angesprochen haben, die Zulässigkeit von Vorratsdaten-speicherungen wird nirgends in Frage gestellt. Das Gericht strebt vielmehr durchweg eine solide konstruierte Vorratsdatenspeicherung an. Genauso durchgängig wird freilich auch jeder Zweifel an der Legitimität einer solchen Verarbeitung verdrängt."[30]

[24] BOEHM, F., and COLE, M. D., cit. supra note 5, p. 570.

[25] JACQUÉ, J.P., cit. supra note 9, p. 283.

[26] CASSART, A. and HENROTTE, J-F., "L'invalidation de la directive 2006/24 sur la conservation des données de communication électronique ou la chronique d'une mort annoncée" (The invalidation of directive 2006/24 on retention of electronic communication data or the chronicle of a death foretold), *Revue de jurisprudence de Liège, Mons et Bruxelles*, 2014, p. 954-960, p. 960.

[27] RAUHOFER, J. and MAC SITHIGH, D., "The data retention directive never existed", *SCRIPTed,* Volume 11, Issue 1, April 2014, p. 118-127, p. 127.

[28] VACIAGO, G., cit. supra note 20, p. 69.

[29] OTTO, G. and SEITLINGER, M., "RL 2006/24/EG - Zulässigkeit der Vorratsdatenspeicherung", *Medien und Recht International*, 2014, p. 22-23, p. 22.

[30] SIMITIS, S., "Die Vorratsspeicherung – ein unverändert zweifelhaftes Privileg", *Neue juristische Wochenschrift,* 2014, p. 2158-2160, p. 2160; see also PRIEBE, R., "Reform der Vorratsdatenspeicherung – strenge Maßstäbe des EuGH", *Europäische Zeitschrift für Wirtschaftsrecht,* 2014 p. 456-459, p. 459.

...

Jacqué notes that "by explaining in this case the violations of the principle of proportionality, the Court creates a legal framework that needs to be followed by the legislator [and that the] the judgment actually contains the content of the directive that will replace the annulled text"[31].

Google Spain and the existence of a "right to be forgotten"?

Many authors have questioned the possible recognition of a "right to be forgotten" by way of the Google Spain ruling. In this regard, Griguer believes that "[t]he right to oblivion finally clearly proclaimed by the Court [...] becomes a major tool for managing online reputation. [...] Established as a fundamental right [...], [it] poses a risk of upsetting the ecosystem of the digital world" [32]. However, many authors, such as Kuner, observe that "the ruling does not create a right to be forgotten. A careful reading shows that the right affirmed by the Court is that of obliging the operators of Internet search engines to suppress links to web pages from the list of search results made on the basis of a person's name […], not a right to have data itself deleted from the Internet"[33].

The issue of implementation of such a law has been the subject of numerous doctrinal reactions. Thus, Morgan believes that "the judgment does not establish an absolute or automatic right to removal of information or links from search results […]. While the court indicated that there may be a range of reasons justifying continued inclusion regrettably it did not expand on what these might be, other than where the individual plays a role in public life"[34]. Furthermore, Kulk and Zuiderveen Borgesius complain that "[t]he CJEU does not refer to the detailed and nuanced case law of the European Court of Human Rights on balancing privacy and freedom of expression and] is silent on the right to freedom of expression of search engine operators and of the original publishers of information"[35]. Morrison and White highlight that "Google is a key source of information to the masses and so limiting or removing data from searches needs to be carried out with care. Too rigid an approach could undermine human rights, whereas too much editing and we may start drawing parallels with the position of Winston Smith, the protagonist in George Orwell's Nineteen Eighty-Four, responsible for historical revisionism at the Ministry of Truth"[36].

Commenting on the practical implications of the Google Spain judgement, several authors have stressed that this decision may lead to differences between the results of searches conducted within and outside the Union. [37] Van Eecke and Cornette

[31] JACQUÉ, J.P., cit. supra note 9, p. 283.

[32] GRIGUER, M., "Terms and conditions of exercise of the right to digital oblivion - or the contributions of the ECJ, 13 May 2014, C-131/12", *La Semaine Juridique - entreprise et affaires*, 2014, nº 24, p. 49-50, p. 50.

[33] KUNER, C., cit. supra note 6, p. 8 et s.; see also SÖRUP, T., "EuGH: Löschungsanspruch gegen Google – „Recht auf Vergessen", *Multimedia und Recht,* 2014, p. 464-465, p. 465.

[34] MORGAN, A., "A recent judgement of the European Court of Justice could represent the birth of a whole new sub-species of data-protection jurisprudence", *Gazette of the Incorporated Law Society of Ireland*, 2014, p. 28-31, p. 30 et s..

[35] KULK, S., and ZUIDERVEEN BORGESIUS, F., "Google Spain v. González: Did the Court Forget about Freedom of Expression?", *European Journal of Risk Regulation,* 3/2014, p. 389-398, p. 392 et s.

[36] MORRISON, T., and WHITE, D., "Private eye. Tom Morrison & David White review the world of information law", *New Law Journal,* 2014 p. 17-18, p. 18.

[37] On this point, see also the next section, note 46.

believe, in this regard, that "[t]his societal question [of the restoration of one's public standing or image] is strongly tied to the culture within which the request is made, in contrast to the Google Search service, which is offered worldwide. It, therefore, seems that the Google Spain SL judgment will lead to greater differences between the service offered inside and outside of Europe"[38]. Moreover, some authors warn against the spill over effects of the Google Spain judgment. Spindler believes that due to the media coverage of this decision, the applicant has obtained a mere "Pyrrhic victory"[39], and Leupold believes that this decision will thwart any effective protection of privacy, warning against the "Streisand effect", a media phenomenon in which the will to prevent the disclosure or obtain the removal of information causes the opposite result.[40]

As regards the difficulties that the operator of a search engine would face to comply with the requirements of the Google Spain judgment, Jones admits that "the decision […] poses a serious risk of chilling the online publication of lawful and legitimate third-party content within the EU and thus undermining the internet's great strength as information disseminator […] The internet could be degraded to a battleground for reputation management where search engines are no longer neutral and comprehensive, and worse still could manipulated […] to lead to pre-emptive censorship"[41]. Such considerations have led some authors as Zankl, to reject the Google Judgment as a whole: "Das vom EuGH anerkannte „Recht auf Vergessenwerden" ist abzulehnen. Es beeinträchtigt die Informationsfreiheit, hat keine normative Grundlage und kann nicht durchgesetzt werden."[42] On the contrary, Martial-Brazand Rochfeld believes that "[i]n spite of appearances, the right to be forgotten upheld by the Court appears relatively limited such that the cloak of freedom that is adorned with it seems to be oversized. It must be noted that the "right to be forgotten" tightens its grip on core rights whose articulation with others is by no means unknown"[43] Finally, authors such as Marino moderate the debate by reiterating that "Google Spain has a precise scope [...] it only concerns individuals, like the directive that it interprets [and] only benefits the individuals concerned and not their heirs. Digital eternity is another story…"[44]

[38] VAN EECKE, P., and CORNETTE, A., "What the CJEU has actually decided in Google Spain SL, No. C-131/12", *Computer und Recht,* 2014, p. 101-107, p.107; see also CROWTHER, H., "Remember to Forget Me: The Recent Ruling in Google v AEPD and Costeja", *Computer and Telecommunications Law Review* 2014, p. 163-165, p.165.

[39] SPINDLER, G., "Durchbruch für ein Recht auf Vergessen(werden)? – Die Entscheidung des EuGH in Sachen Google Spain und ihre Auswirkungen auf das Datenschutz- und Zivilrecht", *Juristenzeitung*, 2014, p. 981-991, p. 991.

[40] LEUPOLD, A., "Google und der Streisand-Effekt: Das Internet vergisst nicht", *Medien und Recht International,* 2014, p. 3-6, p. 6.

[41] JONES, J., "Control-alter-delete: the 'right to be forgotten'", *European Intellectual Property Review*, 2014, p. 595-601, p. 599.

[42] ZANKL, W., "EuGH: 'Recht auf Vergessen-werden'", *Ecolex,* 2014, p. 676-677, p. 676.

[43] MARTIAL-BRAZ, N., and ROCHFELD, J, cit. supra note 16, p. 1482.

[44] MARINO, L., cit. supra note 10, p. 768.

The territorial application of Directive 95/46/EC

The question of the potential application of Directive 95/46/EC outside the EU territory has sparked a number of doctrinal reactions. Kuner observes that the Google judgment "is the most authoritative confirmation yet that an EU-based subsidiary of a multinational company with headquarters in another region may be subject to EU data protection law even if it doesn't actually operate the data processing service at issue. […] The judgment seems to place no territorial limits on application of the right, so that it could apply to requests for suppression from individuals anywhere in the world. […] [It] therefore potentially applies EU data protection law to the entire Internet […]. This could lead to forum shopping and 'right to suppression tourism' by individuals with no connection to the EU other than the fact that they use Internet services that are also accessible there"[45]. However, Jones believes that "[t]he judgment will not apply outside the EU. Searching from the United States, for example, where the First Amendment's free speech provision usually trumps privacy concerns, may reveal information relating to the private data of an EU citizen, and it remains open for companies with no EU establishment to serve [the material the Court ruled should be forgotten]"[46]

In any event, as regards the application of the European law on data protection vis à vis Google Inc. as well as Google Spain, Schmidt-Kessel, Langhanke and Gläser observe that "the decision clarifies that the ways of thinking of European private law are different those of national private laws. This difference also applies to public law and the law on personal data" [47]

The liability of the operator of a search engine

Commenting on the Google Spain ruling, several authors such as Benabou noted that "[w]hat is striking [...] lies in the clear distinction made by the Court between the processing performed by the search engine and that performed by the editor of the source pages [...] A true 'tom-tom' for the Internet [48], the search engine does not just to relay information and carry the Internet users to that destination; it aggregates this material and prioritises it in order to ease the locating of information [...]. Therefore it is not only justified but even effective to act against the engine." [49] In the same way, Busseuil notes that "[t]he Court again condemns the neutrality of intermediaries [...] [T]he liability of the search engine can mitigate the impossibility of acting against the editor of the web page when it is not subject to the European Union law"[50]

[45] KUNER, C., cit. supra note 6, p. 15.

[46] JONES, J., cit. supra note 41, p. 600 et s.; see also the next section.

[47] SCHMIDT-KESSEL, M., LANGHANKE, C. and GLÄSER, C."Recht auf Vergessen une piercing the corporate Veil - zugleich Anmerkungen zur Google-Entscheidung des EuGH, Rs. C-131/12, Google Spain SL une Google Inc." *Zeitschrift für Gemeinschaftsprivatrecht*, 2014, p. 192-197, P. 197

[48] See also MARTIAL-BRAZ, N., and ROCHFELD, J., cit. supra note 16, p. 1483, who uses the expression "tom-tom of the digital age".

[49] BENABOU, V.-L., and ROCHFELD, J., "Les moteurs de recherche, maîtres ou esclaves du droit à l'oubli numérique? (Search engines, master or slave of the right to digital oblivion?) Act I: Le moteur, faciliteur d'accès, agrégateur d'informations et responsable de traitement autonome" (The engine, access facilitator, aggregator of information and independent processing controller), *Recueil Dalloz,* 2014, p. 1476, 1478 et s..

[50] BUSSEUIL, G., "Arrêt Google : du droit à l'oubli de la neutralité du moteur de recherche", *La Semaine Juridique - entreprise et affaires,* 2014, nº 24, p. 1327

However, some authors question the appropriateness of the liability of search engine operators. Kulk and Zuiderveen Borgesius believe that "search engine operators may not be the most appropriate party to balance the fundamental rights involved"[51]. Similarly, Marino considers that "one may regret this lack of principle of subsidiarity that contributes to freeing site publishers from any liability when they should be first in line. One can also complain about a critical flaw in the solution, since if we are content with using Google - which is certainly very used - we can simply use another search engine to search for information. Some will turn away from Google"[52]. More generally, Härting wonders if the same solution would have been retained against a large European search engine, suggesting that the decision would be partly directed against American Internet companies. "Hätte das Gericht genauso entschieden, wenn es sich bei Google um einen europäischen Weltkonzern handeln würde? Ich glaube nein. Denn die Richter dürften nicht ganz unbeeinflusst gewesen sein von der zunehmenden Dämonisierung amerikanischer Internetkonzerne in Europa."[53]

Moreover, a part of the doctrine, such as Bäcker, criticises the interests weighed by the Court. He laments the lack of consideration of interests of persons wishing to publish information on the Internet and believes that the inherent logic of the law on personal data does not take the current issues into account: "Das Urteil krankt daran, dass der EuGH die Bedeutung von Suchmaschinen für die Netzkommunikation aus seiner einseitigen Risikoperspektive bestimmt. […] Gerade Kommunikatoren außerhalb der herkömmlichen Massenmedien sind […] auf leistungsfähige Suchmaschinen existenziell angewiesen. […] Das Google-Urteil verdeutlicht, dass hergebrachte datenschutzrechtliche Regelungsmuster auf die netzöffentliche Kommunikation und ihre Intermediäre kaum passen."[54] However, Aubert, Broussy and Cassagnabère feel that "[i]t is clear that this solution tipped the balance to the detriment of the right to information of Internet users and the entrepreneurial freedom of the search engine. But it is the price to be paid for the popularity of these concepts, and especially a reassuring sign that the Court has taken into account the current state of technology and underlying economic models in the information society"[55].

Finally, according to some authors such as Kelsey, the Google Spain ruling can be transposed to other Internet players. She concludes by stating that "[t]he approach of the Court […] seems ripe for application to other internet platforms which "process" data in similar ways, such as, potentially operators in the field of social media"[56].

[51] KULK, S., and ZUIDERVEEN BORGESIUS, F., cit. supra note 35, p. 394 et s.

[52] MARINO, L., cit. supra note 10, p. 768.

[53] HÄRTING, N.,"Google Spain - Kommunikationsfreiheit vs. Privatisierungsdruck", *Betriebs-Berater,* 22/2014, p. I.

[54] BÄCKER, M., "Ein unschöner Paukenschlag", *Wettbewerb in Recht und Praxis*, 7/2014, Die erste Seite.

[55] AUBERT, M., BROUSSY, E., CASSAGNABERE, H., cit. supra note 15, p. 1148 et s.

[56] KELSEY, E., "Case Analysis - Google Spain SL and Google Inc. v AEPD and Mario Costeja González: Protection of personal data, freedom of information and the 'right to be forgotten", European Human Rights Lake Review, , 2014, p. 395-400, p. 400.

...

Conclusion

The doctrinal responses to the two rulings commented upon follow two main principles. On the one hand, the two rulings were, for the most part, considered a physical and institutional, or even constitutional reinforcement of the protection of personal data at the EU level. Spiecker gen. Dohmann considers that they have ended the "right of the strongest and fastest": "Dem 'Recht des Stärkeren und Schnelleren', das gegenwärtig im internationalen Informationsmarkt und im Zeitalter der NSA auch im Staat-Bürger-Verhältnis herrscht, haben jedenfalls sowohl das Vorratsdatenspeicherungs- als auch in besonderem Maße das Google- Spain-Urteil spürbar Einhalt geboten und Europa als einen ernstzunehmenden Akteur im Informationsmarkt wieder stärker etabliert." [57]

On the other hand, however, many authors question the practical consequences and application of the two rulings. With regard to the Digital Rights Ireland ruling, while the comments are generally optimistic, Spina believing in particular "that [it] could pave the way for a bigger role of risk regulation in EU data protection law"[58], many authors have reservations about the implementation of the Google Spain ruling"[59]. Thus, Snedden and Sirel consider that "[t]he judgement leaves open a number of questions likely to be the subject of further litigation". In any event, Cassart and Henrotte believe that "[at] this stage, it is difficult to guess how the right to be forgotten will be understood by citizens [...]. The success of social media and other services that are personal data-intensive demonstrates, unfortunately, how little most of the Internet users acknowledge privacy"[60].

On a more general note, Boehme-Neßler concludes that the oblivion is important for the progress of a digital society; the Google Spain ruling can be the basis to find a balance between private and public spheres, between memory and oblivion: "Ohne Vergessen ist auf die Dauer kein Fortschritt möglich. Auch und gerade in der Informationsgesellschaft ist es deshalb wichtig, Daten zu löschen und Informationen zu vergessen. Diese Erkenntnis hat der EuGH jetzt grundrechtlich verankert. Das wird - hoffentlich - der Anfang einer Entwicklung, die zu einer gesellschaftlich akzeptierten Balance zwischen Privatsphäre und Öffentlichkeit, zwischen Erinnern und Vergessen führt."[61]

[KAUFMSV] [HANLEVI] [GARCIAL]

- - - - - - - - - - -

[57] SPIECKER GEN DÖHMANN, cit supra note 4, p. 1113

[58] SPINA, A., "Risk Regulation of Big Data: Has the Time Arrived for a Paradigm Shift in EU Data Protection Law?", *European Journal of Risk Regulation*, 2/2014, p. 248-252, p. 249.

[59] SNEDDEN, S., and SIREL, A., "Forget that you ever knew me", *The Journal of the Law Society of Scotland*, 2014, p. 14-15, p. 15.

[60] CASSART, A., and HENROTTE, JF, "Google Spain ruling: the revelation of a right to erase rather than the creation of a right to be forgotten", *Revue de jurisprudence de Liège, Mons et Bruxelles,* 2014, p.1183-1191, p. 1191.

[61] BOEHME-NEßLER, V., "Das Recht auf Vergessenwerden - Ein neues Internet-Grundrecht im Europäischen Recht", *Neue Zeitschrift für Verwaltungsrecht*, 2014, p. 825-830, p. 830

...

Information

The texts and documents that the following information refers to are extracted from publications available at the Court library.

The references under the case law decisions (IA/..., QP/..., etc.) refer to the case numbers in internal DEC.NAT. and CONVENTIONS bases. The records relating to these decisions can be found in the research and documentation department.

The case law notes included in the "Doctrinal echoes" section have been carefully selected. A comprehensive list of the published notes in the internal NOTES base.

The publication *"Reflets"* is available on Curia (www.curia.europa.eu) under "Library and Documentation/Legal information of interest for the Union" and on the intranet of the Directorate-General of the Library, Research and Documentation.

The following members have contributed to this issue: Pawel Banczyk [PBK], Bernd Bertelmann [BBER], Erwin Beysen [EBN], Marina Borkoveca [BORKOMA], Antoine Briand [ANBD], Maria Helena Cardoso Ferreira [MHC], Keiva Marie Carr [CARRKEI], Anna Czubinski [CZUBIAN], Ingrid Dussard [IDU], Patrick Embley [PE], Victoria Hanley-Emilsson [HANLEVI], Sally Janssen [SJN], Sven Gael Kaufmann [KAUFMSV], Diana Kušteková [KUSTEDI], Giovanna Lanni [GLA], Michael George Loizou [LOIZOMI], Loris Nicoletti [NICOLLO], Garyfalia Nikolakaki [GANI], Maria Pilar Nunez Ruiz [NUNEZMA], Ragne Piir [PIIRRAG], Jerker Olsson [JON], Veera Pedersen [PEDERVE], Cristina Maria Prunaru [CLU], Sabina Ruffo [RUFFOSA], Saša Sever [SAS], Florence Simonetti [SIMONFL], Nadezhda Todorova [NTOD], Zsófia Varga [VARGAZS], Loïc Wagner [WAGNELO].

Including: Anna Dannreuther [DANNRAN], Guus De Bruijn [DEBRUGU], Alejandra Garcia Sanchez [GARCIAL], Adam Jurago [JURADAD], trainees.

Coordinators: Síofra O'Leary [SLE], Loris Nicoletti [NICOLLO].