University of Central Lancashire Cyprus Campus

Nicosia

16 April 2019

Roundtable discussion

"The role of the Court of Justice in enhancing data protection in the European Union"

Koen Lenaerts[*]

Dear Professors,
Dear students and friends,

I am very grateful to the organisers of this event for giving me the opportunity to open this roundtable discussion on a subject that has been an important topic for discussion in recent times.

The Digital Revolution has given rise to a new awareness that personal data must be protected properly. New technology allowing us to search on the internet, to communicate easily, to be permanently available and to lead what some have called a "digital life" has numerous advantages. However, our digital life also inevitably generates data that could reveal the user's identity - data which can be of interest to both public authorities and private companies, as it "may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities

[*] President of the Court of Justice of the European Union and Professor of European Union Law, Leuven University. All opinions expressed are personal.

carried out, the social relationships of those persons and the social environments frequented by them."[1]

One of our shared European values being the respect for individual privacy, any information concerning the identity of individuals should, in principle, benefit from data protection.

The legal and social importance of the right to data protection can be inferred from EU primary law itself. In fact, in contrast to the wording of the European Convention on Human Rights, Article 8 of the Charter of Fundamental Rights of the European Union (hereafter 'the Charter') has conferred on that right an autonomous character. While remaining closely linked to the right to respect for private life enshrined in Article 7, it has been "emancipated" from the latter as it has become more and more crucial in the digital age.

Over the past decade, the Court has been called upon to decide cases in the field of data protection with increasing frequency. One telling indication of the importance of data protection is the number of recent Grand Chamber judgments relating to that fundamental right.

The very first example in our case-law that deals with the issue of data protection – without, however, using that term – is the *Stauder* case of November 1969[2]. The *Stauder* case also represents the starting point for the development of the case law on fundamental rights at EU level, decades before the Charter of Fundamental Rights of the European Union came into being.

In order to stimulate the sale of surplus quantities of butter in the common market, the Commission allowed Member States to enable consumers receiving social welfare to buy butter at a reduced price. The German language version of the Commission decision

[1] CJEU, 8 April 2014, *Digital Rights Ireland Ltd*, Joined Cases C-293/12 and C-594/12, EU:C:2014:23, para. 27.

[2] CJEU, 12 November 1969, *Stauder v City of Ulm – Sozialamt*, EU:C:1969:57.

required the consumer to use a coupon issued in his or her name. Taking the view that this requirement to divulge his name to the retailer infringed his fundamental rights, Mr. Stauder seized a German administrative court,[3] which referred the question to the Court of Justice.

The Court of Justice observed that the German and Dutch versions of the decision contained translation errors and that the decision did not in fact require identification by name, but only that the coupon should refer to the person concerned. Since the Member States were thus able to choose from a number of methods, the Court of Justice found that, interpreted in this way, the provision at issue contained nothing capable of infringing the fundamental human rights enshrined in the general principles of Community law and protected by the Court. The irony of this case is that, although Mr. Stauder sought protection of his privacy in the main proceedings, his name has become known to a far larger audience than just his retailer as a result of the case.

I should also mention the much more recent *Volker und Markus Schecke* case of 2010[4] where farmers benefitting from EU agricultural funds objected to the fact that their names and the amounts received were published, as provided for in two EU regulations. Applying the Charter of Fundamental Rights of the European Union to facts that occurred before its formal entry into force, the Court of Justice decided that publishing the names of individuals and the amounts that they receive constituted a disproportionate measure with regard to the objective of transparency. Therefore, the Court declared the relevant provisions of EU law invalid.

May of last year saw the entry into force of the General Data Protection Regulation[5] – better known under the acronym GDPR. It replaces the 1995 Data Protection Directive,

[3] Verwaltungsgericht Stuttgart.

[4] CJEU, 9 November 2010, *Volker und Markus Schecke GbR* (C-92/09) and *Hartmut Eifert* (C-93/09) *v Land Hessen*, EU:C:2010:662.

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1).

which needed to be adapted to a fast-changing and increasingly complex environment. Some references for a preliminary ruling concerning this new regulation are currently pending before the Court of Justice. A first judgment referring in its operative part to the GDPR was given in January of this year.[6]

When enforcing the individual's right to data protection, it is important to bear in mind that the right to privacy is not unlimited. In fact, as the Court ruled in the *Schecke* case – in a formula codified by the legislator at recital 4 of the GDPR – "the right to the protection of personal data is not […] an absolute right, but must be considered in relation to its function in society."[7]

It is for the legislator – both at national and at European level – to strike a reasonable balance between conflicting rights and interests. It is then for the courts to assess this balance in the light of the different instruments protecting fundamental rights. The Charter comes into play when a question is raised concerning the legality either of an EU act or of an act of a national authority implementing European Union law.

Data protection law can be described as having two dimensions, since it involves striking the correct balance not only between private interests and the public interest, such as the interest in combating crime, but also between competing private interests, such as the right to privacy on the one hand and the freedom of expression or the right of access to information on the other hand.

[6] CJEU, 16 January 2019, *Deutsche Post AG v Hauptzollamt Köln*, C-496/17, EU:C:2019:26. The Court ruled in this case that the customs authorities may require an applicant for "authorised economic operator" status to send to them the tax identification numbers, allocated for the purposes of collection income tax, concerning solely the natural persons who are in charge of the applicant or who exercise control over its management and those who are in charge of the applicant's customs matters, and the details of the tax offices responsible for the taxation of all those persons, to the extent that that data enables those authorities to obtain information on serious or repeated infringements of customs legislation or taxation rules or on serious criminal offences, committed by those natural persons and relating to their economic activity.

[7] CJEU, 9 November 2010, *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, C-92/09 and C-93/09, EU:C:2010:662, para. 48.

Let me begin by outlining the public dimension of the right to data protection, i.e. the relationship between public authorities and individuals.

The EU and Member States are both engaged in the fight against serious crime, even more urgently following the horrifying terrorist attacks which have struck numerous Member States and third countries over the last few years. In adopting legislation to combat serious crime, the legislator is obviously pursuing a legitimate interest. The legislator's margin of appreciation is nonetheless constrained by the fundamental rights protected by the Charter.

The 2014 *Digital Rights Ireland* case[8] illustrates that point.

With public security in mind, the EU legislator had adopted in 2006 a directive[9] requiring Member States to oblige electronic communication service providers to keep a record, for at least 6 months and for a maximum of up to two years, of all data relating to electronic communications' traffic and location. The objective was, in particular, to facilitate the prevention and prosecution of serious crime, including terrorist attacks.

The Data retention Directive entailed *de facto* an indiscriminate interference with the right to data protection "of practically the entire European population",[10] regardless of whether the persons concerned were suspected of any crime.

However, in a society based on the fundamental value of individual freedom, restrictions imposed in respect of that freedom have to be limited to what is strictly necessary for the protection of the public interest.

[8] CJEU, 8 April 2014, *Digital Rights Ireland* and *Seitlinger and Others*, Joined Cases C-293/12 and C-594/12, EU:C:2014:238.
[9] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54).
[10] CJEU, 8 April 2014, *Digital Rights Ireland Ltd*, para. 56.

As regards the *retention* of data as such, the Court considered that the directive failed to provide, in the light of the objective of fighting serious crime, for any differentiation, limitation or exception. As regards *access* to the data retained, the directive failed to lay down the conditions under which the national authorities could have access to those data and make use of them. With respect to the data retention period of 6 to 24 months, the directive failed to state any objective criteria justifying its length. Moreover, since the directive did not require the data to be retained within the EU, it also failed to ensure the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security. Thus, the Court of Justice concluded that the EU legislator had imposed unnecessary and disproportionate restrictions on the rights enshrined in Articles 7 and 8 of the Charter and therefore declared the Data Retention Directive invalid.

A follow-up case, *Tele2 Sverige*,[11] concerned national measures implementing the Data Retention Directive that had been found to be invalid in *Digital Rights Ireland*. The Court confirmed that the same high standard of data protection applies to national authorities. Thus, only the objective of "fighting serious crime" could justify a far-reaching interference with the right to data protection and such an interference has to be limited to what is strictly necessary.

A high level of personal data protection should nevertheless not be such as to impede criminal investigations. The recent judgment in *Ministerio Fiscal* demonstrates that the Court of Justice takes into account the needs of criminal investigations.[12] The main proceedings concerned a robbery involving the theft of a wallet and a mobile phone in Spain. The investigating authority requested access to data for the purpose of identifying the owners of SIM cards activated using the stolen phone.

This raised the question whether access to personal data retained by a telecommunications operator could only be granted in order to combat "serious crime", which under Spanish law does not cover a robbery such as the one at issue in the main proceedings. The

[11] CJEU, 21 December 2016, *Tele2 Sverige* and *Watson and Others*, C-203/15 and C-698/15, EU:C:2016:970, para 102.
[12] CJEU, 2 October 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788.

Audiencia Provincial de Tarragona (Provincial court of Tarragona) sought guidance from the Court on the degree of "seriousness" of the offence capable of justifying access to the data.

The Court of Justice expressly distinguished this case from *Tele2 Sverige*. The Court stressed that that latter case concerned a serious interference into data protection rights, as the data retention – and access – at issue was such as to allow *precise conclusions* to be drawn concerning the private lives of the persons whose data had been collected.[13] Such interference can indeed be justified only by the objective of fighting serious crime. However, in *Ministerio Fiscal*, the interference itself was not serious: the requested access only concerned the telephone numbers corresponding to the SIM cards used in the stolen mobile telephone and the data relating to the identity of the owners of those cards, but not to the communications carried out using it or its location. The objective of preventing, investigating, detecting and prosecuting 'criminal offences' generally can indeed justify a limited interference of that kind.[14]

In addition to its mission of balancing public interests and individual rights, the Court of Justice has also been called upon to arbitrate between conflicting private interests.

This can be illustrated by reference to the seminal 2014 *Google Spain* judgment.[15]

In this case, the name of a Spanish national appeared in two newspaper announcements for a real-estate auction held in 1998 from which it could be inferred that he had been the subject of proceedings for the recovery of social security debts. A search based on that person's name on Google retrieved those two announcements, which he considered to be both detrimental to his reputation and no longer relevant. He therefore requested, before the Spanish courts, that Google be ordered to remove or to conceal that data relating to him. The *Audiencia National* (National High Court, Spain) sought guidance from the

[13] *Ibid.*, para. 54.
[14] *Ibid.*, paras 57, 61 and 62.
[15] CJEU, 13 May 2014, *Google Spain and Google*, C-131/12, EU:C:2014:317.

Court of Justice, in essence, as to whether that request could find any support in the 1995 Data Protection Directive.

As a first step, the Court classified the activity of a search engine – which consists in finding, indexing, storing and making available information containing data, including personal data – as the "processing of personal data" within the meaning of that directive. The Court then qualified the operator of the search engine as a "controller" in respect of that processing and held that that operator, at the request of the person concerned, had to remove all references to web pages containing the name of that person when the information appears to be inadequate, irrelevant or *no longer* relevant, or excessive in relation to the purposes of the processing.[16] The Court made it clear that the fundamental rights of the person concerned under Articles 7 and 8 of the Charter override, as a rule, not only the economic interests of the operator of the search engine but also the interest of the general public in finding that information. However, the Court did not rule out the possibility that there may be cases where it is rather the interest of internet users in having access to the information which should prevail. This could be the case, for example, where the person concerned plays a role in public life.[17]

This case clearly shows the Court of Justice's attachment to data protection rights and served as a basis for 'the right to be forgotten' – or the right to erasure – which is now enshrined in the GDPR.[18]

In two pending preliminary reference procedures also concerning Google, the Court is now called upon to provide additional guidance as to *the circumstances in which* the operator of a search engine has to accede to a request for the dereferencing of sensitive

[16] *Ibid.*, para. 94.
[17] *Ibid.*, para. 97.
[18] Art. 17.

data,[19] and to determine whether dereferencing should be undertaken at *national, EU or world level*.[20]

In two recent cases decided in 2018, the Court further specified the notion of a "controller" within the meaning of the 1995 Data Protection Directive, which remained unchanged in the GDPR.[21] Thus, in *Wirtschaftsakademie Schleswig-Holstein*, the Court decided that the administrator of a Facebook fan page falls within that notion and is thus jointly responsible with Facebook for the processing of data of visitors to the fan page.[22] That is so, in essence, because the administrator contributes to determining the 'purposes and means' of the processing of personal data through cookies which Facebook places on fan pages. In *Jehovan todistajat*, the Court held that a religious community, such as the Jehovah's Witnesses, is a 'controller', jointly with its members who engage in preaching, for the processing of personal data carried out by the latter in the context of door-to-door preaching organised, coordinated and encouraged by that community.[23]

Before I conclude, let me highlight a case decided very recently,[24] in which the Court had to strike a balance between the right to privacy and the freedom of expression.

The main proceedings concerned Mr. Buivids who had made a video recording in a Latvian police station while he was making a statement in the context of administrative proceedings brought against him involving the imposition of a penalty. As he considered that the police officers had been acting unlawfully, he published the video on YouTube. The Latvian Data Protection Agency ordered Mr. Buivids to remove the video from that platform, in particular because he had not informed the police officers of the intended purpose of the processing of their personal data. The Latvian Supreme Court asked the

[19] Questions referred by the French *Conseil d'Etat* on 15 March 2017, C-136/17, *G.C., A.F., B.H., E.D. v Commission nationale de l'informatique et des libertés (CNIL).*

[20] Questions referred by the French *Conseil d'Etat* on 21 August 2017, C-507/17, *Google Inc. v Commission nationale de l'informatique et des libertés (CNIL)*.

[21] Article 4 (7): 'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

[22] CJEU, 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, EU:C:2018:388.

[23] CJEU, 10 July 2018, *Jehovan todistajat*, C-25/17, EU:C:2018:551.

[24] CJEU, 14 February 2019, *Sergejs Buivids*, C–345/17, EU:C:2019:122.

Court of Justice whether such a recording and publication fall within the scope of the 1995 Data Protection Directive, and, if so, whether such a publication may be regarded as a processing of personal data for journalistic purposes.

The Court considered that, as it was possible to identify the police officers on the video, the images constituted personal data, and that the recording and publishing of the video constituted processing of those data.

However, the Court stressed that the directive obliges the Member States to provide for exemptions when the processing of personal data is "carried out solely for journalistic purposes", but only to the extent necessary for reconciling the right to privacy with the freedom of expression. That journalistic exemption was nevertheless defined in particularly broad terms, as it covers activities which aim at 'the disclosure to the public of information, opinions or ideas'.[25] The Court left it to the Latvian Supreme Court to decide whether M. Buivids could benefit from that exemption in the main proceedings.

The case-law that I have discussed demonstrates the Court of Justice's commitment to upholding the right to privacy in general and the right to personal data protection in particular, while always keeping in mind the necessity to strike a balance with legitimate public objectives or with other fundamental rights. There is little doubt that the Court will have plenty of new opportunities in the future to develop its case-law on data protection further when interpreting the vast and complex set of rules contained in the GDPR.

Thank you for your attention.

[25] CJEU, 14 February 2019, *Sergejs Buivids*, paras 53 and 68.