UTRECHT JOURNAL OF
INTERNATIONAL AND EUROPEAN LAW

Mistale Taylor, '"Safeguarding the Right to Data Protection in the EU", 30th and 31st October 2014, Paris, France' (2015) 31(80) Utrecht Journal of International and European Law 145, DOI: http://dx.doi.org/10.5334/ujiel.cw

CONFERENCE REPORT

"Safeguarding the Right to Data Protection in the EU", 30th and 31st October 2014, Paris, France

Mistale Taylor[1]

[1] Utrecht University, the Netherlands
M.S.C.Taylor@uu.nl

This contribution is based on presentations and discussions at the conference "Safeguarding the Right to Data Protection", held in Paris on the 30th and 31st October, 2014. Vladimir Marinescu, of the Academy of European Law (hereafter: ERA), in cooperation with the *Cour de Cassation*, organised the event. The conference looked at developments in EU data protection law with a focus on data protection as a fundamental right. Speakers discussed recent jurisprudence from the Court of Justice of the European Union (hereafter: CJEU or the Court), the European Court of Human Rights (hereafter: ECtHR) and national courts. The conference covered four main focus areas: EU data protection law; civil and criminal law aspects of data protection and the internet; data protection as a cornerstone of European fundamental rights protection; and data protection remedies. This contribution elaborates upon some of the most pertinent issues speakers discussed.

Keywords: data protection; fundamental rights; EU law

I. Introduction

A. Speakers and Issues Covered

On the 30th and 31st October 2014, the *Cour de Cassation*, in the magnificent *Palais de Justice* in Paris, played host to a mix of judges and prosecutors, academics, data protection and information lawyers, data protection officers, EU and national public servants, and compliance and information officers. Such was the magnitude of the event and diversity of attendees, that all discussions were simultaneously interpreted from and into English, German and French.

A wide range of high-calibre speakers, from various academic, legal and political backgrounds, explored the abovementioned subjects. Bertrand Louvel, First President of the *Cour de Cassation*, Paris, and Wolfgang Heusel, the Director of ERA, Trier, opened the conference. Niilo Jääskinen, Advocate General of the European Court of Justice, Luxembourg, outlined recent CJEU jurisprudence in the field of data protection and its impact on EU legislation. Jean-Paul Jacqué, professor at the College of Europe and former Director of the Legal Service of the Council of the European Union, Brussels, then explored the potentially growing role of the EU Charter of Fundamental Rights in the field of data protection. Director of Fundamental Rights and Citizenship, DG JUST at the European Commission, Brussels, Paul Nemitz, updated attendees on EU legislation by looking at the legislative package on data protection.

In a discussion chaired by Honorary Dean of the *Cour de Cassation* and Vice President of CNIL, Paris, Marie-France Mazars, several speakers presented on and discussed legal implications of data protection and the internet. Paul Van den Bulck, partner at McGuireWoods, Brussels, and Wolfgang Bär, Head of Internet Crimes Unit at the Bavarian Ministry of Justice, Munich, examined implications of cloud computing and virtualisation of data in a civil and criminal law context. Wojciech Wiewiórowski, Inspector General for the Protection of Personal Data (GIODO), Warsaw, and Vice Chair of the Article 29 Working Party, then looked at data protection after Snowden and PRISM, namely, the legal limits to foreign and European intelligence and surveillance. CEO of Aconite Internet Solutions, Dublin, Cormac Callanan discussed profiling, crawling and cooperation with the internet industry to draw conclusions on data protection and social networks.

Moving onto the fundamental rights dimension of data protection, Johannes Masing, Member of the German Federal Constitutional Court, Karlsruhe, and Professor at the University of Freiburg, outlined the

scope of the fundamental right to data protection in Germany. ECtHR judge, Strasbourg, Robert Spano, examined recent ECtHR case law in the data protection field. To round off the conference, Peter Hustinx, European Data Protection Supervisor, Brussels, and Thilo Weichert, Schleswig-Holstein Commissioner for Data Protection and Freedom of Information, Kiel, outlined the role of data protection supervisors. Finally, Anne-Elisabeth Crédeville, Judge, First Civil Chamber, *Cour de Cassation*, Paris, discussed judicial protection as a data protection remedy.

The present report summarises the contributions by Bertrand Louvel, Wolfgang Heusel, Niilo Jääskinen and Paul Nemitz, as they provide a useful introduction to the subject of data protection in the EU, and cover both legal and policy issues. The report also outlines some points made by Peter Hustinx, as this moves from the theoretical to the practical aspects of data protection. Finally, the contribution touches upon some points made by Jean-Paul Jacqué on the growing role of the EU Charter in data protection. From here, this conference report will show how data protection has moved from an economic necessity to a fundamental right in the EU, and how data protection is increasingly being characterised as a human right. Indeed, the very name of the conference on which the report is based shows the importance and increased ubiquity of data protection as a fundamental right in the EU.

I. Bertrand Louvel: Current data protection discussions

Bertrand Louvel opened the conference by anchoring the conference in current discussions on transparency, surveillance, digital identities and fundamental rights.

Formerly, there existed an obligation to disclose information to citizens, but now transparency has taken on a new form as a guarantee of probity. It is a requirement for all forms of democratic control and is now an everyday reality for all of us.

Today, with video surveillance and biometric data visible to big brother, it is difficult for us to stay concealed. Citizens are worried about increasingly efficient surveillance systems. The internet is a strange world as it was never structured or designed. Subjects have a new digital identity, which is partly determined by someone's will, but often escapes it. Subjects can create a virtual alter ego through which they share their thoughts and sometimes manipulate them, often by beautifying their actions or pretending to be someone else. These actions leave markers by which our reputation and standing are assessed. In a globalised economy, is it necessary to adapt to global expectations? Open data gives us a glimpse of State secrets and people's private lives. As such, there is a need for protection and a duty of non-interference in private lives. There is also a duty to protect these freedoms through constitutional documents, such as the EU Charter. The effectiveness of fundamental rights thus becomes a major challenge.

II. Wolfgang Heusel: ERA conferences on data protection

Wolfgang Heusel began by noting that data protection has been high on the legal, political and judicial agenda of EU in the past few years. The growing importance of data protection is exemplified by a series of annual conferences, which usually take place in spring. Unlike the last ERA conference on data protection, which dealt with recent developments in the field, such as reform, data transfers and the consequences of the PRISM affair, the focus of the present conference was on the right to data protection for citizens, which is an aspect of fundamental rights.

III. Niilo Jääskinen: Recent CJEU jurisprudence in the field of data protection and its impact on EU legislation

Niilo Jääskinen discussed the recent, historical judgements in the CJEU's *Digital Rights Ireland* and *Google Spain* cases. He contextualised his presentation by noting that the internet has given us a dream of unlimited freedom of information. Conversely, technological advances, which create the possibility for everything to be surveyed, have given us the means to suppress that freedom.

A. Case One: Digital Rights Ireland

Digital Rights Ireland, decided 8 April, 2014, concerned the validity of Directive 2006/24, which obliged various internet and telecommunications companies to retain data to combat serious crime and terrorism.[1] The Directive established an obligation for telecommunications companies and internet operators to retain data on all data traffic, the identity of the person instituting the communication, and the relevant location

[1] CJEU, *Joined cases Digital Rights Ireland (C-293/12) and Kärntner Landesregierung (C-594/12)*, judgement of 8 April, 2014; Data Retention Directive, Directive 2006/24.

and means of communication. The Directive did not require that the content of communication be retained. The relevant data was retained for a period of at least six months and at most two years. Three provisions in the EU Charter of Fundamental Rights, namely Article 7 on the right to protection of private and family life; Article 8 on the right to data protection; and Article 11, on the right to freedom of expression, provided the legal grounds for possible annulments.

A1. Proportionality Assessment

The case has had a strange life before the Court. The Court decided on some infringement actions about non-implementation of the Directive against Spain, Ireland, Germany and Greece. The Court had touched on the Directive in some preliminary rulings cases, but had not really interpreted it. After quite a long time and some important battles before constitutional courts, the CJEU had to take a stand and determine the Directive's validity.

The main issue the Court considered was proportionality: did the Directive go too far? One criterion in the proportionality analysis is that the Directive's provisions must not constitute an interference in a fundamental right. In short, the Court considered the Directive disproportionate. The Court said that the Directive, in practice, places the whole EU population under surveillance, rendering its scope extremely large. A notably large quantity of the retained data was completely unhelpful and unrelated to the objectives of combating serious crime. The Court ruled that the EU legislature had exceeded the limits imposed by principle of proportionality in the light of Articles 7, 8 and 52(1) of the EU Charter. Consequently, Directive 2006/24 was invalid. The Court found it unnecessary to discuss Article 11 in detail because it already found the Directive invalid on the basis of Articles 7 and 8.

There is usually a grace period for the legislator to provide for new and valid provisions, but the Court found the infringement upon and interference with fundamental rights so strong, that there was no justification for temporary application of the Directive.

A2. Further Issues

The Directive left unexplained the issue of using the data. The only obligation was for national legislation to provide that data be retained, but issues of who had access to the data were left unregulated. The retention period the Directive instituted was both long and imprecise. There were no criteria on how a Member State should decide between the temporal retention possibilities. The Directive did not require that data be retained within the EU. As such, it was quite possible that service providers retained data in China or the US, that is, jurisdictions where the Charter does not apply.

A3. Consequences

There have been some notable, and potentially unforeseen, consequences of the *Digital Rights Ireland* decision. Firstly, the decision has caused a legislative hurdle in many Member States. What happens to the national legislation that implements the Directive? Jääskinen assumes Member States have and will take different approaches as the issue has returned to national competence. In some Member States, for example, national legislation has been sharpened to take into account the Court's reasoning. Secondly, in point 36 of the judgement, the Court gave the impression that every instance of processing personal data is an interference in Article 8, the fundamental right to data protection, which differs from what many experts have thought to be the true interpretation of Article 8.

B. Google Spain

The *Google Spain* case, decided 13 May, 2014, revolved around a data subject who wanted Google to remove links between his name and certain pages on *La Vanguardia* newspaper's internet archives.[2] In 1998, *La Vanguardia* published on the forced sale of his property due to his debts. The Court now believes that, 15 years later, that information is completely misleading and should not be there. The case raised four rather complicated questions, discussed below.

B1. Is the activity of a search engine 'processing of personal data' and is the operator of the search engine the 'controller'?

Google has crawlers or spiders that visit every internet page linked to another page. They then use algorithms to index all the words and search engine finds, forming links on the basis of relevance. From an

[2] CJEU, *Google Spain SL and Google Inc (C-131/12),* judgement of 13 May 2014.

internet law perspective, the issue could be whether a search engine operator is a content provider or only an intermediary. This raises questions of whether, when you provide links to third party pages, you are republishing the content of these pages or whether you are an intermediary. The Court was of the view that Google is the controller of processing personal data, and is therefore liable under data protection law for their content when it creates the possibility to link the name of an identifiable person with content.

B2. If the operator sets up a branch selling advertising space in a Member States, is that an 'establishment' by the controller? Accordingly, was Google subject to Spanish legislation that implements the EU Data Protection Directive?

Google Spain is a subsidiary of Google Inc; it is only responsible for marketing and selling advertising space. Most core functions of Google happen in the US. The Court took the stance that the Directive and, in consequence, Spanish law, was applicable to Google Inc. This was the only point where the Court followed the Advocate General's opinion.

This part of the judgement has raised all manner of questions. There is an obligation to remove data from EU sites, but what happens to google.com? Is Google bound to apply EU law to non-EU sites? In this sense, there is a conflict with the US' first amendment and EU fundamental rights. Should Google establish a Chinese-style firewall around its EU activities?

B3. Is the operator obliged to remove from the search results links to web pages containing personal information even if that information stays on the original pages and when that publication is lawful?

It is legally irrelevant that the data, which might be truthful, accurate and non-prejudicial for the data subject, has already been published. Removal is applicable directly against search engine operators and the data subjects can request that information that is considered excessive, irrelevant or inadequate be removed. The internet user's right to information must give way to the data subject's right to data protection. Usually, the right to data protection is stronger than the right to freedom of information, but there might be an exception in terms of public interest. If the data plays a role in public life, it might be that it should not be removed.

B4. Does the Directive enable the data subject to require the operator to remove from the list of results based on his name links to web pages that are published lawfully by third parties and that contain true information relating to him, if that information may be prejudicial to him or that he wishes it to be 'forgotten' after a certain time?

There are many questions regarding implementation. Google created a form where you could identify yourself and mention the pages you wished your name not be associated with. Google determines whether or not they have accepted the removal of links. Google established an advisory body of experts and has published regular transparency reports.

Google has accepted about 41% of removal requests. The majority have been declined, but Google has removed links in a considerable number of cases. The majority of cases concern social media. They also commonly concern articles in established media, such as *The Guardian* and *The BBC*. Google has a policy that they inform newspapers of possible removals, so the newspapers have the opportunity to oppose Google's decision. It is interesting to see how many cases where Google has declined to remove links will lead to a procedure before DPAs and before national Courts. The numbers are so huge that it could create quite an impossible situation for national DPAs.

IV. Paul Nemitz: The legislative package on data protection – an update on EU legislation

Paul Nemitz looked at the origins of European data protection laws and then moved to present-day EU legislation. Current data protection laws were drawn up in 1995, when the internet was in its infancy. To contextualise that, in 1995, a digital camera cost $US 1,000; now, we all carry one. In 1995, biometrics were used in high security access control; today they are used for low-cost operations, such as smartphone fingerprints. In 1995, law enforcement relied on face-to-face interviews; now investigators check Twitter, Facebook and similar activities with or without a warrant. In 1995, cybercrime and data breaches did happen, but no one predicted that such breaches would eventually amount to hundreds of millions of dollars. In 2013, more

than 100 million individuals' personal data had been compromised. This exemplifies a need to give a new impetus and set a new standard for Europe in data protection.

Nemitz then went on to discuss the current status of negotiations in the European Council on the reform, key outstanding issues, the importance of CJEU jurisprudence and important issues for the future, such as big data and mass spying. On 13 October, 2014, the European Council, committed to a timely adoption of the proposed General Data Protection Regulation (GDPR) by 2015. After 4,000 amendments, to have a very large majority in support of the GDPR in the European Parliament shows there is no political obstruction to adopting this reform. It is very rare in European law-making that the Parliament has a position before the Council; normally it is the other way around. Parliament adopted the Moraes Report following the Snowden revelations, which highlights how important it is to complete data protection reform. These developments ultimately show how sensitive the present Parliament is to the protection of the fundamental right to data protection.

Ministers of the European Parliament adopted the Data Retention Directive in nine months. Some say, in painting a gloomy picture of the Council, that when a matter concerns law enforcement, legislation is passed quickly, but when the matter purports to strengthen fundamental rights, it goes slowly. To ensure the digital single market really works in practice, identical rules on paper will not be enough. It is important to move from a directive, which must be implemented by Member States thereby leading to less transparency, to a regulation. For citizens moving between Member States and for the internal markets, directives are not good news. Europe has slowly moved increasingly from directives to regulations. The issue of coherence or application of national administrations in the EU is not specific, but specific to data protection is that independent authorities of Member States have to apply this law. There is tension between a constitutional level of independence and the need for coherence. The European Commission never proposed a central European Data Protection Authority. Individual DPAs will still make these decisions.

The one-stop-shop principle addresses the fact that internet services do not stop at national borders. There will be one single supervisory authority for businesses, instead of 28. This is important for big, medium and small sized companies. It will create a level playing field. Companies in third States, such as the US, which offer services to EU residents, will have to play by our rules and offer our level of data protection both for reasons of protecting fundamental rights and for fairness of competition. As such, the new system will prevent forum shopping. Citizens will always have the right to take their complaints to a local authority.

The European Commission's perception is that with two judgements in such close proximity, on the Data Retention Directive (*Digital Rights Ireland*) and *Google Spain*, and the upcoming *Max Schrems* case, the CJEU has taken the lead in the judicial structure of data protection. This is especially in comparison with third States. Europe is the worldwide leader in legislation and practice on protection of personal data.

A. Safe Harbour

Two prominent data protection issues are surveillance and big data. In November 2013, the Commission publishing such a communication to rebuild trust in transatlantic data flows. The US should commit to making use of agreements. The Commission wants to review the safe harbour agreement, which involves an adequacy declaration limited to US companies self-certifying that they comply with EU standards. Principles and practice have to be updated. The suspension of safe harbour is on the table if there is no solution to the Commission's 13 demands as specified in November 2013.

B. Big Data

Big data provides important findings serving the economy and public interest. It is characterised by its volume, velocity of data and algorithms. We should not fall prey to the impression often created that big data is commonly a matter of personal data. Much big data does not involve personal data at all, for example, weather information, natural sciences, technology and financial markets. Social media, loyalty cards and clinical trials are personal data in context of big data. The Commission has acknowledged that the fundamental right to data protection fully applies in a big data context.[3]

Some say key the principles of data protection is the purpose limitation cannot work with big data because the whole nature of big data is that you collect everything and then purpose it afterwards to maximise benefit to the public of using personal data for big data. These people say personal data is the oil or currency of the future. This comparison is flawed: unlike oil and money, personal data pertains to an identifiable human being, who has rights, who is a subject and not an object like money and oil. There is a need to maximise

[3] European Commission, Green paper on mobile health, Brussels, 10.4.2014, COM(2014) 219 final.

the benefits of big data, while ensuring human rights to privacy and data protection. Organisations and governments must ensure they adhere to the Article 8 of the EU Charter and EU data protection legislation. The proposed General Data Protection Regulation will improve the protection of personal data for big data analytics.

In conclusion, the credibility of EU law and the credibility of EU action are at stake. Two cases have confirmed the validity of a fundamental-rights approach in the internet age. The Commission accepts technology and, for example, law made by companies such as Google does not rule. Rather, the rule of law, democracy, and law made in parliaments and interpreted in courts do. New data protection regulation will provide a functioning internal market, which will provide growth to address challenges, such as unemployment.

V. Peter Hustinx: The role of data protection supervisors

Peter Hustinx aimed to address where we are in ensuring more effective data protection supervision and enforcement. It is not entirely appropriate to see data protection supervision only as a remedy; it goes beyond this. The existence of an independent supervisor has implicitly been a distinct feature of European data protection for a long time and this status has gradually confirmed over time with the constitutionalisation of independent supervision as a feature of data protection.

A. Roles of the three main key actors: data subject, data controller and supervisory authority

In short, the data subject is the beneficiary of protection and owner of rights, the data controller is responsible for delivering data protection and the supervisory authority is the guardian of data protection's well-functioning.

It is important to realise the controller should ensure data protection. The controller is the addressee of all legal expectations, and obligations and responsibilities. The data subject is the beneficiary of that protection. As the term 'subject' suggests, the data subject as a subject of rights. That said, rights are not very valuable if they're not delivered in practice. Some think Data Protection Authorities (hereafter: DPAs) deliver data protection, however the focus is on the controller. DPAs play a crucial role, but are not the only actors and not even the main actors ensuring data protection. Instead, DPAs are the guardians of well-functioning data protection. If everything goes well, they do not need to be involved. Data protection in the EU is a system based on complaint-driven supervision, which leads to long lines of complaints to deal with. DPAs are consumed by cases and are not sufficiently proactive to deal with the big systemic problems. There is a need to empower DPAs to be act more *ex ante* than *ex post*.

VI. Jean-Paul Jacqué: A growing role for the Charter of Fundamental Rights in the field of data protection?

Jean-Paul Jacqué, one of the fathers of the EU Charter on Fundamental Rights, looked at the growing role of the EU Charter in the data protection field. Before the EU Charter, there was no specific provision on data protection in EU treaties. Data protection was constructed in market terms to allow free circulation and free delivery of services; it required harmonisation of data protection rules. This does not mean there were no issues of fundamental rights. Prior to the EU Charter, institutions protected data pursuant to general legal principles common to Member State jurisdiction and the European Convention on Human Rights' provisions on private and family life. When texts change, however, reality changes, which is noticeable now in the EU.

VII. Concluding Remarks on Data Protection in the EU: From an Economic Necessity to a Fundamental Right

ERA's conference on safeguarding the right to data protection of the EU exemplified the increasing characterisation of data protection as a fundamental right. It also showed how, especially in Europe, there is strong sentiment that citizens should be protected by, for example, the EU, from having their right to data protection violated. The conference highlighted how data protection, originally constructed as an economic necessity, is increasingly referred to as a human and fundamental right.

A. Data Protection as an Economic Necessity

Data protection has been characterised relatively recently as a human right, indeed, data protection laws are a comparatively new phenomenon. The German state Hessen enacted the first data protection laws in 1970, with various States following suit throughout the 1980s. Today, about 70 States have data protection laws.

The first international instrument regulating data protection, the Organisation for Economic Cooperation and Development guidelines (1980), facilitated global data flows for economic, not human rights, purposes. Another early data protection instrument, the Council of Europe Convention 108, focused more on protecting human rights, especially the right to privacy.[4] In the EU, before the entry into force of the EU Charter on Fundamental Rights, there existed no specific treaty provisions on data protection. It was originally constructed in market terms to allow free circulation and free delivery of services.

B. Data Protection as a Human Right

Data protection's expansion from simply being an economic necessity does not *per se* imply data protection as a human right was negligible in the EU prior to the Charter. The right was protected by the abovementioned Convention 108, various institutions pursuant to general legal principles common to Member State jurisdictions and the ECHR's provision on protecting the right to privacy. In the EU, however, the concept of data protection noticeably evolved from being merely an economic concept to a human right. With the increased ubiquity of technology facilitating data processing, and the resultant rise in personal data, it is likely that the right to privacy needed to expand and morph to include a right to data protection, too. As a human right, data protection is subjective and not an absolute right. It provides direct protection from the State and indirect protection for individuals from other individuals.

C. Data Protection as a Fundamental Right

In the EU, data protection *per se* has only recently been characterised as a fundamental right. In 1999, Working Party 29 recommended that the European Commission, the European Parliament and the Council of the European Union include a right to data protection in the then recently-proposed EU charter on fundamental rights.[5] The Working Party asserted that including a right to data protection was important, *inter alia*, to signify the right's increasing importance in the information society.[6] As a consequence of the Working Party's recommendation, the Charter recognised the right to data protection as a new fundamental right.[7]

The mere fact that ERA hosted a conference called 'safeguarding the fundamental right to data protection' confirms data protection's increasing characterisation as a fundamental right. It will be fascinating to see how the conception of data protection in the EU will grow and transform in the future.

Author Information

Mistale Taylor is a PhD candidate at Utrecht University, focusing on questions of data protection and extraterritorial jurisdiction. She is also a Senior Research Associate at the Public International Law & Policy Group (PILPG) and External Affairs Editor of the *Utrecht Journal of International and European Law*.

[4] Hondius, F. W., 'A Decade of International Data Protection', *Netherlands International Law Review*, Vol. 30, 1983, p. 106; OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980); CoE, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg (Convention 108), 28.I.1981.

[5] Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, 'Recommendation 4/99 on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights', 5143 /99/EN WP 26, 7 September 1999, *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp26_en.pdf, p. 2.

[6] Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, 'Recommendation 4/99 on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights', 5143 /99/EN WP 26, 7 September 1999, *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp26_en.pdf, p. 2.

[7] http://ec.europa.eu/justice/fundamental-rights/files/networkcommentaryfinal_en.pdf.

How to cite this article: Mistale Taylor, '"Safeguarding the Right to Data Protection in the EU", 30th and 31st October 2014, Paris, France' (2015) 31(80) Utrecht Journal of International and European Law 145, DOI: http://dx.doi.org/10.5334/ujiel.cw

Published: 27 February 2015

]u[*Utrecht Journal of International and European Law* is a peer-reviewed open access journal published by Ubiquity Press.

OPEN ACCESS