UKAEL Annual Lecture

King's College, London 19 January 2023

Christopher Vajda KC

Data Protection: Made in Europe and Exported Globally

I am both delighted and honoured to be giving this year's UKAEL annual lecture.[1] The UKAEL is an association with which I have a long personal association going back some 40 years ago when I joined a young barrister. Shortly before the London FIDE conference in 2002 I was asked by Lord Slynn, the then President, to become the Treasurer. My task was to be raise enough funds in order to host the conference. I'm glad to say that we were so successful that after the conference we had enough money for the Committee to honour Lord Slynn with a dinner to match his exacting gastronomic standards. In deciding on the topic of my talk, I think certainly among the most novel, and interesting cases that I sat on as a judge at the Court of Justice of the European Union ("CJEU") were those on data protection. Hence most of those cases went to the Grand Chamber and invariably prompted large numbers of Member States to intervene. Nothing has changed much in that respect since I left the Court. Virtually all the cases that I will mention are Grand Chamber cases. Of course, such cases are not the unique preserve of the CJEU as a rich jurisprudence has developed not only at the European Court of Human Rights in Strasbourg but also in the national courts within Europe. The increasing number of such cases is of course readily explained by the fact that most of us today lead a large part of our life online and generate a huge amount of communications data which is capable of revealing an enormous amount about our lives. Hence rules have developed as to how, if at all, that data should be accessible to third parties, in particular various organs of the State.

There is no way that I could attempt to give a comprehensive lecture on this vast subject tonight so I will limit myself to looking at the origins of data protection in Europe, the threshold concepts of personal data and processing before looking at the legality of data retention under EU and ECHR law and finishing by looking at the international dimension.

[1] Judge at the Court of Justice of the European Union (2012-2020). All opinions expressed here all personal. I would like to record my thanks to Christina Thompson, a law student at King's College, London who undertook much of the research for this talk.

I The Origins of Data Protection in Europe

As long ago as 1890 in a celebrated article in the Harvard Law review[2] Louis Brandeis and Samuel Warren noted the potential for "recent inventions and business methods" to undermine the autonomy of individuals and made the case for legal protection not just to privacy in its traditional sense but what they called "the more general right of the individual to be left alone". Although they were thinking of then recent inventions such as the camera their concern applies even more forcefully to the era in which we now live where there is a vast amount of personal data about our lives, habits and behaviour which is stored in databases that today are largely electronic. It took, however, a very long time for those concerns to be translated into legislative acts.

Within Europe, Sweden was the first country to adopt a specific national data protection law in 1973. The legislation was prompted by the specific social and demographic conditions that existed in Sweden at the time.[3] Traditionally, extensive registers on individuals had been kept by public authorities. According to Freese in an article entitled the 'Future of Data Protection',[4] a 'well-brought-up, well-behaved, unmarried adult'[5] was likely to appear in around 100 different registers, while upon marriage that number would apparently double. What we do not know is whether that had any impact on the popularity of marriage in Sweden. The use of computers in public administration also began earlier in Sweden than in other European countries and concerns about the storage of electronic data came to the surface during the course of the population and housing census in 1970.[6]

That same year the German State of Hesse adopted what is considered the world's first data protection law. In 1977 Germany enacted its Federal Data Protection Act. The origins of German legislation can be traced to a concern for the impact that data processing would have on human rights. It was also a population census issue that led the German Constitutional Court in the *Population Consensus Case* of 1983[7] to recognize the right to 'informational self-determination' as the core of data protection in Germany. This concept has since become the

[2] The Right to Privacy 4 Harvard LR 193.
[3] E Kosta, Consent in European Data Protection Law (BRILL 2013) 36.
[4] J Freese, "The future of data protection" in Embassy of Sweden and Nether lands Central Bureau of Statistics (ed) Proceedings of the seminar on openness and protection of privacy in the information society (Voorburg, Netherlands 1987), p. 108.
[5] Kosta, fn.2, p 37.
[6] *Ibid*.
[7] BVerfGE 65, 1-71.

'constitutional root' of data protection in Germany and is itself rooted in the general personality right as derived from the fundamental German value of human dignity enshrined in Articles 1(1) and 2(1) of the Basic Law.[8] Germany can lay claim to be the origin place of many data protection terms and of the notion of "data protection" (*Datenschutz*) itself.

France first legislated for data protection in 1978 in the Law n° 78-17 of 6 January 1978 relative à l'informatique, aux fichiers et aux libertés, the so-called law "Informatique et Libertés". This reference to liberty also appears in the name of the French data controller, *La Commission Nationale de l'Informatique et des Libertés* (CNIL), a body that I will mention later in this lecture. The use of the word "liberty" indicates that data protection in France is seen as a development of the concept of individual liberty, dear to French values, which is enshrined in Article 2 of the Declaration of Human and Civic Rights of 1789.[9]

In the United Kingdom the debate on privacy and data protection had started already in the 1960s. Indeed, it was the second European country after Sweden[10] to set up a government commission to investigate whether there was a need for data protection legislation, albeit the first legislation arrived only in 1984 in the form of the Data Protection Act. This was replaced by the Data Protection Act 1998 which in turn was superseded by the Data Protection Act 2018. The 2018 Act gives effect to and supplements the EU General Data Protection Regulation ("GDPR").

At the pan European level, the European Convention on Human Rights ("ECHR"), which dates from 1950, provides protection for an individual's privacy in Article 8 but makes no reference to the data protection. In 1976 the Council of Europe established an intergovernmental Committee of Experts on Data Protection, tasked with drafting a Data Protection Convention for the new technological age. In 1981 the Council of Europe enacted Convention No 108, known as the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data ("the Data Protection Convention"), which came into force in 1985. The Data Protection Convention includes the principles which have become fundamental

[8] Article 1 [Human dignity – Human rights – Legally binding force of basic rights] (1) provides "Human dignity shall be inviolable. To respect and protect it shall be the duty of all state authority." Article 2 [Personal freedoms] (1) provides "Every person shall have the right to free development of his personality insofar as he does not violate the rights of others."

[9] "The aim of every political association is the preservation of the natural and imprescriptible rights of Man. These rights are Liberty, Property, Safety and Resistance to Oppression."

[10] Footnote 3, p 54.

in data protection law across Europe: the need to obtain and process data fairly and lawfully, to ensure that it is accurate and up to date, limiting its storage to specific purposes and time periods, and delineation of certain types of 'sensitive data'. All members of the Council of Europe have ratified the Convention as indeed have some third states such as Argentina, Mexico, Morocco, Tunisia, and Uruguay.

At the EU level the first legislative proposal only emerged in 1990 when the Commission proposed a Data Protection Directive.[11] In the absence of any reference to data protection in the Treaties this measure was based on the need to promote the efficiency of the internal market and the 'free flow of personal data between the Member States' (art 1(2)). It was adopted in 1995 as Directive 95/46/EC ("the Data Protection Directive or DPD"). In 1997 a limited reference to data protection was introduced into the EC Treaty by the Treaty of Amsterdam. Article 286 EC provided that Community acts on the protection of individuals with regard to the processing of personal data should also apply to EU institutions and bodies and it established an independent supervisory body to monitor this. In 2009 much more substantive changes were made by the Lisbon Treaty, known as the TFEU. Article 16 TFEU introduced an explicit legal basis for the enactment of data protection legislation meaning that it would no longer be necessary to rely solely on the internal market as the legal base for data protection. Additionally, the TFEU gave the EU Charter of Fundamental Rights ("the Charter"), which had been adopted in 2000, the same legal status as the EU Treaties. The Charter, as a more modern instrument compared to the ECHR, provides for a specific right to the protection all personal data in its Article 8, in addition to a right to privacy in Article 7. Article 52(1) permits a limitation of rights where such limitation is provided for by law, respects the essence of those rights and freedoms, meets a public interest objective and complies with the principle of proportionality. So far as the relationship with the ECHR is concerned, Article 52(3) provides it is to be a floor not a ceiling. The DPD has now been replaced by the GDPR[12] which has as its legal base Article 16 TFEU thus signalling that its character is no longer an internal market one.

II Threshold issues: the concept of personal data and data processing

[11] See European Commission, 'Communication on the Protection of Individuals in Relation to the Processing of Personal Data in the Community and Information Security' COM (1990) 314 final.
[12] Reg. 2016/679.

In most legal systems for data to be protected it must generally be personal and processed.[13]

Personal data is defined in the GDPR as 'any information relating to an identified or identifiable natural person' ('data subject').[14] An 'identifiable natural person' is 'one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.[15] A more concise definition to similar effect is to be found in Article 2(a) of the Data Protection Convention which defines 'personal data' as 'any information relating to an *identified or identifiable* individual' (emphasis added). In *Breyer*[16] the CJEU had to determine whether the registering by an online service provider of a dynamic IP address together with the date and time when a website was accessed constituted personal data. Unlike a static IP address, a dynamic IP address changes each time there is a new connection to the Internet and so it does not, by itself, enable a link to be established between a given computer and a connection to the Internet so as to enable one to identify the person who has made the connection. However, the online service provider does have additional information which, if combined with the IP address, would make it possible to identify the user. Not surprisingly the Court found this constituted personal data on the basis that there was no requirement that all the information necessary to identify an individual needs to be in the hands of one person.

Article 4(2) of the GDPR defines 'processing' as any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. It is a broad definition which aims at regulating all or most stages of the data processing cycle.[17] Like the definition

[13] However, data is processed in the course of a purely personal or household activity is excluded from the GDPR by Art. 2(2)(c).
[14] Art 4(1).
[15] Ibid.
[16] C-582/14 EU:C:2016:779.
[17] See also *Big Brother Watch v UK*, European Court of Human Rights, judgment of 25 May 2021 App. Nos. 58170/13, 62322/14, 24960/15, Grand Chamber Judgment, http://hudoc.echr.coe.int/eng?i=001-210077 at [325]: "there can be various stages of processing such as the initial interception and retention of data, the application of specific selectors to the data, the examination of the data and the subsequent retention and use of the data, including sharing it with third parties".

of personal data, this is a threshold concept for the application of the GDPR and thus is interpreted broadly.

A vivid illustration of this is provided by *Google Spain*[18] which is remembered as the right to be forgotten case. Senor González objected to the fact that when a Google search was done on his name, the search resulted in a link to an unflattering newspaper article published some 12 years earlier. The first question was *where* did Google carry out the processing of that article. Google Spain carried on no activity directly linked to the indexing or storage of data contained on third party websites. Rather that was all done by Google Inc in the United States. Nevertheless, the CJEU concluded that Google Spain engaged in processing in Spain because of the inextricable link between the processing carried out by Google Inc in the United States and the selling of advertising services by Google Spain which served to make the service offered by Google's US search engine in Spain profitable. The CJEU justified its broad interpretation of the term "processing" as being necessary to prevent circumvention of the protection granted by the DRD. This is a striking example of where the CJEU adopts a teleological interpretation that is not readily apparent from the strict wording of the text.

Another important point emerges from this case. The complaint against Google was that it had created a link to press articles that were already in the public domain. This illustrates that right to protect one's personal data is wider than the right to privacy. Even publicly available material falls within the ambit of data protection.

III Substantive Protection of Personal Data

That brings me to the substantive protection of personal data. Article 5 of the GDPR lays down the key principles providing the basis for the protection of personal data: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability. Those principles in turn give rise to a number of rights for data subjects but those rights are in turn subject to ten broad categories of restrictions. Among those restrictions one finds national security, defense, public security, the prevention, investigation, detection or prosecution of criminal offences and the protection of the data subject or the rights and freedoms of others. Many of these principles and restrictions were first

[18] C-131/12 EU:C:2014:317.

set out in the Data Protection Convention. Notwithstanding that the GDPR is an extremely detailed piece of legislation running almost to 100 Articles, its provisions are open textured which leaves enormous scope for interpretation by the CJEU aided by the even more broad language of Articles 7 and 8 of the Charter. Thus, it is not surprising that many of the important developments in EU data protection law have come from the Court in Luxembourg rather than the legislator in Brussels.

The major issue on substantive protection is often whether the data processing is justified by one of the categories of restrictions that I have referred to. There is generally no issue that the restriction pursues a legitimate aim (for example national security or the prevention or detection of crime) and the question of whether the measure is prescribed by law is by now reasonably settled. The contentious issue is normally whether the restriction meets the proportionality test, and I will focus on that. There is now a broad consensus, reflected in the jurisprudence of the two European courts, Luxembourg and Strasbourg, and national courts, that a crucial element of the proportionality test requires safeguards to be available where data is subsequently available for use or used by the state. By way of broad generalization this requires independent safeguards, either in the form of a court or an independent administrative authority, to oversee any use of the data, limits on the use of such data and on the period of time for which such data can be retained, and rights of recourse by the data subject. As the German Constitutional Court put it graphically there must be, like a double door, controls for both the transfer of data by telecommunications providers and for access to such data by public authorities.[19] Where, however, there is less consensus is whether such double door controls would permit the State to require generalized transmission or retention of particular types of data in the first place. In 2010 the German Constitutional Court held that a requirement on telecommunication providers to retain all traffic data for a period of six months was not, in principle, incompatible with Article 10 of the Basic Law.[20] However the CJEU in Luxembourg has taken a different view.

The Luxembourg Court

[19] Order of 27 May 2020 1 BvR 1873/13, 1 BvR 2618/13 /Subscriber data II).
[20] First Senate 1BvR 256, 263, 586/08.

In *Digital Rights Ireland*[21] the CJEU annulled, on proportionality grounds, the same EU Data Retention Directive[22] that had been considered by German Constitutional Court some four years earlier in 2010. The retention obligation on providers of publicly available electronic communication services was to retain all traffic and location data for a period between six months and two years in order to ensure that such data was available for the purpose of the investigation, detection, prosecution of *serious* crime as defined by each Member State in its national law. The CJEU held that such traffic and location data, even in the absence of the retention of the content of such communications, would enable very precise conclusions to be drawn concerning the private lives of persons whose data had been retained. Access by public authorities to that data constituted a further interference which the CJEU considered to be "particularly serious". There were three reasons why the proportionality test was not satisfied. First, the retention obligation covered all persons and all traffic data without any differentiation limitation or exception being made in the light of the objective of fighting against serious crime. Secondly, the Directive did not contain substantive and procedural safeguards relating to the access by the competent national authorities to the data and their subsequent use. Thirdly the minimum length of retention, namely six months, did not distinguish between the categories of data on the basis of their possible usefulness for the purpose of the objective pursued or according to the person's concerned.

Two years later in *Tele 2* and *Watson*[23] the CJEU applied the same approach to national legislation providing for the retention of traffic and location data for the purpose of fighting all crime, not just serious crime. Such general retention was impermissible. Double door safeguards did not change the position. The distinction drawn by the CJEU in *Tele 2* in its proportionality analysis between crime and serious crime prompted a subsequent reference in *Ministerio Fiscal*[24]. In that case a wallet and mobile phone had been stolen and the police wanted to have access to data identifying the users of the telephone numbers activated with the stolen phones for a 12 day period prior to the theft. The national court asked whether the retention of such data was permitted by *Tele 2* given that the purpose of access was not in

[21] Joined Cases C-293/12 and C-594/12 EU:C:2014:238.
[22] Directive 2006/42/EC.
[23] Joined Cases C-203/15 and C-698/15 EU:C:2016:970. Incidentally one of the two applicants in *Watson* which was a reference from the English Court of Appeal, was David Davis who, at the time of bringing the challenge that the UK legislation was contrary to EU law, was an MP. However, very shortly before the Advocate General was due to deliver his Opinion David Davis was appointed Secretary of State at the Department for Exiting the EU and he withdrew from the case.
[24] EU:C:2018:788.

relation to *serious* crime. The CJEU said this was permitted. It did so by looking at the data to be accessed, namely the names and addresses of the owner of the SIM cards. It considered that such data involved a lesser interference with fundamental rights then traffic and location data and so the interference was not sufficiently serious to limit access to a case of serious crime. The point of distinction between this case and *Tele 2* was therefore the type and amount of data in issue which was revealed less about the personal life of a data subject than the traffic and location data considered in *Tele 2*.

The next case *La Quadrature*[25] (October 2020), a reference from the French *Conseil d'Etat*, concerned the lawfulness of retention both of traffic and location data and other data for a variety of purposes including national security and fighting various types of crime. The CJEU accepted that the monitoring and retention of all traffic and location data for the purpose of safeguarding national security in a situation where there is a serious threat to national security satisfy the proportionality test provided that in effect the double door and other safeguards were in place.

By contrast, it confirmed the approach that it had taken in *Tele 2* that the general monitoring and retention of data for the purpose of combatting serious crime and to prevent serious threats to public security, was not permitted. Such retention was only permitted provided that it was "targeted" with respect to the categories of data to be retained, that is to say the retention had to be limited to data that is likely to reveal a link with serious criminal offences, to contribute to combating serious crime or to preventing a risk to public security. The targeting could be either in respect of a person – a person with a criminal history – or in respect of a geographical area, for example one with a high crime rate or a transport hub. By contrast, applying the same approach as in *Ministerio Fiscal* of looking at the type of data, the CJEU held that the general monitoring and retention of IP addresses and data relating to civil identity of users of electronic communication systems for the purposes of preventing, investigating, detecting and prosecuting criminal offences and safeguarding public security was permitted. It also permitted the expedited retention (the so-called quick freeze) of traffic and location data for the purpose of combating serious crime.

[25] Joined Cases C-511/18, C-512/18 and C-520/18 EU:C:2020:791.

When the *Conseil d'Etat* gave its judgment in April 2021[26] following the CJEU's judgment it found, on the basis of evidence put before it, that the requirement for targeted retention laid by the CJEU in the cases of public security and serious crime would be ineffective. This was because it would not enable the law enforcement authorities to have access to the data of a person suspected of an offence who had not been previously identified as likely to commit such an act. It was equally critical of expedited retention pointing out that the effectiveness of such a procedure depended on the data having actually been retained in the first place. To address these deficiencies the *Conseil d'Etat* felt able to interpret the CJEU's judgment to the effect that the law enforcement authorities could use the expedited retention procedure to access data that had been retained for *national security purposes* for the different purpose of investigating *serious crime and threats to public order.*

The *Conseil d'Etat* has not, however, had the last word on this as there have three further references to the CJEU all of which went to the Grand Chamber. The first two raised the question of whether an individual can seek to quash a criminal conviction on the ground that the national law permitting the use of traffic and location data by the prosecution did not meet the CJEU's test for the lawful retention of data. In *Prokuratuur/HK*[27] an individual sought to challenge her conviction in Estonia for theft and robbery. The CJEU considered that retention of this data enabled one to draw precise information on the private life of a user of electronic communications and it was therefore precluded by EU law. I assume that the conviction had to be quashed – though this of course is a matter for the national court.

The next case, *GD*[28], involved the use of electronic data in criminal proceedings leading to a conviction for murder. The Irish Supreme Court, which made the reference in March 2020 some 6 months before *La quadrature* was decided by the CJEU, considered that, and I quote from the judgment, "*only the general and indiscriminate retention of traffic and location data allows serious crime to be combated effectively, which the targeted and expedited retention (quick freeze) of data does not make possible*." These are precisely the same evidential conclusions on targeted and quick freeze retention that the *Conseil d'Etat* reached in April 2021. Nevertheless, the CJEU was not for turning. It refused to modify the approach it had laid down in *La Quadrature*. Instead, the CJEU asserted that "*Effectiveness of criminal proceedings*

[26] Nos 393099, 394922, 397844, 397851, 424717, 424718, FR:CEASS:2021:393099.20210421.
[27] Case C-746/18 EU:C:2021:152.
[28] Case C-140/20 EU:C:2022:258.

generally depends not on a single means of investigation but on all means of investigation available to the competent national authorities".[29] Even if correct as a general statement, that does not answer the point as to the relative effectiveness of various methods of investigation. The CJEU went to state that the combination of permissible measures in *La Quadrature*, namely targeted and expedited retention together with data relating to the civil identity of users and IP addresses should be sufficient for an effective criminal investigation. It elaborated on this by, for example, explaining that geographic targeting could include places vulnerable to terrorist attacks such as transport hubs. It then went on to reject the argument of the Danish Government that the national authorities should be able to access for the purpose of fighting *serious crime*, data that had originally been retained in a general and indiscriminate way for the purposes of addressing a *serious threat to national security*. This was of course precisely the line of reasoning used by the *Conseil d'Etat* to address the concerns of France following the CJEU's judgment in *La Quadrature*. The rejection of this argument by the CJEU means that it does not accept the interpretation by the *Conseil d'Etat* of its judgment in *La Quadrature*. *GD* has now returned to Ireland and judgment is awaited as to whether GD's murder conviction will have to be quashed.

The last case that I will mention on this topic is *Spacenet,*[30] where the CJEU gave judgment in September 2022 on a reference from the Federal Administrative Court in Germany. This was a dispute between telecommunication providers who objected to German legislation requiring them to retain traffic and location data relating to their customers. You will recall that an earlier version of this legislation had been considered by the German Constitutional Court in 2010. The referring court pointed out that the ambit of data retained was less than in previous cases decided by the CJEU, the period of retention was short (four and ten weeks for location and traffic data respectively), and there were effective double doors. It also referred to the Strasbourg Court case law which had held that Article 8 of the ECHR did not preclude national provisions providing for the bulk interception of cross-border flows of data in view of the large number of threats that states faced from terrorists and organised crime. The German court did not accept the invitation from the CJEU to withdraw its reference in the light of the CJEU's subsequent judgment in *La Quadrature*. For its part the CJEU was unmoved by the points made by the German court. It reaffirmed its approach in *La Quadrature* (and *GD*). So far as the

[29] [69].
[30] Joined Cases C-793/19 and 794/19 EU:C:2022:702.

ECHR was concerned, the CJEU distinguished the cases referred to by the national court as concerning the bulk interception of data relating to international as opposed to national communications. But in any event the CJEU pointed out that Article 52(3) of the Charter did not preclude a high level of protection under EU than under ECHR.

What can one deduce from these cases? First, the CJEU has taken a position of high principle that there can be no general retention of data other than where there is a grave and present risk to national security. The CJEU has done so despite evidence put before it about the shortcomings of targeted and quick freeze retention. Secondly, the approach of the CJEU does not appear to have met with universal approval in the national courts which can be seen by the references made to the CJEU asking it to reconsider its case law. Indeed, as we have seen, its approach is different from that of the German Constitutional Court in 2010. While, of course, the CJEU is under no obligation to reconsider its previous case law, the CJEU has done so in the past when it has recognized, with the aid of a subsequent of a reference, that a previous judgment might require modification. I am thinking, for example, of the *Tarico/MAS* dialogue[31] where the CJEU was persuaded by the Italian Constitutional Court to modify its approach to the interpretation of the Charter. It has chosen not to do so here.

The Strasbourg court

As we have seen, the Strasbourg Court has also had to grapple with the lawfulness of bulk interception under Article 8 of the Convention. One of them was *Big Brother Watch*[32], a case that arose out of the Snowden revelations made in 2013 about the UK's bulk interception of cross-border communications by its intelligence services. The Court accepted that bulk interception and its transmission to States' intelligence services was permissible subject to certain safeguards. Indeed, it reiterated its previous case law that "bulk interception regimes did not *per se* fall outside the States' margin of appreciation." It added "*in view of the proliferation of threats that states currently face for networks of international actors, using the Internet both for communication and as a tool, and the existence of sophisticated technology which would enable these actors to avoid detection … the court considers that the decision to operate a bulk interception regime in order to identify threats to national security or against*

[31] C-105/14 *Tarico* EU:C:2015:555 and Case C-42/17 *MAS and MB* EU:C:2017:936.

[32] *Big Brother Watch and Others v. the United Kingdom*, App. Nos. 58170/13, 62322/14, 24960/15, Grand Chamber Judgment (Eur. Ct. Hum. Rts. May 25, 2021), http://hudoc.echr.coe.int/eng?i=001-210077.

essential national interests is one which continues to fall within this margin".[33] The approach of Strasbourg court is to lay down minimum safeguards for such regimes in order, inter alia, to avoid the scope for abuse. In effect a double door approach.

Of course, it is not surprising that the Strasbourg, which has to apply the ECHR in 46 different jurisdictions, will, in principle, give those States a greater latitude than the Luxembourg court which applies the Charter to 27 States who are part of a close economic and political Union. Nevertheless, even taking that into account, the approach of the Strasbourg Court appears to be more evidence based. Thus in *Big Brother Watch* the Strasbourg Court relied, *inter alia*, in on the evidence contained in the report drawn up by David Anderson QC, as he then was, at the time independent reviewer of terrorism legislation, who concluded that bulk interception was an essential capability and that although he and his team had considered alternatives to bulk interception, including targeted interception, they concluded that no alternative or indeed combination of alternatives would be sufficient to substitute for the bulk interception power. By contrast, you will recall that in *GD* the CJEU effectively did not accept the evidence on the need for bulk retention put forward by the referring court but took, it might be said, a rather *a priori* approach by simply observing that effectiveness of criminal proceedings generally depends not on a single means of investigation.

IV The International Dimension

I turn now finally to the international dimension. As we have seen with the interpretation given to the term "processing" in *Google Spain*, the territorial scope of data protection law is important. I will look at two aspects: first, whether the right to be forgotten can apply extraterritorially and then secondly, the mechanism whereby the EU regulates the flow of data between the EU and third countries, including the UK.

In another Google case, *Google LLC*[34] (September 2019) the French data controller ordered Google to remove the name of persons who wished to be forgotten not just from its French website but worldwide. This raised the question of the territorial scope of the GDPR. Given worldwide access to the web one can see why CNIL, the French data controller, sought an order

[33] *Ibid*. [340]
[34] C-507/17 EU:C:2019:772.

that had worldwide effects. However, the CJEU concluded that there was nothing in the text of the GDPR to suggest that it was intended to impose a de-referencing obligation on national versions of search engines outside the EU. Furthermore, there were two other important considerations in play. First, not all third countries permit what is now called de-referencing. That raises delicate questions of public international law as to whether it would be permissible for EU law to impose such an obligation in a third country. Secondly, given that the right to be forgotten is not an absolute right but one that must be balanced against other rights such as the freedom of expression how would it be possible for the CJEU to seek to balance those competing interests in third countries where the balance between those rights might be struck differently than within the EU. As the CJEU observed, even within the EU a de-referencing order does not necessarily apply across the EU as the right to freedom of expression, the right of the relevant individual and the interests of the public in accessing that information may vary from Member State to Member State.

I turn finally to the regulation of data flows between the EU and third countries. The GDPR and its predecessor require an authorisation from the European Commission for such flows which needs to examine whether that third country ensures an "*adequate level of protection*"[35] of transferred personal data. In 2000 the Commission had issued its so-called Safe Harbour decision whereby it found that the United States ensured an adequate level of protection for data transferred from the EU to the US. In *Schrems I*[36] the redoubtable Mr. Schrems, then barely out of university, challenged the transfer of his Facebook data from Ireland to the US on the ground that there was not an adequate protection against use of that data by US public authorities. The CJEU agreed with Mr. Schrems. It interpreted an adequate level of protection to mean "essentially equivalent"[37]. It found that the safe harbour scheme was only applicable to U.S. companies that chose to comply to it and the US public authorities were not subject to it. Furthermore, national security public interest and law enforcement requirements of the United States prevailed over any Safe Harbour rules that U.S. companies chose to adopt. It also objected to the generalised storage of all personal data of all the persons whose data was transferred from the EU without any limitation being made in the light of the objective being pursued and there being no possibility for an individual to pursue a legal remedy under Article

[35] Art. 45(1) of the GDPR.
[36] Case C-362/14 EU:C:2015:650.
[37] [73].

47 of the Charter in order to have access to his data or to obtain the rectification or deletion of the data. The Commission's decision was therefore declared invalid. The scope of this judgment is remarkable in analysing whether the US data protection regime is essentially equivalent to that of the EU regime right down to looking at whether the remedies in the US comply with Article 47 of the Charter.

The next adequacy decision by the Commission in the form of the EU-U.S. Privacy Shield fared no better. In *Schrems II*[38] (July 2020), the CJEU declared invalid this adequacy decision. Once again, the CJEU found that the requirements of US National Security public interest and law enforcement, if I may use this term, trumped the safeguards in the EU-U.S. Privacy Shield. And once again the CJEU examined in detail whether the various US regimes satisfied the EU proportionality test on retention of data by public authorities and Article 47 of the Charter and found them wanting.

As a result, the EU and the US returned to the negotiating table. Just before Christmas the Commission launched the process to adopt a new adequacy decision to address the concerns of the Court in *Schrems II.*[39] The major change is that President Biden has issued an Executive Order in October 2022 which imposes limitations and safeguards on access to data by U.S. intelligence agencies and establishes an independent impartial redress mechanism to handle and resolve complaints from Europeans concerning the collection of their data for national security purposes. Thus, the US has now sought to accommodate the concerns of the EU, even in an area as sensitive as national security, so as to ensure the free flow of data from the EU to the US. The draft adequacy decision is now open for consultation within the EU and it remains to be seen whether sufficient changes have been made to preclude yet another trip to Luxembourg by Mr Schrems.

These cases are a a striking example of what Anu Bradford refers to in her book "the Brussels Effect: how the European Union Rules the World", published in 2020.

Where does the UK, post Brexit, fit into all this? When the UK left the EU, it agreed a "bridging period" to apply to data transfers between the EEA and the UK during which such transfers

[38] C-311/18 EU:C:2020:559.
[39] https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7631

would not be treated as a transfer to a third country. On 28 June 2021 the EU adopted an adequacy decision. The UK has now joined some 12 other third country jurisdictions including Japan, Korea, and Switzerland in having an adequacy decision. Despite some concerns expressed in some EU quarters, the UK adequacy decision is not at all surprising given that the UK has incorporated the GDPR into UK law and the existence of all the provisions on retained EU law. To put this into perspective, the UK and EU regimes are much more aligned than the US and EU regimes, even following President Biden's Executive Order. However, the Commission has indicated that it will review the decision if there is future divergence from EU standards and the UK adequacy decision is time limited.

On 22 September 2022 the so-called Brexit Freedoms Bill[40] was introduced into Parliament. Its stated purpose is to '*provide the Government with all the required provisions that allow for the amendment of retained EU law and remove the special features it has in the UK legal system'*. A couple of months earlier in July 2022 the Government laid the Data Protection and Digital Information Bill[41] before Parliament. The Bill forms part of the UK's National Data Strategy which aims to demonstrate post-Brexit opportunities "*for unlocking the value of data*" while at the same time seeking to retain the UK's adequacy decision. How this will be done remains to be seen. For example, the Bill envisages a similar regime to that under the GDPR for the transfer of data from the UK to third countries where the standard of the third country is not "*materially lower*" rather than "*essentially equivalent*". However, there is plainly room for tension with the EU if the UK approves the transfer of data to a third country that has not received an EU adequacy decision.

One can therefore see that the UK is taking a radically different approach to alignment with EU laws on data protection than it is in other areas of EU law where it is promoting regulatory divergence. Why the UK is treating the flow of data between the UK and EU differently from the flow of other services and goods between the UK and the EU is perhaps a topic for another UKAEL event. Thank you very much.

[40] The Retained EU law (Revocation and Reform) Bill, https://bills.parliament.uk/bills/3340.
[41] https://bills.parliament.uk/bills/3322.