Andrea Caligiuri (ed.), *Legal Technology Transformation. A Practical Assessment*
(Editoriale Scientifica 2020) **ISBN:** 978-88-9391-985-2

PROTECTION OF PERSONAL DATA AND HUMAN RIGHTS BETWEEN THE ECHR AND THE EU LEGAL ORDER

ALFREDO TERRASI

1. *Introduction*

Moving from an international law perspective, in an analysis on personal data protection across Europe the focus can be set on two different but deeply linked issues: human rights protection, on the one hand, and free circulation of such data, on the other.

One can easily see that the abovementioned issues could bring to a clash, in so far as they imply different interests at stake. In other words, dealing with data protection results in the individuation of a fair balance between free movement of data and protection of individual privacy.

As a consequence, such a balance has to be settled keeping in consideration the relationship between the right to private life and the right to data protection (if it can be drawn as autonomous) or between privacy and data protection rules.

With the present paper, in fact, I will try to enlighten the differences among privacy and data protection, having regard to the case-law of the Court of Justice of the European Union (hereafter "CJEU" or "Court of Luxembourg") and the case-law of the European Court of Human Rights (hereafter "ECtHR" or "Court of Strasbourg"), taking into account the scope of the relevant norms, within the proper reference system. Consequently, the path I will follow is twofold: the EU provisions on data protection and their implementation, on the one hand, and the Council of Europe legal context for data protection, on the other.

After a brief analysis of the two above mentioned regulatory systems and the way they are interpreted by the competent Courts, I will try to draw up some brief conclusive remarks.

2. *Council of Europe and Data Protection*

Human rights treaties, both on universal and regional level, historically do not deal with the issue of data protection as such. Nor it does the European Convention of Human Rights (hereafter "ECHR" or "Strasbourg Convention"). The main reason of this lack can be found in the time of the drafting. The concept of personal data, in fact, assumed importance when the first personal computers were built.

In other words, the central role of data protection is strictly connected to the evolution of the so-called information technology and, as a consequence, since the end of seventies the Council of Europe (hereafter "CoE") has undertaken the drafting of

several instruments, binding or not, which deal with the use that public authorities can make of information pertaining to individuals.

Whilst Art. 8 ECHR, establishing the right to private and family life, makes an express reference to domicile and correspondence, nothing is provided on personal information (such a lack, as we will see afterwards, significantly influences the ECtHR case-law). In order to fill the abovementioned gap, in 1981 the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention on data protection) was opened to signature.[1]

Such a Convention is the cornerstone of data protection principles across Europe. It was, in fact, used by the European Commission as a starting point for the drafting of EU norms.

It's worth noting that the Convention on data protection has been complemented in 2001 by a protocol,[2] providing for obligations regarding supervisory authorities and transborder data flows and updated, in 2018, by an amending protocol.[3] These protocols were adopted in order to give an effective regulation to personal data use, taking in account the technological innovation.

In addition to the abovementioned conventional instruments, the CoE Committee of Ministers drafted several recommendations, dealing with very specific facets of personal information protection. As regards information technology issues, such as artificial intelligence or facial recognition, the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data adopted specific guidelines.[4] Both recommendations and guidelines can be used as an interpretation aid in the implementation of the Convention on data protection.

2.1. *Data Protection before the ECtHR*

In the present paper it will not be possible to conduct a comprehensive analysis of the ECtHR case-law on personal information and their elaboration by public authorities. Such a premise, moreover, implies a relevant limit to data protection standards, as drawn by the Strasbourg Court, if one considers that obligations stemming from Art. 8 are essentially negative and thus usually impose *non facere* duties among

[1] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, signed in Strasbourg on 28 January 1981, European Treaty Series No. 108, entered into force on 1st October 1985.

[2] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, signed in Strasbourg on 8 November 2001, European Treaty Series No. 181, entered into force on 1st July 2004.

[3] With the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, signed in Strasbourg on 10th October 2018, European Treaty Series No. 223), not yet entered into force, the CoE has brought up to date the Convention on data protection. The substantive principles on data protection laid down in such a Convention were not repealed. On the contrary these principles are now targeted to regulate the use of personal information in the digital era, through the express recognition of a right to personal autonomy and the right to control one's personal data (see, on the point, the Explanatory Report to the Amending Protocol, para. 10).

[4] Guidelines on Artificial Intelligence and Data Protection adopted on 25 January 2019 by the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD (2019)01).

Member States. As a consequence, the use of personal data that private actors can make doesn't fall within the scope of the right to private life.

The ECtHR started dealing with data protection related issues at the end of seventies. In *Klass v. Germany*,[5] the Court established a particularly narrow proportionality test for secret surveillance measures (with the exception of measures adopted to face terrorism) but did not take into proper consideration the fact that such a surveillance was directed to acquire personal information about individuals.

Similarly, in the *Malone* case,[6] the Strasbourg Court, called upon to assess the consistency of wiretapping system, used by UK telecommunication authorities, with Art. 8 ECHR, concluded for the lack of legal basis for such a measure. As a consequence, the Court did not deal with the fact that the wiretapping outcome consisted in personal information on telecommunication network users.

Judge Pettiti, with a concurring opinion, considered that by wiretapping technique, "the authorities are enabled to deduce information that is not properly meant to be within their knowledge. It is known that, as far as data banks are concerned, *the processing of neutral data may be as revealing as the processing of sensitive data*" (emphasis added). Such a statement was based on the analysis of the CoE practice on data protection, with particular regard to the abovementioned Strasbourg Convention on personal data.

With the subsequent *Leander* case,[7] the concept of personal data finally steps into the ECtHR case-law. For the first time, in fact, the Court stated that both the storing and the release of personal information amount to an interference with the right to private life of the data subject. In other words, in the Court's view the fact that public authorities collect personal information about an individual, and adopt a detrimental decision based on such information, is enough to ascertain an interference in the right guaranteed by Art. 8 ECHR. However, it remains unclear whether the mere collection of personal an information about an individual by public authorities amounts to an interference with such a provision.

Kokott and Sobotta[8] argued that the crucial point is the scope of private life. In the Authors opinion, in fact, "Strasbourg requires an additional element of privacy in order for personal information to be included in the scope of private life". Such an additional element can be found, in strict connection with the circumstances of the case, in the systematic collection and storage of personal data (as in *Rotaru* case[9]) or in the fact that criminal conviction data are aged (as in *M. M.* case[10]). In *Amann* case,[11] on the contrary, the Strasbourg judges seem to consider that the storage of personal data amounts to an interference in the right to private life regardless of the concrete use of such data, without asking for further conditions. Some years later, the Grand Chamber stated, in

[5] ECtHR, *Klass and Others v. Germany*, Application No. 5029/71, judgment of 6 September 1978.
[6] ECtHR, *Malone v. UK*, Application No. 8691/79, judgment of 2 August 1984.
[7] ECtHR, *Leander v. Sweden*, Application No. 9248/81, judgment of 26 March 1987.
[8] J. KOKOTT and C. SOBOTTA, *The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR*, in *International Data Privacy Law*, 2013, p. 224.
[9] ECtHR [GC], *Rotaru v. Romania*, Application No. 28341/95, judgment of 4 May 2000.
[10] ECtHR, *M. M. v. UK*, Application No. 24029/07, judgment of 13 November 2012,
[11] ECtHR, *Amann v. Switzerland*, Application No. 27798/95, judgment of 16 February 2000.

Marper case,[12] that "in determining whether the personal information retained by the authorities involves any of the private-life aspects mentioned above, the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained" (para. 67).

If the Court used the Strasbourg Convention approach, it would state that any operation on personal information by public authorities amount to an interference with Art. 8 ECHR. Notwithstanding, following the case-by-case method, the Court did not clarify which factors can lead to classify on operation on personal data by national authorities as an interference within the meaning Art. 8 ECHR.

As a consequence, it is not clear whether an individual, whose data are elaborated by a state organ, can rely on the right to private life protection or not. Nor it is possible to infer from the ECtHR case-law on data protection, if Art. 8 ECHR calls on the Member States to guarantee to data subjects the right of access, rectification or erasure of personal information, elaborated by national authorities.

One could wonder whether the gap existing among right to privacy and right to data protection can be filled up or not. As already seen, it is not a theoretical question as such. On the contrary, the effectiveness of data protection can be affected by the abovementioned gap.

In recent years, the Strasbourg Court has moved towards a more data-oriented approach. In fact, the Convention on data protection, once mentioned without practical consequences, has become an important hermeneutic instrument when personal data issues are at stake. Whilst in the already cited *Leander* case the Court made no reference to such a Convention, since the *Rotaru* case, the Court seems to take into account, at least, some of the substantive principles enshrined in Art. 4 to Art. 8 of the Convention on data protection.

One could wonder whether the Court has competence on the application of the Convention on data protection or not. Pursuant to Art. 32 ECHR, in fact, "the jurisdiction of the Court shall extend to all matters concerning the interpretation and application of the Convention and the Protocols thereto". Such a provision should lead us to the conclusion that the ECtHR is not entitled to give effect to the Convention on data protection. Notwithstanding, the ECHR, as any international agreement, falls within the scope of the Vienna Convention on the Law of Treaties. As a consequence, the Court, when asked to implement the Convention, can legitimately make an interpretation consistent with Art. 31 of the abovementioned Vienna Convention.

It is worth noting that, in accordance with the abovesaid provision, treaties can be interpreted taking into account "any relevant rules of international law applicable in the relations between the parties" (Art. 31(3)(c)). If one considers that the State parties to the ECHR are parties to the Convention on data protection as well, it is unquestionable that the Strasbourg Court can rely on the latter (just like other treaties, concluded within the CoE framework) to solve hermeneutic questions related to the former.

The Court, as already pointed out, since *Rotaru* case has made use of the Convention on data protection, in two different ways: in order to confirm a decision based on other

[12] ECtHR [GC], *S. and Marper v. UK*, Applications Nos. 30562/04 and 30566/04, judgment of 4 December 2008.

provisions, on the one hand, and in order to conduct the necessity in a democratic society test, on the other. The former is not particularly relevant, since the concrete solution is based on ECHR norms; the latter, on the contrary, shows a significant change in the Court approach to data protection.

As far as ECHR apparently does not deal with personal information elaboration by public authorities, the use of specific normative parameters is crucial. The Court, in fact, in *Marper* case, implemented the substantive principles laid down in the Strasbourg Convention, embedding them in the relevant legal standard stemming from Art. 8 ECHR. In the abovementioned case, the Court was called upon to deal with the lawfulness of the storage of biometric data of non-convicted individuals after the termination of the criminal proceedings against the plaintiffs. The UK police, indeed, retained DNA profiles and fingerprints of Mr. Marper and Mr. S, even if the proceedings against them did not bring to a criminal conviction. The plaintiffs asked the police for the erasure of such biometric data and UK authorities rejected the requests.

The Strasbourg Court, once ascertained that the measures at stake were in accordance with the law and pursued a legitimate aim, dealt with the proportionality of biometric data retention, asserting that "the domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored" (para. 103). Noteworthy, the Court recalled Art. 5 of the Convention on data protection, using the same terminology of the abovementioned provision.

Moreover, in the assessment of the proportionality of the contested measures, the Court stated that the respondent State failed to strike a fair balance between the competing public and private interests, insofar as UK police could retained biometric data for an indefinite period. In *Marper*, conclusively, the Court took a substantive principle stemming from the Convention on data protection and used it to assess the necessity in a democratic society of the contested measures.

Notwithstanding, the Court kept a privacy-oriented approach, without taking into proper account the peculiarities of data protection. In other words, the data protection substantive principles violation did not absorb the proportionality assessment but were just one element in such an assessment.

Even the subsequent case-law on personal information shows the same theoretical approach. One can wonder whether the Court considers that privacy and data protection perfectly overlap or not. The scope of the right to private life is, obviously, much wider than the scope of data protection rules. But, unfortunately, the Court seems to leave outside the scope of Art. 8 some data protection issues. As a consequence, ECHR, up to now, does not guarantee effective legal standards of data protection, at least for the misuse of personal information by private entities, such as big data, commercial companies and telecommunication societies. Moreover, even when public authorities are involved, the marge of appreciation recognized under Art. 8 ECHR is broader than the exceptions to data protection principles.

If the ECHR were not able to guarantee an effective protection of personal information, it could depend on the fact that a right to data protection has never been drawn up by the Strasbourg Court, in the framework of the right to private life. An autonomous right to data protection, on the contrary, can be derived by the EU legal

system. As a consequence, it is worth verifying the effectivity of such a right, having regard, on the one hand, to the EU regulatory framework and, on the other hand, the case-law of the CJEU.

3. *Data protection in EU legal system*

European Union, since the nineties, issued a comprehensive piece of legislation on data protection and data free movement within the EU Member States (directive 95/46/CE,[13] hereafter "data protection directive"). Even if some of the substantive principles on data elaboration overlap with the corresponding principles laid down in the Convention on data protection, the rationale of the former is quite different form the rationale of the latter, insofar as the establishment of data protection rules is a prerequisite for the circulation of data across Europe.

It is worth noting that in the Charter of Fundamental Rights of the European Union (hereafter "Charter of Nice") a right to data protection has been clearly defined in Art. 8, whilst the right to private life is provided for in Art. 7. It is well known that the Charter of Nice has become a binding primary piece of legislation with the entry into force of the so-called Lisbon Treaty.

In the Praesidium explanations relating to the Charter,[14] an explicit reference was made to the data protection directive, as well as to Art. 286 of the EC Treaty (replaced by Art. 16 of Treaty on the Functioning of the European Union). Moreover, the Praesidium mentioned the Convention on data protection and Art. 8 ECHR as further basis for the drafting of Art. 8 of the Charter.

One can wonder whether such references can influence the implementation of the right to data protection in EU or not. It is, in fact, difficult to see how a EU secondary law can be used to interpret a EU primary provision.

One more element to take into account in this patchwork normative framework is, obviously, the entry into force, in 2018, of the General Regulation on Data Protection[15] (GDPR). Such an instrument, in fact, repeals the data protection directive. As a consequence, the GDPR could have an influence on the scope of Art. 8 of the Charter.

It has to be noted that Art. 8 of the Charter did not get a concrete judicial implementation before 2014, leaving unsolved several issues on the human rights standards stemming from it.

3.1. *Art. 8 of the Charter on Nice before the CJEU*

The Court of Luxembourg started dealing with data protection issues in 2003, with two decisions that shaped the scope of the data protection directive.[16] A step forward

[13] Directive 95/46/EC of the European Parliament and of the Council, of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[14] Explanations Relating to the Charter of Fundamental Rights of the European Union, in European Union Official Journal C 303/02 of 14th December 2007, p. 320-321.

[15] 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)

[16] CJEU, case C-465/00, *Österreichischer Rundfunk*, judgment of 20 May 2003, and case C-101/01, *Bodil Lindqvist*, judgment of 6 November 2003.

in drawing an autonomous right to data protection was done in 2014[17] and 2015.[18] The Court, in fact, finally relied on the Charter of Nice, in order to determine the legality of EU secondary legislation dealing with personal information elaboration.

In the first of the abovementioned decisions, the Court dealt with the consistency of the so-called data retention directive[19] with Articles 7 and 8 of the Charter. Noteworthy, the Court used the aforementioned provisions as the only relevant standard of review. More particularly, the Irish High Court delivered a request for preliminary ruling to the CJEU, in order to ascertain whether the directive at stake was legal or not. Such a piece of legislation, in fact, required the telecommunication companies and internet providers to retain a huge amount of data (as set forth in Art. 5 of the directive) concerning fixed network telephony, mobile telephony and internet access.

First of all, the Court dealt with the scope of Articles 7 and 8 if the Charter, affirming that the collection and storage of data by telephone and internet companies fell within such a scope. Whilst the relevance of the right to private life of individuals whose communication data were stored under the data retention directive was undisputed, it is worth noting that the Court conceded that both the storing of such data and the access of the competent national authorities to the data amounted to an interference in the right to data protection, as laid down in Art. 8 of the Charter.

The Luxembourg judges considered that the abovementioned interferences respected the essence[20] of the fundamental rights at stake (within the meaning of Art. 52(1) of the Charter). Such a conclusion is not convincing, at least as Art. 8 is concerned, if one considers that the directive required to communication companies to retain the data of any individual for a period between six months and two years and to transfer such data to national authorities upon request. As a matter of fact, we are dealing with a bulk storage of personal information, on the one hand, and with a violation of the purpose limitation principle, insofar as the data were collected by the companies in order to execute a contractual obligation and then transferred to national authorities for law enforcement aims, on the other.

The Court, in the end, decided to declare invalid the whole data retention directive, on the ground of the lack of proportionality (the strict necessity test) in terms of limitation of the right to data protection and the right to private life. In the Court view the directive "applies to all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives" and "it therefore entails an interference with the fundamental rights of practically the entire European population" (para. 56).

In other words, the CJEU declared the data retention directive invalid because of the excessively wide scope and because of the absence of substantive and procedural

[17] CJEU, joined cases C-293/12 and C-594/12, *Digital Rights Ireland*, judgment of 8 April 2014, and [GC] case C-131/12, *Google Spain SL*, judgment of 13 May 2014.

[18] CJEU [GC], case C-362/14, *Maximilian Schrems*, judgment of 6 October 2015.

[19] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

[20] As observed by Brkan (M. BRKAN, *The Essence of the Fundamental Right to Privacy and Data Protection: Finding the Way Through the Maze pf the CJEU's Constitutional Reasoning*, in *German Law Journal*, 2019, p. 868), the Court "acknowledges the independent value of the concept of essence by markedly verifying whether the essence of the fundamental rights has been interfered with".

conditions to file a complaint to national authorities. However, one point remains unclear: the relationship between Art. 7 and Art. 8. The legal reasoning on the point is that "the protection of personal data resulting from the explicit obligation laid down in Article 8(1) of the Charter is especially important for the right to respect for private life enshrined in Article 7 of the Charter" (para. 53). One could wonder whether the violation of Art. 8 entails the simultaneous violation of Art. 7 or not. If so, one should reach the conclusion that the right to data protection, in the EU legal order, is a specification of the right to private life rather than an autonomous fundamental right.

3.2. Google and Facebook saga

After Digital Rights Ireland decision, the Court dealt with two issues that involved big data (Facebook and Google) and became a kind of saga, with decisions in 2014-15 and then in 2019-20. I will try to briefly analyse such decisions, from the point of view of the interaction between Art. 7 and Art. 8.

In *Google Spain* case, the Court undertook an analysis on browsers responsibility for the content of third parties' webpages, from a data protection perspective. Spanish judges, in fact, addressed a request for preliminary ruling, asking the Court to ascertain whether search engines, pursuant to the data protection directive, could be considered as data processors.[21]

In the Court's view, Google could be considered, under Art. 2(d) of the data protection directive, as data controller. As a consequence, it could be held responsible of data protection rules violations.

Noteworthy, the Court argued that, in order to ascertain if data processing was legitimate, Art. 7(f), of the directive had to be interpreted in the light of Articles 7 and 8 of the Charter. Significantly, the Court expressly stated that "processing of personal data, such as that at issue in the main proceedings, carried out by the operator of a search engine is liable to affect significantly the fundamental rights to privacy and to the protection of personal data when the search by means of that engine is carried out on the basis of an individual's name" (para. 80). Being such an interference potentially serious, the search engines rights under data protection directive should not necessarily override internet users' interest. On the contrary, such a balance has to be struck, having regard to the nature of the information in question and its sensitivity for the data subject's private life.

Conclusively the Court affirmed that the directive at stake, interpreted in the light of Articles 7 and 8 of the Charter, recognizes the prevailing interest of the data subject over the economic interest of the operator of the search engine but also over the interest of the general public in having access to that information upon a search relating to the data subject's name.

In *Google Spain* the Court used the abovementioned Charter provision as a hermeneutic canon, whilst in Digital Rights Ireland they were considered as standard

[21] On the point, the Court stated that "in exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine 'collects' such data which it subsequently 'retrieves', 'records' and 'organises' within the framework of its indexing programmes, 'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of search results" (para. 28). Therefore, Luxembourg judges gave a broad interpretation of data protection directive' scope.

of review. In both cases, anyway, Articles 7 and 8 have been used simultaneously, without shaping a difference between their scopes.

The Court came back to speak out on search engines obligation to anonymize search results upon request of the data subject in 2019,[22] when required by French data protection authority for a preliminary ruling. Apparently, the Court did not rely on the Charter, in order to determine the extension of the de-referencing obligation for search engine operators, when required to do so by the data subject. On the contrary, Luxembourg judges based the decision on Art. 17 GDPR (dealing with the right to be forgotten), even if request for a preliminary ruling was issued by French authorities when the data protection directive was still applicable.

Quite surprisingly, the Court stated that the de-referencing obligation stemming from Art. 17 GDPR did not compel Google to erase any reference to the data subject asking for it from all the versions of the search engines. On the contrary, such a de-referencing is compulsory only on the versions of that search engine corresponding to all the Member States. If one considers that internet users can search the internet through search engines of third countries, the statement of the CJEU creates a lack of protection insofar as the right to be forgotten (within the meaning of Art. 17 GDPR) is substantially ineffective. As a consequence, such an interpretation of the abovementioned provision does not seem to be consistent with the right to data protection, as enshrined in Art. 8, at least as regards the right to rectification (which includes the right to erasure).

Moving from Google to Facebook, it is worth noting that the Court had to deal with a very difficult issue: the rules applicable to transborder data flows across the Atlantic Ocean. In effect, the case-law on transborder data flows is very complex, as far as law enforcement and commercial issues are involved.[23] The present analysis is focused on a particular case: how can private companies transfer data, collected in the EU (and which follow under the scope of data protection directive and GDPR), to the United States.

In 2015 the Court had to deal with the consistency of Facebook automatic data transfer from EU servers to US servers with the EU legal order. The legal basis for such a transfer was the so-called safe harbour (established by a European Commission decision on adequacy[24] of the level of data protection US legal order can afford to data). Insofar as US do not have a federal legislation on data protection, the EU Commission, laying on Art. 25(6), of data protection directive, established a kind of self-regulation

[22] CJEU [GC], case C-507/17, *Google LLC*, judgment of 24 September 2019.

[23] For a comprehensive analysis of the data flow among EU and US, see W. GREGORY VOSS, 'Cross-Border Data Flows, the GDPR, and Data Governance' (2020) Washington International Law Journal 485.

[24] Pursuant to Art. 25 of the data protection directive, EU Member State can authorize transborder data flows only if the recipient (third) State ensures "an adequate level of protection". Such an adequacy finding is usually made by the European Commission with a decision. With regard to the US legal order, the absence of common data protection rules within the Federation prevented the Commission from assessing the adequacy of US as such. Consequently, with decision 2000/520/EC, adopted on the basis of Art. 25(6) of the directive, the Commission established that "the Safe Harbour Privacy Principles, as set out in Annex I to this Decision, implemented in accordance with the guidance provided by the frequently asked issued by the US Department of Commerce on 21 July 2000 as set out in Annex II to this Decision are considered to ensure an adequate level of protection for personal data transferred from the Community to organisations established in the United States".

code that US companies had to sign in order to legitimately receive data collected in EU.

Such a system relied on declarations made by US companies, committing to respect the safe harbour data protection principles, under the control of the US Department of Commerce. Right to privacy and right to data protection of European citizens were very ineffective, if one considers that, *inter alia*, no redress was recognized by US legal order. Consequently, the CJEU, on the basis of a request for a preliminary ruling issued by Irish High Court, had to deal with the consistency of the safe harbour system with Articles 7 and 8 of the Charter.

The Court declared the Commission decision invalid, interpreting Art. 25(6) of the data protection directive in the light of the abovementioned fundamental rights. More precisely, according to the Court the ineffective protection of data, transferred from the European Union to the United States, had to be qualified as an interference with Article 7 and 8 of the Charter and such interference could be consistent with the Charter only in so far as it was strictly necessary. Moreover, in the Court's view, "legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception" (para. 93).

In the case at stake, Articles 7 and 8 of the Charter were considered as a unique interpretative yardstick and, just as in *Digital Rights Ireland*, the Court did not shape a distinction between right to private life scope and right to data protection scope.

After the safe harbour system was declared void, European and American authorities negotiated in order to adopt a new legal basis for transborder data flows between private entities. The negotiation led to the approval of the Privacy Shield.[25] Such a data transfer mechanism, however, was brought before the CJEU, which rendered the decision so-called *Schrems II*.[26]

It is a very recent and controversial decision, insofar as the Court was asked to forbid any data flow which involved companies on the two sides of the Atlantic Ocean. Once again, Facebook data transfers from Ireland to US were at stake, after a request for preliminary ruling filed by the Irish High Court.

The main difference between *Schrems I* and *Schrems* II is that the complaint was suited to the Irish High Court when GDPR was already in force. As a consequence, the Court took into account Art. 46 GDPR instead of Art. 25 of the data protection directive. However, the Privacy Shield was approved under the latter provision and it is not clear whether the *tempus regit actum* principle was deemed relevant or not.

Moving from a human rights' perspective, the Court dealt with the circumstance that commercial data on individuals, once transferred to US companies, could be in the availability of US law enforcement surveillance programs, since companies could be asked for data without specific rules.[27] According to the CJEU, in fact, the provision of

[25] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176).

[26] CJEU [GC], case C-311/18, *Maximilian Schrems v. Facebook Ireland LTD*, judgment of 16 July 2020.

[27] The Court observed, on the point, that "It is thus apparent that Section 702 of the FISA does not indicate any limitations on the power it confers to implement surveillance programmes for the purposes

the privacy shield dealing with that issue did not grant data subjects actionable rights before the courts against the US authorities.

Consequently, in the Court's view, the lack of limitations for US law enforcement authorities, when accessing personal data transferred pursuant to the Privacy Shield, was not consistent with Art. 45 GDPR, interpreted in the light of Articles 7 and 8 of the Charter, insofar as "the Privacy Shield Decision cannot ensure a level of protection essentially equivalent to that arising from the Charter, contrary to the requirement in Article 45(2)(a) of the GDPR that a finding of equivalence depends, inter alia, on whether data subjects whose personal data are being transferred to the third country in question have effective and enforceable rights" (para. 181).

From the brief analysis of the abovementioned CJEU decisions, it might be possible to infer that in the EU legal order data protection issues are deemed crucial. GDPR rules seem to be more privacy oriented than data protection directive ones; moreover, the Court makes reference to Articles 7 and 8 of the Charter quite often, in order to interpret data elaboration criteria in the light of fundamental rights issues.

4. *Conclusive remarks*

Data protection issues are gaining great importance both from a legal and a political point of view. I have tried to shape a kind of common thread with regard to the definition of legal data protection standards in the EU and in the CoE systems.

The norms on data elaboration differ, so as their rationale, in the two abovementioned frameworks. One could think that data protection is more effective within the Council of Europe context than in the EU legal order, insofar as the the CoE main focus is on human rights, whilst EU protects the four freedom of circulation as well as human rights.

Notwithstanding, from the analysis just carried out on ECtHR and CJEU case-law on data protection emerges a quite different result. The Strasbourg Court, in fact, manages data protection issues in the light of Art. 8 ECHR and, thus, privacy related matters seem to absorb them in a proportionality exam. The ECtHR case-law, in fact, shows the lack of awareness with regard to data protection rules, even when the Court has recourse to the data substantive principles stemming from the Convention on data protection.

On the contrary, the Luxembourg Court has acquired a relevant expertise on data protection rules. Obviously, it depends on the fact that EU legal order, since the nineties, have several norms, both on primary and secondary level, dealing with personal information elaboration. Moreover, the binding nature of the Charter of Nice has brought Art. 8 to become a cornerstone of the whole data protection framework. The Court, in fact, since 2014 has issued some decisions, dealing with either interpretation or validity of secondary norms on data protection, and the right to data protection, enshrined in Art. 8 of the Charter is always a hermeneutic parameter.

However, there is one thing that brings together Luxembourg and Strasbourg in dealing with data protection: neither the former nor the latter have shaped, up to now, a coherent definition of the individual right to data protection. And none of them

of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those programmes" (para. 180).

succeeded in, or even tried to, drawing up a distinction between right to private life scope and right to data protection scope. As a consequence, it remains unclear whether the latter can be implemented autonomously or an interference in the right to data protection always amount to an interference in the right to private life as well.