UNIO - *EU Law Journal*. Vol. 5, No. 1, January 2019, pp 4-15.

School of Law – University of Minho

The digital world and the new frontiers of the European courts case-law

José Luís da Cruz Vilaça*

ABSTRACT: Finding the right balance between achieving the full potential of the digital economy in terms of innovation and economic growth, on the one hand, and protecting the core values of our societies, including fundamental rights and the rule of law, on the other hand, has become a pressing issue for political and judicial authorities. Data generated by electronic communications is an important tool in the fight against organized crime and terrorism, whose effectiveness depends on the use of modern research techniques. However, the pursuance of that general interest objective must be balanced against the need to protect the fundamental rights to privacy and to personal data from the most serious interferences.

KEYWORDS: digital economy – Charter of Fundamental Rights of the European Union – rights to privacy and to the protection of personal data – complex economic appraisals – principle of proportionality.

* Former judge, President of Chamber of the Court of Justice of the European Union (CJEU). Former Advocate General and President of the Court of First Instance of the European Communities (now the General Court). Professor of EU law. Founding partner of Cruz Vilaça & Associados – Law firm.

I. Strategic options and the regulatory framework for digital markets[1]

Digital technologies, in particular the Internet, are transforming the world.

Indeed, advances in technology have not only drastically changed the way data are collected, processed, stored and used in social relations, but also entailed a new challenge to the European Union (hereinafter, "*the EU*") in particular its legislators and regulators.

It then comes as no surprise that the European Commission has made of the so-called "*Digital Single Market Strategy*", launched in May 2015,[2] one of its political priorities.[3]

As initially defined by the Commission, the Strategy covers 16 specific measures based on three key pillars.

The aim is, firstly, to improve consumer access to digital goods and services throughout Europe by adopting rules on consumer protection, unjustified geo-blocking,[4] copyright and the VAT regime, or by identifying the main competitive concerns in this sector.[5]

Secondly, the Strategy aims at creating appropriate conditions for the development of digital networks and innovative services by reviewing the rules on telecommunications and privacy in electronic communications, as well as by combating illegal content.

The focus is, thirdly, on the optimization of the growth potential of the digital economy by promoting the free movement of data, standardization and interoperability, as well as enhancing the digital skills of citizens with a view to boosting employability.

It must be said that the European Commission succeeded in completing the main thrust of its three pillars program in January 2017 and presented 35 legislative proposals and policy initiatives between May 2015 and January 2017.

A "*mid-term review*" of the Strategy was published in May 2017 in which the Commission identified three broad areas where it considers that more vigorous action is needed at Union level.

More precisely:[6]

1. To promote the accessibility, movement and storage of *non-personal data* in the European Union;[7]

2. To strengthen *cybersecurity* within the European Union;

---

[1] I thank my associate and former legal secretary at the CJEU Carla Abrantes Farinhas for her valuable contribution to the preparation of this paper.

[2] See Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "*A Digital Single Market Strategy for Europe*", COM (2015) 192 final, 6 May 2015. See also the Institutional Report by Piedade Costa de Oliveira for the Topic I, "*The Internal Market and the Digital Economy*" of the XXVIII FIDE Congress, Lisbon/Estoril, 23-26 May 2018, in special pp. 164-176.

[3] This is one of the 10 European Commission's policy priorities foreseen in its Program for Employment, Growth, Equity and Democratic Change.

[4] Geoblocking: when online consumers see their access to a website denied based on their location or are redirected to a local store with a different price.

[5] The Commission launched a sectoral inquiry into competition in e-commerce in May 2015 to identify possible concerns in this area resulting from the businesses' practices .

[6] See http://europa.eu/rapid/press-release_MEMO-17-1233_en.htm.

[7] Non-personal data are outside the scope of the General Regulation on Data Protection (GDPR), cited below.

3. To regulate the *commercial practices of online platforms* and to ensure the prompt and effective removal of illegal online content.

Among the milestones already achieved, the following are worthy of note:

- The end of roaming charges at the retail level, on June 15, 2017;[8]
- Cross-border portability of online content services since the beginning of 2018;[9]
- The application, since May 2018, of the General Data Protection Regulation (GDPR); [10]
- The adoption of a regulation aimed at ending the unjustified geographical blockade from December 2018;[11]
- The presentation in April 2018 of a proposal for a regulation on promoting fairness and transparency for business users of online intermediation services.[12]

As can be seen, this is a broad and profound legislative and regulatory activity in a field of decisive importance for strengthening the competitiveness of the European economy in the context of the global digital economy, designed to enable citizens and businesses in the EU to enjoy a set of opportunities created by digital technology, while respecting the fundamental rights of citizens.

II. The economic importance of the "*Big Data*" and the challenges and risks to the European economy, privacy and the individual rights of citizens

The value of the European data economy is estimated to be around €739 billion in 2020, with the completion of the Digital Single Market contributing €415 billion to the European economy, involving an additional growth of €250 billion over the current Commission's mandate, thus allowing hundreds of thousands of new jobs to be created.[13]

The long-term impact on GDP growth of the digital economy reform efforts already undertaken was estimated at more than 1%, with additional reform efforts leading to additional GDP growth of 2.1%, which compares with about 0.27% of GDP of benefits resulting from the current level of cross-border e-commerce.[14]

---

[8] See http://europa.eu/rapid/press-release_IP-17-3241_pt.htm.

[9] Regulation 2017/1128 of the European Parliament and of the Council of 14 June 2017 on cross-border portability of online content services in the internal market, OJ L 168, 30.6.2017, p. 1-11.

[10] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Regulation on Data Protection - RGPD), OJ L 119, 4.5.2016, p. 1-88. This regulation is not specifically addressed to the digital sector, but is generally applicable to activities subject to Union law, with the exception of Title V, Chapter 2, of the EU Treaty, relating to the common foreign and security policy.

[11] Regulation 2018/302 of the European Parliament and of the Council of 28 February 2018 aimed at preventing unjustified geographical blockade and other forms of discrimination based on nationality, place of residence or place of establishment of customers on the market amending Regulation No 2006/2004 and 2017/2394 and Directive 2009/22 - OJ L 60I, 2.3.2018, p. 1-15.

[12] See https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0238&from=EN.

[13] See Jean-Claude Juncker, "*Policy Guidelines for the Next European Commission - A New Beginning for Europe: My Program for Employment, Growth, Equity and Democratic Change*", July 15, 2014, available on: https://ec.europa.eu/commission/publications/president-junckers-political-guidelines_en.

[14] See Commission Staff Working Document, "*A Digital Single Market Strategy for Europe - Analysis and Evidence*", SWD (2015) 100 final, 6 May 2015.

Every second, around the world, through smart phones, computers, unmanned vehicles and other types of equipment, increasingly large amounts of data from multiple sources – commonly called "*Big Data*" – are being generated.

Finding the right balance between achieving the full potential of the digital economy in terms of innovation and economic growth on the one hand, and protecting the core values of our liberal and democratic societies, on the other hand, has become a pressing issue for the various political actors and, in their field of action, the courts. That is why the transformation of the digital economy creates major challenges for respect for the values on which the EU is founded – including democracy, fundamental rights and the rule of law.

Recent developments show that one of the most valuable assets in digital markets – the *data* – can be used to the detriment of the protection of privacy and family life, which are fundamental rights enshrined in Articles 7 and 8 of the Charter and Article 16 (2) TFEU, which must be respected both by the institutions and bodies of the Union and by the Member States when they are implementing Union law [Article 51 (1) of the Charter].

Indeed, if access to personal data is made available to third parties without the authorization of the holders, the possibility of accessing large amounts of data opens the door to manipulation of public opinion, which may even affect voters' choices. Suffice it to mention, by way of example, the various media episodes carried out by Facebook. The company has been harshly criticized for the hesitant and belated way that it managed the discovery of suspicious Russian activity on the social network (which may have favoured Donald Trump's election) or that it allowed the Cambridge Analytica company to have access to personal information about millions of people.[15]

As the Financial Times recently reported on its front page, the personal data of 500 million Starwood customers belonging to the Marriott International group dating back to 2004 may have been hacked! Ensuring that data is properly protected and not misused is essential to accomplishing the full potential of the digital economy.

At the same time, the conditions under which modern markets are organised in the digital age change radically in nature, forcing market and competition regulators to adapt to the new business, transaction and communication models that the digital economy provides for.

III. Application of competition law in digital markets

Competition rules must be applied, in light of the existing regulatory framework, in order to remedy market failures arising from the conduct of undertakings that engage in collusive practices or abuse their dominant position, or which could, through an operation of concentration, significantly impede effective competition in digital markets. Although, as Commissioner Margrethe Verstäger has pointed out on a number of occasions, EU competition rules have the necessary plasticity to adapt to new realities, the speed with which digital markets have evolved and the high degree of technicality that characterizes these markets make the application of these

[15] See Sheera Frenkel, Nicholas Confessore, Cecilia Kang, Matthew Rosenberg **and** Jack Nicas, "*Delay, Deny and Deflect: How Facebook's Leaders Fought Through Crisis*" *The New York Times*, November 14, 2018, https://www.nytimes.com/2018/11/14/technology/facebook-data-russia-election-racism.html.

rules in the digital age especially complex.

The Commission's Decisions in *Google Shopping*, 2017,[16] and *Google Android*, 2018,[17] are particularly illustrative in this respect: in the first case, the Commission analysed about 1.7 billion surveys to assess how people behave online! These decisions are also impressive by the amount of the fines imposed, which were € 2.45 and € 4.34 billion respectively!

Those cases led some to claim the need to dismember, in the near future, the "*giants*" installed in the digital sector, companies like Google, Amazon or Facebook. The Economist recently published an excellent article entitled "*The next capitalist revolution*",[18] stressing the need to protect competition in this sector.

The reality is that, over a little more than a decade, Facebook has managed to connect 2.2 billion people and has built, through messages, photos and *likes*, one of the most extensive repositories of personal data available.

Such data are indispensable not only for competition between operators in online markets but also for operators active in other sectors.

One of the issues that the Commission examined before approving Microsoft's acquisition of LinkedIn in 2016 was whether the combination of data from both companies would cause significant barriers to competition for other operators. In this context, the so-called 'Neo-Brandeis School' in the United States has advocated a broad and pluralistic conception of the objectives pursued by competition law that may incorporate concerns that go beyond strictly efficiency considerations, including privacy protection.

Some national competition authorities in the EU are examining the conduct of undertakings relating to the collection and misuse of data on digital markets under an new prism concerning the prohibition of abuse of a dominant position.

In this respect, the German competition authority – the *Bundeskartellamt* – seems inclined to consider that Facebook is abusing its dominant position on the German social networking market by making use of its network subject to the possibility of collecting data from users generated through the use of other websites and applications such as WhatsApp and Instagram, and to integrate them into one's Facebook account.

In this context, and in view of the less formalist approach in the application of competition law promoted in recent years, as well as the increasingly high fines imposed on undertakings, it is more important than ever to emphasize the case-law of the Court of Justice of the European Union (hereinafter referred to as "*CJEU*", "*Court of Justice*" or simply "*the Court*") according to which the discretion enjoyed by the Commission in matters involving complex assessments is not tantamount to a "*blank check*" in favour of the latter.

Thus, if the CJEU is not to substitute itself for the Commission in the analysis of facts and evidence or in defining its political priorities in the field of competition, it is incumbent on it to exercise in depth its powers of review of legality and, where appropriate, to ensure that the principle of effective judicial protection enshrined in Article 47 of the Charter of Fundamental Rights of the EU (hereinafter "*the Charter*"

[16] Commission Decision of 27.6.2017 relating to proceedings under Article 102 of the Treaty on the Functioning of the European Union and Article 54 of the Agreement on the European Economic Area [AT.39740 - Google Search (Shopping)] - C (2017) 4444 final.

[17] Commission Decision of 18 July 2018, Case AT.40099 – Google Android.

[18] See "*The next capitalist revolution*" *The Economist*, November 15, 2018, https://www.economist.com/leaders/2018/11/15/the-next-capitalist-revolution.

or "*the European Charter*") is respected.[19]

The Court took an important step towards strengthening judicial control of abuses of a dominant position in its judgment in the Grand Chamber case in *Intel* of September 2017,[20] where it annulled for the first time a decision of the General Court of the European Union (hereinafter "*General Court*") concerning the application of Article 102 TFEU.

In that judgment, the Court of Justice, by rejecting the fundamental premise of the Commission's decision and the General Court's ruling according to which it was unnecessary to examine all the relevant circumstances of the case, clarified the case-law initiated by *Hoffman-La Roche*, of 1979,[21] and sent a decisive message to the European Commission: that it cannot rely on any kind of "*facilitation*" when it makes use of presumptions of abuse to justify an infringement of Article 102 TFEU.[22]

It must be acknowledged that such an evolution in the case-law, supported by developments in economic science over the last decades, does not make it easier for the competition regulator or the courts to assess the legality of their acts.[23]

IV. Protection of personal data and fundamental rights in the digital age

1. The General Data Protection Regulation (GDPR), the Google Spain jurisprudence and the "right to be forgotten"

The GDPR[24] is an important step towards restoring or enhancing public confidence in the benefits of digitisation, in particular by promoting greater citizen control over the data concerning them.

Article 17 of the GDPR establishes and regulates what is known as the "*right to erasure"* or the *"right to be forgotten*",[25] a typical right of the digital age. It has its origin in the judgment of the Court of Justice (Grand Chamber) of 2014 in *Google Spain,*[26] the first case in which the Court was called upon to interpret a directive in the context of Internet search engines.

It is important to know the main lines of this case.

The reference for a preliminary ruling was made in the context of a dispute opposing Google Spain and Google Inc (hereinafter referred to as "*Google*") to

[19] See, for example, Judgment *Schindler Holding e.a./Comissão*, case C-501/11 P, of 18 July 2013, EU:C:2013:522, paragraphs 36 to 38.

[20] Judgment of 6 September 2017*, Intel v Commission*, C-413/14 P, EU:C:2017:632.

[21] Judgment of 13 February, 1979, *Hoffmann-La Roche/Comissão*, 85/76, EU:C:1979:36.

[22] See, for an analysis of the *Intel* jurisprudence in its context, my article: J. L. da Cruz Vilaça, "*The intensity of judicial review in complex economic matters - recent competition law judgments of the Court of Justice of the EU*", *Journal of Antitrust Enforcement,* vol. 6, issue 2 (2018): 1-16, https://academic.oup.com/antitrust/advance-article-abstract/doi/10.1093/jaenfo/jny003/4978137.

[23] The digital age gives rise to specific legal challenges of a particular complexity. For instance, when prices are set according to an algorithm that undertakings may claim to be confidential and commercially sensitive, assessing the legality of such practice may become particularly complex.

[24] Regulation 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 (General Data Protection Regulation) – OJ L 119/1, 4.5.2016. Available on: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679.

[25] In the French version, "*le droit à effacement*" or "*le droit à l'oubli*".

[26] Judgment of 13 May 2014, *Google Spain*, C-131/12, EU:C:2014:317.

the Spanish Data Protection Agency (AEPD, hereinafter "*the Agency*") and to Mr. Costeja González. In 2010, Mr. González filed a complaint against the newspaper La Vanguardia and against Google based on the fact that whenever an internet user entered his name on Google's search engine, he would obtain links to two pages of La Vanguardia, which contained an announcement of a real-estate auction connected with attachment proceedings for the recovery of social security debts, on which Mr. González's name was mentioned.

It was the latter's understanding that the reference to the asset's attachment process, which had been completely resolved several years ago, was no longer relevant to the public, and that both La Vanguardia and Google should delete or amend those pages. The Agency rejected the complaint in so far as it concerned La Vanguardia, on the grounds that the publication of the information in question was justified on grounds of public interest[27] and was therefore legitimate.

On the other hand, the complaint was upheld in so far as it concerned Google. The Agency considered that search engine operators were subject to data protection legislation and that the disclosure of personal data to third parties against the will of the person concerned was liable to breach that person's fundamental rights.

Google brought appeals against that decision before the Audiencia Nacional, which referred the questions to the Court of Justice for a preliminary ruling.

In its judgment the Court drew from several provisions of Directive 95/46[28] (Articles 6, 12 and 14),[29] read in conjunction with Articles 7 and 8 of the Charter, the right to have inadequate, irrelevant or excessive information about a person ceasing to appear in the results list when doing a search from the name – the so-called "*delisting*" – without requiring that the inclusion of information in the results list causes or may cause damages to the person in question.

The Court also pointed out that that right prevails in principle not only over the economic interest of the search engine operator but also over the public interest in finding that information, unless there are special reasons to the contrary, for example, in connection with the role played by that person in public life, which would justify a preponderant public interest in having access to the information in question. The recognition of the need to ensure "*effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data*",[30] guided the decision of the Court of Justice.

In the *Schrems* judgment of 2015, the Court made this formula even more robust by emphasizing the need to ensure "*highest level of protection of those fundamental rights and freedoms*".[31]

In the *Google Spain* judgment, the Court stated that "*processing of personal data, […] 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, since that processing enables any internet user to*

[27] In fact, the publication had been made by order of the Ministry of Labour and Social Affairs, with the aim of publicizing to the maximum what happened in the sales at public auction.

[28] Directive 95/46 of the European Parliament and the Council, of 24 Oct. 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data - OJ L 281, 23.11.1995, p. 31-50.

[29] Concerning the principles of data quality, data erasure and blocking rights, as well as the right of opposition.

[30] See Judgment *Google Spain*, paragraph 53.

[31] Judgment of 6 Oct. 2015 (Grand Chamber), *Maximilian Schrems*, C-362/14, EU:C:2015:650, para. 39.

obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet – information which potentially concerns a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty".[32]

The effect of interference with individual rights "*is heightened on account of the important role played by the internet and search engines in modern society, which render the information contained in such a list of results ubiquitous*".[33]

In the meantime, the French Conseil d'État also submitted to the CJEU in 2017 two requests for a preliminary ruling, which are still pending when presenting this paper,[34] with a view to clarifying certain aspects of the "*right to be forgotten*", in particular, whether this right should be absolute and automatically operate when sensitive information is concerned and also what its territorial scope is.[35]

2. The fight against crime and terrorism, the discretion of the legislator and the balancing of interests and rights at stake; the judgments in Volker und Markus Schecke *and* Digital Rights Ireland

The obligation to ensure respect for privacy and personal data has already led the Court to declare all or part of important Union legislation to be invalid. That case-law brings to the surface issues of a cross-cutting nature, in particular, the "*eternal*" question of any system of constitutional justice, namely the interrelationship between the discretion of the legislator and scrutiny by the courts, more precisely, the way in which a court of a constitutional nature must exercise its control while respecting the margin of discretion which is recognized to the legislator in any democracy in matters that imply sometimes very complex political, economic and social choices. In that context, the principle of proportionality, which forms part of the general principles of Union law and is enshrined in Article 52 (1) of the European Charter, has played a leading role in the Court's findings.

In accordance with settled case-law, such a principle requires that "*measures adopted by European Union institutions do not exceed the limits of what is appropriate and necessary in order to attain the objectives legitimately pursued by the legislation in question; when there is a choice between several appropriate measures recourse must be had to the least onerous, and the disadvantages caused must not be disproportionate to the aims pursued*".[36]

Thus, in 2010, in the *Volker und Markus Schecke* case,[37] the Court held that several provisions of Regulation No. 1290/2005 of 21 June 2005 on the financing of the common agricultural policy and of Regulation No 259/2008 of 18 March 2008, concerning the publication of information on the beneficiaries of funds from the EAGF[38] and the EAFRD,[39] in so far as, in respect of the natural persons receiving aid

[32] Judgment *Google Spain,* para. 80 (my highlight).
[33] *Idem, ibidem.*
[34] Cases C-136/17 e C- 507/17.
[35] See Greg Sterling, "*Two major changes potentially coming to EU's Right to Be Forgotten with global implications*", *Search Engine Land*, May 16, 2017, https://searchengineland.com/two-major-changes-potentially-coming-eus-right-forgotten-global-implications-275047.
[36] Judgment of 22 Jan. 2013 (Grand Chamber), *Sky Österreich*, C-283/11, EU:C:2013:28, para. 50.
[37] Judgment of 9 Nov. 2010 (Grand Chamber), *Volker und Markus Schecke*, C-92/09 and C-93/09, EU:C:2010:662.
[38] European Agricultural Guarantee Fund.
[39] European Agricultural Fund for Rural Development.

from these funds, those provisions required the publication of personal data relating to any beneficiary, without limitations or distinctions according to relevant criteria, such as the periods during which they received such aid, their frequency or the type or importance thereof.

In the view of the Court of Justice, the Council and the Commission did not seek to "*strike such a balance between the European Union's interest in guaranteeing the transparency*[40] *of its acts and ensuring the best use of public funds, on the one hand, and the fundamental rights enshrined in Articles 7 and 8 of the Charter, on the other*".[41]

Particularly striking in this regard is the judgment in *Digital Rights Ireland*[42] of 2014, in which the CJEU declared Directive 2006/24,[43] on the retention of data generated by electronic communications, invalid in its entirety on grounds of infringement of the European Charter.

Personal data is not, today, only valuable assets for private companies. It is also essential information for criminal police agencies and judicial authorities, especially in combating organized crime and terrorism. But in the 'Big Data' era, the track that each of us leaves in using electronic equipment or social networks and by staying connected to the Internet can easily slip into abusive interference in the private sphere of people.

In the *Digital Rights* case, the Court examined the obligation under Directive 2006/24 for electronic communications service providers to retain certain categories of data in order to allow possible access to them by national authorities competent for the prosecution of criminal offenses of special gravity.

The Directive did not impose an obligation to collect and retain the *content* of communications, but only so-called *'metadata'*, necessary to find and identify the source and destination of a communication, to determine its date, time and duration, the type of communication equipment or the location of mobile communication equipment.

These data include, in particular, the name and address of the registered subscriber or user, the home telephone number and the telephone number of the recipient, as well as an IP address for the Internet services.

Such data permits, inter alia, to identify the person with whom a subscriber or a registered user has communicated and through which medium and to determine how often the subscriber or the registered user communicates with certain people for a certain period.

Although the content of the communications and the information consulted is not concerned, the Court emphasized, that those metadata, "*taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them*".[44]

---

[40] The principle of transparency in Union law is enshrined in Articles 1 and 10 TEU and 15 TFEU. See paragraph 68 of the judgment.

[41] See paragraph 80 of the judgment.

[42] Judgment of 8 April 2014, *Digital Rights Ireland*, C-293/12 and C-594/12, EU:C:2014:238.

[43] Directive 2006/24 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 – OJ L 105, p. 54.

[44] See paragraph 27 of the judgment.

The Court acknowledged that the data generated by electronic communications is an important and useful tool in the fight against crime, in particular, organized crime and terrorism, whose effectiveness in protecting the rights to freedom and security set out in Article 6 of the Charter depends on the use of modern research techniques.

It concluded, however, that pursuing this general interest objective did not justify the particularly serious interference that Directive 2006/24 entailed in the fundamental rights enshrined in Articles 7 and 8 of the Charter.

The Court thus held that the retention of data, in the manner laid down in Directive 2006/24, was disproportionate in several respects. In particular:

- the data retention obligation covered virtually the entire European population, all electronic means of communication and all traffic data, even applying to persons for whom there was no evidence of serious crime;
- no exception was made for communications subject to professional secrecy;
- the Directive did not lay down objective criteria which would limit access and use by the competent national authorities to the data necessary to combat infringements sufficiently serious to justify the interference caused;
- it was envisaged that the data would be kept for a period of between 6 and 24 months, without specifying that the precise determination of this period should be based on objective criteria, in order to ensure that it was limited to what was strictly necessary;
- the Directive did not provide sufficient guarantees against the risks of abuse and access to and unlawful use of the data retained;
- nor did it require the data to be stored in the territory of the Union, with the result that it could not be held that the control, required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security was fully ensured.

The motto for this in-depth analysis by the CJEU was set out in paragraph 48 of the judgment, where the Court stated that "*in view of the extent and seriousness of the interference [in the fundamental rights at issue] the EU legislature's discretion is reduced, with the result that review of that discretion should be strict*".

3. The weighing of interests: more or less serious interference in individual rights; the judgments in Schrems *and in* Ministerio Fiscal

The risk of not ensuring an adequate level of protection was again assessed by the Court in the *Schrems* judgment of 2015 on the interpretation of Directive 95/46,[45] in particular, Article 25 on the transfer of personal data to a third country.[46]

Here again, the Court ruled in favour of a strict interpretation of the conditions for the application of the Directive. The Court stated that "*in view of, first, the important role played by the protection of personal data in the light of the fundamental right to respect for private life and, secondly, the large number of persons whose fundamental rights are liable to be infringed where personal data is transferred to a third country not ensuring an adequate level of*

[45] Directive 95/46 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 - OJ L 281, 23.11.1995, p. 31-50.

[46] On the judgment, see Fanny Coudert, "*Schrems v. Data Protection Commissioner: a slap on the wrist for the Commission and new powers for data protection authorities*", *European Law Blog*, October 15, 2015, available on: https://europeanlawblog.eu/2015/10/15/schrems-vs-data-protection-commissioner-a-slap-on-the-wrist-for-the-commission-and-new-powers-for-data-protection-authorities/.

protection, the Commission's discretion as to the adequacy of the level of protection ensured by a third country is reduced, with the result that review of the requirements stemming from Article 25 of Directive 95/46, read in the light of the Charter, should be strict".[47]

The dispute opposed Maximilian Schrems, a young and active Austrian citizen, of Facebook, and the Data Protection Commissioner of Ireland. The case was predicated on the latter's refusal to investigate a complaint that Facebook Ireland transferred the personal information of its users to the United States and stored them on servers located in that country.

Max Schrems relied in particular on the revelations made by Edward Snowden on the activities of the United States Information Services, namely the National Security Agency (NSA).

For its part, the Data Protection Commissioner argued it was covered by the Commission Decision 2000/520,[48] in which the Commission considered that the United States provided an adequate level of protection.

The Court concluded that that decision, which was based on the existence of a *Safe Harbour* mechanism, itself based on the self-certification by US companies of compliance with certain principles, was invalid in that:

- the Commission did not ensure that the United States would effectively guarantee an adequate level of protection;[49]
- the Commission's decision deprives the national supervisory authorities of the powers conferred on them by Directive 95/46 to examine, with complete independence, any request relating to the protection of the rights and freedoms of a person with regard to the processing of his personal data.[50]

It remains to be said that the balancing of the interests involved in relation to the objectives and the relative gravity of the interference does not always lead to the same kind of conclusions.

Thus, in October 2018, in the case *Ministerio Fiscal*, concerning the interpretation of Directive 2002/58 on privacy and electronic communications,[51] in conjunction with Articles 7 and 8 of the Charter, the CJEU validated the access by Spanish judicial police for a limited period of time to personal data held by electronic communications service providers with a view to identifying SIM card holders activated on a stolen mobile phone, such as their surname, forename and, where appropriate, their address.[52]

While admitting that such access constituted an interference with the fundamental rights of the right holders laid down in Articles 7 and 8 of the Charter, the Court held that, in those circumstances, interference was not such as to prevent access for the prevention, investigation, detection and prosecution of criminal offenses, in such a way that it would be limited to the fight against serious crime.

---

[47] Judgment, paragraph 78.

[48] Commission Decision 2000/520 of 26 July 2000 pursuant to Directive 95/46 on the level of protection afforded by the Safe Harbour Principles and the Frequently Asked Questions (FAQ) issued by the Department of Commerce of the United States of America - OJ 1994 L 215, p. 7.

[49] See paragraphs 97 and 98 of the judgment.

[50] Paragraph 99 to 106 of the judgment.

[51] Directive 2002/58 of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications - E-privacy directive), OJ L 201, 31/07/2002, p. 37-47.

[52] See paragraphs 48 and ff. of the judgment.

The data at issue did not allow for precise conclusions to be drawn as to the private life of individuals and, therefore, access to those data could not be classified as a 'serious interference' with the fundamental rights of the persons concerned.

It was not therefore a situation identical to that which had been examined by the Court in *Digital Rights Ireland* and in the judgment of 2016 in *Tele2 Sverige* and *Watson*,[53/54] where the ECJ ruled on the implications for Member States' legislations of that first judgment. These were 'serious' interferences which, in accordance with the principle of proportionality, could only be justified in terms of prevention, investigation, detection and prosecution of criminal offenses, with a view to combating 'serious' crime.

The Court nevertheless stated in the latter judgment that Member States may adopt rules enabling, in a preventive way, a *selective conservation* of traffic and location data for the purpose of combating serious crime, provided that it "*is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary*",[55] that access by the competent authorities is subject to prior checking by a court or an independent administrative authority and that the data in question are kept in the territory of the Union.

From the case-law referred so far, it is possible to draw two main inferences:

- First, that a careful assessment of each particular situation must be carried out, taking into account the seriousness of both the interference with fundamental rights and the infringement under investigation;
- Second, that the Court's scrutiny tends to be more intense when it comes to seeking an appropriate balance between individual rights and freedoms, on the one hand, and public order and security requirements, on the other hand, even more so as these are likely to involve the preservation of rights as fundamental as the right to life and physical integrity.

This development of the case-law can contribute not only to transforming the relationship between the Union legislature and the CJEU, but also to bring the latter closer to a real constitutional court, more focused on protecting fundamental rights and preserving checks and balances than on achieving the objective of the internal market.

In any case, as someone has already noted, "*[t]here is a symbolic dimension to the fact that the strict scrutiny was first applied to the right to privacy: 'the' human right in the information age*".[56] I have no doubt that the digital age will continue to confront the Union's courts with new challenges and opportunities, due to the profound impact it is already having on the evolution of modern societies.

---

[53] Judgment of 21 Dec. 2016, *Tele2 Sverige* and *Tom Watson*, C-203/15 and C-698/15, EU:C:2016:970, available on: http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=5907371.

[54] On this judgment, see Orla Lynskey, "*Tele2 Sverige AB and Watson: continuity and radical change*", *European Law Blog*, January 12, 2017.

[55] See paragraph 108 of the judgment.

[56] M. P. Granger and K. Irion, "The Court of Justice and The Data Retention Directive in Digital Rights Ireland: Telling Off The EU Legislator and Teaching a Lesson in Privacy and Data Protection," *European Law Review,* vol. 39, issue 6 (2014): 835-850, http://dare.uva.nl/search?identifier=66f958db-8cb6-4c2c-b58f-827af88824b3.