E-JOURNAL OF LAW

Regulation (EU) 2016/679 on The Protection of Personal Data In Light of The "Cambridge Analytica" Affair

Dimitris LIAKOPOULOS*

Abstract

The present work is concentrated on the analysis of the Regulation (EU) 2016/679 making an application in the worldwide case of Cambridge Analytica. We try to analyze the new legislation from the part of the European Union, the new problems created, the shortcomings, achievements, trends, challenges and the silence on some points coming to make connection with the Regulation bruzells I-Bis and the jurisdictional forum for modal cases that try to protect the data protection both at international and European level.

Keywords: Reg. 2016/689, protection of personal data, Cambridge Analytica, CJEU, GDPR, IOT, data breach.

* Full Professor of European Union Law at the Fletcher School-Tufts University (MA in international law and MA of Arts in Law and diplomacy). Full Professor of International and European Criminal and Procedural Law at the De Haagse Hogenschool-The Hague. Attorney at Law a New York and Bruxelles. ORCID ID: 0000-0002-1048-6468. The present work is updated until June 2019. (email address: prof.d.liakopoulos.984@gmail.com)

Regulation (EU) 2016/679 on The Protection of Personal Data In Light of The "Cambridge Analytica" Affair

Introduction

The information and communication society is a type of society that makes knowledge and its sharing the key elements around which to develop activities that characterize social and economic living. The growing possibility offered by technological supports to easily exchange contents of various types, overcoming traditional time-space barriers, has, over the years, deeply innovated the traditional way of understanding economic activity, the modalities of interaction between the subsidiaries and the provision of public services that now fully nurture the interactivity, versatility, speed and totality of the services offered by the network.

In the last decade, however, this peculiar extremely dynamic and changeable process has taken a further step forward with the spread of increasingly advanced technologies, based on the exchange of data and information. First of all, we refer to the phenomenon of the internet of things (IOT)[1] that makes it possible to transform objects, such as cars, buildings, but also televisions and home appliances, into closely connected goods, capable of storing, processing and mutually exchanging thousands of data in order to guarantee increasingly advanced and personalized consumption experiences[2]. On the other

[1]T. Kerikimäe, Regulating technologies with European Union. Normative realities and trends, ed. Springer, Berlin, 2014.

[2]European Commission DG Communications Networks, Content & Technology, Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination, Final Report, 2013. The analysis showed that the use of this technology will guarantee an economic growth of over 20 billion euro within the European Union by the year 2020 and represents one of the pillars of the creation of the European digital single market (so-called Digital single market).

hand, through the use of these techniques, the same cities become more and more "smart", year after year, because they are able to transform the potential offered by new digital platforms into increasingly efficient services for citizens[3], optimizing their use resources available and in some cases also guaranteeing a lower environmental impact[4].

A further phenomenon is represented by the proliferation of big data[5], huge amounts of data and information of various types that, produced at great speed starting from a plurality of different sources, are used in

[3]Smart Cities and Communities (EIP-SCC) which aims to stimulate technological growth in sectors where "energy production, distribution and use, mobility and transport and information and communication technologies (ICT) are closely linked and can offer new interdisciplinary opportunities to improve services, reducing the consumption of energy and resources and emissions of greenhouse gases and other pollutants". On the point see COM (2012) 4701, Communication from the European Commission, Cities and Intelligent Communities European Innovation Partnership, 2012. For further details see: R. Riva Sanseverino, Competitive urban models, in E. Riva Sanseverino, R. Riva Sanseverino, V. Vaccaro, G. Zizzo (ed.), Smart rules for smart cities, ed. Springer, Palermo, 2014, pp.4ss.

[4]The achievement of a "resource-efficient Europe" is one of the seven flagship initiatives promoted at supranational level and in the Member States in the context of the H2020 strategy which, as is well known, aims at achieving smart growth, through the development of knowledge and innovation; sustainable, based on a greener economy, more efficient in resource management and more competitive; inclusive, aimed at promoting employment and social and territorial cohesion. See, COM (2010) 2020, Communication from the European Commission, Europe 2020-A strategy for smart, sustainable and inclusive growth. In this regard, as stated in the roadmap drawn up in 2011 by the European Commission, for the realization of this initiative it is necessary to define "a strategic framework that prizes innovation and resource efficiency and that creates the conditions for new opportunities. for greater security of supply thanks to the redesign of products, the sustainable management of environmental resources, the promotion of recycling and reuse, the replacement of materials and the saving of resources". In the same spirit see also: COM (2011) 0571, Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Roadmap for a Resource-efficient Europe, 2011.

[5]L. Moerel, Back to basics: when does EU data protection law apply? In International Data Privacy Law, 1 (2), 2011, pp. 94ss.

a combined manner for the provision of highly advanced and modeled performances on the needs of users[6]. Finally, the diffusion of cloud computing technologies (so-called cloud computing) that allow to store these massive masses of data remotely, exploiting the extraordinary storage potential of the internet[7] network should be emphasized. IOT, big data and cloud computing represent, therefore, the three directives on which the current technological evolution is moving[8] and their

[6]Council of Europe: Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data; Strasburgo, 2017. For the big data see: COM (2014) 442 Final, Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Towards a thriving data-driven economy 2014. For further analysis see also: I.S. Rubinstein, Big data: The end of privacy or a new beginning?, in International Data Privacy Law, 3 (2), 2013. B. Van Der Sloot, S. Van Schendel, Ten questions for future regulation of big data: A comparative and empirical legal study in Jipitec, in Journal of Intellectual Property, Information Technology and E-Commerce Law, 7 (2), 2016.

[7]Cloud computing refers to a set of technologies and ways of using IT services that allow the storage, processing or transmission of data, in on demand mode, through the Internet, starting from a set of pre-existing and configurable resources. On this topic, refer to the Document COM (2012) 529 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Exploiting the potential of cloud computing in Europe. in Italy the Guarantor for personal data protection in May 2012 drew up a vademecum for companies and the public administration regarding the choice and use of cloud computing entitled "Cloud computing. Protect your data so you do not fall from the clouds".

[8]Internet of things, Big data and cloud computing they are the cornerstones of the strategy known as the Digital single market. See, COM (2015) 192 final, 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. Adopted on 6 May 2015, this project includes 16 specific heterogeneous initiatives that revolve around three fundamental pillars: 1) access: aimed at guaranteeing consumers and market operators efficient access to digital goods and services across the European Union; 2) the context: aimed at guaranteeing the best conditions and a level playing field that is able to bring out innovative digital services and networks; 3) the economy and society: aimed at maximizing the potential growth of the digital economy. The objective pursued is the creation of a digital single market based on exploiting the potential and extraordinary

combined action is completely modifying the physiognomy of contemporary societies, favoring the birth of a new era characterized by "hyper-connected". It is evident that, in this particular scenario, the datum becomes a strategic resource and a factor of economic development; an element of collective growth and cultural wealth, placing the individual at the center of digital society[9]. Behind the extraordinary advantages of the personalization of services there is the risk of an excessive compression of the fundamental rights of the individual, deriving from the overexposure of extremely delicate aspects of their personal sphere[10]. The ever more extensive digitalization determines, in fact, the fragmentation of the identity of the individual into thousands of small pieces, which through the data reverberate outside projecting more or less intimate aspects of their person. The incessant flow of such personal information has favored in recent years the emergence of increasingly refined profiling techniques

pervasiveness of information and communication technologies. The initiatives linked to this strategy are, in fact, wide and heterogeneous, moving from the field of e-commerce to that of the protection of personal data, passing for the protection of copyright, the evolution of the audiovisual market up to digitization of public administration services. A transformation, therefore, with a wide spectrum based on the advantages deriving from the increasingly advanced digitalisation of European society. On the theme cf. among others, the first assessment of the objectives achieved so far in the context of the aforementioned strategy implemented in 2017. See also: COM/2017/0228 final, Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, on the mid-term review of the implementation of the Digital Single Market Strategy A connected digital single market, 10 May 2017.

[9]M.L. Ambrose, M.L. Friess, N. Matre, J.V. Seeking, Digital redemption: The future of forgiveness in the internet age, in Santa Clara Computer and High Technology Law Journal, 29, 2012.

[10]S. Wachter, Normative challenges of identification in the internet of things: Privacy, profiling, discrimination, and the GDPR, in Computer law & security Review, 34, 2018, pp. 438ss. I. S. Rubinstein, Big data: The end of privacy or a new beginning?, op. cit.

that, through the aggregation, intersection and reorganization of the collected data, allow users to be divided into distinct categories based on characteristics homogeneous, in order to supply "tailor-made" products through the prediction of consumption decisions and related behaviors. Empowered by the extraordinary evolutionary rapidity of technological tools, such peculiar personal data processing activities can not only exacerbate existing discrimination and stereotyping situations, but risk leading to phenomena of "penalizing propensities"[11], limiting the actual possibilities of choice of the individual, leading to the extreme consequence of inhibiting the exercise of its fundamental freedoms or limiting the provision of essential services[12].

2.The value of personal data in modern digital societies

[11]I. S. Rubistein, Big data: The end of privacy or a new beginning?, op. cit.,

[12]As evidenced by the Guidelines drawn up by Article 29 Working Party regarding profiling and automated decision-making processes, such specific treatments can not only accentuate existing social discrimination situations, but are potentially able to incardinate a person within a given category, limiting the possible alternatives of choice. For example, following a profiling activity, a site inevitably tends to offer its customers products and services related to their needs and preferences, excluding others and thus drastically limiting the freedom of choice of these subjects. It is evident that with the refinement of the profiling techniques especially in an automated manner and, therefore, in the absence of human intervention, and the extension of the tools made available to the data controllers, such activity, if not regulated, risks also affect the sphere of fundamental rights of individuals, affecting, for example, the relative freedom to associate or the conscious exercise of the right to vote, as well as influence the contractual positions of the subjects within a contract. Finally, based on predictive calculations, profiling can lead to inaccurate predictions causing further damage in terms of access limitations to certain services or products. See, Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.

Now far from that "right to be let alone", codified by Warren and Brandeis in the right to privacy in 1890[13], the full and conscious realization of the single within modern data-centric societies now runs along the tracks of personal data protection, with the aim of protecting it from the danger of concealed acquisition of information, of intrusion into its private sphere and of improper use of the collected data[14].

The right to the protection of personal data is also known as "information privacy", "informational privacy", "data privacy", all expressions in which it is emphasized that the object of the right is information or data, although strictly speaking data and information are non-coincident terms. The necessary exceptionality character to the fundamental right of the protection of personal data is enshrined in cases C-293/12 and C-594/12, *Digital Rights Ireland* of 25 July 2014[15] where it is stated that the Directive 2006/24/EC (canceled by the same

[13]S.D. Warren, L.D. Brandeis, The right to privacy, in Harvard Law Review, 4 (5), 1890.

[14]Regulation (EU) 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/EC.

[15]CJEU, joined cases, C-293/12 and C-594/12, Digital Rights Ireland of 25 July, ECLI:EU:C:2014:238, published in electronic reports of the cases. See in argument: T. Wisman, Privacy: Alive and kicking, in European Data Protection Law Review, 80 (1), 2015, pp. 81ss. F. Fabbrini, Human rights in the digital age: The European Court of Justice ruling in the Data Retention Case and its lessons for privacy and surveillance in the United States, in Harvard Human Rights Journal, 28, 2015, pp. 72ss. In particular the author states that: "(...) the lesson that the ECJ judgment in Digital Rights Ireland carries for the United States, however, is that the distinction between private and public retention does not matter. As the ECJ ruled with regard to a system in which private companies collect the metadata, it is the retention in itself that constitutes an infringement on the right to privacy (...) the ECJ's decision poses a pressing question: namely, whether collection, retention, and storage of metadata that tells so much about an individual's personal life should be within the remit of the government's policy tools in the fight against terrorism at all (...)".

decision)[16] by not providing clear and precise rules governing the extent of the interference in the fundamental rights enshrined in artt. 7 and 8 of the Charter of Fundamental Rights of the European Union (CFREU), entails an interference with such fundamental and far-reaching fundamental rights in the legal order of the Union, without such interference being regulated precisely by provisions permitting ensure that it is effectively limited to what is strictly necessary. The same decision also states the essential role of the supervisory authority by an independent authority, which is an essential element of respect for the protection of individuals with regard to the processing of personal data[17]. The same arguments are more widely developed in the Schrems case[18] where it is stated that a European legislation involving interference in fundamental rights guaranteed by artt. 7 and 8 of the CFREU must provide, according to the settled case law of the Court of Justice of the European Union (CJEU)[19], clear and precise rules governing the scope and application of the measure in question and imposing minimum requirements so that persons whose personal data

[16]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, OJ L 105, 13.4.2006, p. 54–63, date of end of validity 8 April 2014. L. Feiler, The legality of the Data Retention Directive in light of the fundamental rights to privacy and data protection, in European Journal of Law and Technology, 1 (3), 2010.

[17]See in this spirit the sentence: C-614/10, European Commission v. Austria, ECLI:EU:C:2012:631, published in electronic Reports of the cases, par. 37.

[18]C-362/14, Schrems of 6 October 2015, ECLI:EU:C:2015:650, published in electronic Reports of the cases.

[19]M. Škrinjar Vidović, Schrems v. Data protection commissioner (case C-362/14) empowering national data protection authorities, in Croatian Yearbook of European Law and Policy, 11, 2015, pp. 270ss.

are affected have sufficient guarantees to enable their data to be effectively protected against the risk of abuses as well as against any access and illicit use of the aforementioned data. In particular the CJEU emphasizes the need for the individual to be able to use legal remedies to exercise their right to control over their personal data, control that constitutes the essence of the right to the protection of personal data, and reiterates the need effective judicial review, designed to ensure compliance with the provisions of EU law, is inherent in the existence of a rule of law[20].

The need is to prevent the data, treated for purposes that fall outside the will of the subject, may cause situations of discrimination, theft or identity usurpation; affect one's reputation or result in any significant economic or social harm. Moreover, in the light of the ever more invasive profiling techniques[21], in this complex scenario the protection

[20]Position of old ispiration thourgh the sentences: C-294/83, Les Verts v. European Parliament of 26 September 1984, ECLI:EU:C:1986:166, I-03331, par. 23. C-222/84, Johnston of 15 May 1986, ECLI:EU:C:1986:206, I-00621, parr. 18-19. C-428/06 at C-434/06, Heylens of 11 September 2008, ECLI:EU:C:1987:442, I-06747 par. 14, and joined cases: C-428/06 at C-434/06, UGTRioja and others of 11 September 2008, ECLI:EU:C:2008:488, I-06747 par. 80.

[21]According to our opinionstarting from the awareness that man is a social animal and as such at the center of a network of relationships renouncing the protection of personal data from any undue interference, it means risking to nullify any other form of freedom and endanger all fundamental rights. The stresses that the European Regulation itself under analysis in recital 4) states that "The processing of personal data should be at the service of man. The right to the protection of personal data is not an absolute prerogative, but must be considered in the light of its social function and must be reconciled with other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognized by the Charter, enshrined in the Treaties, in particular respect for private and family life, domicile and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom of business, the right to an effective remedy and

of data takes on a further significance beyond the protection of the individual, establishing itself as an instrument for the protection of the community.

The correct processing of personal data, especially of a sensitive nature, constitutes a prerequisite, in fact, indispensable to the full and conscious exercise of other fundamental rights by removing phenomena of compression of moments of interaction between the subjects, which are not acceptable within democratic societies. It follows that the prediction of a reasoned system of rules destined to what we can define it as "the new oil of the digital economy" finds justification and legitimacy in its being functional to the democratic character of modern societies. It not only has value in itself, but it works to ensure that the community is able to channel the potential of new technologies to new and desired levels of growth, but without ever sacrificing the fundamental values to which it is inspired and which represent the cause and end of its existence.

3.Towards a new European Framework for personal data.

Faced with an extremely complex picture, in which the drive for innovation inevitably intertwines with the need to protect the identity sphere of individuals, the democratic growth of digital societies and, at the same time, it is good to underline it, also the security of

an impartial judge, as well as cultural, religious and linguistic diversity. See also in argument for details: V. Boehme-Nessler, Privacy: A matter of democracy. Why democracy needs privacy and data protection, in International Data Privacy Law, 6 (3), 2016.

infrastructures national and supranational criticism[22], in 2012 the European legislator undertook a long process aimed at identifying new rules common to all Member States regarding the protection of personal data[23]. At the basis of this decision there was, first of all, the conviction that the current system of rules, operating under the auspices of the "mother" Directive 95/46/CE[24], was no longer able to meet the complex

[22]The White Paper on Cybersecurity adopted in May 2018 shows that data protection also represents national and supranational priorities, as violations can also be perpetuated against critical information or information related to relevant infrastructures such as transport systems, energy supply, and telecommunications. In this sense, the part indicating that: "A country that does not put cybersecurity at the center of its digital transformation policies is a country that seriously risks its own economic prosperity and its independence.

[23]The presentation by the European Commission of the complete package on the protection of personal data in which they were presented for the first time is the proposal for a regulation that is the subject of this essay, and the proposal for a directive concerning the protection of individuals with regard to the processing of personal data by the competent authorities for the purposes of prevention, investigation, detection and prosecution of criminal offenses or the execution of criminal sanctions, and the free movement of such data, intended to replace the 2008 Framework Decision on data protection. The "Privacy Package" includes: a proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general data protection regulation)-2012/0011 (COD); proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data-2012/0010 (COD). See in argument: M. Hawsen, J.H. Hoepman, R. Leenes, Privacy and identity management for emerging services and technologies, ed. Springer, Berlin, 2014. M. Sebastian Haase, Datenschutz rechtliche Fragen des Personenbezugs, Mohr Siebeck, Tübingen, 2015.

[24]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, OJ L 281, 23.11.1995, p. 31-50, no longer in force, Date of end of validity: 24/05/2018 and modified from Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016, p. 1-88. See in argument: P. De Hert, V. Papakonstantinou, The proposed data protection Regulation replacing Directive

challenges adequately. coming from the increasingly intense use of profiling techniques and connection technologies. This intrinsic weakness was exacerbated due to the excessive fragmentation of territorial legislation, which exposed European citizens to high levels of protection and action, no longer eligible in such an advanced phase of the integration process and even counter-productive in the face of new protection requirements. of a cross-border nature, deriving from the extraordinary increase in the use of social networks and websites of non-European origin. The difficulties deriving from the absence of a homogeneous regulatory approach at European level, connected to an initial inevitable reluctance towards the increasingly invasive use of personal data, favored in some sectors, moreover, a climate of widespread skepticism towards the use of these technologies, preventing full exploitation of their potentials[25]. In order to make it

95/46/EC. A sound system for the protection of individuals, in Computer Law & Security Review, 28 (2), 2012, pp. 132ss. A. Mantelero, Cloud computing, trans-border data flows and the European Directive 95/46/EC: Applicable law and task distribution, in European Journal for Law and Technology, 3 (2), 2012. B. Van Alsenoy, Liability under EU data protection law: From Directive 95/46 to the General Data Protection Regulation, in Journal of Intellectual Property Information Technology and e-Commerce, 7, 2017, pp. 272ss.

[25]For example, reference is made to the health sector in which the use of new technologies has brought significant advantages in terms of diagnosis speed and effectiveness of the implemented therapies. Consider the introduction of the electronic dossier or the multiplication of electronic and wearable medical devices that have revolutionized traditional care and assistance activities. However, as the digitalization of health tools and related interconnectedness increased, there was a parallel increase in their vulnerability to attacks of an external nature. This awareness has very often been translated into a climate of widespread skepticism towards the use of these new technologies in a sector as sensitive as the health sector. As underlined, "it must also be considered that health data (and their high information potential) are the subject of enormous, sometimes illicit, interests. It is no coincidence that the goal of the most recent cyberattacks have been the information systems of healthcare companies and hospitals, blocking, even temporarily, access to health data for extortion purposes".

possible to overcome these critical issues and to orientate the advantages connected to what has been called the "fourth industrial revolution"[26] towards a conscious and efficient growth of European society, without at the same time provoking an unacceptable compression of the sphere of fundamental rights of the citizens, the Union has created a series of initiatives aimed at identifying shared rules that are able to "ferry" the Member States towards the new digital era[27]. This variegated path has culminated, at least with reference to the

Furthermore, the presence of different rules at national level accentuated this attitude of distrust, strongly limiting the propensity to transferability of health data at European level for medical and curative purposes. See also: Regulation (EU) n. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. In argument: A. Büllesbach, Concise european IT law, Kluwer Law International, The Hague, 2010, pp. 489ss.

[26]Publicly announced for the first time at the 2011 Hannover trade fair with the "Industrie 4.0: Mit dem Internet der Dinge auf dem Weg zur 4.0 industriellen Revolution" ("Industry 4.0: The Internet of Things on the Road to the Fourth Industrial Revolution"), the fourth industrial revolution indicates the extraordinary evolution of production and supply of goods and services caused by the use of new digital technologies. The widespread presence of sensors and wireless networks, as well as the use of robots and increasingly intelligent devices associated with extraordinary computing power and big data analysis at lower costs than in the past, has revolutionized the way of to conceive the industry worldwide, guaranteeing greater flexibility and speed in production, as well as an increase in the qualitative and quantitative level of the products produced. See: European Parliament: Industry 4.0 Digitalisation for productivity and growth, 2015. European Commission, Digital Transformation of European Industry and Enterprises-report from the Strategic Policy Forum on Digital Entrepreneurship, 2015.

[27]The European Commission, as part of the broader strategy dedicated to the creation of the Digital Single Market, launched in 2016 the initiative known as the "Digitizing European Industry Initiative" aimed at ensuring that every in Europe, regardless of size, location and sector, can take advantage of the benefits of digital innovation. The initiative is based on the following four fundamental pillars: 1) Creation of a European platform for national initiatives in the field of industrial digitization; 2) Digital innovations for everyone: digital innovation hubs; 3) Strengthening the leadership through partnerships and industrial platforms, 4) The determination of a regulatory framework suitable for the digital age; 5) Prepare citizens for the digital future. As part of this initiative, the NIS directive was adopted and important documents were

phase of closer regulation, in the adoption of a special "personal data protection package" consisting of Regulation (EU) 2016/679 (entry in force 30 May 2018)[28] concerning the protection of individuals with regard to the circulation of personal information[29] and from Directive 2016/680/EU[30] concerning the areas of prevention, contrast and repression of crimes. From their reading, the dual purpose that animates the entire regulatory system immediately emerges: on the one hand, the desire not to lose the extraordinary evolutionary path represented by the new digital technologies, which have now become a strategic factor for

signed for the implementation of new technologies in various important sectors for European society. Remember, among others, the "EU eGovernment Action Plan 2016-2020-Accelerating the digital transformation of government" dedicated to the digitization of public administration and the creation of digital services for users. COM (2016) 179 final; The "European Cloud Initiative-Building a competitive data and knowledge economy in Europe"-aimed at creating a European economy based on the exchange of data and information through the use of technologies such as cloud computing. Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. COM(2016) 178 final.

[28]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) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1-88.

[29]Regulation (EU) 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/EC (General Data Protection Regulation).

[30]Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89-131. For further details see: M.M. Caruana, The reform at the EU data protection framework in the context of the police and criminal justice sector: Harmonisation, scope, oversight and enforcement, in International Review of Law, Computers and Technology, 31, 2017.

the growth of modern advanced societies worldwide; on the other the necessity that such evolution does not compromise the core of the fundamental rights recognized to the individual that are expression and legitimation of the European constitutional traditions.

As the matter of fact for the Union to be able adopt the Data Protection Directive on Police Matters it should be in accordance with the principles of subsidiarity and proportionality. The European Union may adopt measures in accordance with the principle of subsidiarity as set out in the TEU. The EU Institutions acts must be appropriate for attaining the pursued legitimate objectives and do not exceed the limits of what is necessary and appropriate to achieve those objectives. The principle establishes two tests: the test of suitability and the test of necessity. The first measures whether the mean being used is suitable to reach the pursued ends. The second measures the competing interests: the consequences of restrictions, the right to legal protection, and if the consequences can be justified. The new Directive does not go beyond the principle of proportionality. The Directive´s objectives (the protection of the natural persons´ fundamental rights and freedoms and their right to the protection of personal data and to ensure the free exchange of that data by competent authorities within the EU) can be more sufficiently achieved at the Union level.

4.Regulation (UE) 2016/679.

The General Data Protection Regulation (GDPR), approved by the European Parliament and the Council on 27 April 2016 and became

operational in all the Member States from 25 May 2018[31], adopts a series of fundamental principles that were already at the basis of the previous framework of discipline in matter founded on the Directive 95/46/CE[32].

In particular, the text, consisting of 99 articles and 173 recitals, immediately assigns the dignity of fundamental right to the protection of personal data, transferring the result of the long process of recognition of this protection claim to the new regulatory framework that is at European level. its most complete realization in art. 8 (1) of the CFREU[33] and in art. 16 (1) of the Treaty on Functioning of the European Union (TFEU)[34]. By virtue of its autonomous nature and the

[31]Directive (EU) 2016/680 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 by the competent authorities for the purposes of prevention, investigation, detection and prosecution of offenses or implementation of criminal sanctions and the free movement of such data and repealing Council Framework Decision 2008/977/JHA with the aim of replacing the Framework Decision 977/2008/EC on the protection of personal data exchanged by police authorities and justice. The Directive, published in the Official Journal of the European Union together with the Regulation and in force since 5 May 2016, has been the subject of transposition in the 2016-2018 biennium by all Member States.

[32]G. Buttarelli, The EU GDPR as a clarion call for a new global digital gold standard, in International Data Privacy Law, 2, 2016.

[33]Proclaimed by the Parliament, the Council and the European Commission in Nice on 7 December 2000, the Charter, following amendments and adaptations, was submitted to a new proclamation on 12 December 2007 in Strasbourg. Under the first subparagraph of Art. 6 (1) of the Treaty on European Union, the Charter proclaimed in 2007 has the same legal value as the Treaties.

[34]R. Bieber, F. Maiani, Précis de droit européen, ed. Stämpfli, Bern, 2011. C. Blumann, L. Dubouis, Droit institutionnel de l'Union européenne, LexisNexis, Paris, 2013, pp. 478ss. C. Boutayeb, Droit institutionnel de l'Union européenne: Institutions, Ordre juridique et Contentieux, LGDJ, Paris, 2014, pp. 119-125. J.L. Clergerie, A. Gruber, P. Rambau, L'Union européenne, ed. Dalloz, Paris, 2014, pp. 543-545. M. Dony, Droit de l'Union européenne, Bruxelles, Editions de l'Université de Bruxelles, 2014. J.C. Gautron, Droit européen, Dalloz, Paris, 2012, pp. 24ss.

relevance of the relative guarantee within the company, this right, like the other subjective legal situations deserving of protection, is considered a non-absolute prerogative[35], requiring a suitable balance with the other fundamental rights recognized to European citizens, respecting the principle of proportionality[36].

In practice-of aid-the CJEU has also carried out an interpretative operation similar to that of a constitutional court as

[35]According to our opinion the necessary balance between the protection of personal data and other fundamental rights is explicitly stated in recital 4) of the Regulation. With the premise that treatment should be at the service of man, the text specifies that: "The right to protection of personal data is not an absolute prerogative, but must be considered in the light of its social function and must be reconciled with other rights fundamental principles, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognized by the Charter, enshrined in the Treaties, in particular respect for private and family life, domicile and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom of enterprise, the right to an effective appeal and an impartial judge, as well as cultural, religious and linguistic diversity. This system highlights the European legislator's conviction that the challenges deriving from the new digital age can not be fully sustained by the subject who transfers data, "overloading" the moment of consensus with meaning and effectiveness. The process of volitional formation of the individual that is expressed with the assent to the treatment is an indispensable condition, but, in the age of big data, absolutely not enough. It is necessary that those who use other people's personal information, having the necessary technical and organizational skills, behave consciously and actively projected to protect their users, while inspiring the entire treatment, from the time of acquisition of information to its conservation, to principles of personal data protection.

[36]P. Cardonnel, A. Rosas, N. Wahl, Constitutionalising the EU judicial system. Essays in honour of Pernilla Lindh, Oxford University Press, Oxford, 2012, pp. 292ss. S. Peers, T. Hervey, J. Kenner, A. Ward, The EU Charter of Fundamental rights: A commentary, Oxford University Press, Oxford, 2014, pp. 1414ss. H. Von Der Groeben, J. Schwarze, A. Hatje, Europäisches Unionsrecht, ed. Nomos, Baden-Baden, 2015, pp. 820ss. K. Stern, M. Sachs, Europäische Grundrecht Charta, ed. C.H. Beck, München, 2016, pp. 756ss.

völkerrechtsfreundlich?)[37], using judging techniques proper to the control of constitutionality and thus covering the role of ultimate guarantor of the proportionality of the rules not only compared to the European Court of Human Rights (ECtHR), but also to national constitutional courts. The CJEU has never limited itself to simply drawing inspiration from the jurisprudence of the ECtHR regarding the protection of personal data, but proceeded to incorporate it directly into its decisions. But this happened without the CJEU ever mentioning either the correspondence clause provided for by the Nice Charter to art. 52 par. 3[38] nor the clause on the level of protection pursuant to art. 53 of the CFREU[39], avoiding rather accurately to compare the

[37]M. Claes, M. De Visser, The Court of Justice as a Federal Constitutional Court: A comparative perspective, in E. Cloots et al., Federalism in the European Union, hart Publishing, Oxford & Oregon, Portland, 2012, pp. 84ss.

[38]According to our opinion: The question arises as to how this standard test for justification of limitations of fundamental rights sits with art. 52(1) CFREU which is indeed increasingly applied in cases governed by the Charter provisions. That article comprises a number of elements: the limitation must be provided by law; it must respect the essence of the right or freedom at stake; it must be justified either by an objective of general interest recognized by the Union or by the need to protect the rights and freedoms of others; and, finally, the principle of proportionality has to be respected. As to the grounds of general interest that may serve to limit art. 47 CFREU such as overriding considerations pertaining to the security of the EU or of its Member States when the disclosure of information is at issue or the existence of swift, effective and less costly dispute settlement or certain judicial proceedings, it would not seem that art. 52(1) brings about important changes compared to the pre-Charter regime. The same is true in relation to the proportionality test. For the analysis of the above article see: K. Lenaerts, Exploring the limits of the EU Charter of Fundamental Rights, in European Constitutional Law Review, 2012, pp. 375ss. N. Lazzerini, (Some of) the fundamental rights granted by the Charter may be a souce of obligations for private parties: AMS, in Common Market Law Review, 51 (4), 2014, pp. 908ss. J. Krommendijk, Principled silence or mere silence on principles? The role of the EU Charter's principles in the case law of the court of Justice, in European Constitutional Law Review, 11 (2), 2015, pp. 322ss.

[39]S. Greer, J. Gerards, R. Slowe, Human rights in the Council of Europe and the European Union. Achievements, trends and challenges, Cambridge University Press,

exemptions provided by the directive to justify interference in private life with the hypotheses provided by the ECHR. The CJEU goes so far as to recognize a direct effect on Directive's data protection provisions, so that citizens can invoke these forecasts directly in front of the national courts by paralyzing the application of internal rules contrary to the European Directive.

In speciem, the CJEU attempted to place the new CFREU art. 8 right into the previous case law, which had been marked by a connection between the EU´s personal data protection and the ECHR art. 8. The case C-92/09, *Schecke* and *Eifert o*f 9 November 2010[40] shows the CJEU willingness to begin ruling based on the CFREU while at the same time using the ECHR and the ECtHR´s case law. The CJEU stated that the TEU art. 6(1) gives the CFREU the same value as the Treaties. The validity of the rules in question had to be evaluated based on the Charter art. 8(1) gives everyone the right to the protection of personal data. The CJEU saw this right as closely connected to the CFREU art. 7 right to respect for private life. The Advocate General (in case *Schecke* and *Eifert*) considered in her opinion that: "(...) the two rights referred to in the case were the right to respect for private life by the ECHR Art. 8 and the right to data protection by Convention of Council of Europe,

Cambridge, 2018, pp. 80ss. E.A. Alkema, R. Van Der Hulle, Safeguard rules in the european legal order: The relationship between article 53 of the European Convention on Human Rights and article 53 of the Charter of the Fundamental Rights of the European Union, in Human Rights Law Journal, 15 (1), 2015, pp. 19ss.

[40]CJEU, joined cases C-92/09 and C-93/09, Schecke and Eifert of 9 November 2010, ECLI:EU:C:2010:662, I-11063, parr. 45-47. For further analysis see: O. Lynsky, The foundations of European Union data protection data, Oxford University Press, Oxford, 2015, pp. 64.

and that these rights were similar to the CFREU art. 7[41]. In the case called Scarlet[42] the CJEU for the first time made its main reference to CFREU art. 8. The Advocate General advised the CJEU to interpret the CFREU in the light of the ECHR. The ECHR art. 8 corresponds to the CFREU art. 7 and 8 and the ECHR art. 10 corresponds to the CFREU art. 11[43]. The CFREU rights need to be interpreted similarly with the ECHR. The CJEU prioritized the CFREU to interpret the EU data protection laws. It linked them to both the right to protection of personal data and the right to respect for private life and not only to the right to the protection of personal data. The CJEU focused on the fact that the question was about protection of the right to intellectual property and this right´s protection must be balanced against other fundamental rights. The system for filtering and blocking electronic communications might violate the customer´s rights to protection of their personal data and freedom to receive or impart information protected by the CFREU. In 2011 at the case C-543/09, *Deutsche Telekom*[44], the CJEU claimed for the first time that the purpose is to ensure the right to protection of personal data. The CJEU stated that the e-Privacy Directive clarifies

[41]Opinion of Advocate General Sharpston on case C-92/09 and C-93/09, Schecke and Eifert of 17 June 2010, ECLI:EU:C:2010:353, I-11063 par. 71. E. Costa, Consent in european data protection law, Martinus Nijhoff Publishers, Boston & Leiden, 2013, pp. 184ss. G.G. Fuster, The emergence of personal data protection as a fundamental right of the EU, ed. Springer, Berlin, 2014. T. Marsden, Internet co-regulation european law. Regulatory governance and legitimacy in cyberspace, Cambridge University Press, Cambridge, 2011, pp. 239ss.

[42]CJEU, C-70/10, Scarlet of 24 November 2011, ECLI:EU:C:2011:771, I-11959.

[43]CJEU, C-70/10, Opinion of Advocate General Cruz Villalón in case Scarlet of 14 April 2011, ECLI:EU:C.2011:255, parr. 30-34.

[44]CJEU, C-543/09, Deutsche Telekom of 5 May 2011, ECLI:EU:C:2011:279, I-03441. P. Cardonnel, A. Rosas, N. Wahl, (eds) Constitutionalising the EU judicial system: Essays in honour of Pernilla Lindh, op. cit., pp. 105ss.

and supplements the data protection protection. The CFREU art. 8(2) allows the processing of personal data if conditions are met (fairly, for specified purposes and based on the consent of the person concerned, or another legitimate basis). Then in October 2012 the CJEU turned more towards the Union´s own legislation. In the CJEU case C-614/10, *European Commission v. Austria* of 16.10.2012, the question was about the independence of an Austrian data protection authority. The CJEU found that processing of personal data has to be subjected to control by an independent authority and this is based on the primary law of the EU, the CFREU art. 8(3) and the TFEU art. 16(2).

Once the protection of personal data has been reiterated as a fundamental right, the new regulatory framework proceeds to implement it following a double directive: on the one hand, it widens and strengthens the tools made available to the individual to guarantee his own protection claim; on the other hand, it initiates a process of profound responsibility for the data controllers (accountability)[45], drawing an articulated and complex system of obligations to be guaranteed throughout the supply chain of personal data[46].

5.The individual in front of the new panorama of personal data protection.

[45]J. Lindquist, New challenges to personal data processing agreements is the GDPR fit to deal with contract, accountability and liability in a world of the internet of things?, in International Journal of Law and Information Technology, 26 (1), 2018, pp. 47ss.

[46]N.G. De Andrade, Right to personal identity: The challenges of ambient intelligence and the need for a new legal conceptualization, in S. Gutwirth (eds), Privacy and data protection. An element of choice, ed. Springer, Berlin, 2011, pp. 67ss.

Directive 95/46/EU has granted the individual a wider margin of action and a more extensive system of instruments of protection that are regulated in Chapter III entirely dedicated to these subjects.

This decision is justified in light of the objective of giving back to European citizens the power to control their personal data in the incessant flow of information in the new digital age[47], so that consent to treatment is the final expression of a process of training the will absolutely conscious, informed and free from all sorts of external conditioning that can alter the authenticity of its will. To this end, the European legislator has expanded, through art. 13, the set of information that the holder, or in the case of the manager, is obliged to provide to the user, establishing, moreover, that they must be transmitted in a concise, transparent, intelligible and easily accessible manner, with particular attention to the case in which the recipients are minors. In addition, the information transmitted to the interested party must indicate the data controller and the purposes pursued, as well as contain an appropriate specification of the period for the retention of data and the criteria used to define the duration.

[47]This objective is explained in recital 4) of the 2016/679 European Regulation and has been the guiding thread of the debate that preceded the implementation of the reform on the protection of personal data. On this point, read the proposal for a Regulation of the European Parliament and of the Council concerning the protection of individuals with regard to the processing of personal data and the free movement of such data (General Data Protection Regulation)/COM/2012/011 final-2012/0011 (COD) and among others the press release of the European Commission of 25 January 2012 "Data protection reform in the EU-More protection for individuals, less costs for businesses".

To strengthen this area, the forecast according to which in the event of access exercise is also implemented on the part of the interested party referred to in art. 15, information on the data collected and the methods of processing must be provided promptly and, in any case, at the latest within one month. In case of delay due to the number or complexity of the requests received, the holder is obliged to justify its causes and to inform the subject of the possibility of making a complaint to the competent supervisory authority and to propose a judicial appeal. A more detailed regulation is also envisaged for the exercise of the rights of opposition[48] and of

[48]The European Regulation introduces some changes and at the same time refines the content of the right to object with respect to what was previously governed by Artt. 14 and 15 of Directive 95/46/EC. Firstly, in light of the technological evolution occurred, it extends its exercise in a specific and direct way also to the scope of the personal data profiling activities and provides for the user the possibility to oppose the treatment even through automated means in the case of information society services. Furthermore, like the directive, the Regulation in art. 21 recognizes the interested party the right to oppose in the event that the treatment is necessary for the execution of a task in the public interest or is connected to the exercise of public authority to which the data controller is invested or is necessary for the prosecution legitimate interest of the owner or third parties. However, unlike in the past, the legislator seems to have introduced a double limitation in this context. First of all, by eliminating the term "at least" before the indication of the cases just described, it seems to have limited the scope of this right solely to such situations, without allowing the interested party further margins of action, if not for treatments aimed at direct marketing to pursuant to art. 21, par. 2. Furthermore, the Regulation introduces an important balancing criterion, establishing first that in the event of opposition to the holder, it is permissible to continue processing personal data if it is able to demonstrate the existence of binding legitimate reasons for proceeding with the processing which prevails over interests, on the rights and freedoms of the interested party or for the establishment, exercise or defense of a right in court. Furthermore, where personal data are processed for scientific or historical research purposes or for statistical purposes in accordance with Art. 89 (1), the data subject shall have the right to object to the processing of personal data for reasons connected with his particular situation. concerning him, except in cases where the activity is necessary for the execution of a task of public interest.

rectification[49], to which is added the provision, for the first time, of the right to data portability[50].

European Regulation (216/679), instead, dedicates a specific article to this right, art. 16, placing on the holder of the treatment the specific charge to fulfill this request without unjustified delay. Furthermore, pursuant to art. 19, the same is required "to communicate to each of the recipients to whom personal data have been transmitted, any corrections or cancellations or limitations of processing carried out in accordance with art. 16, art. 17, par. 1, and art. 18, unless this proves impossible or involves a disproportionate effort "and" to communicate to the interested party those recipients if the person requesting it"[51].

The most significant change introduced by the Regulation within the rights of the data subject is, however, represented by the recognition of

[49]Although Directive 95/46/EC recognizes the right to rectify data, it delimits the related exercise to the scope of the right of access, at the request of the interested parties in the case of incomplete information, inaccurate or stored in a way incompatible with legitimate purposes pursued by the controller in accordance with art. 12, lett. b).

[50]The recognition of the right to portability is one of the big news expected by the European legislator within the new regulatory framework. Sanctioned by the art. 20, this positive legal situation aims to pursue the objective, repeatedly declared, of guaranteeing the subjects concerned to regain full control of their personal data. In order to allow not only to "follow the path" realized by their own information, but also to determine what new paths to take, the Regulation recognizes the right for each interested to obtain "in a structured format, commonly used and readable by automatic device the personal data concerning him/her provided to a data controller and has the right to transmit this data to another data controller without impediments by the data controller who supplied them".

[51]J. Lindquist, New challenges to personal data processing agreements is the GDPR fit to deal with contract, accountability and liability in a world of the internet of things?, op. cit.

the so-called right to be forgotten[52]. Pursuant to art. 17 and recitals 65), 66) and 156), the subject has the possibility to request that their personal data be deleted and no longer subjected to treatment in case they are no longer necessary for the purposes for which they were collected; have been unlawfully treated or in the case of withdrawal of consent or exercise of the right to object. This provision is inserted in the wake of the long jurisprudential and doctrinal debate that has affected the european law in recent years about the need to ensure adequate protection of the identity of those affected by the risks arising from the phenomena of technological convergence and digitalization that make tends to "immortal" the data once it has been entered in the internet circuit[53]. The goal is to preserve the normal evolution of individuals

[52]As is known, the term right to be forgotten means the right interest of every person not to remain indeterminately exposed to further damage that brings to its honor and its reputation the repeated publication of a previously legitimately disclosed news. In particular, reference is made to the right of an individual not to see his current image distorted due to a new diffusion of news related to events or affirmations that in the past have seen him as protagonist, but which no longer correspond to the one that it is the real projection of one's own identity within society. On the characteristics of the right to be forgotten. See, L.X. Rano, La force du droit à l'oubli, in Mèmoire de D.E.A.Informatique et Droit 2003-2004.

[53]The recognition of this right at European level over the years has been rather complex and complex until the ruling of the CJEU in case: C-131/12, Google Inc./Agencia Española de Protección de Datos, Mario Costeja González of 13 May 2014, ECLI:EU:C:2014:317, published in electronic reports of cases.. The ruling has taken on particular importance as for the first time it has been recognized in the hosting providers' direct involvement in the management of personal data of its users, overcoming the now consolidated idea of a substantial irresponsibility related to the impossibility concrete to exercise direct control over the same data. In particular, the Court has argued that the activity usually carried out by search engines, consisting precisely in an activity of searching for information published or posted by third parties on the Internet, of automatic indexing, temporary storage and making available of users according to a particular order of preference, should be qualified as "processing of personal data", pursuant to the then current art. 2, letter b) of Directive 95/46/EC. In light of this reconstruction, the CJEU has arrived-and this is the crux of the sentence-to identify a real obligation for search engines to suppress on request,

with respect to the digital projection of their personal identity; a process that, as is now known, is inevitably misrepresented by the a-temporal nature of the network. Again with respect to right to be forgotten[54], the Regulation has also incorporated the related limits, in order to guarantee a fair balance between protection of personal identity and other fundamental rights. It is in this sense that the derogations provided for in paragraph 3 of art. 17, where it is established that the right to be forgotten[55] does not apply when the treatment is necessary for the exercise of the right to freedom of expression and information; for the

from the list of results, the links that lead to pages web published by third parties and containing information relating to the person "object of research" in the event that the information in question causes prejudice to the interested party. In this regard, the Court has held that this right prevails "in principle, not only on the economic interest of the search engine operator, but also on the interest of that public in accessing the aforementioned information during a research concerning the name of this person". The "Google Spain" ruling paved the way for the first and true recognition of the right to be forgotten by the European legislator in the field of personal data protection with the provision, as highlighted, of art. 17 dedicated to it within the 2016/679 Regulation. See in argument: S. Kulk, F. Zuiderveen Borgesius, Google Spain v. Gonzàlez: Did the court forget about freedom of expression? Case C-131/12 Google Spain Sl. And google Inc v. Agencia Espaňola de protecciòn de datos and Mario Costeja Gonzàlez, in European Journal of Risk Regulation, 5 (3), 2014, pp. 390ss. R. Polčák, B. Dan Jerker Suantesson, Information sovereignty: Data privacy, sovereign powers and the rule of law, Edward Elgar Publishers, Cheltenham, 2017. M. Arming, F. Moons, J. Schefzig, Vergiss, Europa! Ein Kommentar zu EuGH Urt. v. 13.5.2014-case C-131/12-Google/Mario Costeja Gonzàlez, CR 2014, 460, in Computer und Recht, 30 (7), 2014.

[54]E. Frantziou, Further developments in the right to be forgotten: The European Court of Justice's judgment in Case C-131/12, Google Spain, SL, Google Inc v. Agencia Espanola de Proteccion de Datos, in Human Rights Law Review, 14 (4), 2014, pp. 762ss. D. Mcgoldrick, Developments in the right to be forgotten, in Human Rights Law Review, 13 (3), 2013, pp. 762ss.

[55]D. Hoffman, P. Bruening, S. Carter, The right to obscurity: How we can implement the Google Spain decision, in North Carolina Journal of Law & Technology, 17, 2016, pp. 440ss. J. Rosen, The right to be forgotten, in Stanford Law Review, 88, 2012, pp. 92ss. J. Ausloos, The right to be forgotten worth remembering?, in Computer Law & Security Review, 28, 2012, pp. 144ss.

fulfillment of a legal obligation; for reasons of public interest in the health sector; for the exercise or defense of a right in court or for purposes of archiving, in the public interest, of scientific or historical research or for statistical purposes.

6.The risk based approach between rules and processing of personal data.

The real heart of the new legislation on the protection of personal data is undoubtedly represented by the system of obligations placed on the subjects who collect, process and use such valuable information. It is at this point that the change of perspective of the European legislator emerges in favor of a new and, above all, hoped attitude of overall "respect" of the owners towards the use of the personal data of others.

This is the so-called risk based approach which is at the basis of the entire european Regulation and which shifts the focus of attention from the weak part of the relationship to the holder of data collection and use, with the consideration that respect for the sphere of intimacy of individuals can not be fully realized unless there is a full and conscious assumption of responsibility on the part of those who exploit this information for their own benefit. The subjects who are variously involved in the data supply chain are required to abandon the attitude of passive adaptation to the rules that characterized them in the previous regulatory framework, in order to adopt a proactive approach aimed at protecting individuals. This change of perspective is fully realized in

the articulated system of rules that emerges from the reading of Chapter IV dedicated to the owners and managers of the treatment.

The first important element is certainly represented by the forecast in the new regulatory framework of the principles known as privacy by default and privacy by design. Art. 25, entitled "Data protection from design and protection by default", establishes, in fact, that "taking into account the nature, state of the art and implementation costs as well as the nature, scope of application, context and purpose of treatment"[56], the holder must take all appropriate technical and organizational measures to ensure that the activity is fully disclosed in compliance with the rules on privacy. The inspiring idea of this rule is to ensure that data protection becomes the common thread of the whole activity, permeating the whole treatment, from the embryonic phase of conception and development, up to the phase of use of the collected data, whatever the technology or methodologies used. This principle translates into the implementation, for example, of techniques of minimization[57], pseudonymisation and encryption of personal data collected and deemed indispensable for the achievement of the purposes identified, as well as measures that limit the risks of loss,

[56]J. Lindquist, New challenges to personal data processing agreements is the GDPR fit to deal with contract, accountability and liability in a world of the internet of things?, op. cit.

[57]This provision imposes not only the specific delimitation and contextual communication to the interested parties of the various objectives pursued through the activity, but, in light of the provisions of art. 5, par. 1, lett. c) of Regulation 679/2016, also a more careful delineation by the owner of the minimum data necessary to achieve the same, in order to ensure that the "sacrifice" of the individual's identity is minimal compared to the result expected by both parties of the report.

alteration or access to unauthorized information[58]. Furthermore, the holder, pursuant to art. 24 of the Regulation in conjunction with the recitals n. 74), 76) and 77), not only must implement these measures, but also be able to demonstrate that they are sufficient and appropriate to ensure compliance of the treatment with the new discipline.

In this passage, the qualitative leap in terms of the protection of the subjects involved: establishing that privacy should forge the entire treatment in order to prevent the data from escaping the sphere of control of the interested party, these principles, if correctly implemented, aim to ensure that the actual use of information takes place exclusively from an explicit manifestation of the data subject's consent and that it is exclusively the latter that defines the desired level of intensity of exploitation of their personal information, providing assent to depending on the desired purpose[59].

Furthermore, again with a view to guaranteeing a proactive attitude on the part of the data controllers, the new regulatory framework, in

[58]The discipline dictated by art. 25 of the European Regulation is complemented by the content envisaged by recitals 24)-29) which define in a more detailed manner the techniques and measures to be implemented to ensure compliance with the principles of privacy by design and by default. However, these are non-exhaustive indications that, in light of the risk based approach, require a case-by-case evaluation by the owners and the data processors who take into account the nature, the technologies and the aims pursued. Further practical indications can also be found in the Guidelines dedicated to the principle of transparency. See, Article 29, Data protection working party, Guidelines on transparency under Regulation 2016/67, WP260, adopted from 29 November 2017.

[59]This aspect assumes particular importance in the extended panorama of social networks and associated applications in which often, by default, consent is modeled according to the opt-out principle according to which the active intervention of the interested party is necessary to no longer be subjected to a specific treatment of their personal data.

addition to establishing ex-ante intervention procedures, also regulates the procedures to be implemented in the event that a potentially capable of causing physical or immaterial damage to natural persons[60]. Art. 33, in fact, establishes that in the eventuality in which there is a violation of personal data (data breach)[61] the holder is held, within 72 hours from the moment in which it has come to knowledge and, in any case without unjustified delay, to inform the competent supervisory authority. Appropriate and prompt information must be given, as soon as possible, to the interested party, if the violation is such that it entails a high risk for the rights and freedoms of natural persons[62]. Finally, in order to

[60]In particular, the art. 40 provides for the possibility for associations and bodies representing the categories of data controllers to define in detail the methods by which to ensure compliance with the multiple rules of the Regulation, obviously taking into account the specificities of the sector of reference, as well as the specific needs of micro, small and medium-sized enterprises. The control of compliance with these codes will subsequently be entrusted to a specific body accredited by the competent control authority after assessing the possession of an adequate level of competence in the matter. With reference, instead, to the second aspect, the art. 42 recognizes and promotes the creation of certification mechanisms, seals or trademarks capable of proving the implementation of certain procedures or technical and organizational measures in compliance with the relevant regulatory framework. The legislator emphasizes, however, that these instruments do not exonerate the holder from the control interventions by the competent authorities and the possible provision of sanctions in case of violation of the rules of the Regulation. In these forecasts we read the will to achieve, after an inevitable phase of experimentation and settlement, a potential procedural uniformity at European level, through the selection and identification of best practices implemented by the owners united by similar purposes and the involvement of default of experts on the protection of personal data in the normal management and organization of treatments.

[61]L. Moerel, The long arm of EU data protection law: Does the data protection Directive apply to processing of personal data of EU citizens by websites worldwide?, in International Data Privacy Law, 1 (1), 2011, pp. 29ss. B. Koops, The trouble with European Data Protection Law, in International Data Privacy Law, 4, 2014, pp. 252ss.

[62]With reference to this fulfillment, however, the art. 34, par. 3 of the Regulation provides for an important exemption if the data controller demonstrates that, before the event, has adopted techniques that make the personal data non-decipherable by unauthorized parties or have been subsequently adopted measures able to avert the

minimize the "data breach" cases, the european legislator has foreseen a further novelty, consisting of a specific impact assessment of the processing of personal data. Data protection impact assessment is one of the non-mandatory procedures-if not in specific cases[63]-for all data controllers, but whose implementation is strongly recommended[64]. More specifically, art. 35 provides that whenever the activity, "when it involves the use of new technologies", shows a high risk for the rights and freedoms of natural persons, the holder is required to perform a specific procedure aimed at to evaluate the impact of the treatment, taking into account the nature of the scope, the context and the intended purposes[65].

occurrence of the above risk. Moreover, in the event that this type of notice is too burdensome, the Regulation allows the holder to proceed with a public communication as long as the interested parties are informed appropriately and with the same effectiveness.

[63]According to art. 35, par. 3, the cases in which the impact assessment is required obligatorily concern the treatments whose object consists of: a) a systematic and comprehensive assessment of personal aspects concerning individuals, based on an automated treatment, including profiling, and on which decisions are founded that have legal effects or have a similar impact on such natural persons; b) a large-scale treatment of personal data belonging to the particular categories listed in art. 9 o data relating to criminal convictions and crimes pursuant to art. 10; c) a large-scale systematic surveillance of an area accessible to the public.

[64]See, Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 (WP 248), Guidelines on impact assessment on data protection and determination of the possibility that the treatment "may present a high risk" for the purposes of Regulation (EU) 2016/679), adopted on 4 April 2017 as amended and adopted by last 4 October 2017.

[65]As stated in the Guidelines drawn up by the WP29, the use of the expression "rights and freedoms" is justified by the belief that the processing of personal data, given the danger that lies behind an incautious realization of these activities, must be balanced not only with the pre-eminent rights to data protection and privacy, but also with the set of fundamental fundamental rights for a full and conscious evolution of the personality of the subject concerned, such as freedom of speech, freedom of thought, freedom of circulation and religious freedom. It is precisely from this assessment that

7.The “Cambridge Analytica” case.

With regard to the protection of personal data, 2018 will be remembered not only for the launch in the European landscape of a particularly stringent and innovative system of rules, but also as the year in which one of the most important incidents of violation of information never perpetuated came to light-or at least made known-in the internet age. With a timely "theatrical script", the two events inevitably came to intertwine and overlap, offering an extraordinary opportunity for reflection on the ability of the debut regulatory framework to respond adequately to increasingly insidious and changing challenges in an extremely dynamic context.

The story, known as "Cambridge Analytica" from the name of the company[66] accused of having unlawfully used the personal data of

the data controller should proceed backwards in identifying the existence or not of risks related to his activity and consequently assessing the need to carry out an impact assessment. See in argument: Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679. Furthermore, it should be stressed that impact assessment is a preventive control procedure for the protection of personal data. This means that in the event that the analysis confirms the presence of a high risk in the absence of adequate security measures, the holder is obliged, pursuant to art. 36, to consult the supervisory authority before proceeding with the treatment. The latter within a period of eight weeks, extendable up to six weeks, is required to provide a written opinion in which to assess the actions that the owner has planned to carry out to ensure compliance with the relevant legislation and propose, if necessary, further procedures to avoid the occurrence of the violation of personal data.

[66]Cambridge Analytica, founded in 2013, was a company specialized in collecting data from the use of social networks for the implementation of political profiles through the use of behavioral microtargeting techniques. Through the processing of this information, the company, in particular, proceeded to a combined analysis of the same and to the creation of predictive models to be used during election campaigns. Following the accusation of illegitimately using millions of personal data due to the

millions of users of the social network Facebook, originated in 2015 following the start of a collaboration between the platform and the developer of an application called "this is your digital life". Like thousands of other apps and websites that daily take advantage of the platform to offer a variety of different services, even this unique application allowed users to take advantage of their products using simply the same access credentials of the platform. In exchange, thanks to a consensus issued by users often superficially, collected all the information shared and the activities performed by the user on their bulletin board with the stated purpose to establish the profile and psychological prediction of the related future behaviors, accomplices also conditions of use of the most permissive platform[67], the app was able not only to collect heterogeneous information about those who had voluntarily decided to use the services, but also to view the boards of the so-called "friends", who were therefore "robbed" of their personal data in a completely unaware, not having expressed any consent in this regard.

Facebook's failure to foresee a limit to the process of extrapolating information from third parties, indirectly and especially involuntarily involved in processing, has created a crack in the platform's operating

absence of the explicit consent of the subjects involved, the company ceased its activities. Furthermore, on 2 May 2018 declared that he had initiated insolvency proceedings in the United Kingdom and, in parallel, bankruptcy in the United States.

[67]Until 2015, when the conditions of use of the platform have become increasingly restrictive, Facebook allowed these apps to obtain, with the simple consent of the user who decided to download the application, not only the multiple information present on one's own profile, but also those that can be derived directly and indirectly from the profiles of all the "friends" of the interested subject.

system. A treasure that has pushed the developer to sell, in violation of the agreements previously taken with the social network, such valuable data to "Cambridge Analytica", a company that used personal information to perform profiling activities of a political nature. Behind the use of an application with an apparent playful nature, therefore, one of the most serious violations of personal data in the recent history of digital technologies has materialized, bringing to light the fragility of the current data protection system and the high risks connected to an improper use of personal information[68], the story offers the extraordinary opportunity to evaluate the effectiveness of the debut European regulatory framework by applying it to a concrete and complex case such as the one that involved the social network Facebook.

To this end, the analysis will be conducted by comparing the conditions of use of the platform, a subject in these days of a deep and complex revision work in the light of the new GDPR[69], in force at the time of the

[68]Following the spread of the "Cambridge Analytica" affair, Mark Zuckerberg, founding member and managing director of the social network Facebook, was heard on 10 and 11 April 2018 by the commissions gathered at the Senate and the United States House to illustrate the operation of the platform and provide more information and details about the "loss" of personal data stolen from more than 80 million profiles worldwide. The following month Zuckerberg was instead heard by the European Parliament on the same issue. Finally, the Article 29 Data Protection Working Party, the independent European working group which dealt with issues relating to personal data protection until 25 May 2018, now replaced pursuant to art. 68 of the European Regulation 2016/679 by the European Committee for the protection of personal data, confirmed the full collaboration with the activities initiated by the Facebook Contact Group established by the data protection authorities of Belgium, France, Germany, the Netherlands and Spain.

[69]Following the occurrence of the "Cambridge Analytica" affair and the concomitant application of the new European regulation on the protection of personal data, the

facts, in order to assess if the system of rules put in place by the new Regulation, if it had already been operational, could have avoided or at least curtailed what happened and identified whether there is still room for improvement in the new European regulatory framework.

8.Regulation (EU) n. 2016/679 and Regulation Bruxelles I-Bis: Coordination aspects and "problems" of jurisdiction.

Taking note of the Cambridge Analytica case we connect to Chapter VIII of the Regulation, which contains a two-stage protection mechanism, the first of which contemplates, pursuant to art. 77 of the Regulation, the right to complain about any infringement of the rights protected by the Regulation before a supervisory authority, to be identified alternatively in the authority of the Member State of habitual residence of the data owner or in the Member State where he carries out his work, or in the authority of the Member State in which the violation took place. The second stage, following the submission of a complaint to a national supervisory authority, contemplates, pursuant to art. 78 of the Regulation, the right to an effective judicial remedy against an unfavorable decision of the national supervisory authority. In view of the nature of such an authority and of the public function which it exercises, the Regulation necessarily provides that such appeals must arise before the courts of the Member State in which the supervisory

platform initiated a vast and profound reorganization and recalculation of the current conditions of use, of the legislation on data and community standards. These changes, still underway, seem to follow the categories and principles introduced by the European legislator within the new regulatory framework. The latest revision is dated 19 April 2018.

authority which issued the unfavorable decision is established. In cases where the owner of the personal data and the holder or the controller have respectively their habitual residence and place of establishment in different member countries, or the violation took place in a different member country-situations which are rendered undeniably more frequent by the increasingly widespread use of electronic means for the conclusion of the most various types of transactions, which involve the acquisition and processing of personal data of the users-they are frequently likely to pose the problems of determining the jurisdiction that they are typical of civil disputes of an international nature, these are the subject of an increasingly dense network of instruments adopted by the European Union in the field of judicial cooperation in civil matters.

Particular importance occupies in this area the Regulation (EU) no. 1215/2012 or "Bruxelles I-Bis"[70], concerning the discipline of

[70]Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, entry in force from 10 January 2015. See in argument: P.A. Nielsen, The new Brussels I Regulation, in Common Market Law Review, 50, 2013, pp. 503ss. P. Hay, Notes on the European Union's Brussels-I "Recast" Regulation, in The European Legal Forum, 2013, pp. 2ss. M. Pohl, Die Neufassung der EuGVVO-im Spannungsfeld zwischen Vertrauen und Kontrolle, in Praxis des Internationalen Privat-und Verfahrensrechts, 33, 2013, pp. 109ss. A. Nuyts, La refonte du règlement Bruxelles I, in Revue Critique de Droit International Privé, 85, 2013, pp. 3ss. I.P. Beraudo, Regards sur le nouveau Règlement Bruxelles I sur la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale, in Journal du Droit International, 2013, pp. 742ss. A. Staudinger, Schiedsspruch und Urteil mit vereinbarten Wortlaut, in Festschrift für Friedrich Graf von Westfalen, Dr. Otto Schmidt Verlag, Köln, 2010, pp. 662ss. V. Rijavec, W. Jelinek, W. Brehm, Die Erleichterung der Zwangsvollstreckung in Europa, ed. Nomos, Baden-Baden, 2012, pp. 214ss. G. Payan, Droit européen de l'exécution en matière civile et commerciale, ed. Bruylant, Bruxelles, 2012. B. Köhler, Dual-use contracts as

jurisdiction and the recognition and enforcement of judgments in civil and commercial matters. According to a general indication contained in the recital n. 147 of Preamble[71], it must be considered that the criteria established by the law in question are destined to prevail, by virtue of a criterion of specialty ratione materiae accepted by the Brussels I-Bis Regulation in its art. 67[72], on the general rules contained in the latter Regulation, which may be applied only to the extent that they are not incompatible with the special regulations.

The provision relating to the subjective cumulation pursuant to art. 8, par. 1 of the Brussels I-Bis Regulation[73]-the application of which may

consumer contracts and no attribution of consumer status of a third party to the proceedings under Brussels-I Regulation, in Praxis des Internationalen Privat-und Verfahrensrecht, 37 (6), 2017. J.P. Beraudo, Regards sur le nouveau règlement Bruxelles I sul la compètence judiciaire, la reconnaisssance et l'exècution des dècisions en matière civile et commerciale, op. cit., pp. 744ss. L. Grard, La communautarisation de "Bruxelles I", in Revue Gènèrale de Droit International Public, 118, 2013, pp. 530ss. P. Beaumont, M. Danon, K. Trimmings, B. Yüksel, Cross-border litigation in Europe, Hart Publishing, Oxford & Oregon, Portland, 2017.

[71]D. Liakopoulos, European integration and its relation with the jurisprudence of European Court of Human Rights and private international law of European Union, in Homa Publica. Revista Internacional de Direitos Humanos e Impresa, 2 (2), 2018, pp. 300ss.

[72]F. Gascòn-Inchausti, La reconnaissance et l'exécution des décisions dans le règlement Bruxelles I bis, in E. Guinchard (eds), Le nouveau règlement Bruxelles I bis. Règlement n° 1215/2012 du 12 décembre 2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale, ed. Larcier, Bruxelles, 2014, pp. 210ss.

[73]M.A. Rodrìguez Vàzquez, Una nueva fórmula para la supresión del exequátur en la reforma del reglamento Bruselas I, in Cuadernos de Derecho Transnacional, 6, 2014, pp. 330ss. J. Velàzquez Gardeta, La indefensión del demandado como excepción en el proceso civil internacional dentro de la Unión Europea, in J. Goizueta, M. Cienfuegos (eds.), La eficacia de los derechos fundamentales de la UE. Cuestiones avanzadas, Cizur Mayor, Thomson Reuters-Aranzadi, Madrid, 2014, pp. 216ss. R. Dammann, S. Milllet, L'action en revendication exercée au titre d'une clause de réserve de propriété relève-t-elle du champ d'application du règlement Bruxelles I?, in Revue Lamy Droit Civil, 7, 2010, pp. 32ss. C. Kessedjian, L'espace judiciaire civile et commercial européen: le règlement "Bruxelles I" refondu, in Revue Gènèrale de

benefit a more effective judicial protection of the data owner's rights, in the case, for example, in which he intends to act at the same time against several data controllers or controllers in different Member States before the courts of the Member State in which one of them is established-they can also operate with respect to the actions introduced by the data holders on the basis of the criteria set out in art. 79 of the Regulation on the protection of personal data[74]. At the time of admitting, with a view to contributing to the objective of offering the data controller a more effective judicial protection of their rights, the integration of, to say the truth, rather meager discipline in point of jurisdiction brought by the Regulation n. 2016/679 with certain procedural instruments, such as the attributive connection, offered by the ordinary discipline of jurisdiction in civil and commercial matters brought by the Brussels I-Bis Reg., *an eadem ratio* should allow the derogation from the jurisdiction criteria set by the Regulation n. 2016/679 to the extent that this works in favor of the owner of personal data. In these terms, it appears that the tacit extension provided for by art. 26 of the Brussels I-Bis Reg.[75],

Droit International Public, 117, 2013, pp. 546ss. C.H. Van Rhee, Harmonisation of civil procedure: An historical and comparative perspective, in X.E. Kramer, C.H. Van Rhee, Civil litigation in a globalizing World, T.M.C. Asser Press, The Hague, 2012, pp. 41ss.

[74]P. Franzina, Jurisdiction regarding claims for the infringement of privacy rights under the General Data Protection Regulation, in A. De Franceschi (ed.), European contract law and the digital single market. The implications of the digital revolution, ed. Intersentia, Cambridge, Antwerp, Portland, 2016, pp. 82ss. CJEU, C-133/11, Folien Fischer AG v. Ritrama s.p.a. of 25 October 2012, ECLI:EU:C:2012:664, published in electronic Reports of the cases, par. 41 ss.

[75]R. Money-Kryle, Legal standing in collective redress actions for breach of EU rights: Facilitating or frustrating common standards and access to justice? in B. Hes, M. Bergström, E. Storskrubb, EU civil justice: Current issues and future outlook, ed. Bloomsbury, 2016. S.A. De Vries, European Union and ECHR: Conflict or harmony?,

considering that the jurisdiction criteria contemplated by art. 79, par. 2, of Regulation n. 2016/679 apply only to the actions proposed by the owner of the data towards the owner or the controller, for which the possible acceptance by the latter of the jurisdiction of a judge of a Member State other than those covered by this. The last Regulation, which was seised by the data owner, would still benefit the latter, which would thus be exempted from having to introduce a new action before the courts of a different Member State. The norm of art. 3, par. 1 of the Regulation, in this regard, appears to incorporate the broad interpretation of the scope ratione personarum of the previous European regulations on the processing of personal data made by the CJEU in the *Google Spain* ruling, stating that the regulation contained in the Regulation it applies irrespective of whether the processing of data has materially taken place within the Union or not, it being sufficient that it is imputable to an establishment of the controller or responsible in the Union[76].

The alternative criterion constituted by the habitual residence of the data owner presents an undeniable assonance with the criterion of the center of the interests of the person claiming to be the victim of a privacy violation or other personality right, used by the CJEU in the

in Utrecht Law Review, 9, 2013, pp. 80ss. J. Meeusen, F. Van Overbeeke, L. Verhaert, The link between access to justice and european conflict of laws after Lisbon, much ado about nothing?, in Rabels Zeitschrift für ausländisches und internationales Privatrecht, 81, 2017.

[76]R. Polčàk, B. Dan Jerker Suantesson, Information sovereignty: Data privacy, sovereign powers and the rule of law, op. cit.

eDate[77] ruling concerning violations of these rights are committed through information published on Internet sites and localized to the place where the person claiming to be injured has his habitual residence, and proves apt to coincide with the judge of the place of the event in an action for damages from illicit fact. The option that art. 79, par. 2, of Regulation n. 2016/679 provides in favor of the court of the Member State of habitual residence of the data owner lends itself to the same objection that has been addressed to the forum of the center of interests of the person who claims to be the victim of a violation of privacy or other personal rights, contemplated by the Court of Justice in the interpretation of the special criterion today contained in art. 7, par. 2, of Regulation n. 1215/2012 accepted in the eDate ruling. This objection concerns the risk of unduly prejudicing, in favor of the person who claims to be injured, the equality of arms between the litigants, which is an integral part of the right to the fair trial protected by art. 6, par. 1, of the European Convention of Human Rights (ECHR) and, being the application, in one case or another, of an act of the European Union, by art. 47 of the CFREU[78]. Also the rules concerning the coordination

[77]CJEU, Joined cases C-509/09 and C-161/10, e-Date Advertising GmbH v. X, Martinez v. MGN Ltd of 25 October 2011, ECLI:EU:C:2011:685, I-10269. See also in the sense of considering applicable, with some temperaments, the solution accepted in the case eDate in the hypothesis in which to complain about an injury of honor or reputation as a result of news published on an Internet site is a legal entity and the action of this is mainly aimed at obtain the removal of the defamatory news from the host site, the conclusions of the Advocate General Bobek in case: C-194/16, Bolagsupplysningen OÜ c. Svensk Handel AB of 13 Kuly 2017, ECLI:EU:C:2017:554, published in electronic Reports of the cases.

[78]D. Liakopoulos, Interactions between European Court of Human Rights and private international law of European Union, in Cuadernos de Derecho Transnacional, 10 (1), 2018, pp. 252ss.

between parallel actions largely reflect, even in the absence, even in this case, of any express reference, the model offered by the rules concerning lis pendens and privative connection contained in Regulation no. 1215/2012 or "Bruxelles I-Bis", and already, except for some variations, in the previous Regulation n. 44/2001 or "Brussels I" and even earlier in the 1968 Brussels Convention. The same ratio does not seem to adequately justify the adoption of specific provisions in terms of coordination between parallel proceedings. These appear, at a closer examination, diverging in different aspects, revealing moreover a certain inaccuracy in the terms in which they are drafted, from the model offered by the provisions contained to the same end in the "Brussels I-Bis" Regulation, the essential core of the which, taken from the previous "Brussels I" Regulation, is included in corresponding terms also in other regulations adopted in various areas in the context of judicial cooperation in civil matters.

The Regulation itself, in art. 80, reserve in the trial to active bodies in the field of promotion of the protection of personal data, which may act both, pursuant to par. 1 of the law now summoned, on behalf of the data owner, both pursuant to par. 2 of the law itself, to protect a widespread interest in the regularity of the processing of personal data, regardless of a mandate received from the data owner, provided that the law of the Member State of the forum provides for it. Furthermore, it should be noted that, in the economy of the considered material, it is to be considered more likely that a need for coordination may arise between parallel proceedings concerning violations of the provisions of the Regulation under examination by a particular owner or controller,

which, if it follows the methods for processing data that are not compatible with the provisions of the Regulation, is likely to reiterate the same violations against a plurality of personal data holders, rather than between actions proposed by the same data owner in respect of different owners or controllers, given that, where actions of the latter type refer to the same treatment attributable to several subjects as owners or managers, the remedy is, as already noted, for a verse offered to substantial level from the provisions of the Regulation and, on the other hand, to be sought ex ante and precisely in the mechanism of the subjective cumulation contemplated by art. 8, par. 1, of the "Brussels I-Bis" Regulation.

Finally, it can not fail to note that the inadequacy of the way in which in Regulation n. 2016/679 was coordinated the rules introduced by it in matters of jurisdiction and of relations between parallel proceedings with the discipline contained in this regard in the "Brussels I-Bis" Regulation is ultimately found to be hindering due to of the uncertainty in which these rules will be applied, the pursuit of the objective of ensuring that the owner of personal data will have effective judicial protection of the rights recognized by the Regulation itself, which the EU legislator has in fact intended to pursue accompanying the substantive regulation contained in the Regulation of specific jurisdiction rules for actions aimed at protecting the rights guaranteed by it.

9.Online sharing platforms and applicability of the European Regulation.

The extent of sharing and data collection has reached such high levels on a global scale that a decisive widening of the reference horizon of the effectiveness of the new rules on the subject is required. This requirement emerges clearly in the new regulatory framework and is fully satisfied by the joint action of art. 3 and recitals 22), 23) and 24).

Notwithstanding the fact that the new rules concern only personal data of natural persons, with reference to the territorial scope, in fact, the text specifies that the rules apply not only to cases in which the data controller or the controller is established in the Union, "regardless of whether or not the processing is carried out within European borders"[79], but also to all those activities involving personal data relating to persons in the Union and whose holder or manager is not be established in one of the European states. In this case, the treatments in question must relate not only to the supply of goods or to the provision of services to the aforementioned parties within the European territory, irrespective of the obligation of a payment of the interested party, also to monitoring their behavior in the case where it takes place in the Union. The Regulation with the art. 3, therefore, incorporating the orientation of the CJEU[80] and the Group. Art. 29 introduces an important element of

[79]J. Lindquist, New challenges to personal data processing agreements is the GDPR fit to deal with contract, accountability and liability in a world of the internet of things?, op. cit.

[80]In particular see form the CJEU: joined cases: C-141/12 and C-372/12, Y.S. and others of 17 July 2014, ECLI:EU:C:2014:2081; C-127/13 P, Strack v. Euuropean Commission of 2 October 2014, ECLI:EU:C:2014:2250; C-212/13, Ryneš of 11 December 2014, ECLI:EU:C:2014.2428; joined cases: C-446/12 and C-449/12, Willelms and others of 16 April 2015, ECLI:EU:C:2015:238; C-615/13 P, ClientEarth and PAN Europe v. EFSA of 16 July 2015, ECLI:EU:C:2015:489; C-580/13, Coty Germany of 16 July 2015, ECLI:EU:C:2015:485; C-201/14, Bara and others of 1st

rupture with respect to the past through the enlargement of the principle of establishment that dominated the previous legislation on the matter[81].

October 2015, ECLI:EU:C:2015:638; C-434/16, Novak of 9 February 2018, ECLI:EU:C:2018:994; joined cases: C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and others of 8 April 2014, ECLI:EU:C:2014:238, all the above cases are published in electronic Reports of the cases. For further analysis see also: P. Craig, G. De Bùrca (eds.), The evolution of EU Law, Oxford University Press, Oxford, 2011. P. Craig, European Union administrative law, Oxford University Press, Oxford, 2018. S. Weatherill, Law and values in the European Union, Oxford University Press, Oxford, 2016, pp. 151ss.

[81]The determination of the territorial scope of application of the Directive n. 95/46/CE essentially revolved around the traditional principle of establishment. Pursuant to art. 4, par. 1, lett. (a) the national provisions transposing the Directive operated in the event of processing carried out "in the context of the activities of an establishment of the controller in the territory of the Member State". In this sense, the applicability of the regulatory framework depended on the performance of an activity carried out by a company permanently present in one of the European states. In the case of non-European subjects, the rules operated only if the manager had "automated or non-automated tools located in the territory of that Member State". With the extraordinary increase in the use of the Internet and, above all, of the social networks that of the a-territoriality make their strength, this approach in view of an effective protection of personal data has gradually become less and less efficient. In fact, from the field of application of the law, the great extra-European giants that for years dominate the world panorama of the communications market have escaped. Supported by the opinion n. 8/2010 of Article 29 Working Group and the judgments "Google Spain" and "Weltimmo" both oriented to an extension of the applicability of European standards beyond the principle of establishment, the European legislator has expanded the scope of effectiveness of the new legislation, specifically declaring in recital 23) that this choice is aimed at preventing a natural person from being deprived of the protection to which he is entitled whenever the treatment is carried out by an entity not established by the Union and connects to the offer of goods or services regardless of whether there is a related payment or to monitor the behavior of interested parties in the Union. Furthermore, he underlines that the Regulation clarifies that the notion of establishment affirming in recital 22) that it "implies the actual and actual performance of activities within the framework of a stable organization. In this regard, the legal form taken, whether it is a branch or a branch with legal personality, is not decisive". The CJEU's failure to refer to the ECHR in Google suggests that its judgment is premised on a fundamental assumption that recognising a right to be forgotten necessarily affords a higher level of protection for human rights altogether than the ECHR minimum threshold requires. However, as noted above, the CJEU failure both to define the reach of the obligations enshrined in artt. 7 and 8 of the CFREU and, where need be, to balance them with the need to protect art. 11 of the

The legislator has come to delimit the "european" area of personal data protection that does not bend to the logic of the incessant flow of information, but which is completely dedicated to european citizens regardless of where data processing is physically executed. The application of the rules, in fact, overflows the national boundaries, legitimized by the a-territorial character of the Internet, and finds full justification in the ultimate aim of protecting the personal identity of individual users.

To strengthen the applicability of the new Regulation, in particular, the Facebook platform then provides the forecast, also taken from the recital 23), according to which the assessment must also take into account the intended use of the company's assets and services "regardless of whether there is a related payment"[82]. In this case, the reference to the functioning of the large social networks is evident, and

CFREU, means that that assumption remains, for the time being, unsubstantiated. According to our opinion the CJEU can be criticised for a manifest disregard of the important fundamental rights issues regarding the right to be forgotten noted above, which have not only been previously discussed in the European Court of Human Rights (ECtHR) context, but were also clearly presented to the CJEU. See in argument also from the CJEU the case: C-131/12, "Google Spain", Google Inc./Agencia Española de Protección de Datos, (AEPD) and Mario Costeja González", op. cit., and case C-230/14, Weltimmo of 1st October 2015, ECLI:EU:C.2015:634. See in particular: P. Voigt, A. Von Dem Bussche, The European Union General Data Protection Regulation (GDPR): A practical guide, ed. Springer, Berlin, 2017, pp. 23ss. O. Lynskey, Control over personal data in a digital age: Google Spain v. AEPD and Mario Costeja Gonzalez, in Modern Law Review, 78 (3), 2015, pp. 522-534. D. Svantesson, The CJEU's Weltimmo data privacy ruling: Lost in the data privacy turmoil, yet so very important case C-230/14, Weltimmo, EU:C:2015:639, in Maastricht Journal of European and Comparative Law, 2, 2016, pp. 334ss.

[82]J. Lindquist, New challenges to personal data processing agreements is the GDPR fit to deal with contract, accountability and liability in a world of the internet of things?, op. cit.

above all the platform under analysis that make use of personal data by exploiting the apparent gratuity of the services provided.

The traceability of this platform and those that share a profiling activity with it can also be obtained from the reading of the recital 24) which states that "to establish whether a treatment activity is comparable to the control of the behavior of the person concerned, it is advisable to check whether the natural persons are tracked on the Internet, including any subsequent use of personal data processing techniques consisting in the profiling of the natural person, in particular for taking decisions concerning them or analyzing or predicting their preferences, behavior and personal positions"[83]. Therefore, the techniques of aggregation of personal data, if they fall within the typical activity of the owner, require the latter to be subject to the new regulatory framework[84].

10.The accountability model of the owner of the processing of personal data applied to the "Cambridge Analytica" affair.

A transfer made possible, according to the subjects involved, by the failure to implement adequate additional and subsequent control techniques with reference to the flow of data acquired from the commercial partners that operate and cooperate with the platform.

[83]J. Lindquist, New challenges to personal data processing agreements is the GDPR fit to deal with contract, accountability and liability in a world of the internet of things?, op. cit.

[84]Recital 23) of the GDPR considers that factors such as the use of a language or a currency normally used in one or more Member States, with the possibility of ordering goods and services in that other language, or the mention of customers or users in the European Union.

In this sense, the perpetuated violation can not be identified in the illegal use of data by the developer of the app, but in the subsequent transmission of the same to a third company whose primary activity, moreover, consists in profiling users to political ends. To further worsen the already serious situation, there was the decision of the Facebook CEO not to immediately inform the competent authorities of what happened, despite the violation was known from 2015, but to simply ask the political profiling society the destruction of information obtained illegally, without having further confirmation of it.

Under the full application of european Regulation, this failure to prompt communication would have itself integrated a serious violation of the legislation because in contrast to the system of general obligations expected of the data controller and, in particular, with the duty to notify the control authority pursuant to art. 33. The provision in question requires the subject to take action within 72 hours, and in any case without undue delay, specifying the nature of the violation, the categories of data involved and the presumed number of stakeholders, as well as describing the possible harmful consequences. In fact, timeliness is considered vital for the purpose of limiting the damages that potentially can fall on the subjects, as the delay in intervention risks to weaken the effectiveness of the remedies, exacerbating already extremely critical situations related to the loss of control over own personal data[85].

[85]As explicitly stated in recital 85) of the Regulation "a breach of personal data may, if not adequately and timely, cause physical, material or immaterial damage to natural

It is evident that with the failure to comply with this system of rules, that network of active cooperation between supervisory authorities and data controllers is being broken, the creation of which the Regulation considers crucial for the current protection of the personal identities of those concerned within an extremely changeable and complex landscape.

In addition to the violation of the aforementioned reporting obligations, in the case of application of the new regulatory framework, the art. 34, which, as is known, requires the owner to inform the interested parties in detail about the violation of their information[86].

In a framework of discipline strongly focused on the process of empowerment of the owners and at the same time on strengthening the control of the subjects on their personal data, however, the analysis finds its salient point not so much in the system of ex post remedies implemented by the social network; in the evaluation of the technical and organizational tools previously prepared in order to avoid the realization of such interference outside the private sphere of its users. The new European Regulation aims to stimulate a proactive attitude on

persons, for example loss of control of personal data concerning them or limitation their rights, discrimination, theft or misappropriation of identity, financial loss, unauthorized decryption of pseudonymisation, prejudice to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social damage to the individual concerned".

[86]Recital 7) of the Regulation identifies the creation of a climate of trust as one of the determining factors for the development of the digital economy throughout the European market. In particular, the European legislator observes that "natural persons should have control over their personal data and that legal and operational certainty is strengthened for both natural persons and economic operators and public authorities".

the part of all the owners, orienting them towards an organization of their activities that is completely oriented towards respect for privacy, intended as an inspiring principle able to concretely and completely permeate the entire supply chain of use of the data, from the moment of their collection to the final one of their conservation and elimination.

First of all, in a situation of full vigor of the new legislation, the social network, realizing "a systematic and global assessment of personal aspects related to natural persons, based on an automated treatment, including profiling, and on which decisions are based legal effects or have a similar impact on these natural persons "should have necessarily proceeded to an impact assessment of the treatment on fundamental rights pursuant to art. 35 paragraph 3, lett. a) of the Regulation with consequent documentation of all the technical and operational measures adopted in order to prevent situations of violation of the users' sphere of identity. Moreover, it is undoubted that the profiles that the social network realizes starting from data and sharing activities carried out by its users foresee the continuous use of new technologies, whose impact on the fundamental rights and freedoms of the people involved is not always predictable. The use of increasingly sophisticated techniques would have forced the platform, pursuant to art. 36, to consult the supervisory authority in order to identify the possible related risks and establish shared protection systems. Finally, the implementation of a treatment activity such as that carried out by Facebook, which by its very nature, scope and/or purpose, includes the regular and systematic monitoring of data subjects on a large scale and often also of sensitive

data categories according to art. 9, would inevitably also impose the appointment of a Data Protection Officer (DPO)[87].

In a regime of full application of the Regulation, the platform would have been recognized as not compliant with the new accountability system of the holder provided for in Chapter IV of the Regulation. This would have led to the immediate application of the most rigorous framework of sanctions introduced by the new regulation, with the provision pursuant to art. 83, paragraph 4 to which must be added any additional deterrent measures recognized to the supervisory authorities by art. 58.

11.The model of operation of the Facebook platform and the role of consensus between Regulation (EU) 2016/679.

[87]The data protection officer represents an absolute novelty within the personal data protection landscape since no such obligation is foreseen in the previous Directive 95/46/EC. Art. 37 of the Regulation provides that in the event that the processing is carried out by a public authority or a private entity whose main activity consists of a systematic and regular monitoring of large-scale subjects or provides for the collection of particular categories of personal data and of data relating to criminal convictions and offenses, the holders in question must be assisted by a professional who has specific knowledge of the legislation being analyzed. the appointment of the person responsible for personal data is one of the non-mandatory provisions established by the regulation, but also strongly recommended by the European legislator. In the work of strengthening the rules regarding the protection of personal data, the need to identify a support figure has been highlighted, which, thanks to its collaboration and technical-legal support, makes decisions regarding the protection of personal data. The identification of this figure connected to the respect of the aforementioned obligations, would have allowed the platform to realize a first and above all incisive network of controls supported by moments of sharing and support by the supervisory authorities, favoring the implementation of protection tools. ex ante evaluated in a double dimension, private on the one hand, public on the other, in a spirit of full cooperation in the interests of users.

The new European Regulation has been given the task of acting as a point of contact between the data controller and the competent authority, facilitating the mutual exchange of information and communications, as well as facilitating the necessary consultancy, investigation and control of the latter. On the one hand, the number and the delicacy of the tasks entrusted to him allow us to assert that in a short time this figure will assume a pivotal position in public and private companies. Pursuant to art. 38, in fact, the DPO must be "promptly and adequately involved (by the owner and the manager) in all matters concerning the protection of personal data". On the contrary, it seems possible to hypothesize that the ability of companies to fulfill the obligations established by the European Regulation and not be "overwhelmed" by the system of sanctions it provides will depend largely on the "expertise" of the person in charge of personal data; from the ability of these to identify and define a suitable system of technical and organizational measures appropriate to the activities carried out. An expertise, however, and this represents a significant point of reflection, not only technical, but inevitably also of a legal nature. The DPO, in fact, must be able to understand ex ante, from the planning of the activities, which data will be involved, classify them and in the case of personal data identify which risks could be related to their treatment. In light of this preventive assessment, it will then have to support the data controller in the choice of technical and organizational measures to be implemented to ensure compliance with the new rules and, in the mandatory cases envisaged by the new legislation, provide an opinion on the impact assessment previously described, supervising the correct

performance pursuant to art. 35. In addition, it will have to carry out a continuous activity of information, advice and guidance in relation not only to the holder, but also to the employees assigned to the treatment activity and to guarantee a thorough cooperation with the competent supervisory authority. Only in this way will it be possible to compare it appropriately with the modalities of explaining the will of the user expected at the time from the platform being analyzed and to evaluate in a comparative manner the effectiveness of the new regulatory framework.

The volitional act of the subject involved within the european Regulation constitutes one of the six alternative requirements on which the lawfulness of the processing ex art. 6[88], confirming the approach envisaged by the previous provisions on the matter. However, in a climate of growing attention to the subject's ability to consciously grant the use of their personal data, the role assigned to that moment is certainly strengthened.

Sinking its roots in the definition dictated by the previous Directive 95/46/EC enriched by the contributions made by the "opinion on the

[88]Pursuant to art. 6, in fact, the processing is considered lawful if at least one of the following conditions occurs: expression of consent by the interested party; processing is necessary for the execution of a contract or pre-contractual measures; it is necessary to fulfill a legal obligation; it is essential to safeguard the vital interests of the interested party or others; it is necessary to satisfy the public interest or to fulfill a public power; it is necessary for the pursuit of the legitimate interests of the data controller or of third parties, provided that the interests or the fundamental rights and freedoms of the data subject who require the protection of personal data do not prevail, especially if the data subject is a minor. On the lawfulness of the processing see, Article 29 Data Protection Working Party Guidelines on Consent under Regulation 2016/679, WP259, adopted from 28 November 2017.

definition of consent" adopted by WP29 on July 13, 2011[89], the consensus, in fact, re-emerges in the new regulatory landscape in an enhanced manner, thanks to the addition of the character of unequivocability alongside the previous connotations of freedom, specificity and information. This new qualification requires that the assent is manifested through an explicit statement or an unequivocal action, which leaves no doubt about the will of the person concerned to make available to the owner their personal data. It follows that the treatment activity can never start on the basis of a passive or omissive attitude of the subject, as often happens on the net with the provision of pre-selected boxes (opt-out), but requires a positive activity, aimed at witness the conscious approval of the same. Even more indicative in this sense is the extension of cases in which the legislator has imposed not only an expression of approval, endowed with the characteristics previously indicated, but also of an explication of the consensus marked by profiles of specificity. The explicit consent, in fact, in the new regulatory framework is required not only with reference to the processing of data belonging to particular categories sensitive data) as per art. 9, case already provided for in the previous directive, but also during the transfer to a third country or an international organization in the absence of adequate guarantees pursuant to art. 49, paragraph 1, lett. a) and in the particularly current case of automated decision-making processes[90], including profiling, governed by art. 22.

[89]Article 20, Working Party, Opinion 15/2011 on the definition of consent (WP187).
[90]The guidelines specify that, for the purposes of the Regulation, for the (entirely) automated decision-making process, this particular type of treatment must be

Justified by the more pronounced risk profiles of the situations in which it is required, therefore, explicit consent pushes the boundary of the awareness of the interested parties forward, requiring additional effort at the moment of manifestation of interest. In the silence of the Regulation, the Guidelines interpret this further commitment, when possible, in the realization of a written and signed approval by the interested party, or in the case of online platforms or sites, in filling out a specific form or in loading a personal document[91].

In order for the assent of the interested party to be explicit as a "manifestation of free will, specific, informed and unequivocal" pursuant to art. 4, n. 8 of the Regulation, it is essential that the activity is carried out in full compliance with the framework of the principles identified by the European legislator, identified in lawfulness, correctness and transparency, as well as adequacy, relevance, limitation to which is added the presence of specific, explicit and legitimate purposes. It is the contemporary action of such dimensions that, in fact, makes the treatment respectful of the new legislation.

Once the meaning of the consensus has been defined within the new regulatory framework and the principles legitimating the use of

understood, in which every decision is taken exclusively through technological tools, without any human involvement. In this sense, these processes constitute an autonomous and distinct activity from the profiling and not necessarily the two treatments operate simultaneously. See in argument: Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251), adopted from 3 October 2017 and updated 6 February 2018, pp. 8ss.

[91]Article 29 Working Party, Guidelines on consent under Regulation 2016/679 (WP259), adopted from 28 November 2017 and updated 10 April 2018, pp. 18ss.

personal information are identified, it is possible to analyze the model adopted by Facebook in order to make a comparison that allows to identify the critical issues that have characterized, and that for some aspects still characterize, the processing of personal data of users of the platform.

The conditions of use of the social network in force at the time of the "Cambridge Analytica" case, now the subject of a careful and profound change in the light of the new European Regulation, were divided into two separate documents called "Declaration of rights and of the responsibilities" and "Regulations on data"[92]. From the reading of the

[92]The "Regulations on data" updated to 29 September 2016 and the "Declaration of rights and responsibilities" of 31 January 2018 constituted the backbone of the rules applied by Facebook to guarantee the protection of personal data of its users before the entry into force of the European regulation and the occurrence of the "Cambridge Analytica" affair". In particular, the first document dictated the conditions of use of the platform, regulating the relationships between users, social networks and the brand complex, ancillary products and services, called "Facebook Services". The legislation on the data, however, was instead a document mainly illustrative in which information was provided about the type of data collected and the methods of use and sharing with partners, suppliers and third parties. These documents, which can be consulted up until a few days before the application of the GDPR, are no longer present on the platform. The new terms and conditions on privacy, updated to April 19, 2018, still provide a breakdown of the legislation between different documents, according to a logic that, in fact, does not differ much from the previous one. However, the impact of the new European discipline and the "Cambridge Analytica" affair is clearly visible. Beyond the reorganization of the entries of the conditions of use along the lines of the changes introduced by the European legislator, the legislation on data includes a section explicitly dedicated to the new European Regulation and named "How to exercise the rights provided by the GDPR?". Furthermore, the following note is particularly relevant, demonstrating that the platform's focus on these aspects is now inevitably very high: "we are working to further restrict access to developer data in order to prevent misuse. For example, we will remove developer access to your Facebook and Instagram data if you have not used their app for three months, and we are changing Facebook Login so that the next version will reduce the data that an app can request without sending the app for analysis, including only name, username and biography of Instagram, profile picture and e-mail address. To request more data, our approval will be mandatory".

two texts it was possible to extrapolate an articulated informative that, behind the apparent veil of clarity dictated by the simplicity of the terms used, concealed, however, a maze of rules little transparent and sometimes contradictory.

The first and important critical issues concerned-and still concern-the purpose for which the platform claimed to collect and use personal data and the level of transparency of the communication made in favor of the recipients of the service. It is undoubted, in fact, that the average user is convinced that Facebook uses their personal information to offer a platform that can connect people through the sharing of images, thoughts, photos and news of various kinds, in order to break down the distance that time and space inevitably tend to erect in the course of life. On the other hand, this is the idea that the social network still transmits scant to potential users in the initial page dedicated to new registrations. A goal, moreover, that was also reiterated in the section dedicated to "data law", where it was specified that the company's mission was to "make the world more open and connected" by allowing "people to share content". It is evident that this was a message of inevitable impact on customers, further strengthened by the affirmation of the perpetual free service.

However, borrowing two important terms from the line of business studies, the slogan "Give people the power to build community and bring the world closer together"[93], on closer inspection does not

[93]Declaration of Mark Zukerberg.

constitute the real mission of the company, but relates to its vision, that is to say to that set of values and principles that the platform declares to want to carry out in a prospective manner and which inspires all of its activity[94]. In other words, it represents the image that Facebook wants to communicate to the market, but not the way in which it aspires to achieve this goal.

For the purposes of evaluating the purposes of the treatment, on the other hand, the attention can not but dwell on what is usually called the corporate mission and in the system of strategic business objectives that consist in offering a wide range of communication services in a broader sense. in exchange for the use of personal data of users for profiling purposes.

The mission, less attractive than the corporate vision, but closer to the concrete reality, has remained deliberately for years in dim light, because it is able to reveal an "uncomfortable" aspect for potential customers, that is to say the absence of free service.

The exchange of utility-social services by the platform and information by users-in fact, was not immediately apparent from the documents made available, reinforcing the belief that most of the people using this platform are not aware of the engine underlying its operation. To confirm this hypothesis, there is also the assessment that in the

[94]G. Armstrong, P. Kotler, Marketing an introduction, ed. Pearson, London, 2016. P. Kotler, Marketing management, 15th edition, ed. Pearson, London, 2017. M. J. Baker, Marketing Strategy and Management, ed. Springer, London, 2000.

Statement of rights and responsibilities of Facebook[95], the use of data for purposes exceeding the simple use of the platform was "unveiled" only in art. 9, where for the first time the social network explicitly expressed its willingness to offer advertising and other commercial content or sponsored content and to this end stated that users using the platform actually accepted to authorize the use of their name, profile image and shared information[96]. Evidently the lack of explicit indication of the purpose underlying the collection and processing of personal data is in contrast with the principle of transparency pursuant to art. 5, lett. b), considered one of the cornerstones of the european Regulation[97]. Do not specify that the value of the service is represented

[95]M.A. Moreno, N. Goniu, P.S. Moreno, D. Diekema, Ethics of social media research. Common concerns and practical considerations, in Cyberpsychology, Behaviour and Social Network, 16 (9), 2013, pp. 709ss.

[96]In particular, in the document entitled "Declaration of rights and responsibilities" we read: "Our goal is to offer advertising and other commercial content or valuable content that is valuable to our users and advertisers. To this end, users accept the following: 1. Users provide Facebook with permission to use their name, profile picture, content and information in connection with commercial, sponsored or related content (e.g. favorite brands) published or supported by Facebook. This statement implies, for example, that the user allows a company or another entity to offer a cash compensation to Facebook to show the name and/or image of the user's Facebook profile with its contents or your information without receiving any compensation. If the user has selected a specific audience for their content or information, we will respect his choice at the time of use; 2. Facebook does not provide advertisers with the information or content of users without the consent of the latter".

[97]As indicated in recital 39) of the 2016/679 Regulation, the principle of transparency consists in the transmission of information regarding the processing of data that are easily and comprehensibly to recipients, characterized by a clear and simple language. Transparency also requires that such communications be complete with reference to the methods of processing and the related purposes in order to sensitize individuals to the risks that lie behind the incorrect and illegal use of their personal information. For further information see, Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, adopted from 29 September 2017 and modificated in 11 April 2018.

by the transfer of personal information, often of a sensitive nature because directly or indirectly capable of unveiling the personal and confidential aspects of the person, it means encouraging the deceptive belief that the platform is free, encouraging a rather casual use. On the contrary, the explicit indication of the existence of profiling purposes could have allowed a more conscious attitude on the part of users, explaining that behind the apparent gratuitousness of the service there is an intense active treatment of personal data, which has now become an exchange good of extraordinary value within the modern "hyper-connected" companies.

A slightly different situation was instead found in the platform data regulation that specified from the beginning the intent of the platform to collect personal information, even highlighting five macro-categories depending on the services used by the user. However, to this greater clarity about the type of data transferred did not correspond to an adequate transparency regarding the motivation for which they were and are still collected. The purpose of the treatment, in fact, was diluted in a multiplicity of distinct and separate objectives, considered all necessary and indispensable for the operation of the platform. This obviously in violation of the framework of the principles set forth in art. 5 of the Regulation, according to which the information to be collected requires a specific, explicit and legitimate purpose so that the user has the possibility to decide in a resolute and aware manner whether or not to provide his/her data. On the other hand, even if we wanted to bring these different needs within the scope of a single major objective represented by the proper functioning of the platform, it would not have

been possible to place two of the different purposes listed in particular: the guarantee of safety and protection accounts and creating personalized advertising ads. The request for information necessary to guarantee a safe and protected sharing space against external violations inevitably presents different connotations in terms of intended use and type of data to be processed compared to a request aimed at pursuing purely economic needs. Furthermore, it should be noted that the creation of commercial content of interest to the user implies a profiling activity to which the European regulation, due to the high risks associated with it, recognizes specific protection tools, including the specific right envisaged art. 22 in favor of the interested party to oppose decisions based solely on automated processing, including profiling, able to produce legal effects concerning him or to significantly affect his person.

The concentration of multiple different objectives was however evidently in contrast with what was outlined by the new European regulatory framework. In light of the "granularity" of the data and in line with the aim of ensuring continuous and above all conscious control by the interested party, the Regulation establishes that consent must not only be specific (art. 4), but case in which "the treatment has more finality, the consent (must) be given for all these" (recital 32)[98]. It is

[98]The term "granularity" refers to the multiform and plural nature of the data collected during the treatment activity. According to this interpretation, the control of personal data can only be carried out concretely if the data subject can express a granular consent, that is to say specific for one or more specific and distinct purposes. See in argument: Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, op. cit., p.10 ss.

only the concrete and effective possibility of choosing whether and for what purpose to grant personal data that the consent has the possibility to be fully realized as a "manifestation of free will, specific, informed and unequivocal"[99]. On the contrary, the multiplicity of ends in the absence of a targeted assent imprisoned the user's action, forced passively to accept or refuse to make their data available for multiple uses not specifically delineated, in clear contrast with the principle of centrality of the person underlying the current regulatory framework. Finally, the provision of a comprehensive consent valid for all the purposes highlighted prevented the user to exercise an explicit consent as required in the case of automated processing of data by art. 22.

12.Crisis in the conscious consensus model: The case of Facebook.

Section 2 of the "Declaration of rights and responsibilities" attributed, in fact, to the user the property "of all contents and information published on Facebook" recognizing the possibility of checking also the way in which they were shared. This is an idea that emerged several times in the conditions of use of the platform, but which fell into the reality of the social network was devoid of concreteness. It was enough, in fact, to continue reading the same section to find out that, in reference to the contents protected by the intellectual property right, the user, when deciding to use the platform, recognized to the same "a non-

INFORMATION COMMISSIONER'S OFFICE (ICO), Consultation: GDPR consent guidance, March 2017.

[99]J. Lindquist, New challenges to personal data processing agreements is the GDPR fit to deal with contract, accountability and liability in a world of the internet of things?, op. cit.

exclusive, transferable license, that (could) be granted as sub-license, royalty free and valid worldwide, which (allowed) use of content posted on Facebook or in connection with Facebook"[100].

Beyond the limited clarity of the textual data, the contradiction that was inherent in this part of the document is evident: in fact, the property of the loaded contents was first recognized to the user, creating the (false) conviction of actually controlling them, but shortly after this illusion came to the forefront of the recognition of an unspecified "license" that allowed the use-not specified in the type and mode-of the same by the platform.

Continuing reading, section 9 entitled "Information on advertising and other commercial content published or made available by Facebook" specified that with the use of the platform, the user also agreed to grant "permission to use (...) the name, profile picture, content and information in relation to commercial, sponsored or related content (eg favorite brands) published or supported by Facebook (...)"[101]. Immediately thereafter, in contradiction as indicated above, the platform was careful to point out that the transmission of such personal data to advertisers was subject to the consent of the interested parties,

[100]J. Lindquist, New challenges to personal data processing agreements is the GDPR fit to deal with contract, accountability and liability in a world of the internet of things?, op. cit.

[101]Proceeding in the reading, the following indication emerged: "This statement implies, for example, that the user allows a company or another entity to offer a cash compensation to Facebook to show the name and/or profile image of the user's Facebook with its contents or its information without receiving any compensation. If the user has selected a specific audience for their content or information, we will respect his choice at the time of use (...)".

but no indication was given about how the users could consciously express their explicit consent to this peculiar treatment of profiling character. Other criticalities emerged in the homologous section present in the document "Nor information on data". In this document, the platform declared to transmit to the companies that are part of the group[102], among which points out that there are other important social networks such as Whatsapp and Instagram, a range of personal information of extraordinary breadth that derived not only from the continuous monitoring of actions performed directly by the user, such as viewing certain contents, reading specific types of news or locating uploaded images or places visited, but also by moments of "contact" that connect the person concerned to third parties such as sharing photos, exchanging comments or content of various kinds[103].

Finally, further sharing of personal information was envisaged for customers, service providers and other partners who also support the company from the point of view of the technical infrastructure. In this case, the platform specified that these subjects should have respected the obligations of confidentiality without violating the regulations on

[102]In addition to these, an indefinite series of information acquired in an indirect way was added because they were provided by external partners who collaborate with the platform or transmitted by advertisers and related to the user's consumption behavior. For this type of additional processing of personal data, the possible combination of which could give rise to more complex and sensitive information, the platform not only did not provide specific forms of consent, but stated openly that their use would have followed the various conditions of use of new owners.

[103]It should be borne in mind that, as also underlined in the Guidelines, individual data collected separately if combined can give rise to more complex information of a sensitive nature whose treatment, due to the high risk profiles associated with it, can only be achieved if the requirements established by art. 9, paragraph 2.

data and the specific agreements stipulated between the parties, but it is evident that in the absence of detailed indications about the purposes pursued and the type of information shared, nor the content of the "specific agreements" between the parties, the generality of the forecast was clearly in contrast with the framework of principles that underlie the legitimate processing of data according to the European legislator. From what has been highlighted, then, the user was faced with a constellation of different and fragmented rules that effectively prevented an effective control of the path followed by his personal data, acquired and exploited by different subjects, for different purposes and too often not transparent.

But the peak of the complex and tangled model of the use of personal data of its users was certainly represented by the set of information that Facebook claimed to share with third-party applications and websites that use the services of the platform. At this point the analysis moves on a path, if possible, even more obscure and tortuous, which brings, at the end of the circle, to the story that started this study: the "Cambridge Analytica" case.

The passage of the personal data from the channel to the tendency-but not necessarily-safer of the platform to the variegated panorama of external services that constituted the most critical node of the whole model outlined by Facebook and that, in fact, triggered the "Cambridge Analytica" case. The platform has not been able to prevent particularly serious situations of harm and connected to the complete loss of control of the information of its users. No explicit consent has been provided

for this particular type of further processing that exceeds the stated purpose of the platform; nor have they been identified ad hoc control procedures aimed at ensuring continuous monitoring of the legitimate use of personal data. In other words, Facebook, underestimating the riskiness of its collection and processing of data, was deficient in the most delicate part of its model of consent. In the absence of even more stringent rules for the transfer of such data and procedures of manifestation of consent by the user structured in such a way as to guarantee the effective and conscious determination of the subject, the Facebook universe has created its "black hole" that has absorbed millions of personal information of a more or less sensitive nature, leaving them at the mercy of purely economic interests, with extremely serious consequences for the personal sphere of users and inadmissible for a democratic society also in its evolution digital type.

13.Limits and perspectives of the new legal framework on personal data protection in the light of the "Cambridge Analytica" case.

If Directive 95/46/CE focused the attention almost exclusively on the type of data collected and on the guarantee tools made available to the interested parties, the GDPR instead puts its accent on the responsibility of the data controller, based on the belief that protection can only start ab origin from the subject who decides to undertake, dictating the relative conditions and purposes, an activity of exploitation of such precious information. The accountability of the data controller is the "backbone" of the entire European Regulation: it is from this principle that all the regulatory innovations in the matter are unraveled and is

based on the proactive attitude of the owner, supported and encouraged by the competent authorities, which launches the peculiar protection path traced by the legislator.

A process of accountability that is also fully expressed by the relevant decision to restrict the burden of proof on this subject: in fact, pursuant to the Regulation, the holder is required not only to carefully examine his activity in order to identify the most appropriate technical and organizational measures to limit situations that are harmful to the identity of the parties involved, but at the same time to demonstrate, depending on the type of treatment implemented, that they have done everything possible to protect their users.

It follows, therefore, that the European legislator with this act has decided to completely change the traditional point of view of the protection of personal data, moving it from the recipient of protection to the subject who actively uses this information. And it is precisely on this reorganization that the essential elements of the entire regulatory framework have been redefined.

If accountability is the cardinal principle of the new European regulatory framework, precisely the limited accuracy in determining the protection measures of its users has represented, however, the most important element of criticality of the treatment system implemented by Facebook and, consequently, triggering the "Cambridge Analityca" affair. For years, the social network has pursued its commercial aims delineating a double level of exploitation of personal data of its

customers: a more superficial and obvious, consisting of the explicit activity of sharing images, personal photos, thoughts and comments made directly by the interested parties; and another subtile, at times intentionally and maliciously concealed, distinguished by the analysis of the actions, not all of them consciously realized, of the users of the social network.

It is a real multi-level system of collecting precious personal information that has been made possible to develop thanks to the image of a free sharing platform and a system of non-transparent conditions of use, which has transmitted to users the deceptive perception of having, always and in any case, full control of personal data.

Once the dual structure at the base of the functioning of the social network has been identified, it becomes obviously important to assess whether the new regulatory framework could effectively limit or prevent the harmful consequences deriving from the undue removal of information from millions of personal profiles.

With reference to the first and most superficial data collection level mentioned above, in accordance with what has been highlighted, it is possible to state that the application of the new rules would certainly have affected, increasing, at least, the degree of security of the platform. The complex system of obligations imposed on holders who carry out treatments at such a high risk for privacy, providing for an ex-ante impact analysis, as well as mandatory consultations with the competent authorities (art. 36) and communications required in case of violations

(artt. 33 and 34), would have, in fact, facilitated the identification of behaviors maliciously or culpably detrimental to the personal identity of users. The platform would also have been naturally encouraged towards the preparation of more adequate technical and organizational protection measures and their dynamic renewal in view of the use of new digital techniques. A rethinking of the model of activity based on the principles of privacy by design and by default that would have been encouraged, on the other hand, not only by the deterrent nature of the more incisive system of sanctions foreseen[104], but above all by the actual impossibility of carrying out a similar activities within the European landscape in violation of the fundamental elements that legitimize treatment in the new regulatory framework. In particular, Facebook would have been forced to explicitly and transparently indicate the existence of qualitatively different purposes, to request forms of consensus absolutely differentiated due to the granularity of the data collected and, with reference to the profiling activities performed by the same platform, to make available specific techniques

[104]The reinforcement of the responsibility of the person in charge of the treatment is also reflected in the increase in penalties in the event of failure to comply with the new legislation. The Regulation, in fact, recognizes to national supervisory authorities the possibility to impose pecuniary and administrative sanctions, following a case-by-case assessment of the nature, severity and duration of the violation and the degree of responsibility of the subject above, taking into account the measures security that he has or should have implemented. For specific categories of violations, the Regulation at art. 83, paragraph 6, recognizes, in particular, the possibility to impose pecuniary administrative sanctions up to 20.000.000EUR, or for companies, up to 4% of the total annual turnover in the previous year, if higher. On the other hand, it is up to the individual Member States to determine the rules on penalties for infringements not explicitly regulated by the current legislation on the protection of personal data.

for acquiring consent or opposing automated processing in compliance with the provisions of art. 22.

Similar considerations also apply to the determination of the storage times of personal data, which to date are not specified in the conditions of use in violation of art. 5, paragraph 1, lett. e), as well as for the realization of the exercise of right to be forgotten, governed for the first time by art. 17.

Limits in terms of applicability and effectiveness of the European Regulation compared to the multilevel structure realized by Facebook are found, however, with reference to the second and most hidden level of data processing. The sharing of personal information of its users by the platform with group companies, customers, technical partners and developers of external applications, as foreseen by the conditions of use, completely undermines the model of informed consent and, consequently, the full effectiveness of the Regulation.

The tendentially unlimited extension of the value chain of personal information due to subsequent retransfers based on superficial approvals by users, as occurred in the "Cambridge Analytica" case, inevitably determines the separation of the data from the person, dragging it along a spiral indeterminate of continuous use, which prevent effective control over it.

The discipline dedicated to the retransmission of personal data is contained in Chapter V and refers to transfers to non-European countries or international organizations, limiting their implementation

to only three specific cases[105]. The aim is obviously to avoid that the subjects involved are exposed to different forms of protection and security and, above all, not qualitatively up to the new European framework.

The forecast, of absolute importance in the current digital world devoid of territorial barriers, is however able to obviate only in part to situations similar to that happened with the "Cambridge Analytica" case. An intervention by the European legislator directly and specifically aimed at regulating the ever-expanding and heterogeneous phenomenon of transfers of personal data for reasons of profiling or shared use, such as for example with "social media plugins"[106], which

[105]Regulation 2016/679 provides that the transfer can be considered legitimate in three specific situations. Firstly, when authorized by the European Commission on the basis of an adequacy decision pursuant to art. 45. In order to ensure that the transfer of personal data is carried out in accordance with specific conditions that do not undermine the level of protection guaranteed by the new regulatory framework, the Regulation entrusts the European Commission with the task of drawing up a list of third States and of international organizations able to offer an adequate protection system. Based on this decision, which must be carried out in accordance with specific indicators established in art. 45, the holders will have the possibility to transmit personal information to the countries present in this list without having to request specific authorizations from a control authority. The second case concerns those situations in which the data controller or the controller has provided adequate guarantees on the condition that the data subjects have access to rights and effective remedies pursuant to art. 46. Finally, the Regulation allows the transfer in the case in which there are binding corporate rules pursuant to art. 47. Pursuant to art. 4, n.20 of the European Regulation for binding corporate rules must be understood: "policies on the protection of personal data applied by a data controller or controller established in the territory of a Member State to the transfer or transfer complex of personal data to a data controller or controller in one or more third countries, within a business group or group of companies performing a common economic activity".

[106]In the computer field, the plugin is a program that interacts with another program to extend or extend its original features. These tools, therefore, can have multiple applications depending on the specific purposes that you want to pursue. The most common are those that, as indicated in the text, allow you to use an application using

make it possible to use the services of personal profile (and in particular the credentials) created on a more well-known social network, such as Facebook, Google or Twitter, as a mechanism for accessing and recognizing these particular methods of treatment, involving the multiple different owners and the intersection of heterogeneous purposes that should, in fact, be subject to even more stringent rules, based on complete and exhaustive instructions in favor of the interested parties and legitimated only on the basis of explicit and detailed consents push towards the legislative provision of specific and autonomous modalities approval of such practices, by identifying suitable techniques to arouse the attention of users, since the traditional ways of collecting consents are not sufficient. In the absence of such elements, the risk of a permanent loss of personal data within the complex and complex landscape of the network is still present and increasingly relevant, despite the incisive rules provided for by the new regulatory framework.

There is no doubt that in an extremely dynamic landscape where data is now the cornerstone of data-centric companies, but at the same time risks becoming easy prey, the new regulatory framework introduced by Regulation 2016/679 is today a fundamental and solid protection tool. However, the challenges to be faced along the digitalisation horizon seem to be still multiple and relevant.

---

the same login credentials of a social network to which you are already registered, not having to create others. In other cases, the plugins allow you to share information on a third party site (news, phrases, photos) on the personal profile created on the social network.

It is necessary to continue on the path of regulating complex and increasingly sophisticated forms of collection and profiling of personal data, which daily threaten the normal evolution of the identity of the subjects involved, sanctioning undue external exploitation for purposes that lie outside the sphere of determination of individual.

This implies regulatory interventions explicitly aimed at any subsequent and further phases with respect to the collection and processing of personal data, with the provision of specific rules and limitations in the event that the holder intends to proceed with the subsequent transmission of the information in his possession or use the collaboration of third parties. In particular, it is essential to provide specific and above all separate forms of consent, different from those envisaged for the "original" treatment, which are able to alert the user to the potential implications deriving from the use of such external applications and to allow them to check the path taken by its personal data. Therefore, it is necessary to accept the challenge and defend the reasons of the rules, which are also those of freedom and democracy.

Parallel to the process of strengthening the accountability of the owners and multiplying the moments of collaboration between these subjects and the competent authorities, it will be fundamental to start a process of empowering the digital user, so that we reach the full awareness that in the world of free access platforms the exchange asset is not represented by a monetary value, but is constituted by the subject itself and by the relative baggage of personal information. Where the normative data is not able to arrive and experience the control of the

authorities in this area, it is the prudent and conscious behavior of the user who must intervene, in the belief that personal data are increasingly a precious asset to be preserved and, above all, not to be left unconsciously flowing in the space without boundaries of the network.

14.Concludind remarks.

The fruitful intertwining between conscious and timely regulatory intervention, proactive attitude of the data controllers and the responsibility of digital users will increasingly be an indispensable factor for sustainable and intelligent growth, especially with reference to the ever-widening areas of application and use of personal data. In the absence of such a combined action, on the contrary, it is reasonable to expect the perpetuation of the risk that the increasingly invasive use of new technologies, as a tool for growth and development of the community based on the fertile sharing of information and knowledge, will turn into a vehicle limiting personal freedom and fundamental rights, transforming the much desired digital society into a highly dystopian society.

In conclusion, international documents and meetings within the European Union are always a good starting point for a universal discussion on this type of subject. If the same media[107] will do their part to foster it by guaranteeing the independence and pluralism of information, equally emphasized in state declarations, there will

[107]J. Oster, European and international media law, Cambridge University Press, Cambridge, 2016, pp. 365ss.

absolutely be the commitment of all to overcome the digital divide with cooperation and dialogue within a non-formal framework but of substantial peace and democracy. We are witnessing a front page from which often is shown an excessive permeability towards a global administration that legitimizes the false theses adopted to justify wars, to indirectly reveal decisions entrusted to events so delicate that it would be differently not questionable, but wrapping them in reassuring opaque fabric of embedded information, where other information professionals have claimed and painstakingly conquered a space of autonomy and tearing that network, have challenged attempts to deny certain crimes, giving strength and visibility to those who still today obstinately seek to reason with the internet turned off!

References

Alkema, E.A., Van Der Hulle, R., Safeguard rules in the european legal order: The relationship between article 53 of the European Convention on Human Rights and article 53 of the Charter of the Fundamental Rights of the European Union, in Human Rights Law Journal, 15 (1), 2015, pp. 19ss.

Ambrose, M.L. Friess, M.L., Matre, N., Seeking, J.V., Digital redemption: The future of forgiveness in the internet age, in Santa Clara Computer and High Technology Law Journal, 29, 2012.

Arming, M., Moons, F., Schefzig, J., Vergiss, Europa! Ein Kommentar zu EuGH Urt. v. 13.5.2014-case C-131/12-Google/Mario Costeja Gonzàlez, CR 2014, 460, in Computer und Recht, 30 (7), 2014.

Armstrong, G., Kotler, P., Marketing an introduction, ed. Pearson, London, 2016. P. Kotler, Marketing management, 15th edition, ed. Pearson, London, 2017.

Ausloos, J., The right to be forgotten worth remembering?, in Computer Law & Security Review, 28, 2012, pp. 144ss.

Baker, M.J., Marketing Strategy and Management, ed. Springer, London, 2000.

Beaumont, P., Danon, M., Trimmings, K., Yüksel, B., Cross-border litigation in Europe, Hart Publishing, Oxford & Oregon, Portland, 2017.

Beraudo, I.P., Regards sur le nouveau Règlement Bruxelles I sur la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale, in Journal du Droit International, 2013, pp. 742ss.

Bieber, R., Maiani, F., Précis de droit européen, ed. Stämpfli, Bern, 2011.

Blumann, C., Dubouis, L., Droit institutionnel de l'Union européenne, LexisNexis, Paris, 2013, pp. 478ss.

Boehme-Nessler, V., Privacy: A matter of democracy. Why democracy needs privacy and data protection, in International Data Privacy Law, 6 (3), 2016.

Boutayeb, C., Droit institutionnel de l'Union européenne: Institutions, Ordre juridique et Contentieux, LGDJ, Paris, 2014, pp. 119-125.

Büllesbach, A., Concise european IT law, Kluwer Law International, The Hague, 2010, pp. 489ss.

Buttarelli, G., The EU GDPR as a clarion call for a new global digital gold standard, in International Data Privacy Law, 2, 2016.

Cardonnel, P., Rosas, A., Wahl, N., (eds) Constitutionalising the EU judicial system: Essays in honour of Pernilla Lindh, Oxford University Press, Oxford, 2012, pp. 105ss.

Caruana, M.M., The reform at the EU data protection framework in the context of the police and criminal justice sector: Harmonisation, scope, oversight and enforcement, in International Review of Law, Computers and Technology, 31, 2017.

Clergerie, J.L., Gruber, A., Rambau, P., L'Union européenne, ed. Dalloz, Paris, 2014, pp. 543-545.

Costa, E., Consent in european data protection law, Martinus Nijhoff Publishers, Boston & Leiden, 2013, pp. 184ss.

Craig, P., De Bùrca G., (eds.), The evolution of EU Law, Oxford University Press, Oxford, 2011.

Craig, P., European Union administrative law, Oxford University Press, Oxford, 2018.

Dammann, R., Milllet, S., L'action en revendication exercée au titre d'une clause de réserve de propriété relève-t-elle du champ d'application du règlement Bruxelles I?, in Revue Lamy Droit Civil, 7, 2010, pp. 32ss.

De Andrade, N.G., Right to personal identity: The challenges of ambient intelligence and the need for a new legal conceptualization, in S. Gutwirth (eds), Privacy and data protection. An element of choice, ed. Springer, Berlin, 2011, pp. 67ss.

De Hert, P., Papakonstantinou, B., The proposed data protection Regulation replacing Directive 95/46/EC. A sound system for the

protection of individuals, in Computer Law & Security Review, 28 (2), 2012, pp. 132ss.

De Vries, S.A., European Union and ECHR: Conflict or harmony?, in Utrecht Law Review, 9, 2013, pp. 80ss.

Dony, M., Droit de l'Union européenne, Bruxelles, Editions de l'Université de Bruxelles, 2014. J.C. Gautron, Droit européen, Dalloz, Paris, 2012, pp. 24ss.

Frantziou, E., Further developments in the right to be forgotten: The European Court of Justice's judgment in Case C-131/12, Google Spain, SL, Google Inc v. Agencia Espanola de Proteccion de Datos, in Human Rights Law Review, 14 (4), 2014, pp. 762ss.

Franzina, P., Jurisdiction regarding claims for the infringement of privacy rights under the General Data Protection Regulation, in A. De Franceschi (ed.), European contract law and the digital single market. The implications of the digital revolution, ed. Intersentia, Cambridge, Antwerp, Portland, 2016, pp. 82ss.

Fuster, G.G., The emergence of personal data protection as a fundamental right of the EU, ed. Springer, Berlin, 2014.

Gascòn-Inchausti, F., La reconnaissance et l'exécution des décisions dans le règlement Bruxelles I bis, in E. Guinchard (eds), Le nouveau règlement Bruxelles I bis. Règlement n° 1215/2012 du 12 décembre 2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale, ed. Larcier, Bruxelles, 2014, pp. 210ss.

Grard, L., La communautarisation de "Bruxelles I", in Revue Gènèrale de Droit International Public, 118, 2013, pp. 530ss.

Greer, S., Gerards, J., Slowe, R., Human rights in the Council of Europe and the European Union. Achievements, trends and challenges, Cambridge University Press, Cambridge, 2018, pp. 80ss.

Hawsen, M., Hoepman, J.H., Leenes, R., Privacy and identity management for emerging services and technologies, ed. Springer, Berlin, 2014.

Hay, P., Notes on the European Union's Brussels-I "Recast" Regulation, in The European Legal Forum, 2013, pp. 2ss.

Hoffman, D., Bruening, P., Carter, S., The right to obscurity: How we can implement the Google Spain decision, in North Carolina Journal of Law & Technology, 17, 2016, pp. 440ss.

Kerikimäe, T., Regulating technologies with European Union. Normative realities and trends, ed. Springer, Berlin, 2014.

Kessedjian, C., L'espace judiciaire civile et commercial européen: le règlement "Bruxelles I" refondu, in Revue Gènèrale de Droit International Public, 117, 2013, pp. 546ss.

Köhler, B., Dual-use contracts as consumer contracts and no attribution of consumer status of a third party to the proceedings under Brussels-I Regulation, in Praxis des Internationalen Privat-und Verfahrensrecht, 37 (6), 2017.

Koops, B., The trouble with European Data Protection Law, in International Data Privacy Law, 4, 2014, pp. 252ss.

Krommendijk, J., Principled silence or mere silence on principles? The role of the EU Charter's principles in the case law of the court of Justice, in European Constitutional Law Review, 11 (2), 2015, pp. 322ss.

Kulk, S., Zuiderveen Borgesius, F., Google Spain v. Gonzàlez: Did the court forget about freedom of expression? Case C-131/12 Google Spain Sl. and google Inc v. Agencia Españ ola de protecciòn de datos and Mario Costeja Gonzàlez, in European Journal of Risk Regulation, 5 (3), 2014, pp. 390ss.

Lazzerini, N., (Some of) the fundamental rights granted by the Charter may be a souce of obligations for private parties: AMS, in Common Market Law Review, 51 (4), 2014, pp. 908ss.

Lenaerts, K., Exploring the limits of the EU Charter of Fundamental Rights, in European Constitutional Law Review, 2012, pp. 375ss.

Liakopoulos, D., European integration and its relation with the jurisprudence of European Court of Human Rights and private international law of European Union, in Homa Publica. Revista Internacional de Direitos Humanos e Impresa, 2 (2), 2018, pp. 300ss.

Liakopoulos, D., Interactions between European Court of Human Rights and private international law of European Union, in Cuadernos de Derecho Transnacional, 10 (1), 2018, pp. 252ss.

Lindquist, J., New challenges to personal data processing agreements is the GDPR fit to deal with contract, accountability and liability in a world of the internet of things?, in International Journal of Law and Information Technology, 26 (1), 2018, pp. 47ss.

Lynskey, O., Control over personal data in a digital age: Google Spain v. AEPD and Mario Costeja Gonzalez, in Modern Law Review, 78 (3), 2015, pp. 522-534.

Lynsky, O., The foundations of European Union data protection data, Oxford University Press, Oxford, 2015, pp. 64.

Mantelero, A., Cloud computing, trans-border data flows and the European Directive 95/46/EC: Applicable law and task distribution, in European Journal for Law and Technology, 3 (2), 2012.

Marsden, T., Internet co-regulation european law. Regulatory governance and legitimacy in cyberspace, Cambridge University Press, Cambridge, 2011, pp. 239ss.

Mcgoldrick, D., Developments in the right to be forgotten, in Human Rights Law Review, 13 (3), 2013, pp. 762ss

Meeusen, J., Van Overbeeke, F., Verhaert, L., The link between access to justice and european conflict of laws after Lisbon, much ado about nothing?, in Rabels Zeitschrift für ausländisches und internationales Privatrecht, 81, 2017

Moerel, L., Back to basics: when does EU data protection law apply? In International Data Privacy Law, 1 (2), 2011, pp. 94ss.

Moerel, L., The long arm of EU data protection law: Does the data protection Directive apply to processing of personal data of EU citizens by websites worldwide?, in International Data Privacy Law, 1 (1), 2011, pp. 29ss.

Money-Kryle, R., Legal standing in collective redress actions for breach of EU rights: Facilitating or frustrating common standards and access to justice? in B. Hes, M. Bergström, E. Storskrubb, EU civil justice: Current issues and future outlook, ed. Bloomsbury, 2016.

Moreno, M.A., Goniu, N., Moreno, P.S., Diekema, D., Ethics of social media research. Common concerns and practical considerations, in Cyberpsychology, Behaviour and Social Network, 16 (9), 2013, pp. 709ss.

Nielsen, P.A., The new Brussels I Regulation, in Common Market Law Review, 50, 2013, pp. 503ss.

Nuyts, A., La refonte du règlement Bruxelles I, in Revue Critique de Droit International Privé, 85, 2013, pp. 3ss.

Oster, J., European and international media law, Cambridge University Press, Cambridge, 2016, pp. 365ss.

Payan, G., Droit européen de l'exécution en matière civile et commerciale, ed. Bruylant, Bruxelles, 2012.

Peers, S., Hervey, T., Kenner, J., Ward, A., The EU Charter of Fundamental rights: A commentary, Oxford University Press, Oxford, 2014, pp. 1414ss.

Pohl, M., Die Neufassung der EuGVVO-im Spannungsfeld zwischen Vertrauen und Kontrolle, in Praxis des Internationalen Privat-und Verfahrensrechts, 33, 2013, pp. 109ss.

Polčák, R., Dan Jerker Suantesson, B., Information sovereignty: Data privacy, sovereign powers and the rule of law, Edward Elgar Publishers, Cheltenham, 2017.

Rano, L.X., La force du droit à l'oubli, in Mèmoire de D.E.A.Informatique et Droit 2003-2004.

Rijavec, V., Jelinek, W., Brehm, W., Die Erleichterung der Zwangsvollstreckung in Europa, ed. Nomos, Baden-Baden, 2012, pp. 214ss.

Riva Sanseverino, R., Competitive urban models, in E. Riva Sanseverino, R. Riva Sanseverino, V. Vaccaro, G. Zizzo (ed.), Smart rules for smart cities, ed. Springer, Palermo, 2014, pp.4ss.

Rodrìguez Vàzquez, M.A., Una nueva fórmula para la supresión del exequátur en la reforma del reglamento Bruselas I, in Cuadernos de Derecho Transnacional, 6, 2014, pp. 330ss.

Rosen, J., The right to be forgotten, in Stanford Law Review, 88, 2012, pp. 92ss.

Rubinstein, I.S., Big data: The end of privacy or a new beginning?, in International Data Privacy Law, 2, 2013.

Sebastian Haase, M., Datenschutz rechtliche Fragen des Personenbezugs, Mohr Siebeck, Tübingen, 2015.

Škrinjar Vidović, M., Schrems v. Data protection commissioner (case C-362/14) empowering national data protection authorities, in Croatian Yearbook of European Law and Policy, 11, 2015, pp. 270ss.

Staudinger, A., Schiedsspruch und Urteil mit vereinbarten Wortlaut, in Festschrift für Friedrich Graf von Westfalen, Dr. Otto Schmidt Verlag, Köln, 2010, pp. 662ss.

Stern, K., Sachs, M., Europäische Grundrecht Charta, ed. C.H. Beck, München, 2016, pp. 756ss.

Claes, M., De Visser, M., The Court of Justice as a Federal Constitutional Court: A comparative perspective, in E. Cloots et al., Federalism in the European Union, hart Publishing, Oxford & Oregon, Portland, 2012, pp. 84ss.

Svantesson, D., The CJEU's Weltimmo data privacy ruling: Lost in the data privacy turmoil, yet so very important case C-230/14, Weltimmo, EU:C:2015:639, in Maastricht Journal of European and Comparative Law, 2, 2016, pp. 334ss.

Van Alsenoy, B., Liability under EU data protection law: From Directive 95/46 to the General Data Protection Regulation, in Journal of Intellectual Property Information Technology and e-Commerce, 7, 2017, pp. 272ss.

Van Der Sloot, B., Van Schendel, S., Ten questions for future regulation of big data: A comparative and empirical legal study in Jipitec, in Journal of Intellectual Property, Information Technology and E-Commerce Law, 7 (2), 2016.

Van Rhee, C.H., Harmonisation of civil procedure: An historical and comparative perspective, in X.E. Kramer, C.H. Van Rhee, Civil litigation in a globalizing World, T.M.C. Asser Press, The Hague, 2012, pp. 41ss.

Velàzquez Gardeta, J., La indefensión del demandado como excepción en el proceso civil internacional dentro de la Unión Europea, in J. Goizueta, M. Cienfuegos (eds.), La eficacia de los derechos fundamentales de la UE. Cuestiones avanzadas, Cizur Mayor, Thomson Reuters-Aranzadi, Madrid, 2014, pp. 216ss.

Voigt, P., Von Dem Bussche, A., The European Union General Data Protection Regulation (GDPR): A practical guide, ed. Springer, Berlin, 2017, pp. 23ss.

Von Der Groeben, H., Schwarze, J., Hatje, A., Europäisches Unionsrecht, ed. Nomos, Baden-Baden, 2015, pp. 820ss.

Wachter, S., Normative challenges of identification in the internet of things: Privacy, profiling, discrimination, and the GDPR, in Computer law & security Review, 34, 2018, pp. 438ss.

Warren, S.D., Brandeis, L.D., The right to privacy, in Harvard Law Review, 4 (5), 1890.

Weatherill, S., Law and values in the European Union, Oxford University Press, Oxford, 2016, pp. 151ss.