Quaderni di Diritto Mercato Tecnologia

Rivista Scientifica

ISSN (Online edition): 2239-7442

QUADERNI DI

diritto mercato tecnologia

Numero 4
Anno V
Ottobre/Dicembre 2015

CON CONTRIBUTI DI:

Giuseppe Vitalleti, Stefano Pisani, Vinca Giannuzzi Savelli, Davide Borelli, Andrea Puligheddu, Francesca Corrado.

SOMMARIO

Mercato, concorrenza e regolazione

Biotecnologie, ogm e vita

Diritti della persona e responsabilità in rete

COMITATO REFERENTE

- Margarita Castilla Barea
- Emanuele Bilotti
- Fernando Bocchini
- Roberto Bocchini
- Francesco Di Ciommo
- Cesare Galli
- Fiona Macmillan
- Marco Maugeri
- Enrico Minervini
- Anna Papa
- Francesco Ricci
- Maria Pàz Garcia Rubio
- Cristina Schepisi
- Antonella Tartaglia Polcini
- Raffaele Trequattrini
- Daniela Valentino
- Filippo Vari
- Alessio Zaccaria

COMITATO DI REDAZIONE

- Davide Mula, Università Europea di Roma (Coordinatore del Comitato di Redazione)
- Martina Provenzano (Vice-coordinatore del Comitato di Redazione)
- Emanuela Arezzo, LUISS Guido Carli (Curatrice degli aggiornamenti dell´ordinamento giuridico degli Stati Uniti d'America)
- Alessio Baldi (Curatore degli aggiornamenti giurisprudenziali del Tribunale di Firenze)
- Enrico Bonadio (Curatore degli aggiornamenti dell'ordinamento giuridico del Regno Unito)
- Linda Briceño Moraia, Università degli Studi di Pavia (Curatrice degli aggiornamenti dell´ordinamento giuridico della Spagna)
- Mattia dè Grassi di Pianura, CERNA, Mines ParisTech (Curatore degli aggiornamenti dell'ordinamento giuridico della Francia)
- Maximiliano Marzetti, Universidad Católica Argentina Santa Maria de los Buenos Aires (Curatore degli aggiornamenti dell'area geografica del Sud America)
- Tobias Malte Mueller, Università di Mainz (Curatore degli aggiornamenti dell´ordinamento giuridico della Germania)
- Valerio Mosca (Curatore degli aggiornamenti giurisprudenziali Tar Lazio e Consiglio di Stato in materia di diritto della concorrenza, pratiche commerciali scorrette, diritto e regolazione delle comunicazioni elettroniche)
- Gilberto Nava, Università della Tuscia di Viterbo (Curatore degli aggiornamenti giurisprudenziali Tar Lazio e Consiglio di Stato in materia di diritto della concorrenza, pratiche commerciali scorrette, diritto e regolazione delle comunicazioni elettroniche)
- Francesca Nicolini, Università degli studi di Roma Tor Vergata (Curatrice degli aggiornamenti dell'ordinamento giuridico comunitario)
- Maria Francesca Quattrone, Università LUISS Guido Carli (Curatrice degli aggiornamenti giurisprudenziali in materia di proprietà intellettuale)
- Federica Togo, Università di Firenze (Curatrice degli aggiornamenti dell´ordinamento giuridico della Germania)
- Sveva Bernardini, Università Europea di Roma
- Anna Chiara Calabrese, Università Europea di Roma
- Oreste Calliano, Università degli studi di Torino
- Virgilio D'Antonio, Università degli studi di Salerno
- Massimiliano Dona, Università Europea di Roma
- Philipp Fabbio, Università deli studi di Reggio Calabria
- Valeria Falce, Università Europea di Roma
- Marilena Filippelli, IMT Institute for Advanced Studies
- Francesco Graziadei, LUISS Guido Carli
- Monica La Pietra, Università Europea di Roma
- Elena Maggio, Università Europea di Roma
- Federico Mastrolilli, Università Europea di Roma
- Giuseppina Napoli, Università Europea di Roma
- Andrea Nuzzi, Università Europea di Roma
- Giovanni Nuzzi, Università Europea di Roma
- Maria Cecilia Paglietti, Università degli studi Roma Tre
- Eugenio Prosperetti, Università degli studi di Roma La Sapienza
- Ana Ramalho, Università di Amsterdam

- Andrea Renda, LUISS Guido Carli
- Annarita Ricci, Università degli studi di Bologna
- Giovanni Maria Riccio, Università degli studi di Salerno
- Eleonora Sbarbaro, LUISS Guido Carli
- Marco Scialdone, Università Europea di Roma
- Benedetta Sirgiovanni, Università degli studi di Roma Tor Vergata
- Giorgio Spedicato, Università degli studi di Bologna
- Claudia Stazi, Università degli studi Roma Tre
- Alessandra Taccone, Università Europea di Roma
- Francesco Vizzone, Università Europea di Roma

Collaboratori

- Roberto Alma
- Gianni Capuzzi
- Angelo Castaldo
- Giuseppe Cassano
- Iacopo Pietro Cimino
- Massimo Di Prima
- Lifang Dong
- Nicoletta Falcone
- Raffaele Giarda
- Lucio Lanucara
- Lucia Marchi
- Raffaele Marino
- Giuseppe Mastrantonio
- Marianna Moglia
- Valeria Panzironi
- Cinzia Pistolesi
- Augusto Preta
- Silvia Renzi
- Claudia Roggero
- Guido Scorza
- Paola Solito
- Ferdinando Tozzi

New VAT-based resource for financing the EU Budget L'integrazione postuma

di
Giuseppe Vitalletti

Abstract
L'autore segnala l'esigenza di contrastare le frodi fiscali tramite un maggiore controllo delle vendite al dettaglio. Un controllo efficace su tali vendite volto alla prevenzione richiede anzitutto di individuare il luogo in cui l'evasione abbia effettivamente inizi. Quindi, l'autore suggerisce l'adozione di una tassazione concentrata sui consumi, a lungo attesa, come strumento chiave per la riforma del sistema fiscale italiano ed europeo

The author highlights the need to prevent fiscal evasion by focusing on retail sales.
An effective fiscal control on retail sales requires identifying the actual place where the core of the evasion starts. Then, the author suggests a long awaited evolution from income taxation to consumption taxation as the key to reform the National and European fiscal systems

1. I will discuss the paragraph of Gabriele Cipriani's text *Financing the EU Budget* carrying the title "New VAT-based resource", pages 37-39 [1]. As first part of the intervention, I will say briefly something on the new policy of the *Agenzia delle Entrate*, on the suggestion of what Stefano Pisani said. Then I will discuss the relevant part of Cipriani's book. Afterword I will speak about the possibilities of modifying the Sector Studies in the Italian legislation, as a real instrument against tax evasion: briefly, the studies must indicate non total sales, but only the sales to consumers, with adequate external instruments to check the results. Finally I will draw the consequences for the financing of the EU Budget, through an extension of the policy adopted in Italy. This would have deep consequences on the VAT clearing mechanism.

2. Stefano Pisani, the *Agenzia delle Entrate* director, said that the emphasis of the *Agenzia*, on the new General Direction of Rossella Orlandi, is the necessity to prevent evasion, rather than trying simply to reduce it *ex-post*. I agree totally. The real effort of modifying the Studies Sector goes exactly in such direction. The control of the Sales to Consumption means in fact to check the real place where the bulk of evasion starts. This was clear from the

beginning of the Seventies, when VAT was introduced in Italy, as a levy on Consumption. Only later VAT was considered a Value Added Tax, loosing in practice this very important characteristic. Then the Studies Sector concentrated on the magnitude of the firms: all firms inferior to certain sales thresholds were monitored. The importance of Sales to Consumption as the generating event of evasion went so completely lost: the sales of all firms was monitored (a too large extension), provided inferior to certain thresholds (in this case the extension on the contrary is too small).

3. Gabriele Cipriani, in his book, pages 37-39 shows at page 37 a Table presenting the structure of the EU budget financing for the years 2012-2020 as estimated by the Commission following its proposal to introduce a new VAT-resource and a financial transaction tax. The table shows a drastic reduction of "Existing National Contributions"; a small increase of "Traditional Own Resources"; an increase from zero to more than 40% of the "New Own Resources", of which almost half is a new VAT resource. About this last item he says that the Commission had two options: a parallel system to that operating in the member states and a revenue transfer mechanism. The first option has been discarded because the Commission thought that a VAT-based resource alongside member states' VAT would have led in practice to the creation of a double VAT system. The Commission opted therefore for the simplest solution, which implies a sort of masked transfer mechanism from the single States. This option derives the same amount with respect to the first option, except that is constructed, at its base, on the normal rate of VAT. Precisely: **a)** the Commission has to calculate, on statistical basis, a single EU-wide average proportion of VAT receipts. This, of course, from the standard rate transactions in every member state**; b)** each member state has to apply this "artificial" rate to its total VAT receipts; has to apply the 2% to the result; and finally to pay it to the UE. These baroque differences of calculation would "transform" a transfer into a own resource of Europe.
Both options are highly unsatisfactory, since they fail to construct something effective against tax evasion. Moreover, both are unable as regards the implementation of the definitive **VAT** regime: this is one of the biggest problems. Finally, both options are unable to say something on the division of the two big sectors which regard the tax, Goods with respect to Services (see Longobardi, cap. 26) [2]. We shall note, in paragraph 5, that the new rule illustrated in the paragraph 4 has decisive advantages on these three matters.

4. In 2004, in Italy, it was approved on my impulse (at such a moment I was the economic adviser of the Treasury and Finance Minister), in the text of the

Financial Law (now substituted by the Stability Law), a new regulatory mechanism for **VAT: the schedule VT**. The provision was inside the rules which regard the "voluntary fiscal agreement" (a mechanism which modified the Sector Studies, opening the possibility of an agreement for the next future, and not only for the past). The emphasis, however, was fiscal federalism: for the first time in the history of **VAT**, the obligation to indicate separately the Sales to Consumption, and the rates which apply to them, and the rest of Sales (and their rates), was introduced in the annual declaration of such a tax. Moreover, if the Sales to consumption were outside the region of residence of the **VAT** activity, there was the obligation to indicate the other regions, and the volumes concerned. In this way the possibility was opened to substitute the fictitious (i.e. calculated by Istat) quotas of regional Consumption with the real amount of **IVA** generated in the regional territory. The rule is still living: the law **42** of **2009** (not implemented yet) makes this possibility operative for **VAT**. The first manifestation of the idea had been in the 1996 article by Marè and Vitaletti *La tassazione dei consumi nell'Unione europea: effetti economici e ipotesi di riforma* [3]. Marè is one of the persons who participates at this meeting. The publication of the article was requested by the Minister of Finance at that time, Fantozzi.
In my 2014 book *Le due facce della luna. Il riformismo nell'economia politica*, in paragraph 18, I elaborate on these *facts* [4], advancing a new idea for the Sector Studies (they were made by a society, belonging to the Agenzia delle Entrate and the Bank of Italy, of which I was President between 2001 and 2004). They started in 1993, and evolved later. With the agreement of the categories interested, about 200 Studies Sectors are now formulated, for all the small activities, the bulk of the Italian economic activity. In particular, four "big" sectors are regarded: services, manufacture, commerce and handicraft. All together, about four million firms (see Confartigianato, 2015) [5] are regarded. On the base of parameters indicated by each study and declared by the firms, they indicate a congruous amount of Receipts (or Sales): if firms adhere in their **IVA** declaration to the stated amount, they are almost free from controls. About 80% of firms interested adhere.
The lack of external checks of results, and the fact that evasion on production starts only at the level of Sales to Consumption (only if there is such evasion, *then* it spreads off on production) led me to concentrate on these aspects. First it comes the second aspect, which is easily solved by concentrating the monitoring of the studies to sales of consumption goods and services. Now it is perfectly possible to operate in this sense, even in the case of sellers both to producers and consumers: in fact when sales of **VAT** are toward producers, there is the possibility of a check on the purchaser; when they are toward consumers, this possibility does not exist. As the 2004

and 2009 laws show, there is the possibility to have **VAT** assigned at its real values on the territory (at regional basis; but the possibility is open also to inferior levels).
As to the first aspect, the importance of an external check is decisive, for the control of evasion. That is we should dispose of the amount of consumption in value **by sector** and at a **regional** (or inferior) **level**. This amount must correspond more or less to the truth, to allow checks which minimize evasion. Here at the moment there is a lack of data, which regard the distribution among sectors at regional level: Istat gives in fact the real value of consumption at the level of Regions, but it does not give its distribution among sectors. In the wait that Istat provides to fill the gap, the fiscal institutions may though effectively move, even at a sub regional level. It is necessary that they put together their files of Irpef declarations (at a communal level); the files of personal deposits (disposable through the banks); the files of Irap, net of interests and of the Irpef incomes included in it, but increased with the addition of estimations of tax evasion of Irap (disposable at a provincial level). Then, chosen the territorial level, it is necessary to estimate the flow of consumption among territories, and finally to apply to the amount so found a propensity to consume, distributing the amount according to the same levels of **the studies on the supply side**.
This is the decisive passage: but the fact that the theatre is the consumption sector helps a lot, since consumption happens normally in an open stage. Intermediary figures, both on the side of fiscal institutions and on the side of the sellers (such as commercialists and representatives of the categories), will become the true protagonist of the new fiscal assets.
Sector Studies on the supply side must be also transformed, by simplifying them, and by making them almost obligatory. This is easily obtained in two ways:
i) by awarding a deduction equal to the greater income tax, and, in part, to the greater social contribution, which should reveal to the adherent taxpayer;
ii) by awarding to *all* taxpayers a deduction on their purchases from adhering and not adhering activities. This deduction should be greater, for some years, in the case of not adhering activities. Their real receipts would be revealed, in fact, through the elaboration on the mayor deductions. The deduction would form gradually, by the heap of receipts, which are gradually taken to a point of *Agenzia delle Entrate* in the nearby of the fiscal domicile of the taxpayers. The deduction is made payable at these points, say quarterly.
A central role is assigned on one side to *Agenzia delle Entrate* and *Guardia di Finanza*, and on the other side to the commercialists and the representatives

of categories, in order to distribute the total National Consumption to single activities, through intermediate passages.
Many transformations of the fiscal scene are complementary. First it must come a low level of fiscal pretence on incomes. Then a link between public expenditure and public revenues must be established: local taxes must be assigned with the benefit principle; progressive social security contributions should accord to a correlation principle with their benefits (pensions and health); indirect taxes would guarantee public expenses; certain general, and most of all specific, taxes on income, would be in front of expenditure for redistribution. A new reform fiscal bill, after some years of small changes, will establish principles deeply different from the now prevailing. On these other aspects of taxation we refer principally to the book *Le due facce della luna* [6]. Now it is basic what has been said; the basement of what has been said on laws which are already operative or on the drink for operation; the basement of their extensions on very sound measures.

5. The consequences for VAT at a European level are enormous, and regard all the three aspects already noted at the end of paragraph 3.
a) Evasion in each country is strongly reduced. Here the fundamental role is the foundation of the system in the final statistic Consumption, to which all the rest makes reference. Once each country adheres to this "philosophy", sound (i.e. non based on moral sentiments, as now it is) measures would follow: an enormous problem of the fiscal system would be practically solved.
b) The definitive regime is reached for **VAT**, without problems. In fact one of the main characteristic of the system is the individualization of the true **VAT** revenue on consumption, at whatever level (superior though to minimal thresholds). Of course *the national level is included*. Once the true revenue on consumption at the national level has been individuated, there are two operation which must follow: 1) the adding of the **VAT** revenues from "impurities" (for example revenue from public purchases; or from banks; or from exempt items: altogether about one third of the revenue at EU level, according to Longobardi, chapter 18) [7]; 2) a centrality for compensation at EU level, which has to redistribute the national accrues according to the amounts which emerge in point 1.
A great problem *existing* in the actual **VAT** System, and which has been temporarily "solved" by the recurrence to a transitory (from 1993!) regime, would be solved. One of the principal problems of this transitory system, i.e. the carousel frauds (a system of evasion-elusion which is based on the existence of a point of withdrawal at zero rate, as happens in the interchange among nations) would be solved as well (on the carousel frauds, see Aujean 2011[8]). A first simulation of how this system would work in practice has

been shown by Santoro and Convenevole (2013) [9]. *A quota of the national **VAT** accrual may be assigned to EU*, avoiding all the drawbacks shown in paragraph 3.

c) The system seems able to disentangle the enormous confusion *existing* in **VAT** with regard to the international commerce of Goods (for which the destination principle is applied) and of Services (for which, on the contrary, the origin principle prevail). On these points, disregarded in the public opinion although they are fundamental, see again the formal treatment of Longobardi (Chapter 26) [10].

All together, the passage from Income to Consumption as the key of the fiscal system would innovate deeply it. This move was prefigured in Italy in 1970, with the introduction of **IVA**. Later on, the ideological forces which leads Income as the key figure have mixed with practical interests, giving origin to the present critical situation.

Note:

[*] Il presente contributo è stato preventivamente sottoposto a referaggio anonimo affidato ad un componente del Comitato di Referee secondo il Regolamento adottato da questa Rivista.

[1] Cipriani, G. (2014), *Financing the EU Budget. Moving forward or backwards?*, CEPS, Brussels.

[2] Longobardi, E. (2009), *Economia tributaria*, McGrow-Hills, Milano.

[3] Marè, M. and Vitaletti, G. (1996), La tassazione dei consumi nell'Unione europea: effetti economici e ipotesi di riforma, *Il Fisco*, n.15.

[4] Vitaletti, G. (2014), *Le due facce della luna. Il riformismo nell'economia politica*, Foschi editore, Forlì.

[5] Confartigianato (2015), *Nutrire la piccola impresa, energia per la crescita*, Assemblea 2015, Expo Milano.

[6] Already quoted in footnote 4.

[7] Longobardi, E. (2009), *Economia tributaria*, McGrow-Hills, Milano.

[8] Aujean, M. (2011), Towards a Modern EU VAT System: Associating VIVAT and Electronic Invoicing, *Ec TAX Review*, n.5.

[9] Santoro, A. and Convenevole, R. (2013), Prospettive di riforma dell'Iva e delle accise, intervento nell'ambito del Convegno *Un'agenda fiscale per il nuovo governo*, Riunione intermedia Siep.

[10] Already quoted in footnotes 2 and 7.

An alternative to budgetary balances to assess benefits for the Member States

di
Stefano Pisani

Abstract:
Il saggio mira a dimostrare che l'adozione di un'analisi di carattere macroeconomico basata su indici di input e output e su flussi commerciali tra gli Stati membri permette di superare le criticità teoriche e operative di una strategia europea che si fonda esclusivamente sulla considerazione dei flussi di bilancio. L'esito dello studio si colloca nell'ambito di una visione strategica in cui il fine del bilancio europeo è distribuire risorse in modo ottimale in modo da agevolare lo sviluppo delle economie degli Stati membri.

The goal of the paper is to demonstrate that a proper macroeconomic analysis based on input-output tables as well as on trade flows among Member States is likely to contrast the conceptual and operational drawbacks of a methodology that relies only on budgetary flows. The outcome of the analysis places itself in the context where the purpose of European budget is to redistribute resources among Member a States to support development of Member States economy.

1. Introduction.

The budgetary balances calculation method is actually enshrined in a Council of Ministers' Decision [2]. The principle of the calculation of the Member States' net positions draws thus support by an official methodology. Moreover, data on budgetary balances are regularly published by the

Commission since 1998 [3]. Such calculations become obviously a key element of the decision making process of the Union.
As the Commission itself stresses, *"allocating expenditure to Member States is merely an accounting exercise that gives a very limited view of the benefits that each Member State receives from the Union (...). This accounting allocation, among other drawbacks, gives no indication of many of the other benefits gained from EU policies*" [4].
This study attempts to demonstrate that a proper macroeconomic analysis based on input-output tables as well as on trade flows between Member States may enable us to overcome the conceptual and operational drawbacks of the present methodology, based exclusively on budgetary flows.

2. Main features of the European budget

The Treaty on the functioning of the European Union (art. 311) stipulates that the European budget is financed from "Own resources" of the Community. The "Own resources" system defines the typology of financial resources (Custom and Agricultural duties, Sugar levies, VAT resource, GNI resource and Miscellaneous revenue) as well as the overall ceiling of total resources which can be called [5]. The system, first set up by the Council Decision of April 21st 1970, has been amended several times, mainly in order to modify the burden of financing among Member States. The GNI resource, based on each Member State's Gross National Product, was introduced in 1988 [6] to increase the share of contributions based on the relative prosperity of the Member States.
It should be pointed out that the resources financing the European budget are not administered nor fixed *de facto* in an autonomous way by the Community but rather by the Member States. The European budget's financing is provided by a decision which has first to be unanimously adopted by the EU Council of Ministers and, to come into force, needs to be ratified by the Member States according to their own constitutional rules.

3. The concept of "excessive budgetary imbalance"

In an attempt to manage worries from both kinds of Member States - "net" beneficiaries as well as "net" contributors - the Commission has proposed [7] a generalised correction mechanism, calculated on the basis of the net budgetary balance of each Member State. To satisfy "net" contributors Member States a rebate would be applicable if net contributions exceed 0,35% of each country's GNI, this threshold representing a kind of "reasonable net contribution" (contributions above this would be refunded at

a rate of 66%). On the other side, the total volume of corrections would be limited to 7,5 billion EUR a year (financed by all Member States based on their relative share of GNI), thus insuring "net" beneficiaries Member States (which do not benefit of the rebate) against excessive costs of the mechanism.
However, although the likely Member States' "net" balances have been projected by the Commission against various future financing scenarios, the concept of "imbalance" continues to be based on payments from and to Member States. The inherent drawbacks of such a concept, illustrated in section 5, would therefore apply also to such a new mechanism. Moreover, correcting budgetary imbalances through *ad hoc* mechanisms essentially amounts to refusing to intervene directly on the sources of the imbalances. [8]

4. The share of the financial burden falling on Member States and their budgetary balances

As most of the financing of the European budget derive from the VAT and GNI resources, the “financial” burden is shared among Member States basically in function of their part in the total GNI and, to a lesser extent, on the basis of their final consumption liable to VAT.
Since it provides a balance between contributions paid by the Member States and payments received, the allocation of the EU expenditure made in this frame represents in a way the "official" reference to define winners and losers in the framework of the European Budget. It is on this basis that the Members States consider themselves (and are conventionally considered) "net contributors" or "net beneficiaries". The definition used to this purpose is that of “operating expenditure”, which is an ancillary definition of "allocated expenditure" and differs from the latter in that it omits administrative expenditure relating to EU institutions.

5. Conceptual drawbacks and inadequacies of a method based on budgetary balances

The difference between budget contributions and budget expenditure by each Member State tends to misrepresent the benefits from EU membership. The Commission itself listed a series of reasons for which conventionally measured budgetary balances fail to adequately represent the benefits of EU membership, ending up with results that are not uncontroversial [9]. These re

a) given the diversity of circumstances and productive structures among Member States, a given EU expenditure will not result in the same

economic benefits for all the Member States;

b) EU expenditure only registers the amounts used, for example, to fund agricultural market support measures or payments of direct aid to farmers; the benefits gained, and the costs incurred, by producers and consumers in the Member States are largely due to factors which for obvious reasons go unregistered in the EU budgetary accounts; these factors, which are often very difficult to quantify, are the flow of income from consumer to producer both within and between Member States, the benefits derived from stability of price and security of supply, the effects of the EU subsidies on the allocation of productive resources;
c) around one third of the agricultural spending is devoted to market support measures; however, those measures are supposed to benefit all countries and not only the ones receiving the payments from the European budget;
d) structural expenditure accruing to one Member State has also important spill-over effects, reflecting largely the enhanced interdependence characterising the EU; financing projects in less favoured areas generates production of goods and services in other areas [10].
e) the greatest economic benefits of the Internal Policies are likely to relate to economic integration; the limited usefulness of measuring benefits from EU membership in budgetary terms alone is highlighted by the disparity between the budgetary cost of these policies and their impact in terms of growth and employment.

The methodologies based on budgetary balances furthermore do not take into account important "financial" aspects:

f) the method is based on the calculation of a balance between two sets of data conceptually different, while VAT and GNI resources are financed through general taxation by all taxpayers, a similar parallelism does not exist for the payments made from the European budget to a given country;
g) payments are normally allocated to the Member State in which the principal recipient resides; This is not a guarantee that the payment benefits to the country of residence; a similar situation can arise for research contracts, often implemented by several partners while, for the purpose of allocating the "operating expenditure", the payment is totally attributed to the partner heading the consortium.

The methodology proposed in this paper does not solve all the foregoing problems, but it faces mainly those items under a) – d).

6. Estimating economic benefits accruing from EU expenditure: a methodology based on the increase in the demand of goods and services

We believe that the benefits which each Member State derives from the EU budget could be estimated in a more comprehensive way, avoiding the conceptual and operational drawbacks of the present methodology. The starting point is that each unit of (European) expenditure generates, somewhere (within/outside the EU), a given quantity of production (goods and/or services). This induced production can be further divided by type (agriculture, industry, services, building) and can be assumed as a proxy of the benefits for each EU Member State (and, indeed, for States outside the EU). For this exercise we used basically two tools, the input-output data of the Member States and the actual expenditure they received from the European budget.
The proposal aims to develop a methodological framework to evaluate the global benefits caused by the European Union expenditure to each Member State. The main characteristics of this methodology are:

- clearly specified hypotheses,
- a methodology founded on an economic background largely accepted, and
- an algorithm which is completely standardised.

Furthermore, in this evaluation the main methodological tool is the input-output analysis [11].

6.1 The basic model [12]

In order to evaluate the impacts of EU expenditure on the Member States' economies it is necessary to estimate the global benefits caused by such expenditure. In this study only the expenditure having an effect on production level has been considered.
Basically we assume that the EU gives a contribution *X* to the country *Y* in order to increase the production level of sector *Z* of economic activity. At this stage it is essential to identify the economic sector (*Z*) on which the EU expenditure (*X*) weighs; it is therefore necessary to classify the EU budget in a way consistent with the economic classification. In order to evaluate the global impact on national economy it is necessary to estimate the quantity of additional production of *Z* activated by *X*.
In general, the global benefit of EU expenditure (*B*) can be defined by the equation $B=PI+PE$, where *PI* and *PE* represent the amount of domestic and foreign production due to *X*. With this information it becomes possible to follow the proposed procedure.
The EU gives a contribution in order to increase the production of a particular sector of activity in a specific country; such amounts cause an increase of

production (*PI*) both in the specific sector and in all the other economic activities interrelated with the previous one. The increase of production causes an increase in the imports (*PE*) required to produce *PI*. *PI* + *PE* represent the total benefits; *PI* however is the domestic benefit while *PE* is the foreign component and must be imputed to other countries.
From a statistical point of view, the main difficulty concerns estimating the two amounts *PI* and *PE*. Such an estimate must be realised using a data set with a high degree of reliability and comparability among the EU Member States. We can find both these characteristics in Eurostat's "input-output database".
The input-output model is a matrix in which the horizontal rows show how the output of each sector of the economy is distributed among the others. Conversely, the vertical columns show how each sector obtains from the others its needed input of goods and services. A simplified input-output matrix is showed in Figure 1.
Using the input-output table columns it is, in fact, possible to know the values of input needed to produce output *Z*. In formal terms this can be represented by the equation $Z_i = C_{i1} + C_{i2} + ... + C_{in} + VA_i$; where: C_{i1}, C_{i2}, ..., C_{in} are the values of input used (goods and services purchased) to produce *Z* and *VA* is the value added that correspond to the total payments for primary inputs (capital stock, labour and land). The inputs used in this production (C_i) can be produced in country Y (CI_i), in EU countries (CUE_i) or finally in extra EU countries (CEU_i). Therefore, the previous equation can be written as
$Z = (CI+CUE+CEU)_{i1} + (CI+CUE+CEU)_{i2} + ... + (C+CUE+CEU)_{in} + Va_i$ [1]

Figure 1 **A simplified input-output matrix**

		INDUSTRY PURCHASING					
		Agriculture	Industry	Services	Intermediate consumption	Final demand	Total output
INDUSTRY PRODUCING	Agriculture	CI_{11}	CI_{21}	CI_{31}	$CI_{.1}$	D_1	Z_1
	Industry	CI_{12}	CI_{22}	CI_{32}	$CI_{.2}$	D_2	Z_2
	Services	CI_{13}	CI_{23}	CI_{33}	$CI_{.3}$	D_3	Z_3
	Total costs	$CI_{1.}$	$CI_{2.}$	$CI_{3.}$	$CI_{..}$	$D_.$	Z
	Value added	VA_1	VA_2	VA_3			
	Total output	Z_1	Z_2	Z_3			

It is now evident that each increase in *Z* production determines, *coeteris paribus*, an increase in inputs C_i (because Z_i production needs more resources). These additional resources can come from domestic (CI_i) or foreign production (CUE_i or CEU_i).

In this study we assume that EU expenditure (*X*) in a particular sector of activity causes an increase of production in the same sector. Using the input-output model, by extending equation [1] it becomes therefore easy to calculate both the domestic and foreign results due to *X*. These results represent the total benefits (*B*) and are measured in terms of additional domestic (*PI*) and foreign (*PE*) production. In this way we can quantify not only the benefits in country *Y*, but also the benefits in the whole EU expressed in terms of imports of EU goods and services in country *Y*. We can furthermore split both the domestic and the foreign benefits in "direct" and "indirect". The former are produced in a shorter period than the latter.
In order to analyse more in depth the relationship among the EU countries we need to split between EU and extra EU countries the amount of foreign benefits. We have further to assign to each Member State a share of EU foreign benefits. In order to do this it is necessary to know import-export flows among the EU Member States and between the whole of the EU and all other countries. A specific Eurostat database allows us to group the import-export flows in this way and then to identify from which country *Y* purchases the inputs needed to produce *Z*.
Taking simultaneously into account the input-output data set and the import-export database we can locate the total imports of each country and, consequently, the benefits produced by such imports in the various EU Member States.

6.2 The main characteristics of databases

6.2.1 Input-Output tables

As a starting point of the analysis we use Eurostat's "input-output database". This database contains harmonised input-output tables concerning the EU Member States as well as producing tables (as complete as possible) for the EU as a whole. The input-output system of Eurostat includes detailed information for a given year on production activities, supply and demand of goods and services, inter-industry transactions, primary inputs and foreign trade. The economy is broken down into various branches (agriculture, industry, services), clearly presenting thus the interdependencies between economic variables. Transactions in goods and services are broken down by:

- supplier and user,
- type of use (intermediate or final)
- geographical origin and destination.

Input-output tables also show the cost structure of production activities (intermediate inputs, compensation of labour and capital, taxes on

production). The tables supplied within this database are harmonised with reference to the European System of Integrated Economic Accounts (ESA) [13] In order to use the import flows in an input-output model we need to split the total import flows between final and intermediate uses. In fact, in this analysis the attention is focussed on import flows used in the domestic production process. To this end have been used the symmetric input-output tables both for internal production and for imports. Furthermore, the imports of intermediate goods and services have been split by countries of origin using the database on the statistics of trade (see par. 6.2.2).

6.2.2 Statistics on trade

We use the Eurostat database on the external trade. This database records for each Member State, with reference to the years 1998-2001, the import-export flows broken down by sectors of economic activity and by country of origin. The classification of economic activities of this database is analogous to the input-output classification; the two databases can thus be easily matched.

6.2.3 EU expenditure

The definition of EU expenditure used corresponds to that of " operating expenditure" within the meaning of the exercise carried out annually by the Commission.

"Operating expenditure" is allocated by the Commission to three main budgetary areas: agriculture, structural actions and internal policies. For the purpose of identifying a direct link between the type of expenditure and the type of production directly generated (agriculture, services, industry, building) we have treated these three fields as follows:

- We have deducted from the "allocated operating expenditure" for Agriculture the part relating to budgetary lines like "set-aside" or "early-retirement" which are more of a subsidy than of an incentive to product. Other budget lines have been excluded due to the difficulty of allocating them to one of the four sectors of production selected. The part finally deducted equals 6,6 % of the total allocated expenditure for this section. The rest of the budget lines have been attributed to one of the four sectors of production according to the type of production that each kind of expenditure is likely to generate. The expenditure has been attributed to the Member States according to the budgetary implementation (average 2000 to 2002).
- Concerning expenditure for Structural actions we were forced to choose a different procedure, since the budgetary implementation does not allow the necessary detailed analysis to attribute the expenditure to a sector of

production. We have therefore assumed that we could apply to this part of the operating expenditure the typology of interventions financed for the period 2000-2006. On this basis we have divided by sector of production the operating expenditure by Member State. A small part of the total has been excluded (1,1 %), either because of its subsidy nature or due to difficulty of attribution.

- As far as the internal policies part is concerned, we have assumed that the total was to be attributed to the input of production of services. Each Member State' part in this section of the "operating expenditure" has then been attributed consequently.

7. Concluding remarks

The results of this study should be considered in a context where one of the main aims of the European Budget is to re-distribute resources among Member States so as to fund a more harmonised development of the different economies. It is therefore quite normal that more prosperous Member States should be "net" contributors, although the relative size of their "balance" is ultimately a matter of political choice and acceptance. It seems however established that when evaluating the benefits accruing from European expenditure the analysis of the budgetary flows constitutes a very limited, and in a way misleading, instrument. As the evaluation of these benefits constitutes for the Member States a precondition of fundamental political decisions (first of all, the amount of the resources of the European Budget), a proper analysis would require estimating the increase in domestic output generated by EU expenditure together with the side effects generated in other countries.

Beside the possibility to properly estimate benefits accruing from EU expenditure the proposed methodology has several advantages. In contrast to a method based on budgetary flows the proposed methodology:

1. takes explicitly into account the interrelations among the different productive activities on the basis of an input-output model;
2. quantifies the increase of production as a result of EU expenditure and makes therefore possible to estimate the quantitative and geographical effects of an eventually different sectorial allocation of the EU expenditure;
3. highlights the fact that if the level of the additional production induced is greater than the EU expenditure, this same level depends on the economic structure of each country;
4. stresses the importance of intra-community commercial flows in order to estimate the benefits accruing to country X from EU expenditure in

country Y.

Note:
[*] Il presente contributo è stato preventivamente sottoposto a referaggio anonimo affidato ad un componente del Comitato di Referee secondo il Regolamento adottato da questa Rivista.
[1] S. Pisani is an official of the "'Agenzia delle Entrate", an agency of the Italian Ministry of Economy and Finances (Stefano.Pisani@agenziaentrate.it). Opinions expressed in this paper are personal and in no way commit his employer.
[2] See Art. 4 and 5 of Council Decision 2007/436/EC, Euratom of 7 June 2007. The details of the calculation are set in a Commission working document (Commission working document of 23 May 2007, available on: http://ec.europa.eu/budget/library/biblio/documents/financing/calc_own_res_2007_en.pdf.
[3] In reality such data are calculated at least since 1995. See European Commission (1998), annex 3, page 5.
[4] See European Commission (2003), page 2. Similar concern had been expressed by the European Court of Auditors (1998), Para. 3.29. The Berlin European Council (1999) has also recognised that "[..] the full benefits of Union membership cannot be measured solely in budgetary terms (See Presidency conclusions, point 68). A full statement has been made by the Commission in the Own Resources Report (1998), chapter 2, and in "Budget Contributions, EU Expenditure, Budgetary Balances and relative Prosperity of the Member States", paper presented by President Jacques Santer to the Ecofin Council of October 13, 1997.
[5] The overall ceiling of payment appropriations is currently set at 0,98 % of the total GNI of the Member States. According to the applicable rules, Revenue and Payment appropriations must balance each other. This means that expenditure cannot go beyond this limit.
[6] At the time called the GNP resource.
[7] European Commission Own Resources Report (2004), sections I (pages 6-8) and II (pages 25-40)
[8] See European Commission (1998), page 19.
[9] See the Commission Own Resources Report (1998), chapter 2 and annex 3 and the Commission's reports on allocation of "operating expenditure".
[10] The second interim Commission's report on economic and social cohesion (COM (2003) final of 30.1.2003, page 15) indicates concerning expenditure related to Objective 1 that there are substantial effects outside

the eligible areas. It is estimated that due to the single market one quarter of the expenditure will be employed in other areas, and almost 1/10 even outside the EU.

[11] An input-output model is essentially a simplified general theory of production; it explains the magnitudes of the inter-industry flows in terms of the levels of production in each sector. This model is based on the premise that it is possible to divide all economic productive activities into sectors whose interrelations can be meaningfully expressed in a set of simple input functions. It is not sufficient to consider only one economic system described in terms of interdependent industries; it is also necessary to combine several national models into a larger economic unit. See Leontiev (1966), Chenery (1959).

[12] An empirical application of this method is showed in Cipriani & Pisani (2004).

[13] Which is the Community version of the United Nations' System of National Accounts (SNA). Eurostat (1995), UN (1993).

References

Chenery H. B. (1959) *Inter-industry economics*, John Willey and sons, inc., N. Y.

Cipriani G., Pisani S. (2004) *The European Budget: an alternative to budgetary balance to assess benefits for Member States*, SIEP October 7-8.

EU Commission - Eurostat (1995) *European System of Integrated Economic Accounts*, Luxembourg.

EU Commission, (1997) *Budget contributions, EU expenditure, budgetary balances and relative prosperity of the Member States*, document presented to the Ecofin Council of 17.10.1997

EU Commission (1998) *Financing the European Union*, COM (1998) 560 final, Brussels.

EU Commission (2003) *Allocation of 2002 EU operating expenditure by Member State*, Brussels.

EU Commission (2004) *Financing the European Union*, COM (2004) 505 final, Brussels.

EU Commission - Eurostat (2004) *Handbook of Input Output table,* Luxembourg

European Parliament (1998) *Réforme des ressources propres et positions nettes du budget de l'Union européenne*, PE 228.586, Luxembourg

EU Court of Auditors (1998) *Special report n° 6/98 concerning the system of resources based on VAT and GNP*, OJ C 241 of 31.7.1998.

Leontiev W. (1951) *The Structure of American Economy, 1919-1939*.

Leontiev W. (1966) *Input-Output economics*, Oxford University Press, N.Y
Stone R. (1956) *Input-output and the Social Accounts*, in *The structural interdependence of the Economy*.
UN (1993) *System of National Accounts*, N. Y.
UNIDO (1972) *Guidelines for Project Evaluation*, Vienna.
Weise C. (Deutsches Institut für Wirtschaftsforschung) (1997) *Deutsche Debatte um den EU-Haushalt, Senkung des Nettobeitrags kein Reformersatz*, Wochenbericht 40/97

Tra riservatezza e tutela della salute: un possibile bilanciamento tra diritto alla riservatezza della cartella clinica, diritto della madre a una scelta riproduttiva consapevole e diritto del concepturus a nascere sano

di
Vinca Giannuzzi Savelli
Davide Borelli

Tribunale civile di Napoli, Sez. I, 18 settembre 2014, n. 13212.
Riservatezza – Protezione dei dati personali – Accesso alla cartella clinica del defunto – Ricorso ex art. 152 d.lgs. 196/2003 – Diritto del concepturus a nascere sano.

Svolgimento del processo.

L'istante ha proposto ricorso *ex* art. 152 del d.lgs. 30.6.2003, n. 196 (Codice in materia di protezione dei dati personali, ndr) [*omissis*] al fine di ottenere – per le ragioni analiticamente indicate nell'atto introduttivo – l'annullamento, previa sospensione dell'efficacia esecutiva, del provvedimento del Garante per la protezione dei dati personali [*omissis*].
Con memoria difensiva [*omissis*] il Garante per la protezione dei dati personali ha chiesto dichiararsi inammissibile l'opposizione e, comunque, rigettarla in toto in quanto infondata in fatto ed in diritto.
D.I., seppur regolarmente citata, non si è costituita in giudizio.
Acquisita documentazione varia, concessi i termini per il deposito di note difensive, [*omissis*] dopo la discussione orale, il Giudice Unico ha dato lettura del dispositivo e della contestuale motivazione.
Va preliminarmente dichiarata la contumacia di D.I. che non si è costituita in giudizio seppure regolarmente e tempestivamente citata [*omissis*].
In ordine alla ritualità della costituzione in giudizio della difesa del Garante per la protezione dei dati personali non sfugge a chi scrive che il deposito della memoria difensiva è avvenuto tardivamente [*omissis*] e, dunque, senza il rispetto del termine di dieci giorni di cui all'art. 416 c.p.c. Tuttavia, considerato che la documentazione allegata alla memoria risulta già prodotta in atti da parte ricorrente, di fatto nessun rilievo, ai fini della decisione, assume la tardiva allegazione documentale di parte opposta.
Tanto premesso in punto di rito, prima di passare all'esame del merito della controversia va, in questa sede, evidenziato che parte attrice ha chiesto l'annullamento, previa sospensiva, del provvedimento del Garante oggetto di

impugnativa, per violazione e/o falsa applicazione degli artt. 9 e 92 del d.lgs. 30.6.2003, n. 196.
In particolare l'istante ha dedotto che [*omissis*] D.I., asserendo di aver partorito [*omissis*], presso il Presidio Ospedaliero di B., una neonata di sesso femminile, trasferita il giorno successivo presso il reparto di Terapia Intensiva Neonatale del Presidio Ospedaliero del S. per il sospetto che la stessa fosse affetta da una malattia genetica, e di aver interesse all'accesso alla cartella clinica per l'esigenza di identificare la malattia genetica della figlia al fine di evitare ulteriori gravidanze con esiti infausti per il nascituro, chiedeva all'Azienda Sanitaria, *ex* art. 92 del d.lgs. 30.6.2003, n. 196, copia della cartella clinica della neonata, allegando unicamente copia dell'attestato di nascita rilasciato dal Presidio Ospedaliero di B. e del documento di riconoscimento dell'istante. Tale richiesta, essendo ritenuta in contrasto con quanto disposto dalla normativa sulla privacy in quanto priva di qualsiasi documentazione attestante il collegamento tra la richiedente e la neonata, era rigettata dall'Azienda, una prima volta, [*omissis*], ed una seconda volta, in seguito a reiterazione, [*omissis*]. Avverso il diniego di accesso la D.I. proponeva ricorso al Garante per la protezione dei dati personali, esponendo, per la prima volta, di essere stata ricoverata presso il Presidio Ospedaliero di B., di aver partorito lì, [*omissis*], una neonata di sesso femminile, trasferita il giorno successivo presso il reparto di Terapia Intensiva Neonatale dell'Ospedale S., e di non aver riconosciuto la neonata. Il Garante chiedeva chiarimenti all'Azienda che [*omissis*] comunicava di non aver potuto soddisfare la richiesta perché «*presso la struttura ospedaliera non risultava essere mai stata ricoverata alcuna minore figlia legittima della signora D.I. Tale circostanza rende impossibile procedere nella valutazione della sussistenza o meno di diritti o interessi legittimi che possano rendere accessibili i dati richiesti*». Lo stesso Garante chiedeva ulteriormente all'Azienda di precisare se [*omissis*] risultasse ricoverata una neonata proveniente dal Presidio Ospedaliero di B. e, ricevuta risposta affermativa dall'Ospedale S., accoglieva il ricorso della D.I. ed ordinava all'Azienda l'ostensione della cartella clinica della neonata, condannando l'Azienda alle spese del procedimento.
Ad avviso dell'opponente, il provvedimento era errato sia nella parte in cui riteneva illegittimo il diniego di accesso espresso dall'Azienda S. che in quella in cui condannava l'Azienda al pagamento delle spese e dei diritti della procedura perché: 1) non conteneva alcuna valutazione sia in ordine alla sufficienza dell'istanza che in ordine agli obblighi gravanti sull'Azienda relativamente alla tutela dei dati sensibili; 2) era stato adottato in assenza di qualunque prova circa la legittimazione della D.I. alla proposizione dell'istanza; 3) era stato emesso sulla base di atti e documenti intervenuti

successivamente all'istruttoria conclusasi con il diniego, avendo l'istante, solo in sede di ricorso, precisato di essere la madre naturale della neonata di cui aveva chiesto la cartella clinica, di non aver proceduto al riconoscimento della bambina ed allegato la propria cartella clinica da cui risultava il proprio parto avvenuto presso il Presidio Ospedaliero di B. Inoltre, sempre ad avviso dell'opponente, il provvedimento oggetto di doglianza era errato perché adottato in assenza di prova dell'esistenza di un rapporto parentale, anche di fatto, necessario ai sensi dell'art. 9 del d.lgs. n. 196/2003 per l'accesso ai dati personali concernenti persone decedute, non essendo all'uopo sufficiente la circostanza – puramente casuale e da sola priva di qualunque rilevanza probatoria – che la neonata provenisse dal Presidio Ospedaliero di B. dove la D.I. aveva partorito. Da ultimo era indicata quale circostanza dirimente la circostanza che la neonata, a seguito del rifiuto di riconoscimento, era stata affidata al Tribunale dei Minori [*omissis*], le era stato attribuito un nome di fantasia ed era stata assegnata alla tutela di un tutore. Quindi solo quest'ultimo, in quanto esercente la potestà genitoriale, avrebbe avuto il diritto di accedere ai dati relativi alla neonata oggetto di tutela. Di conseguenza la D.I. avrebbe dovuto presentare istanza al Tribunale per i Minorenni per ottenere informazioni sulla neonata ed eventualmente formulare richiesta di accesso alla relativa cartella clinica.
A confutazione delle argomentazioni dell'opponente la difesa del Garante ha evidenziato, sulla base della più recente giurisprudenza amministrativa, la sussistenza del diritto della D.I. all'accesso alla cartella clinica ai sensi dell'art. 9, co. 3 del d.lgs. 30.6.2003, n. 196 e, dunque, del conseguente obbligo dell'Ospedale di fornire la documentazione richiesta.
Questo giudice ritiene – per le argomentazioni di seguito esposte – pienamente legittimo il provvedimento del Garante che va, dunque, confermato in ogni sua parte.
Nella fattispecie in esame trovano applicazione gli artt. 4, 7 e 9 del d.lgs. 30.6.2003, n. 196. In particolare, considerato che l'istanza della D.I. risulta volta ad ottenere copia della cartella clinica della figlia della richiedente e, dunque, la conoscenza di dati sensibili, cioè di dati personali idonei a rivelare lo stato di salute di una persona, *ex* art. 4, co. 1 del d.lgs. 30.6.2003, n. 196, il diritto alla comunicazione di tali dati in forma intellegibile, concernendo una persona deceduta (circostanza pacifica tra le parti in causa), poteva essere esercitato solo nel caso in cui la predetta avesse un interesse proprio o agisse a tutela dell'interessato o per ragioni familiari meritevoli di protezione. Ebbene, nel caso *sub iudice*, come correttamente evidenziato nel provvedimento del Garante oggetto di impugnativa, ricorrono tutti i presupposti normativi per l'accoglimento della richiesta della D.I.

Ed invero quest'ultima, in qualità di madre, anche solo naturale (avendo la stessa esercitato il diritto a non essere nominata di cui all'art. 30, co. 1 del D.P.R. 3.11.2000, n. 396) di una bambina, nata [*omissis*] presso l'Ospedale di B. e trasferita il giorno successivo presso il reparto di Terapia Intensiva Neonatale dell'Azienda Ospedaliera S. [*omissis*] dove è deceduta [*omissis*], ha legittimamente esercitato il suo diritto di accesso alla cartella clinica al fine di disporre delle informazioni indispensabili all'esecuzione di indagini cliniche necessarie ad accertare la patologia genetica di cui potrebbe essere portatrice e le modalità della sua trasmissione così da poter conseguentemente effettuare una valutazione del rischio procreativo e consentirle un'ulteriore scelta riproduttiva consapevole ed informata (cfr. provvedimento del Garante per la protezione dei dati personali del 22.5.1999 e Corte Cost., sent., 18.11.2013, n. 278).
E' indubbio, infatti, che a base della richiesta di accesso si profilano, in capo all'istante sia la titolarità di un "interesse proprio" alla conoscenza dei dati sensibili della figlia, che la sussistenza di "ragioni familiari meritevoli di tutela".
In ordine al primo requisito va ricordato che affinché l'istanza di accesso sia legittima è sufficiente secondo la precisa definizione dell'art. 22, co. 1, lett. b) della l. 7.8.1990, n. 241 (Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi, ndr) che l'istante sia titolare di un interesse giuridicamente rilevante, personale e concreto e ricollegabile al soggetto stesso da uno specifico nesso e che la documentazione richiesta sia direttamente riferibile a tale interesse oltre che individuata o ben individuabile (cfr. *ex multis* Cons. Stato, Sez. III, sent., 12.6.2012, n. 3459). Ebbene, considerato che la richiesta non è stata proposta da un soggetto qualunque bensì dalla madre naturale della minore deceduta, strettamente legata per ragioni personali, familiari ed affettivi alla minore e motivata dall'esigenza di conoscere le ragioni del decesso, la donna risulta portatrice di una posizione qualificata alla conoscenza della documentazione in questione. Né a considerazioni diverse può pervenirsi sulla base del dato costituito dall'esercizio del diritto da parte della donna, a non essere nominata e ciò in quanto la "mancata genitorialità giuridica" non comporta certo la negazione della "genitorialità naturale" (cfr. Corte Cost., sent., 18.11.2013, n. 278). Dunque, sebbene fosse stato nominato quale tutore il Tribunale per i Minorenni, non sfugge a chi scrive che, essendo deceduta la minore all'epoca dell'istanza di accesso, risulta di fatto venuta meno in capo a tale organo la legittimazione a conoscere i dati sensibili della neonata.
Quanto all'ulteriore requisito, avendo la richiedente documentato con una consulenza genetica la necessità di conoscere le informazioni sanitarie

inerenti la minore per l'esecuzione delle indagini cliniche necessarie ad accertare la patologia genetica di cui la donna potesse essere portatrice e le modalità della sua trasmissione così da poter effettuare una valutazione del rischio procreativo e consentirle un'ulteriore scelta riproduttiva consapevole ed informata, sussistono le ragioni familiari meritevoli di tutela e, dunque, la necessità di tutelare diritti fondamentali, di rango costituzionale, contemplati dagli artt. 2, 29, 31 co. 2 e 32 della Costituzione.

Del tutto inconferente al caso in esame è, inoltre, il richiamo – operato dalla difesa dell'opponente – al disposto di cui all'art. 92, co. 2, lett. b) del d.lgs. 30.6.2003, n. 196. Ed invero in base a tale disposizione la richiesta di rilascio di copia della cartella clinica da parte di soggetti diversi dal diretto interessato può essere accolta, in tutto in parte, solo se la richiesta sia giustificata dalla documentata necessità di tutelare, in conformità alla disciplina sull'accesso documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quello dell'interessato ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale ed inviolabile. Orbene è evidente che tale norma può trovare applicazione solo nei casi – diversi da quello *sub iudice* - in cui si debba operare un bilanciamento di interessi tra l'esigenza di tutela del diritto alla riservatezza dell'interessato – diritto personalissimo che si estingue con la morte del titolare, sopravvivendo solo una forma di tutela dei dati sensibili – come altre forme di tutela – anche dopo la morte, esclusivamente nelle forme specifiche previste dall'art. 9 del d.lgs. 30.6.2003, n. 196 (cfr. Cons. Stato, Sez. V, sent., 9.6.2008, n. 2866; Cons. Stato, Sez. III, sent., 12.6.2012, n. 3459) – ed altri diritti di rango costituzionale.

In ordine agli ulteriori motivi di doglianza dell'opponente, in precedenza riportati nei punti nr. 1 e 3, osserva la scrivente che, come tra l'altro correttamente evidenziato da parte opposta, il Garante, adìto *ex* artt. 145 e ss. del d.lgs. 30.6.2003, n. 196, non essendo tenuto a tanto, ai fini dell'accoglimento della richiesta di accesso alla cartella clinica non ha effettuato alcuna valutazione del comportamento dell'Azienda Ospedaliera dal momento che la funzione del Garante non è quella di giudicare la condotta dei soggetti in causa ma solo di risolvere, in sede amministrativa, il conflitto tra il richiedente l'accesso ed il titolare; compito, in concreto, espletato nel pieno rispetto delle disposizioni sopra richiamate.

Correttamente al solo fine di regolamentare, su richiesta della D.I., l'ammontare delle spese dei diritti inerenti il ricorso ed il riparto degli stessi tra le parti in causa, il Garante ha valutato il comportamento tenuto dall'Azienda Ospedaliera nel corso dell'intero procedimento amministrativo.

Orbene, anche in relazione a tale punto della decisione, il provvedimento appare congruamente e correttamente motivato.

In particolare, ad avviso di questo Giudice, parte opponente nel corso del procedimento instaurato a seguito del ricorso al Garante, non si è adeguatamente attivata per garantire l'effettivo esercizio dei diritti di cui all'art. 7 del d.lgs. 30.6.2003, n. 196.
Ed invero se, per un verso, appare condivisibile la scelta dell'azienda di non dare positivo riscontro alle prime due istanze di accesso della D.I., non altrettanto può condividersi analoga scelta adottata dall'Ospedale nel corso del procedimento instaurato dinanzi al Garante.
Infatti all'atto della disamina della prima e della seconda richiesta della D.I. gli elementi di valutazione forniti all'opponente e documentati allo stesso [*omissis*] sono: 1) generalità della madre e del padre della neonata; 2) sesso di quest'ultima; 3) giorno, luogo ed orario della nascita; 4) Presidio Ospedaliero di provenienza; 5) giorno del ricovero della neonata presso il reparto di Terapia Intensiva Neonatale dell'Azienda; 6) generica indicazione delle ragioni del ricovero e di quelle a base della richiesta.
Ebbene, considerato che tali richieste risultano carenti dell'indicazione delle generalità complete della minore, della durata e dell'esito del ricovero, della patologia diagnosticata o anche solo sospettata nei confronti della neonata, l'Azienda compulsata non è stata posta in condizione di valutare la sussistenza, in concreto, dei presupposti di cui agli articoli – sopra richiamati – per l'accesso alla cartella clinica.
Diversamente la stessa Azienda, nel corso del procedimento amministrativo, ha avuto modo di conoscere ulteriori e decisivi elementi indispensabili per la valutazione e per l'accoglimento della richiesta quali: 1) l'esercizio, da parte della madre, del diritto a non essere nominata *ex* art. 30 del D.P.R. 3.11.2000, n. 396; 2) la durata del ricovero; 3) il luogo e la data del decesso della neonata per una patologia genetica.
La rilevanza e la decisività di tali dati scaturiscono dal fatto che, per un verso, risulta superata l'unica motivazione addotta dall'Azienda Ospedaliera a conforto del reiterato rigetto dell'istanza di accesso costituita dal mancato ricovero presso detta struttura di una figlia legittima della richiedente e che, per un altro, la normativa sopra richiamata, per le ragioni in precedenza esposte, non consente l'interpretazione restrittiva propugnata dall'opponente.
In definitiva le carenze e le omissioni delle prime due richieste della D.I. giustificano la compensazione delle spese del procedimento fino all'ammontare di € 100,00 in quanto espressive di un comportamento poco collaborativo dell'istante. Diversamente, per le spese residue, quantificate in € 400,00, la condanna dell'Azienda Ospedaliera al pagamento delle stesse è correttamente motivata dalla facile accertabilità delle circostanze addotte dalla richiedente a fondamento della sua istanza.

Per tutte le ragioni esposte il ricorso va rigettato perché infondato. [*omissis*]
P.Q.M.
Il Tribunale, in composizione monocratica, letti gli artt. 1 e ss. del d.lgs. 30.6.2003, n. 196, definitivamente pronunciando nella controversa come innanzi proposta, così provvede:

- Dichiara la contumacia di D.I.;
- Rigetta l'opposizione e, per l'effetto, conferma il provvedimento del Garante per la protezione dei dati personali [*omissis*];
- Condanna l'Azienda Ospedaliera di rilievo nazionale S. [*omissis*], in persona del Direttore generale *pro tempore* [*omissis*], alla rifusione delle spese di costituzione e rappresentanza in favore del Garante per la protezione dei dati personali, in persona del Presidente *pro tempore*, elettivamente domiciliato *ex lege* presso l'Avvocatura Distrettuale dello Stato di Napoli [*omissis*];
- Dichiara non ripetibili le spese del procedimento nei confronti di D.I.

Così deciso in Napoli il 18.9.2014

Abstract
La mancata genitorialità giuridica non comporta la negazione della genitorialità in sé quale requisito necessario e sufficiente per l'accesso alla cartella clinica del figlio defunto non riconosciuto, ciò al fine di tutelare il diritto ad una corretta valutazione del rischio procreativo e ad una scelta riproduttiva consapevole ed informata. Il necessario bilanciamento tra diritti potenzialmente confliggenti ha condotto i Giudici della Suprema Corte a ritenere prevalente il diritto della madre (e del concepturus?) rispetto al diritto alla riservatezza del neonato defunto partorito in anonimato.

Anonymously childbirth does not involve the denial of parenting itself as a necessary (and sufficient) condition for the access to the medical records of the deceased not recognized son, this in order to protect the right to a proper procreative risk assessment and an informed reproductive choice. The necessary balance between potentially conflicting rights led the Judges of the Supreme Court with a majority believing the right of the mother (and of the concepturus?) over the right to privacy of the deceased infant birth in anonymity.

Sommario: 1. La vicenda. - 2. Il quadro normativo di riferimento: tra legge sul procedimento amministrativo e normativa sulla protezione dei dati personali. - 3. La tutela della riservatezza e delle "ragioni familiari meritevoli

di protezione" ex art. 9, co. 3 Codice privacy: un possibile bilanciamento tra rapporto parentale biologico e legittimo. - 4. E' configurabile un diritto alla salute della progenie?

1. La vicenda.

La D.I. (*hic et inde*, resistente) partoriva, presso il Presidio Ospedaliero di B., in anonimato [1], una neonata di sesso femminile. Il giorno successivo al parto l'infante veniva trasferita con urgenza al reparto di Terapia Intensiva Neonatale del Presidio Ospedaliero S. a causa di una sospetta patologia congenita, sì grave da determinarne, a pochi giorni dal ricovero, la morte.
Ad un anno dall'infausto evento, la resistente recapitava al Presidio Ospedaliero S. formale istanza di accesso alla cartella clinica della neonata prematuramente scomparsa, allegando all'uopo copia fotostatica dell'attestato di nascita – rilasciato dal Presidio Ospedaliero di B. – e del proprio documento di riconoscimento. Cartella che avrebbe reso possibile – si badi – l'identificazione della patologia genetica potenzialmente trasmissibile alla futura progenie [2]. Ciò nondimeno, la richiesta veniva dall'Azienda sia in prima che in seconda istanza – in seguito a reiterazione della medesima – rigettata, a norma del d.lgs. 30.6.2003, n. 196, in quanto priva di sufficiente documentazione attestante il collegamento tra la richiedente e la neonata.
Avverso tale diniego, la resistente proponeva rituale ricorso al Garante per la protezione dei dati personali, ai sensi dell'art. 145 del d.lgs. 30.6.2003, n. 196. Opportunità, questa, colta dalla donna per fornire ulteriori (nonché, necessarie) indicazioni utili all'attestazione del legame parentale, ovvero «di essere stata ricoverata presso il Presidio Ospedaliero di B., di aver partorito lì, [*omissis*], una neonata di sesso femminile, trasferita il giorno successivo presso il reparto di Terapia Intensiva Neonatale dell'Ospedale S., e di non aver riconosciuto la neonata».
Ritenuto legittimo il ricorso presentato dalla donna, il Garante si premurava di interpellare l'Azienda Ospedaliera S. per chiarimenti. Quest'ultima comunicava di non aver potuto soddisfare la richiesta in quanto non risultava esser mai stata ricoverata presso la struttura ospedaliera alcuna figlia legittima della resistente, rendendo tale circostanza impossibile procedere nella valutazione della sussistenza o meno di diritti o interessi legittimi, presupposti necessari per l'accesso ai dati richiesti. Interpellata ulteriormente dal Garante, l'Azienda dichiarava, peraltro, che «dall'anagrafe dei pazienti ricoverati (il giorno del parto, ndr) risulta essere pervenuta, a seguito di

trasferimento da altro Istituto pubblico (Presidio Ospedaliero di B., ndr)» [3] una neonata.
Considerati sufficienti gli elementi raccolti nelle more del procedimento, il Garante, definitivamente pronunciandosi, ordinava all'Azienda Ospedaliera S. di consentire alla ricorrente l'accesso, entro trenta giorni, a tutti i dati sanitari contenuti nella cartella clinica relativa alla neonata.
Con atto di citazione, ai sensi dell'art. 152 del d.lgs. 30.6.2003, n. 196, l'Azienda Ospedaliera S. proponeva rituale ricorso per l'annullamento, previa sospensione dell'efficacia esecutiva, del provvedimento del Garante.

2. Il quadro normativo di riferimento: tra legge sul procedimento amministrativo e normativa sulla protezione dei dati personali.

La cartella clinica in quanto tale è da considerarsi documentazione sanitaria, ovvero l'insieme dei dati, delle informazioni e degli atti che definiscono ed oggettivano regole e comportamenti di ciascuna struttura organizzativa.
Negli ultimi decenni la cartella clinica inizia a diventare uno strumento essenziale per le strutture sanitarie e al tempo stesso un problema piuttosto complesso. Da semplice registrazione di dati essenziali del paziente (e della sua malattia), si è passati a una raccolta di sempre più numerosi documenti sanitari e informazioni che nella loro articolazione organica e logica devono soddisfare numerose esigenze, non soltanto quelle rigorosamente clinico diagnostico terapeutiche del paziente.
Ciò è dovuto, da un lato, all'incalzante sviluppo tecnologico ed ai notevoli progressi scientifici e, dall'altro, all'evoluzione di una serie di sistemi, quali quello politico, economico e sociale cui è strettamente legata quella che prima era semplicemente considerata assistenza sanitaria e che oggi è diventata un vero e proprio sistema sanitario articolato e complesso.
Se da un lato è evidente il coinvolgimento delle norme concernenti l'accesso agli atti amministrativi ai sensi degli artt. 22 e ss. della legge del 7.8.1990, nr. 241 (di seguito, Legge sul procedimento amministrativo), dall'altro non può negarsi l'esigenza del rispetto della riservatezza quale diritto fondamentale di rango costituzionale, regolato nel dettaglio dal decreto legislativo del 30.6.2003, nr. 193 (di seguito, Codice privacy).
In tema i Giudici ermellini [4] hanno avuto modo di chiarire che la finalità della cartella clinica è quella di riflettere in maniera fedele il decorso e l'evolversi della malattia e degli altri fatti clinici rilevanti, progressivamente e contestualmente al loro verificarsi.
Inoltre, la cartella clinica, redatta da un medico di un ospedale pubblico, è caratterizzata dalla produttività di effetti incidenti su situazioni giuridiche soggettive di rilevanza pubblicistica, nonché dalla funzione della

documentazione di attività compiute (o non compiute) dal pubblico ufficiale che ne assume la paternità.
La prevalente dottrina attribuisce una rilevanza giuridica particolare alla cartella clinica, in quanto è l'unico strumento atto a trattare le informazioni per la cura del paziente e a permettere la comunicazione tra i diversi operatori sanitari.
Data la peculiare rilevanza il medico incaricato della compilazione è considerato un pubblico ufficiale ai sensi e per gli effetti di cui all'art. 357 c.p., mentre il responsabile della compilazione, della conservazione e della buona tenuta è sempre il primario del reparto presso cui il paziente è ricoverato.
Al medico incaricato della compilazione è richiesta particolare attenzione nell'inserimento degli elementi prescritti dall'art. 24 del Decreto del Ministero della Salute del 5.8.1977 [5] e disposti secondo le modalità previste dall'art. 26 del Codice di deontologia medica [6].
La cartella clinica ed i relativi referti devono, poi, essere conservati per un tempo illimitato in quanto rappresentano atti ufficiali essenziali a garantire la certezza dei dati clinici ivi riportati, nonché preziose fonte documentaria per ricerche di carattere storico-sanitario. Proprio in ragione di ciò l'art. 26, co. 3 del Codice di deontologia medica, infatti, prescrive che «in caso di cessazione dell'attività della casa di cura le cartelle cliniche dovranno essere depositate presso l'ufficio comunale o consorziale di igiene».
E' qui che assume, dunque, fondamentale rilevanza giuridica il tema dell'accesso da parte di terzi alle informazioni contenute in cartelle cliniche appartenenti a soggetti estranei, ancorché defunti.
Il giudice amministrativo è, infatti, ai sensi dell'art. 133, co. 1, nr. 6) del decreto legislativo del 2.7.2010, nr. 104 (di seguito, Codice del processo amministrativo), chiamato a contemperare interessi contrapposti. Si rende, dunque, necessaria una valutazione comparativa dei configgenti interessi: da un lato la situazione giuridicamente qualificata dell'istante, titolare di un interesse diretto, qualificato, concreto ed attuale all'esame, presa visione e rilascio di copia della cartella clinica ai sensi dell'art. 22 della Legge sul procedimento amministrativo; dall'altro, il diritto del controinteressato alla riservatezza dei propri dati sensibili [7], ovvero di dati personali idonei a rivelare il suo stato di salute e il proprio orientamento sessuale, in quanto tali tutelati dal Codice privacy.
Risulta piuttosto numerosa la casistica giurisprudenziale in tema di accesso alle cartelle cliniche.
I parametri normativi di riferimento sono sostanzialmente contenuti negli artt. 7, 9, 60, 82 e 92 del Codice privacy.

A norma dell'art. 9, co. 3 del Codice privacy «i diritti di cui all'art. 7 riferiti a dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione». Si badi, peraltro, che l'art. 7 considera non soltanto le posizioni soggettive di chi può esercitare il diritto di accesso (cfr. commi 1, 2 e 3), ma anche di chi può opporsi.
Il Consiglio di Stato [8] in una recente pronuncia ha, infatti, avuto modo di chiarire che l'art. 9, co. 3 Codice privacy «regola anche l'accesso alle cartelle cliniche, dal momento che non può trovare applicazione la disciplina specificamente prevista in materia dall'art. 92 del medesimo Codice, il quale consente l'accesso alle cartelle cliniche solo a persone diverse dall'interessato che possono far valere un diritto della personalità o altro diritto di pari rango». In effetti, se dovesse applicarsi tale disposizione anche dopo il decesso, neanche i più stretti congiunti potrebbero accedere ai dati personali del defunto in assenza dei presupposti richiesti dalla norma, con conseguenze assolutamente paradossali. Peraltro, «non è neppure utile il richiamo per analogia all'art. 82 del medesimo codice, che regola la diversa situazione della prestazione del consenso al trattamento dei dati personali in caso di impossibilità fisica o giuridica dell'interessato e che prevede che il consenso possa essere fornito, in assenza di chi esercita la potestà legale, da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato». Da ciò si deduce che sopravvive una forma di tutela dei dati sensibili – così come altre forme di tutela – anche dopo la morte soggetto, ma nelle forme specifiche e diverse previste dall'art. 9, che individua precisamente gli interessi che possono bilanciare quelli di terzi ad accedere ai dati personali: la tutela del defunto e ragioni familiari meritevoli di protezione.
Infine, l'art. 60 del Codice privacy stabilisce che quando il trattamento concerne dati idonei a rivelare lo stato di salute o la vita sessuale di un soggetto, il trattamento è consentito solo se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi è di rango quantomeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in altro diritto o libertà fondamentale e inviolabile.

3. La tutela della riservatezza e delle "ragioni familiari meritevoli di protezione" ex art. 9, co. 3 Codice privacy: un possibile bilanciamento tra rapporto parentale biologico e legittimo.

La decisione riconosce il diritto della madre biologica ad acquisire la cartella clinica della figlia partorita in anonimato ai sensi dell'art 30, co. 1 del D.P.R.

3.11.2000, nr. 396 e deceduta per gravi patologie congenite pochi giorni dopo la nascita, ciò al fine di «consentirle un'eventuale ulteriore scelta riproduttiva consapevole e informata».
Il diritto alla salute e alla maternità consapevole, a norma degli artt. 31 e 32 Cost., viene, pertanto, ritenuto prevalente rispetto all'esigenza di limitare l'accesso ai dati sensibili del minore solo ai familiari in senso stretto e in genere ai soggetti legittimati (tutori, affidatari) consentendosi quindi anche alla madre biologica innominata – che per sua scelta rinuncia al parto "riservato" e si palesa – di ottenere le informazioni cliniche necessarie.
Il provvedimento offre uno spunto di riflessione su quelle che attualmente sono le forme di tutela e i connessi limiti alla riservatezza nell'ambito dei rapporti parentali sia legittimi che biologici.
L'evoluzione socio-giuridica delle dinamiche familiari ha modificato anche i suoi contenuti relazionali rendendo spesso necessario un approfondimento nell'ambito di situazioni di conflittualità portate all'attenzione dell'autorità giudiziaria.
Quelli che, quindi, in passato erano contrasti sulle informazioni che potevano scambiarsi i coniugi tra loro o con i figli – contrasti risolvibili nell'ambito di una normale dialettica familiare – sono oggi invece approdati nelle aule dei Tribunali.
E così l'accesso a dati "sensibili", o comunque riservati, della persona è stato riconosciuto al familiare titolare di interessi confliggenti ma valutati, di volta in volta, tutelabili in misura maggiore.
Si è, ad esempio, attribuito al coniuge il diritto di visionare la cartella clinica del o della consorte in quanto utile ai fini dello scioglimento del matrimonio [9].
Invero, come a più riprese affermato dalla giustizia amministrativa [10], a norma dell'art. 60 Codice privacy, sussiste il diritto del marito di accedere alla cartella clinica della moglie, nel caso in cui l'istanza di accesso sia giustificata dalla necessità di promuovere validamente un azione giudiziaria volta all'annullamento del matrimonio innanzi al competente Tribunale diocesano; in tal caso, infatti, il fine dello scioglimento del vincolo matrimoniale costituisce una situazione giuridica di rango almeno pari alla tutela del diritto alla riservatezza dei dati sensibili relativi alla salute, in quanto involgente un significativo diritto della personalità.
Anche i dati reddituali del consorte – ove non condivisi in ambito familiare – sono stati considerati accessibili se necessari alla determinazione di un corretto assegno di mantenimento dei figli in un procedimento di cessazione degli effetti civili del matrimonio [11].
Al tempo stesso, è stato consentito l'accesso ai dati reddituali del convivente *more uxorio* dell'altro coniuge in quanto necessari alla determinazione di un

corretto assegno di mantenimento dei figli in un procedimento di separazione personale. Anche in tal caso il diritto di accesso prevale sull'esigenza di riservatezza di terzi, in quanto esercitato per consentire la cura o la difesa processuale di interessi giuridicamente protetti e concernente un documento amministrativo indispensabile a tali fini, la cui esigenza non può essere altrimenti soddisfatta. Di conseguenza, in capo al coniuge separato sussiste, secondo consolidata giurisprudenza [12], nei confronti dell'Agenzia delle Entrate, il diritto di accesso alle dichiarazioni dei redditi del convivente *more uxorio* dell'altro coniuge. Tale istanza di accesso documentale, infatti, essendo rivolta a dimostrare la capacità di reddito del convivente del coniuge separato, è funzionale ad esonerare il richiedente dall'obbligo di corresponsione dell'assegno di mantenimento.
Ad una prima analisi sembra, dunque, potersi affermare che l'ordinamento (o meglio, l'interpretazione che la giurisprudenza fornisce delle norme coinvolte) consente che si attui un'ingerenza nella sfera personale di un familiare solo se strumentale alla difesa di interessi di pari rango, già posti al vaglio giurisdizionale: soltanto a tali condizioni il diritto all'"informazione" prevale sulla riservatezza della persona in funzione di superiori esigenze familiari.
Ma se tal criterio val bene per il componimento di conflitti infra-coniugali, nelle relazioni tra genitori e figli il *favor* è lapalissianamente sbilanciato in favore dei primi.
E' stato, infatti, riconosciuto al genitore il diritto a prender visione del tema svolto dalla figlia durante l'esame di maturità per consentirgli di vigilare sui suoi orientamenti: pertanto, non per verificare il buon esito del percorso formativo intrapreso, ma allo scopo di «avere cognizione piena dei gusti, delle aspettative, degli orientamenti culturali che l'alunna sviluppa […] e che […] spesso, sfuggono ad un sano dibattito strettamente familiare» [13] (sic!).
In tal caso è stata dunque data priorità assoluta (*rectius*, incondizionata) al diritto-dovere spettante al genitore di vigilare sulla crescita del figlio a discapito della sua riservatezza e della sua libertà di espressione, in una visione forse paternalistica ma funzionale al buon andamento della vita familiare.
Buon andamento della vita familiare che diventa parametro scriminante anche per risolvere i contrasti che sorgono per lo scambio di informazioni sulla sfera intima all'interno di relazioni parentali biologiche e non legalizzate.
La Corte Costituzionale con una recente pronuncia [14] ha composto il conflitto tra il diritto del figlio adottato all'informazione sulle proprie origini biologiche e il diritto della madre naturale a restare anonima [15], ai sensi e per gli effetti di cui all'art. 30, co. 1 del DPR 3.11.2000, nr. 396, consentendo

l'accesso alle notizie sulla nascita biologica previo interpello della madre ai fini di un'eventuale revoca dell'anonimato e, dunque, di una auspicata conciliazione familiare.
Su tale scia si inserisce la sentenza in epigrafe che a tutela del diritto alla maternità consapevole ed a protezione dell'unità familiare costituita o costituenda rende conoscibili alla madre "anonima" i dati sanitari del figlio naturale.
Può ragionevolmente dedursi, dunque, che allo stato la riservatezza nei rapporti di parentela è destinata a recedere senz'altro dinanzi ad interessi preminenti come la tutela del nucleo familiare, ma anche in presenza di interessi di pari rango che nei singoli casi concreti vengano ritenuti funzionali al corretto svolgimento della vita familiare. Il rapporto parentale legittimo cede il passo a quello biologico, in funzione di superiori interessi di rango costituzionale.
Nel corso degli anni il concetto stesso di famiglia si è evoluto, trascendendo ora l'elemento sia genetico che biologico, nel senso che la stessa non è più solo quella tradizionale di cui all'art. 29 Cost., ma anche – e soprattutto - quella sociale, intesa come società naturale o formazione sociale, tramite il viatico dell'art. 2 Cost. [16] Ma un eloquente segnale del superamento del binomio verità genetica – verità biologica era già offerto dalla disciplina sull'adozione di minorenni. Infatti, l'art. 27 della legge 4.5.1983, nr. 184 consacra la piena equiparazione tra figlio adottivo e figlio legittimo [17].

4. È configurabile un diritto alla salute della progenie?

Un ulteriore considerazione par qui necessaria. Il diritto alla riservatezza sembra, infatti, cedere il passo non solo a «ragioni familiari meritevoli di protezione» [18] – prescindendo, dunque, della natura del rapporto di filiazione sotteso, biologico o legittimo – ma anche ad un diritto della futura progenie a nascer sana. Approdo ermeneutico probabilmente azzardato, ma, tuttavia, potenzialmente plausibile. Il diritto della madre biologica ad una «ulteriore scelta riproduttiva consapevole e informata» sembra, infatti, collimare perfettamente con un potenziale diritto alla salute della futura progenie.
Ciò nondimeno, i contributi dottrinali [19] e giurisprudenziali in merito sembrano per lo più considerare il diritto alla salute in relazione al solo nascituro concepito e non anche al *concepturus*: eppur tuttavia il codice del '42 in almeno due occasioni riconosce diritti in capo a quest'ultimo in quanto potenziale destinatario di disposizioni testamentarie e di donazioni [20] a norma degli artt. 462 e 784 c.c. La stessa Corte Costituzionale ha, in proposito, riconosciuto che «il patrimonio riservato per testamento o per

donazione ad un nascituro non concepito deve essere considerato come un patrimonio a sé stante» [21].
Gran parte della dottrina e della giurisprudenza ha a lungo dibattuto sul possibile riconoscimento di una capacità giuridica, per così dire, parziale in capo al nascituro concepito.
Secondo prevalente giurisprudenza «l'ordinamento tutela il concepito e l'evoluzione della gravidanza esclusivamente verso la nascita, riconoscendo semmai un "diritto a nascere" e "a nascere sano" e non un diritto "a non nascere" o "a non nascere se non sano" (Cass. civ., sez. III, 29.7.2004, nr. 14488 e Cass. civ., sez. III, 11.5.2009, nr. 10741)» [22].
Il diritto alla salute trova fondamento e tutela nell'art. 32 Cost., non solo come interesse della collettività, bensì come essenziale diritto dell'individuo, non limitandosi alle attività successive alla nascita, ma dovendosi ritenere esteso anche al dovere di assicurare condizioni favorevoli all'integrità del nascituro nel periodo precedente all'evento della nascita [23] [24].
I Giudici ermellini, in una ormai nota sentenza [25], giungono a ritenere il nascituro soggetto giuridico. Essi, in particolare, individuano analiticamente le fonti nazionali e sovranazionali su cui fondano detta ricostruzione: l'art.1 della l. 14.2.2004, nr.40 sulla procreazione medicalmente assistita [26]; l'art.1 della l. 22.5.1978, nr.194, sull'interruzione volontaria di gravidanza [27]; la sentenza della Corte Costituzionale del 10.2.1997, nr.25, che attribuisce al concepito il diritto alla vita, dando atto che il principio di tutela della vita umana sin dal suo inizio è oggetto di riconoscimento da parte della Dichiarazione dei diritti del fanciullo del 1989; l'art. 254, co.1 c.c. che consente il riconoscimento del figlio naturale anche solo concepito; la l. del 29.7.1975, nr.405 sull'istituzione dei consultori familiari; l'art.32 Cost. che, riferendosi all'individuo quale destinatario della tutela della salute, contempla implicitamente la protezione del nascituro; l'art. 3 della Dichiarazione universale dei diritti dell'uomo, che prevede il diritto alla vita spettante ad ogni individuo; nonché l'art.2 della Carta dei diritti fondamentali dell'Unione europea. La Suprema Corte coglie, dunque, l'occasione per affermare che il nascituro concepito risulta comunque dotato di autonoma soggettività giuridica in quanto titolare sul piano sostanziale di interessi personali in via diretta, rispetto ai quali l'avverarsi della *condicio iuris* della nascita è condizione imprescindibile per la loro azionabilità in giudizio per fini risarcitori [28].
Seguendo l'*iter* ragionativo proposto da tanta e tale dottrina, peraltro avallato da consistenti pronunce giurisprudenziali, sembra oggi non potersi negare, dunque, una parziale capacità giuridica al nascituro concepito; parimenti, sembra vicina l'estensione di detto riconoscimento anche al *concepturus*, titolare del diritto a nascere sano, diritto che in tal caso ha consentito alla madre biologica – non legittima – di accedere alla cartella

clinica della neonata morta, comprimendono così il suo fondamentale diritto alla riservatezza dei dati sanitari in esso archiviati.

Note:
[*] Il presente contributo è stato preventivamente sottoposto a referaggio anonimo affidato ad un componente del Comitato di Referee secondo il Regolamento adottato da questa Rivista.
[1] Tale facoltà è riconosciuta alla madre dal disposto di cui all'art. 30, co. 1 (rubricato, per l'appunto, "dichiarazione di nascita") del D.P.R. 3.11.2000, n. 396, ovvero il Regolamento per la revisione e la semplificazione dell'ordinamento dello stato civile, a norma dell'art. 2, co. 12 della l. 15.5.1997, n. 127, a tenore del quale «la dichiarazione di nascita è resa da uno dei genitori, da un procuratore speciale, ovvero dal medico o dalla ostetrica o da altra persona che ha assistito al parto, rispettando l'eventuale volontà della madre di non essere nominata».
[2] Come si legge nel provvedimento adottato dal Garante per la protezione dei dati personali (p. 1).
[3] Come si legge nel provvedimento adottato dal Garante per la protezione dei dati personali (p. 2).
[4] Cfr. Cass. pen., sez. V, 12 luglio 2011, n. 42917. Per approfondimenti si segnala L. Montone, *Nota a Cassazione penale, sez. V, 12 luglio 2011 n. 42917*, in *Riv. it. medicina legale e dir. sanitario*, 2, 2012, p. 722.
[5] L'art. 24, co. 1 e 2 del D.M. del 5.8.1977 concernente la "Determinazione dei requisiti tecnici sulle case di cura private", in particolare, dispone che «è prescritta, per ogni ricoverato, la compilazione della cartella clinica, da cui risultino le generalità complete, la diagnosi di entrata, l'anamnesi familiare e personale, l'esame obiettivo, gli esami di laboratorio e specialistici, la diagnosi, la terapia, gli esiti e i postumi [...] Le cartelle cliniche, firmate dal medico curante, dovranno portare un numero progressivo ed essere conservate a cura della direzione sanitaria».
[6] A norma dell'art. 25 del Codice di deontologia medica dispone che «1. Il medico redige la cartella clinica, quale documento essenziale dell'evento ricovero, con completezza, chiarezza e diligenza e ne tutela la riservatezza; le eventuali correzioni vanno motivate e sottoscritte. 2. Il medico riporta nella cartella clinica i dati anamnestici e quelli obiettivi relativi alla condizione clinica e alle attività diagnostico-terapeutiche a tal fine praticate; registra il decorso clinico assistenziale nel suo contestuale manifestarsi o nell'eventuale pianificazione anticipata delle cure nel caso di paziente con malattia progressiva, garantendo la tracciabilità della sua redazione. 3. Il medico registra nella cartella clinica i modi e i tempi dell'informazione e i termini del

consenso o dissenso della persona assistita o del suo rappresentante legale anche relativamente al trattamento dei dati sensibili, in particolare in casi di arruolamento in protocolli di ricerca».
[7] Ai sensi dell'art. 4, co. 1, lett. d) del Codice privacy sono dati sensibili «i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale».
[8] Cfr. Cons. St., sez. III, 12.6.2012, nr. 3459.
[9] Cfr. Tar Roma, sez. III *quater*, 15.12.2014, nr. 12590 secondo cui «il fine dello scioglimento del vincolo matrimoniale (religioso) costituisce una situazione giuridica di rango almeno pari alla tutela del diritto alla riservatezza dei dati sensibili relativi alla salute, in quanto involgente un significativo diritto della personalità [...] In presenza di tale situazione deve ritenersi sussistente l'interesse personale idoneo a legittimare l'accesso alla cartella senza che sia necessaria alcuna penetrante indagine in merito all'essenzialità o meno della documentazione richiesta né circa le prospettive di buon esito del rito processuale». Negli stessi termini si v. Cons. St., 14.11.2006, nr. 6681, in *Foro amm.*, fasc. 11, 2006, p. 3063.
[10] Cfr. Cons. St., sez. V, 14.11.2006, nr. 6681; Tar Catania, sez. IV, 7.5.2009, nr. 878; Tar Roma, sez. III, 15.12.2014, nr. 12583.
[11] Cfr. Tar Roma, sez. I *quater*, 2.12.2010, nr. 35020.
[12] Cfr. Cons. St., sez. IV, 20.9.2012, nr. 5047.
[13] Cfr. Tar Lecce, sez. II, 20.10.2014, nr. 2597. Per un'ampia trattazione della questione si v. R. Tommasini, *Persona e comunità familiare*, in *Atti Convegni Miscellanee*, Napoli, 1982, pp. 124 e ss.
[14] Cfr. Corte Cost., 22.11.2013, nr. 278.
[15] Il diritto all'identità personale ed alla ricerca delle proprie radici è tutelato da disposizioni di diritto internazionale pattizio ed in particolare dagli artt. 7 e 8 della Convenzione di New York del 20.11.1989, ratificata con legge del 27.5.1991, nr. 176 (Ratifica ed esecuzione della convenzione sui diritti del fanciullo, fatta a New York il 20.11.1989) e dall'art. 30 della Convenzione dell'Aja del 29.5.1993, ratificata con la legge del 31.12.1998, nr. 476 (Ratifica ed esecuzione della Convenzione per la tutela dei minori e la cooperazione in materia di adozione internazionale, fatta a L'Aja il 29.5.1993. Modifiche alla legge 4.5.1983, nr. 184, in tema di adozione di minori stranieri). Già con la sentenza del 25.9.2012 (Godelli c. Stato Italiano) la Corte di Strasburgo aveva ritenuto che l'art 28, co. 7 della legge nr. 184 del 1983 violasse l'art 8 della Cedu nella parte in cui tale articolo non prevede – attraverso un procedimento, stabilito dalla legge, che assicuri la

massima riservatezza – la possibilità per il giudice di interpellare la madre, che abbia dichiarato di non voler essere nominata, su richiesta del figlio, ai fini di una eventuale revoca di tale dichiarazione.

[16] A. Mendola, *Favor minoris e presidio del dato biologico*, in *Diritto fam. pers.*, fasc. 2, II, 2015, pp. 551 e ss.

[17] Sul punto si v. le considerazioni di G. Casaburi, *Procreazione medicalmente assistita: quel che resta della legge n. 40 del 2004*, *Nota ad ord. Trib. Milano 8 aprile 2013 e ad ord. Trib. Catania 13 aprile 2013*, in *Foro it.*, 9, I, 2013, p. 2500.

[18] Così l'art. 9, co. 3 del Codice privacy.

[19] G. Giacobbe, *Problemi civili e costituzionali sulla tutela della vita*, in *Dir. fam. pers.*, II, 1988, pp. 1119 ss.; P. Zatti, *Quale statuto per l'embrione?*, in *Riv. crit. dir. priv.*, 1990, pp. 463 ss.; F.D. Busnelli, *L'inizio della vita umana*, in *Riv. dir. civ.*, I, 2004, pp. 533 ss.; P. Papanti Pelletier, *Il problema della qualificazione soggettiva del concepito*, in *Procreazione assistita. Problemi e prospettive* (Volume di raccolta degli atti del Convegno di studi svoltosi a Roma presso l'Accademia dei Lincei il 31.5. 2005), Brindisi, 2005, pp. 229 ss.; G. Ballarani, *La capacità giuridica "statica" del concepito*, in *Dir. fam. pers.*, II, 2007, pp. 1462 ss.; G. Oppo, *L'inizio della vita umana*, in *Riv. dir. civ.*, I, 1982, pp. 499 ss.; Id., *Scienza, diritto e vita umana*, in *Riv. dir. civ.*, I, 2002, pp. 19 ss.; Id., *Declino del soggetto e ascesa della persona*, in *Riv. dir. civ.*, I, 2002, pp. 830 e ss.; Id., *Procreazione assistita e sorte del nascituro*, in *Il problema della qualificazione soggettiva del concepito*, in *Procreazione assistita. Problemi e prospettive*, Brindisi, 2005, pp. 15 ss.; Id., *Ancora su persona umana e diritto*, in *Riv. dir. civ.*, I, 2007, pp. 259 ss.; Giacobbe E., *Il concepito come persona in senso giuridico*, Torino, 2003; C.M. Bianca, *Diritto civile, I, La norma giuridica. I soggetti*, Milano, 2002, pp. 221 ss.

[20] L'unica condizione posta è che si tratti di figli di una determinata persona vivente al tempo del testamento o della donazione.

[21] Cfr. Corte Cost., 25.5.1957, nr. 79.

[22] Per approfondimenti si v. A. Paganini, *Danno da nascita non desiderata: automatismi probatori e legittimazione del feto rimessi al vaglio delle sezioni unite*, in *Diritto & Giustizia*, fasc. 6, 2015, pp. 68 e ss.

[23] Per approfondimenti si v. G. Ballarani, *La Cassazione riconosce la soggettività giuridica del concepito: indagine sui precedenti dottrinali per una lettura integrata dell'art. 1 c.c.*, in *Dir. fam. pers.*, fasc. 3, I, 2009, pp. 1159 e ss.

[24] Tale principio è stato espresso per la prima volta, in una sentenza in tema di responsabilità medica per omessa diagnosi di malformazioni del feto e conseguente nascita indesiderata (cfr. Cass. civ., 22.11.1993, nr. 11503, in *Foro it.*, 1994, I, p. 2479, nonché in *Nuova giur. civ. comm.*, 1994, I, 690,

con nota di Zeno Zencovich; in *Corriere giur.*, 1994, p. 479; in *Resp. civ. prev.*, 1994, p. 403; in *Giur. it.*, 1994, I, 1, p. 550; ed in *Rass. dir. civ.*, 1995, p. 908. Tale orientamento è stato costantemente seguito dalla Suprema Corte (si v. *ex multiis*, Cass. civ., 20.10.2005, nr. 20320, in *Fam. dir.*, 2006, pp. 253 ss., con nota di G. Facci, *Il danno da nascita indesiderata e la legittimazione al risarci-mento del padre*).

[25] Cfr. Cass. civ., 11.5.2009, nr. 10741.

[26] La Corte Costituzionale, con la sentenza del 28.1.2005, nr. 45, ha ritenuto la legge sulla procreazione medicalmente assistita a contenuto costituzionalmente necessario in relazione agli interessi tutelati, anche a livello internazionale, con riferimento alla Convenzione di Oviedo del 4.4.1997.

[27] Tale disposizione da seguito a quanto affermato dalla Corte Costituzionale con la nota sentenza del 18.2.1975, nr. 27, esplicitando il principio generale della tutela della vita umana sin dal suo inizio.

[28] Cfr. G. Ballarani, *La Cassazione riconosce la soggettività giuridica del concepito: indagine sui precedenti dottrinali per una lettura integrata dell'art. 1 c.c.*, in *Dir. fam. pers.*, fasc. 3, I, 2009, pp. 1159 e ss.

Il caso Schrems- Facebook: analisi e profili di collegamento con la sentenza Google Spain

di
Andrea Puligheddu

Abstract
L'articolo esamina la sentenza Schrems e le sue implicazioni nell'ambito della giurisprudenza della Corte di giustizia in merito alla protezione dei dati personali. In particolare, si propone un parallelismo con la sentenza Google Spain, dove la Corte ha rivelato un'attitudine espansiva nell'applicazione degli articoli 7 e 8 della Carta dei diritti fondamentali dell'UE nei confronti degli operatori Internet. Alla luce di questa decisione, il caso Schrems documenta una particolare attenzione ai poteri delle autorità nazionali rispetto al trasferimento di dati personali verso paesi terzi.

The article aims at exploring the Schrems case and its implications within the context of the recent Court of Justice activism in the field of data protection. In particular, a comparison is drawn with the Google Spain judgment, where the Court of Justice has taken important steps to enforce Articles 7 and 8 of the Charter of Fundamental Rights of the European Union vis-à-vis internet service providers. In the wake of this decision, the Schrems case has focused on the powers of data protection authorities with respect to the transfer of personal data to third countries.

1. Introduzione

In questo lavoro vengono compiute alcune riflessioni riguardanti la recente vicenda che ha investito il contesto europeo in materia di trattamento dei dati online e di trasferimento dei dati dal territorio dell'Unione Europea agli Stati Uniti, ovvero il caso Schrems v. Data Protection Commissioner [1]. Intorno a questa decisione è rapidamente sorto un forte sottofondo mediatico che, se pur con le diverse sfumature, pretende di individuare all'interno della sentenza una dichiarazione di "illiceità" o una sorta di responsabilità in capo alle società che operano il trasferimento dei dati. Tali affermazioni sono

scaturite a partire dalla dichiarazione di invalidità pronunciata dalla Corte nei riguardi della Decisione 2000/520 della Commissione inerente i principi da seguire in materia di trasferimento dei dati dai due contesti territoriali e individuati all'interno di un trattato denominato Safe Harbor [2]. Un simile approccio risulta fuorviante, ed è necessario mettere in atto le dovute distinzioni del caso. Un'attenzione particolare è quella da rivolgere alle elaborazioni contenute all'interno della sentenza, soffermandosi in particolare sul ruolo e sull'indipendenza delle autorità nazionali al riguardo, e sull'alveo di effettività della Decisione. Essi saranno oggetto di una analisi autonoma, a partire dal main reasoning della Corte e soffermandosi sulle conseguenze implicite che tale decisione comporta. Affinché si possa giungere ad una proficua sintesi conclusiva, verranno presi in esame i profili di collegamento riscontrabili tra tale sentenza e la decisione Google Spain [3]. Proprio a partire dal contenuto di quest'ultima pronuncia merita infatti che sia colto il fulcro della decisione sul caso Facebook, così come rapidamente ribattezzato da una consistente parte della cronaca giornalistica, sia per ciò che concerne le prospettive future legate alla invalidità oggetto della pronuncia, sia per quanto riguarda la ritrovata titolarità potestativa degli Stati membri affinché vengano poste in essere misure specifiche a sostegno del diritto alla protezione dei dati personali in una sua forma più adeguata ai principi sanciti in materia dall'Unione Europea.

2. Sintesi dei fatti oggetto della sentenza Schrems-Facebook.

Nel 2008 uno studente austriaco ed attivista in materia di protezione dei dati personali, Max Schrems, effettuava l'iscrizione al noto social network Facebook, di proprietà e gestione dell'omonima società, Facebook Inc., con sede principale a Palo Alto, California. All'atto dell'iscrizione, Schrems rilevava come, al fine di utilizzare i servizi proposti dalla piattaforma, fosse necessario sottoscrivere un contratto con Facebook Ireland, ovvero una controllata di Facebook Inc., sita in territorio irlandese. In particolare veniva in tale atto specificato come la politica promossa dal portale, nei confronti dei dati raccolti attraverso l'utilizzo da parte degli utenti europei registrati, fosse quello di trasferire tali dati sui server di Facebook Inc., ubicato in California. Pertanto veniva a verificarsi di fatto un trasferimento di dati dal territorio di uno stato membro dell'Unione Europea a quello statunitense. Dopo aver esaminato e discusso in varie forme di protesta pubblica la politica adottata dal social network in materia di privacy, Schrems si rivolgeva nel giugno del 2013 all'Autorità per la protezione dei dati Irlandese, invitandola ad agire nei confronti della società californiana nell'esercizio delle proprie competenze statutarie. Pertanto, egli richiedeva il diniego nei

confronti dell'operazione di trasferimento, anche a seguito delle informazioni divulgate da Edward Snowden riguardo le attività perpetrate dai servizi di intelligence statunitensi [4]. Da parte sua, l'Autorità investita della denuncia negava l'obbligo a procedere, rilevando la domanda priva di fondamento. Schrems proponeva di conseguenza ricorso di fronte all'High Court, la Corte d'appello irlandese. Quest'ultima rilevava come un effettivo accesso massiccio ed indifferenziato ai dati personali sarebbe stato "manifestamente contrario al principio di proporzionalità e ai valori fondamentali protetti dalla Costituzione irlandese" [5]. In particolare il giudice irlandese rilevava come la decisione 2000/520 non fosse più adeguata al soddisfacimento dei requisiti previsti dagli articoli 7 ed 8 della Carta dei diritti fondamentali dell'Unione Europea [6], e pertanto fosse necessario rivedere le modalità con cui potessero essere assicurate le garanzie in materia di riservatezza previste dal diritto dell'Unione. Partendo da queste premesse, la High Court decideva di sospendere il procedimento principale e sottoponeva all'attenzione della Corte di Giustizia dell'Unione Europea alcune questioni pregiudiziali. Precisamente, le richieste proposte dalla Corte d'Appello irlandese si dividevano in due partizioni. La prima richiedeva se, nell'atto di decidere in merito ad una denuncia presentata ad un'autorità indipendente, investita delle funzioni di applicazione e gestione della legislazione in materia di protezione dei dati, vi fosse implicito il rispetto di un vincolo di constatazione in senso contrario espresso dall'Unione all'interno della decisione 2000/520, anche in considerazione degli articoli 7, 8 e 47 e delle disposizioni dell'articolo 25 della Direttiva 95/46 [7]. In secondo luogo veniva domandato se detta autorità potesse condurre una propria indagine sulla questione, alla luce degli sviluppi verificatisi nel frattempo, successivamente alla prima pubblicazione della decisione 200/520.

3. Il main reasoning della Corte.

Per comprendere adeguatamente il ragionamento posto in essere dalla Corte in risposta ai quesiti sollevati, occorre procedere per punti. Innanzitutto, all'interno della pronuncia viene rilevato e riconfermato il ruolo indipendente delle Autorità nazionali di controllo, ideato appositamente affinché esse vigilino sul rispetto delle disposizioni in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali. Precisamente la Corte chiarisce il valore spettante al compito di verifica e controllo inerente le misure poste in atto dai titolari del trattamento, affinché esse risultino efficaci e affidabili. Sotto tale luce e rispetto a tale finalità va valutato il loro operato [8], ed in questo senso l'operazione consistente nel trasferimento dei dati personali da uno Stato membro verso un paese terzo costituisce, alla

luce dei fatti, una forma di trattamento perfettamente qualificabile come tale secondo i dettami dell'articolo 2, lettera b) della Direttiva 95/46 EC. A questo punto del reasoning, una volta riconfermata anche la competenza della Corte a decidere in merito alla validità delle decisioni poc'anzi descritte adottate dalla Commissione, il giudice europeo giunge ad affermare uno dei perni centrali dell'intera sentenza, ovvero che "una decisione della Commissione adottata sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46, come la decisione 2000/520, non può impedire alle persone i cui dati personali sono stati o potrebbero essere trasferiti verso un paese terzo di investire le autorità nazionali di controllo di una domanda" [9]. In altre parole le Autorità nazionali investite della questione hanno il dovere e non già la facoltà di operare una attività di vigilanza e controllo nei confronti delle operazioni di trasmissione dati da uno Stato membro ad uno Stato terzo. La Decisione in oggetto non può e non deve in alcun modo derogare a quanto contenuto nella Direttiva al riguardo[10]. Le autorità in questione devono inoltre poter svolgere tale attività d'esame dei requisiti in piena indipendenza [11], ciò anche in ragione della tutela dei diritti sanciti all'interno della Carta dei diritti fondamentali dell'Unione europea, agli articoli 7 ed 8 [12]. Per questo motivo viene ribadito in conclusione della pronuncia che sul primo quesito proposto, "si deve rispondere alle questioni sollevate che l'articolo 25, paragrafo 6, della direttiva 95/46, letto alla luce degli articoli 7, 8 e 47 della Carta, deve essere interpretato nel senso che una decisione adottata in forza di tale disposizione, quale la Decisione 2000/520, con la quale la Commissione constata che un paese terzo garantisce un livello di protezione adeguato, non osta a che un'autorità di controllo di uno Stato membro, ai sensi dell'articolo 28 di tale direttiva, esamini la domanda di una persona relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento di dati personali che la riguardano, i quali sono stati trasferiti da uno Stato membro verso tale paese terzo, qualora tale persona faccia valere che il diritto e la prassi in vigore in quest'ultimo non garantiscono un livello di protezione adeguato" [13]. Da un lato la sentenza traccia chiaramente una linea di attribuzione delle competenze in capo alle autorità nazionali, assicurando la tutela dei diritti del singolo. Infatti la Corte rimette direttamente ad esse la valutazione delle domande inoltrate dai cittadini europei, in merito alle garanzie inerenti il trasferimento dei dati. D'altro canto invece viene ricordato che benché le autorità nazionali debbano agire sotto gli auspici della piena indipendenza sostanziale, ciò non significa che possano aggirare gli atti decisionali della Commissione. In altri termini, un conto è confermare una potestà autonoma in capo alle autorità nel decidere sulle segnalazioni ricevute nella piena esplicazione dei loro compiti e nel pieno godimento di una indipendenza sostanziale; un altro è agire in stato di aperta violazione

dei principi vigenti ed approvati in materia. Per questo motivo il giudice europeo ribadisce in capo alla Corte di Giustizia dell'Unione Europea il potere di pronunciarsi sulla validità delle decisioni della Commissione, riferendosi in questo specifico caso alla Decisione 2000/520. Difatti, la seconda parte della sentenza verte su un giudizio di validità della Decisione in questione, partendo dai dubbi sul livello di protezione accordato ai dati trasferiti nei paesi terzi, così come espressi dal ricorrente in sede di domanda. Come ricordato, va ravvisato all'interno dell'articolo 25 paragrafo 6 della Direttiva una facoltà di adozione in capo alla Commissione di atti attestanti il rispetto da parte di un paese terzo di un adeguato livello di protezione dei dati. In un contesto similmente delineato, la Corte afferma che la Commissione era tenuta ad effettuare la valutazione in merito al fatto che gli Stati Uniti fossero in grado di garantire effettivamente, in considerazione della loro legislazione nazionale o dei loro impegni internazionali, un livello di protezione sostanzialmente equivalente a quello garantito dall'Unione Europea a norma della Direttiva 95/46/C. Secondo il giudice europeo, tale facoltà non è stata sostanzialmente esercitata dalla Commissione, la quale si sarebbe limitata ad un semplice esame dei principi contenuti nel regime di Safe Harbor [14]. In conclusione la Corte dichiara che il contenuto della Decisione 2000/520, e di conseguenza anche i principi [15] concordati per "l'approdo sicuro", siano da considerarsi invalidi [16].

4. Conseguenze e prospetto europeo degli effetti della sentenza

Una volta espresso in questo modo il reasoning della Corte, occorre chiedersi quale attualmente sia il quadro normativo a cui fare riferimento per le operazioni di trasferimento dei dati dall'Unione in ambito extraeuropeo. Un punto di riferimento al riguardo deve essere individuato nel documento del Working Party 29 [17] in cui viene espressa l'intenzione da parte dell'organo di operare quanto prima un'analisi dettagliata dell'impatto della sentenza sotto ogni profilo coinvolto nei sistemi di trasferimento dati [18]. Durante questo periodo viene tuttavia raccomandato che il novero delle regole da seguire debba essere considerato quello delle Binding Corporate Rules [19] e delle Standard Contractual Clauses [20]. Un ulteriore aspetto richiamato dal documento del Working Party è quello legato al sistema di sorveglianza di massa oggetto delle rivelazioni di Edward Snowden, ritenuta una questione chiave all'interno dell'analisi svolta dalla Corte e assolutamente incompatibile con il sistema di tutele predisposto dall'Unione Europea in materia di protezione dei dati [21]. Anche in considerazione dei motivi ora esposti, viene ribadita la necessità di una ulteriore discussione sui principi e le modalità che regolano il trasferimento, auspicando quanto prima

l'individuazione di una soluzione appropriata [22]. Dello stesso avviso risulta essere la Commissione Europea dopo il comunicato rilasciato successivamente, che sostanzialmente conferma ed analizza l'impatto che il giudizio ha nei confronti delle imprese operanti nel territorio europeo che raccolgono e trasferiscono dati in territorio statunitense [23]. Formale e sostanziale ricezione è inoltre quella riscontrabile da parte del Garante per la protezione dei dati personali italiano il quale ha dichiarato decaduta, attraverso specifico provvedimento, l'autorizzazione emanata a suo tempo con cui si consentivano le operazioni di trasferimento, sostanzialmente basata sull'accordo Safe Harbor e sui principi in esso contenuti [24]. Di fronte all'insieme delle risposte evidenziate, un fattore risulta essenzialmente comune: la necessità urgente di un impianto normativo adeguato. Difatti il problema evidenziato anche da parte della dottrina internazionale in merito, sposta il baricentro interpretativo dalle facoltà esercitabili da parte delle Autorità nazionali al comportamento conseguente che d'ora in avanti le società nel settore, aventi un centro d'interesse europeo, proporranno all'interno del mercato corrispondente [25]. Se da un lato infatti non viene sancita alcuna forma di responsabilità specifica in capo alla società operante attività di trasferimento [26], è anche vero che un quadro normativo così invalidato e precario non può incontrare il favore di chi operi commercialmente attraverso la raccolta e l'elaborazione dei dati [27], anche a partire dalla stessa dicitura della Corte che sembrerebbe lasciare spazio ad ulteriori problematiche, in particolare riguardo al significato della dicitura inerente un adeguato livello di protezione richiesto [28].

5. Caso Google Spain e caso Facebook: una sintesi dei valori e dei principi condivisi.

Esaminando i punti enucleati e la dinamica decisionale che caratterizza la sentenza del Caso Schrems, è possibile individuare un parallelismo ben preciso con un ulteriore caso di recente pronuncia da parte della medesima Corte, ovvero il caso Google Spain. Quest'ultima vicenda presenta infatti interessanti aspetti in comune con il caso ora esaminato, che costituiscono importanti tasselli nel quadro della giurisprudenza europea in materia di tutela dei diritti fondamentali. Un primo elemento di interesse è senza dubbio costituito dalla differenza esistente tra le due decisioni in materia di responsabilità dei fornitori di servizi della società dell'informazione. Mentre viene infatti rilevato all'interno del caso Google Spain una forma di responsabilità in capo al motore di ricerca quale soggetto titolare del trattamento dei dati per ciò che concerne l'attività di indicizzazione [29], tale assunto non viene analogamente applicato a Facebook per il quale non è

menzionata alcuna forma di responsabilità per l'adeguatezza del trattamento, e per il quale viene spostato il fulcro sull'appropriatezza dei parametri entro i quali la società avrebbe dovuto agire. Certamente le domande proposte e gli oggetti di doglianza sono nettamente differenti; tuttavia sotto il profilo del comportamento posto in essere, in particolare sul versante del trattamento dei dati personali, le due società californiane possiedono elementi in comune di non poca rilevanza. Meritano di essere menzionati in modo specifico due aspetti: la rinnovata importanza della tutela dei diritti fondamentali della personalità e la questione della territorialità del dato. In entrambi i casi citati, uno dei punti chiave è senza alcun dubbio rappresentato dall'interpretazione da accordare agli articoli 7 ed 8 della Carta dei diritti fondamentali dell'Unione Europea, rispettivamente riguardanti il rispetto della vita privata e familiare e la protezione dei dati di natura personale. Sul tema la giurisprudenza europea sembra essere rimasta sostanzialmente concorde, rinvenendo in entrambi gli articoli la fonte prima da cui attingere per aggiornare ed estendere l'adeguatezza delle tutele del singolo e dei suoi diritti fondamentali [30]. Risulta interessante infatti notare come sia nel caso Google Spain che nel caso Schrems si sia data assoluta rilevanza all'esigenza di tutela dei diritti fondamentali del singolo, da un lato per quanto concerne il diritto all'oblio e le modalità predisposte per la sua integrazione nell'insieme dei servizi proposti, dall'altro nella dichiarazione di necessario controllo da parte delle autorità nazionali di fronte alle richieste di coloro i quali desiderino informazioni relative all'adeguatezza delle tutele predisposte per l'attività di trasferimento. Proprio tale operazione richiama un ulteriore aspetto trattato all'interno di entrambe le decisioni, ovvero la questione della territorialità. Anche se la problematica affrontata in Google Spain verteva sull'applicazione del principio di territorialità, enucleabile dall'articolo 4 della Direttiva 95/46 EC, nei confronti del trattamento effettuato nel contesto delle attività di stabilimento del responsabile di tale trattamento nel territorio di uno Stato membro, la similitudine riscontrabile con il caso oggetto dell'analisi sino ad ora proposta risulta evidente sul piano della essenzialità nell'individuare il territorio a cui fare riferimento per collegare l'attività di trattamento e le relative garanzie. In altre parole, si deve ritenere esteso anche al territorio extraeuropeo il novero di garanzie individuali a tutela dei diritti fondamentali, e tale sussistenza prescinde anche in questo dal luogo in cui il trattamento viene effettuato qualora la società che operi il trattamento eserciti la propria attività nel contesto europeo. Ancora una volta il contesto geografico si rivela non semplicemente rilevante, ma assolutamente decisivo.

6. Conclusioni

A parere di chi scrive, il caso Schrems sembra collocarsi a piena ragione in una ottica di riconferma, da parte della Corte, dell'esigenza di autonomia potestativa da ripartirsi in capo ai singoli Stati membri. Nonostante da un lato essa sia foriera di una rinnovata sensibilità sul tema e sull'impellente necessità di una tutela conforme alle garanzie europee dei loro diritti, dall'altro lato desta perplessità sul fronte della politica del diritto, sollevando interrogativi circa l'adeguatezza degli strumenti normativi che succederanno al trattato e circa la risposta messa in campo dalle società operanti attraverso controllate all'interno dell'Unione, pur avendo centrale dei propri interessi in USA [31]. Per ciò che concerne il versante europeo, risulta particolarmente interessante la chiarezza espressa dalla Corte riguardo il comportamento delle autorità nazionali ed il loro ruolo di entità indipendente nel valutare le domande poste da una persona "riguardo al trattamento di dati personali che la riguardano, i quali sono stati trasferiti da uno Stato membro verso tale paese terzo, qualora tale persona faccia valere che il diritto e la prassi in vigore in quest'ultimo non garantiscono un livello di protezione adeguato". Seguendo il dettato stabilito dall'art. 25 paragrafo 6 della direttiva, interpretato alla luce della Carta dei diritti fondamentali dell'Unione Europea ed in particolare degli articoli 7,8 e 47. Sarebbe lecito dunque attendersi dopo questa pronuncia un maggiore interesse in materia in capo alle autorità garanti e preposte al controllo, ed una maggior attenzione riguardo le richieste debitamente motivate [32]. Certamente una riforma che aggiorni nel più breve tempo possibile la normativa in materia è la soluzione auspicabile per ogni operatore del settore. Sicuramente sono inoltre da attendersi importanti sviluppi conseguenti questa pronuncia e i vari provvedimenti adottati dalle istituzioni europee, in particolare per ciò che concerne il profilo della sorveglianza di massa così come eccepita dal documento del Working Party 29 [33]. Un'interessante fattore di novità potrebbe essere quello apportato dalla proposta del progetto di regolamento per la protezione dei dati personali attualmente al vaglio delle istituzioni europee [34]. Una sintesi dei principi implicati certo non di facile attuazione, ma quanto prima necessaria affinché si rigeneri un clima di reciproca affidabilità verso il quadro normativo del settore.

Note:

[*] Il presente contributo è stato preventivamente sottoposto a referaggio anonimo affidato ad un componente del Comitato di Referee secondo il Regolamento adottato da questa Rivista.

[1] Sentenza C-362/14, Schrems v. Data Protection Commissioner,

[2] Si fa riferimento alla Decisione 2000/520/EC, Official Journal L 215, 2000 P. 0007- 0047

[3] Si fa riferimento alla sentenza C-131/12 Google Spain SL,Google Inc. V. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 13 Maggio 2014. La decisione della Corte rappresenta un vero e proprio milestone case in materia di diritto all'oblio. In particolare, con riferimento al tema trattato in questo elaborato, tale sentenza è stata decisiva per delineare l'orientamento della Corte riguardo all'interpretazione degli articoli 7 ed 8 della Carta dei diritti fondamentali dell'Unione Europea e sulla applicazione estensiva del principio di territorialità.

[4] In particolare veniva rilevato come simili dinamiche avessero pregiudicato in maniera grave i diritti inviolabili dei cittadini europei coinvolti in tali programmi di sorveglianza di massa. Il meccanismo di spionaggio evidenziato dalle rivelazioni di Snowden e mutato ora in un programma di sorveglianza di massa collegabile alla NSA, ha generato una vera e propria ondata di sensibilizzazione nei confronti della sicurezza informatica globale.

[5] Sentenza C-362/14, Schrems v. Data Protection Commissioner, par. 33

[6] Carta dei Diritti Fondamentali dell'unione Europea, 2000/C 364/01

[7] In particolare viene ribadita dalla Corte la necessità di corretta interpretazione del par. 6 ove viene riportato che "La Commissione può constatare, secondo la procedura di cui all'articolo 31, paragrafo 2, che un paese terzo garantisce un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, in particolare di quelli assunti in seguito ai negoziati di cui al paragrafo 5, ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona. Gli Stati membri adottano le misure necessarie per conformarsi alla decisione della Commissione"

[8] Sentenza C-362/14, Schrems v. Data Protection Commissioner, par. 41

[9] Sentenza C-362/14, Schrems v. Data Protection Commissioner, par. 53

[10] Si fa qui riferimento precisamente al contenuto dell'Art. 28 par 4 della Direttiva 95/46 EC "Qualsiasi persona, o associazione che la rappresenti, può presentare a un'autorità di controllo una domanda relativa alla tutela dei suoi diritti e libertà con riguardo al trattamento di dati personali. La persona interessata viene informata del seguito dato alla sua domanda. Qualsiasi persona può, in particolare, chiedere a un'autorità di controllo di verificare la liceità di un trattamento quando si applicano le disposizioni nazionali

adottate a norma dell'articolo 13 della presente direttiva. La persona viene ad ogni modo informata che una verifica ha avuto luogo"
[11] Sentenza C-362/14, Schrems v. Data Protection Commissioner, par. 57
[12] Sentenza C-362/14, Schrems v. Data Protection Commissioner, par. 63
[13] Sentenza C-362/14, Schrems v. Data Protection Commissioner, par. 66
[14] Si veda al riguardo all'interno della pronuncia C-362/14, Schrems v. Data Protection Commissioner, il paragrafo 97, in cui si evince che la Commissione, nella decisione 2000/520, non ha affermato che gli Stati Uniti d'America «garantiscono» effettivamente un livello di protezione adeguato in considerazione della loro legislazione nazionale o dei loro impegni internazionali ; ciò viene riaffermato anche nel comunicato emanato dalla stessa Corte, ove si afferma che "le esigenze afferenti alla sicurezza nazionale, al pubblico interesse e all'osservanza delle leggi statunitensi prevalgono sul regime del Safe Harbor, cosicché le imprese americane sono tenute a disapplicare, senza limiti, le norme di tutela previste da tale regime laddove queste ultime entrino in conflitto con tali esigenze"(comunicato stampa n.117/15 della Corte di Giustizia)
[15] I principi in oggetto sono così riassumibili: 1) Gli utenti devono essere avvertiti sulla raccolta e l'utilizzo dei propri dati personali; 2) Ciascuno deve essere libero di rifiutare la raccolta dei dati e il loro trasferimento a terzi; 3) I dati possono essere trasferiti solo a organizzazioni che seguono principi adeguati di protezione dei dati; 4) Le aziende devono fornire garanzie contro il rischio che i dati vengano smarriti.
[16] In particolare il ragionamento della Corte ruota attorno alla valutazione degli articoli da 1 al 4 della decisone, considerati inseparabili e dei relativi allegati.
[17] Il Gruppo è stato istituito dall'art. 29 della direttiva 95/46, è un organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, dal GEPD (Garante europeo della protezione dei dati), nonché da un rappresentante della Commissione.
[18] Ove è previsto all'interno del document del W.P. Art.29 che "In the meantime, the Working Party will continue its analysis on the impact of the CJEU judgment on other transfer tools. During this period, data protection authorities consider that Standard Contractual Clauses and Binding Corporate Rules can still be used. In any case, this will not prevent data protection authorities to investigate particular cases, for instance on the basis of complaints, and to exercise their powers in order to protect individuals. If by the end of January 2016, no appropriate solution is found with the US authorities and depending on the assessment of the transfer tools by the Working Party, EU data protection authorities are committed to take all

necessary and appropriate actions, which may include coordinated enforcement actions" (http://ec.europa.eu/justice/data- protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf)

[19] Si tratta di uno strumento volto a consentire il trasferimento di dati personali dal territorio dello Stato verso Paesi terzi (extra-UE) tra società facenti parti dello stesso gruppo d'impresa.
Si concretizzano in un documento contenente una serie di clausole (rules) che fissano i principi vincolanti (binding) al cui rispetto sono tenute tutte le società appartenenti ad uno stesso gruppo (corporate). Le Bcr costituiscono un meccanismo in grado di semplificare gli oneri amministrativi a carico delle società di carattere multinazionale con riferimento ai flussi intra-gruppo di dati personali. (Così secondo quanto riportato dal Garante e liberamente consultabile all'indirizzo: http://www.garanteprivacy.it/home/provvedimenti-normativa/normativa/normativa-comunitaria-e-intenazionale/trasferimento-dei-dati-verso-paesi-terzi#3)

[20] La Commissione europea, ai sensi dell'articolo 26(4) della Direttiva 95/46/CE, può stabilire che determinati strumenti contrattuali consentono di trasferire dati personali verso Paesi terzi. Si tratta di una delle deroghe (stabilite nel comma 2 dell'articolo 26 della Direttiva 95/46/CE) al divieto di effettuare il trasferimento verso Paesi che non offrono garanzie "adeguate" in materia di protezione dei dati personali. Utilizzando il testo delle clausole contrattuali in questione in un contratto utilizzato per il trasferimento, l'esportatore dei dati garantisce che questi ultimi saranno trattati conformemente ai principi stabiliti nella Direttiva anche nel Paese terzo di destinazione

[21] "It recalls that it has consistently stated that such surveillance is incompatible with the EU legal framework and that existing transfer tools are not the solution to this issue. Furthermore, as already stated, transfers to third countries where the powers of state authorities to access information go beyond what is necessary in a democratic society will not be considered as safe destinations for transfers. In this regard, the Court's judgment requires that any adequacy decision implies a broad analysis of the third country domestic laws and international commitments."

[22] Il termine indicato all'interno del documento del WP29 è temporaneamente fissato entro la fine Gennaio 2016

[23] Si fa riferimento alla COM(2015) 566, on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems) Per una consultazione dettagliata si invita a consultare la versione integrale

del documento reperibile all'indirizzo: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf

[24] Si fa riferimento al Provvedimento del 22 Ottobre 2015, Trasferimento dati personali verso gli USA: caducazione provvedimento del Garante del 10.10.2001 di riconoscimento dell'accordo sul c.d. "Safe Harbor". In esso viene sinteticamente annunciata la ricezione dell'invalidità del Safe Harbor e dichiarata l'urgenza di una normativa necessaria di sostituzione, con la massima cooperazione da parte dell'Autorità affinché ciò avvenga quanto prima.

[25] "The ruling could have a significant impact on the way American companies can store and transfer data on European citizens. In addition to potentially stricter privacy requirements, American companies may have to navigate more than 20 different policies adopted by European member states, rather than a single E.U. wide policy. In the meantime, U.S. and E.U. officials are continuing ongoing negotiations over the so-called "Safe Harbor 2.0," which would create a more privacy-protective transatlantic agreement. The ruling has also prompted renewed calls for further surveillance reform in the United States". (Così D. Kehl European Court of Justice invalidates key part of EU-USA Safe Harbor agreement, 4/11/2015 e reperibile all'indirizzo: http://jolt.law.harvard.edu/digest/privacy/european-court-of-justice-invalidates-key-part-of-u-s-e- u-safe-harbor-agreement)

[26] In capo a Facebook non è stata riscontrata alcun tipo di responsabilità specifica per le modalità di trattamento dei dati degli utenti, e ciò è da ritenersi analogicamente conseguente per la categoria di società assimilabili da un punto di vista operativo.

[27] In particolare il problema verterebbe sulle modalità con cui garantire la qualità del trattamento. Un'ipotesi possibile potrebbe essere quella di richiedere il semplice consenso per il trattamento dei dati personali all'estero direttamente agli utenti, modificando così le condizioni dei servizi offerti. Resta da vedere se alla luce dei procedimenti descritti nella COM(2015) 566 della Commissione ciò sia concretamente attuabile.

[28] "La Corte[...] non esclude che l'Autorità di controllo di uno Stato membro[...] esamini la richiesta di una persona circa la tutela dei suoi diritti e delle libertà in materia di trattamento dei dati personali a fronte del trasferimento dei suoi dati personali da uno Stato membro a un Paese terzo, quando si ritenga che la legge e la prassi del Paese terzo non garantiscano un adeguato livello di protezione" In particolare risulta complesso poter determinare, data l'assenza di parametri adeguati, quale sia l'asse di riferimento per determinare l'adeguatezza delle misure inerenti le operazioni di trasferimento dati.

[29] Si veda il par. 41 della sentenza google spain in cui viene riconosciuta la responsabilità in capo al gestore di un motore di ricerca qualora l'attività di trattamento si concretizzi "nel trovare informazioni pubblicate o inserite da terzi su Internet, nell'indicizzarle in modo automatico, nel memorizzarle temporaneamente e, infine, nel metterle a disposizione degli utenti di Internet secondo un determinato ordine di preferenza" (Corte di Giustizia Europea, 13 Maggio 2014, C- 131/12 par. 41)

[30] In Google Spain l'interpretazione corretta degli articoli 7 ed 8 della Carta è risultata essenziale per sancire il riconoscimento del diritto all'oblio come diritto fondamentale della persona e come manifestazione strumentale del diritto alla riservatezza in contemperanza con la libertà di espressione (si veda paragrafo 81 della sentenza Google Spain). Similmente anche all'interno della sentenza Schrems il fattore interpretativo degli articoli in oggetto è risultato di fondamentale importanza nella interpretazione dell'articolo 25 paragrafo 6 della Direttiva 95/46/CE, così come ricordato dal giudice europeo in sede conclusiva.

[31] Va ricordato qui qualora non si dovesse addivenire ad una soluzione politicamente condivisa, sarà cura della Corte stessa provvedere all'individuazione di un novero di principi attuabili in materia. Come già ricordato nel documento (metti coordinate) del WP 29, il termine attualmente concordato è la fine del mese di gennaio 2016. Un altro fattore di non scarsa rilevanza è costituito dal giudizio tuttora in corso tra Microsoft ed il governo statunitense (United States v. Microsoft Corporation 253 F.3d 34), che verte sulla soggezione della società al warrant federale anche per dati degli utenti conservati nel suolo UE. Se dovesse infatti permanere il criterio di prevalenza della nazionalità dell'impresa sulla territorialità del dato, saranno favorite le imprese stabilmente residenti all'interno dell'Unione Europea per i dati in essa trattati; mentre se dovesse prevalere il criterio della territorialità su quello della nazionalità dell'impresa, le imprese dominanti resteranno in territorio statunitense e tratteranno il dato all'interno dell'Unione ed attraverso strutture proprie site in territorio europeo.

[32] il testo della pronuncia riporta chiaramente la necessità di una congrua struttura che dimostri la lesione della qualità del trattamento quando dice "qualora tale persona faccia valere che il diritto e la prassi in vigore in quest'ultimo non garantiscono un livello di protezione adeguato"

[33] Al riguardo si veda qui: http://www.nytimes.com/2015/11/07/technology/europe-wants-to-reach-data-transfer-pact-by-early-2016.html?_r=0

[34] In January 2012, the European Commission proposed a comprehensive reform of data protection rules in the EU. The completion of this reform is a policy priority for 2015. The objective of this new set of rules is to give

citizens back control over of their personal data, and to simplify the regulatory environment for business. The data protection reform is a key enabler of the Digital Single Market which the Commission has prioritised. The reform will allow European citizens and businesses to fully benefit from the digital economy. (http://ec.europa.eu/justice/data-protection/)

Il trasferimento dei dati personali dall'Unione Europea verso paesi terzi: la sentenza della Corte di Giustizia che ha dichiarato invalido il regime c.d. "dell'Approdo sicuro".

di
Francesca Corrado

SENTENZA DELLA CORTE (Grande Sezione)
6 ottobre 2015
«Rinvio pregiudiziale – Dati personali – Protezione delle persone fisiche con riguardo al trattamento di tali dati – Carta dei diritti fondamentali dell'Unione europea – Articoli 7, 8 e 47 – Direttiva 95/46/CE – Articoli 25 e 28 – Trasferimento di dati personali verso paesi terzi – Decisione 2000/520/CE – Trasferimento di dati personali verso gli Stati Uniti – Livello di protezione inadeguato – Validità – Denuncia di una persona fisica i cui dati sono stati trasferiti dall'Unione europea verso gli Stati Uniti – Poteri delle autorità nazionali di controllo»
Nella causa C-362/14,
avente ad oggetto la domanda di pronuncia pregiudiziale proposta alla Corte, ai sensi dell'articolo 267 TFUE, dalla High Court (Corte d'appello, Irlanda), con decisione del 17 luglio 2014, pervenuta in cancelleria il 25 luglio 2014, nel procedimento
Maximillian Schrems
contro
Data Protection Commissioner,
con l'intervento di:
Digital Rights Ireland Ltd,
LA CORTE (Grande Sezione),
composta da V. Skouris, presidente, K. Lenaerts, vicepresidente, A. Tizzano, R. Silva de Lapuerta, T. von Danwitz (relatore) e S. Rodin, K. Jürimäe, presidenti di sezione, A. Rosas, E. Juhász, A. Borg Barthet, J. Malenovský, D. Šváby, M. Berger, F. Biltgen e C. Lycourgos, giudici,
avvocato generale: Y. Bot
cancelliere: L. Hewlett, amministratore principale
vista la fase scritta del procedimento e in seguito all'udienza del 24 marzo 2015,
considerate le osservazioni presentate:
– per M. Schrems, da N. Travers, SC, P. O'Shea, BL, e G. Rudden, solicitor, nonché da H. Hofmann, Rechtsanwalt;

– per il Data Protection Commissioner, da P. McDermott, BL, S. More O'Ferrall e D. Young, solicitors;
– per la Digital Rights Ireland Ltd, da F. Crehan, BL, nonché da S. McGarr e E. McGarr, solicitors;
– per l'Irlanda, da A. Joyce, B. Counihan e E. Creedon, in qualità di agenti, assistiti da D. Fennelly, BL;
– per il governo belga, da J.-C. Halleux e C. Pochet, in qualità di agenti;
– per il governo ceco, da M. Smolek e J. Vláčil, in qualità di agenti;
– per il governo italiano, da G. Palmieri, in qualità di agente, assistita da P. Gentili, avvocato dello Stato;
– per il governo austriaco, da G. Hesse e G. Kunnert, in qualità di agenti;
– per il governo polacco, da M. Kamejsza, M. Pawlicka e B. Majczyna, in qualità di agenti;
– per il governo sloveno, da A. Grum e V. Klemenc, in qualità di agenti;
– per il governo del Regno Unito, da L. Christie e J. Beeko, in qualità di agenti, assistiti da J. Holmes, barrister;
– per il Parlamento europeo, da D. Moore, A. Caiola e M. Pencheva, in qualità di agenti;
– per la Commissione europea, da B. Schima, B. Martenczuk, B. Smulders e J. Vondung, in qualità di agenti;
– per il Garante europeo della protezione dei dati (GEPD), da C. Docksey, A. Buchta e V. Pérez Asinari, in qualità di agenti,
sentite le conclusioni dell'avvocato generale, presentate all'udienza del 23 settembre 2015,
ha pronunciato la seguente
Sentenza
1 La domanda di pronuncia pregiudiziale verte sull'interpretazione, alla luce degli articoli 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la «Carta»), degli articoli 25, paragrafo 6, e 28 della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281, pag.31), come modificata dal regolamento (CE) n.1882/2003 del Parlamento europeo e del Consiglio, del 29 settembre 2003 (GU L 284, pag.1; in prosieguo: la «direttiva 95/46»), nonché, in sostanza, sulla validità della decisione 2000/520/CE della Commissione, del 26 luglio 2000, a norma della direttiva 95/46 sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «Domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti (GU L 215, pag.7).

2 Tale domanda è stata presentata nell'ambito di una controversia fra il sig.Schrems e il Data Protection Commissioner (commissario per la protezione dei dati; in prosieguo: il «commissario») concernente il rifiuto, da parte di quest'ultimo, di istruire una denuncia presentata dal sig.Schrems per il fatto che Facebook Ireland Ltd (in prosieguo: «Facebook Ireland») trasferisce negli Stati Uniti i dati personali dei propri utenti e li conserva su server ubicati in tale paese.

Contesto normativo

La direttiva 95/46

3 I considerando 2, 10, 56, 57, 60, 62 e 63 della direttiva 95/46 così recitano:

«(2) (...) i sistemi di trattamento dei dati sono al servizio dell'uomo; (...) essi, indipendentemente dalla nazionalità o dalla residenza delle persone fisiche, debbono rispettare le libertà e i diritti fondamentali delle stesse, in particolare la vita privata, e debbono contribuire (...) al benessere degli individui;

(...)

(10)(...) le legislazioni nazionali relative al trattamento dei dati personali hanno lo scopo di garantire il rispetto dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata, riconosciuto anche dall'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali[, firmata a Roma il 4 novembre 1950,] e dai principi generali del diritto comunitario; (...) pertanto il ravvicinamento di dette legislazioni non deve avere per effetto un indebolimento della tutela da esse assicurata ma deve anzi mirare a garantire un elevato grado di tutela nella Comunità;

(...)

(56) (...) lo sviluppo degli scambi internazionali comporta necessariamente il trasferimento oltre frontiera di dati personali; (...) la tutela delle persone garantita nella Comunità dalla presente direttiva non osta al trasferimento di dati personali verso paesi terzi che garantiscano un livello di protezione adeguato; (...) l'adeguatezza della tutela offerta da un paese terzo deve essere valutata in funzione di tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti;

(57) (...) per contro, (...) deve essere vietato il trasferimento di dati personali verso un paese terzo che non offre un livello di protezione adeguato;

(...)

(60) (...) comunque i trasferimenti di dati verso i paesi terzi possono aver luogo soltanto nel pieno rispetto delle disposizioni prese dagli Stati membri in applicazione della presente direttiva, in particolare dell'articolo 8;

(...)

(62) (...) la designazione di autorità di controllo che agiscano in modo indipendente in ciascuno Stato membro è un elemento essenziale per la tutela delle persone con riguardo al trattamento di dati personali;
(63) (...) tali autorità devono disporre dei mezzi necessari all'adempimento dei loro compiti, siano essi poteri investigativi o di intervento, segnatamente in caso di reclami di singoli individui, nonché poteri di avviare azioni legali; (...)».
4 Gli articoli 1, 2, 25, 26, 28 e 31 della direttiva 95/46 dispongono quanto segue:
«Articolo 1
Oggetto della direttiva
1. Gli Stati membri garantiscono, conformemente alle disposizioni della presente direttiva, la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali.
(…)
Articolo 2
Definizioni
Ai fini della presente direttiva si intende per:
a) "dati personali": qualsiasi informazione concernente una persona fisica identificata o identificabile ("persona interessata"); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale;
b) "trattamento di dati personali" ("trattamento"): qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione;
(...)
d) "responsabile del trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali. Quando le finalità e i mezzi del trattamento sono determinati da disposizioni legislative o regolamentari nazionali o comunitarie, il responsabile del trattamento o i criteri specifici per la sua designazione possono essere fissati dal diritto nazionale o comunitario;
(...)

Articolo 25
Principi
1. Gli Stati membri dispongono che il trasferimento verso un paese terzo di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento può aver luogo soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato, fatte salve le misure nazionali di attuazione delle altre disposizioni della presente direttiva.
2. L'adeguatezza del livello di protezione garantito da un paese terzo è valutata con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati; in particolare sono presi in considerazione la natura dei dati, le finalità del o dei trattamenti previsti, il paese d'origine e il paese di destinazione finale, le norme di diritto, generali o settoriali, vigenti nel paese terzo di cui trattasi, nonché le regole professionali e le misure di sicurezza ivi osservate.
3. Gli Stati membri e la Commissione si comunicano a vicenda i casi in cui, a loro parere, un paese terzo non garantisce un livello di protezione adeguato ai sensi del paragrafo 2.
4. Qualora la Commissione constati, secondo la procedura dell'articolo 31, paragrafo 2, che un paese terzo non garantisce un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, gli Stati membri adottano le misure necessarie per impedire ogni trasferimento di dati della stessa natura verso il paese terzo in questione.
5. La Commissione avvia, al momento opportuno, negoziati per porre rimedio alla situazione risultante dalla constatazione di cui al paragrafo 4.
6. La Commissione può constatare, secondo la procedura di cui all'articolo 31, paragrafo 2, che un paese terzo garantisce un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, in particolare di quelli assunti in seguito ai negoziati di cui al paragrafo 5, ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona.
Gli Stati membri adottano le misure necessarie per conformarsi alla decisione della Commissione.
Articolo 26
Deroghe
1. In deroga all'articolo 25 e fatte salve eventuali disposizioni contrarie della legislazione nazionale per casi specifici, gli Stati membri dispongono che un trasferimento di dati personali verso un paese terzo che non garantisce una tutela adeguata ai sensi dell'articolo 25, paragrafo 2 può avvenire a condizione che:

a) la persona interessata abbia manifestato il proprio consenso in maniera inequivocabile al trasferimento previsto, oppure
b) il trasferimento sia necessario per l'esecuzione di un contratto tra la persona interessata ed il responsabile del trattamento o per l'esecuzione di misure precontrattuali prese a richiesta di questa, oppure
c) il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto, concluso o da concludere nell'interesse della persona interessata, tra il responsabile del trattamento e un terzo, oppure
d) il trasferimento sia necessario o prescritto dalla legge per la salvaguardia di un interesse pubblico rilevante, oppure per co[n]statare, esercitare o difendere un diritto per via giudiziaria, oppure
e) il trasferimento sia necessario per la salvaguardia dell'interesse vitale della persona interessata, oppure
f) il trasferimento avvenga a partire da un registro pubblico il quale, in forza di disposizioni legislative o regolamentari, sia predisposto per l'informazione del pubblico e sia aperto alla consultazione del pubblico o di chiunque possa dimostrare un interesse legittimo, nella misura in cui nel caso specifico siano rispettate le condizioni che la legge prevede per la consultazione.
2. Salvo il disposto del paragrafo 1, uno Stato membro può autorizzare un trasferimento o una categoria di trasferimenti di dati personali verso un paese terzo che non garantisca un livello di protezione adeguato ai sensi dell'articolo 25, paragrafo 2, qualora il responsabile del trattamento presenti garanzie sufficienti per la tutela della vita privata e dei diritti e delle libertà fondamentali delle persone, nonché per l'esercizio dei diritti connessi; tali garanzie possono segnatamente risultare da clausole contrattuali appropriate.
3. Lo Stato membro informa la Commissione e gli altri Stati membri in merito alle autorizzazioni concesse a norma del paragrafo 2.
In caso di opposizione notificata da un altro Stato membro o dalla Commissione, debitamente motivata sotto l'aspetto della tutela della vita privata e dei diritti e delle libertà fondamentali delle persone, la Commissione adotta le misure appropriate secondo la procedura di cui all'articolo 31, paragrafo 2.
Gli Stati membri adottano le misure necessarie per conformarsi alla decisione della Commissione.
(...)
Articolo 28
Autorità di controllo
1. Ogni Stato membro dispone che una o più autorità pubbliche siano incaricate di sorvegliare, nel suo territorio, l'applicazione delle disposizioni di attuazione della presente direttiva, adottate dagli Stati membri.

Tali autorità sono pienamente indipendenti nell'esercizio delle funzioni loro attribuite.
2. Ciascuno Stato membro dispone che le autorità di controllo siano consultate al momento dell'elaborazione delle misure regolamentari o amministrative relative alla tutela dei diritti e delle libertà della persona con riguardo al trattamento dei dati personali.
3. Ogni autorità di controllo dispone in particolare:
– di poteri investigativi, come il diritto di accesso ai dati oggetto di trattamento e di raccolta di qualsiasi informazione necessaria all'esercizio della sua funzione di controllo;
– di poteri effettivi d'intervento, come quello di formulare pareri prima dell'avvio di trattamenti, conformemente all'articolo 20, e di dar loro adeguata pubblicità o quello di ordinare il congelamento, la cancellazione o la distruzione dei dati, oppure di vietare a titolo provvisorio o definitivo un trattamento, ovvero quello di rivolgere un avvertimento o un monito al responsabile del trattamento o quello di adire i Parlamenti o altre istituzioni politiche nazionali;
– del potere di promuovere azioni giudiziarie in caso di violazione delle disposizioni nazionali di attuazione della presente direttiva ovvero di adire per dette violazioni le autorità giudiziarie.
È possibile un ricorso giurisdizionale avverso le decisioni dell'autorità di controllo recanti pregiudizio.
4. Qualsiasi persona, o associazione che la rappresenti, può presentare a un'autorità di controllo una domanda relativa alla tutela dei suoi diritti e libertà con riguardo al trattamento di dati personali. La persona interessata viene informata del seguito dato alla sua domanda.
Qualsiasi persona può, in particolare, chiedere a un'autorità di controllo di verificare la liceità di un trattamento quando si applicano le disposizioni nazionali adottate a norma dell'articolo 13 della presente direttiva. La persona viene ad ogni modo informata che una verifica ha avuto luogo.
(...)
6. Ciascuna autorità di controllo, indipendentemente dalla legge nazionale applicabile al trattamento in questione, è competente per esercitare, nel territorio del suo Stato membro, i poteri attribuitile a norma del paragrafo 3. Ciascuna autorità può essere invitata ad esercitare i suoi poteri su domanda dell'autorità di un altro Stato membro.
(...)
Articolo 31
(...)
2. Nei casi in cui è fatto riferimento al presente articolo, si applicano gli articoli 4 e 7 della decisione 1999/468/CE [del Consiglio, del 28 giugno

1999, recante modalità per l'esercizio delle competenze di esecuzione conferite alla Commissione (GU L 184, pag. 23)], tenendo conto delle disposizioni dell'articolo 8 della stessa.
(...)».
La decisione 2000/520
5 La decisione 2000/520 è stata adottata dalla Commissione sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46.
6 I considerando 2, 5 e 8 di tale decisione così recitano:
«(2) La Commissione può constatare che un paese terzo garantisce un livello di protezione adeguato. In tal caso è possibile trasferire dati personali dagli Stati membri senza che siano necessarie ulteriori garanzie.
(...)
(5) Per il trasferimento di dati dalla Comunità agli Stati Uniti, il livello adeguato di protezione di cui alla presente decisione sarebbe raggiunto ove le organizzazioni si conformino ai "principi dell'approdo sicuro in materia di riservatezza" ("The Safe Harbor Privacy Principles"), in prosieguo "i principi", nonché alle "domande più frequenti" ("Frequently Asked Questions"), in prosieguo "FAQ", pubblicate dal governo degli Stati Uniti in data 21 luglio 2000, che forniscono indicazioni per l'attuazione dei principi stessi. Le organizzazioni devono inoltre rendere note pubblicamente le loro politiche in materia di riservatezza e sono sottoposte all'autorità della Commissione federale per il commercio [Federal Trade Commission (FTC)] ai sensi della sezione 5 del Federal Trade Commission Act, che vieta attività o pratiche sleali o ingannevoli in materia commerciale o collegata al commercio, oppure di altri organismi istituiti con legge in grado di assicurare efficacemente il rispetto dei principi applicati in conformità alle FAQ.
(...)
(8) Nell'interesse della trasparenza, e per salvaguardare la facoltà delle competenti autorità degli Stati membri di assicurare la protezione degli individui riguardo al trattamento dei dati personali, è necessario che la presente decisione specifichi le circostanze eccezionali in cui può essere giustificata la sospensione di specifici flussi di dati anche in caso di constatazione di adeguata protezione».
7 Ai sensi degli articoli da 1 a 4 della decisione 2000/520:
«Articolo 1
1. Ai fini dell'applicazione dell'articolo 25, paragrafo 2, della direttiva 95/46/CE, per tutte le attività che rientrano nel campo di applicazione di detta direttiva, si considera che i "Principi di approdo sicuro in materia di riservatezza", in prosieguo i "principi", di cui all'allegato I della presente decisione, applicati in conformità agli orientamenti forniti dalle "Domande più frequenti" (FAQ) di cui all'allegato II della presente decisione, pubblicate

dal Dipartimento del commercio degli Stati Uniti in data 21 luglio 2000, garantiscano un livello adeguato di protezione dei dati personali trasferiti dalla Comunità a organizzazioni aventi sede negli Stati Uniti sulla base della seguente documentazione pubblicata dal Dipartimento del commercio degli Stati Uniti:
a) riepilogo delle modalità di esecuzione dei principi di approdo sicuro, di cui all'allegato III;
b) memorandum sui danni per violazioni della riservatezza ed autorizzazioni esplicite previste dalle leggi degli Stati Uniti, di cui all'allegato IV;
c) lettera della Commissione federale per il commercio (FTC), di cui all'allegato V;
d) lettera del Dipartimento dei trasporti degli Stati Uniti, di cui all'allegato VI.
2. Le seguenti condizioni devono sussistere in relazione a ogni singolo trasferimento di dati:
a) l'organizzazione che riceve i dati si è chiaramente e pubblicamente impegnata a conformarsi ai principi applicati in conformità alle FAQ, e
b) detta organizzazione è sottoposta all'autorità prevista per legge di un ente governativo degli Stati Uniti, compreso nell'elenco di cui all'allegato VII, competente ad esaminare denunce e a imporre la cessazione di prassi sleali e fraudolente nonché a disporre il risarcimento di qualunque soggetto, a prescindere dal paese di residenza o dalla nazionalità, danneggiato a seguito del mancato rispetto dei principi applicati in conformità alle FAQ.
3. Le condizioni di cui al paragrafo 2 sono considerate soddisfatte per ogni organizzazione che autocertifica la sua adesione ai principi applicati in conformità alle FAQ a partire dalla data di notifica al Dipartimento del commercio degli Stati Uniti (o all'ente da esso designato) del pubblico annuncio dell'impegno di cui al paragrafo 2, lettera a), e dell'identità dell'ente governativo di cui al paragrafo 2, lettera b).
Articolo 2
La presente decisione dispone soltanto in merito all'adeguatezza della protezione offerta negli Stati Uniti, in base ai principi applicati in conformità alle FAQ, al fine di quanto prescritto dall'articolo 25, paragrafo 1, della direttiva 95/46/CE. Essa nulla dispone relativamente all'applicazione di altre disposizioni della stessa direttiva, relative al trattamento di dati personali all'interno degli Stati membri e in particolare dell'articolo 4 della stessa.
Articolo 3
1. Fatto salvo il loro potere di adottare misure per garantire l'ottemperanza alle disposizioni nazionali adottate in forza di disposizioni diverse dall'articolo 25 della direttiva 95/46/CE, le autorità competenti degli Stati membri possono avvalersi dei loro poteri, al fine di tutelare gli interessati con riferimento al trattamento dei dati personali che li riguardano, per

sospendere flussi di dati diretti a un'organizzazione che ha autocertificato la sua adesione ai principi applicati in conformità alle FAQ nei casi in cui:
a) gli enti governativi degli Stati Uniti di cui all'allegato VII della presente decisione, o un organismo indipendente di ricorso ai sensi della lettera a) del "principio di esecuzione" di cui all'allegato I della presente decisione abbiano accertato che l'organizzazione viola i principi applicati in conformità alle FAQ, oppure
b) sia molto probabile che i principi vengano violati; vi siano ragionevoli motivi per ritenere che l'organismo di esecuzione competente non stia adottando o non adotterà misure adeguate e tempestive per risolvere un caso concreto, la continuazione del trasferimento dei dati potrebbe determinare un rischio imminente di gravi danni per gli interessati e le autorità competenti dello Stato membro abbiano fatto il possibile, date le circostanze, per informare l'organizzazione dandole l'opportunità di replicare.
La sospensione dei flussi deve cessare non appena sia garantito il rispetto dei principi applicati in conformità alle FAQ e ciò sia stato notificato alle competenti autorità dell'UE.
2. Gli Stati membri comunicano immediatamente alla Commissione l'adozione di misure a norma del paragrafo 1.
3. Gli Stati membri e la Commissione s'informano altresì a vicenda in merito ai casi in cui l'azione degli organismi responsabili non garantisca la conformità ai principi applicati in conformità alle FAQ negli Stati Uniti.
4. Ove le informazioni di cui ai paragrafi 1, 2 e 3 del presente articolo provino che uno degli organismi incaricati di garantire la conformità ai principi applicati conformemente alle FAQ negli Stati Uniti non svolge la sua funzione in modo efficace, la Commissione ne informa il Dipartimento del commercio degli Stati Uniti e, se necessario, presenta progetti di misure secondo la procedura istituita dall'articolo 31 della direttiva 95/46/CE, al fine di annullare o sospendere la presente decisione o limitarne il campo d'applicazione.
Articolo 4
1. La presente decisione può essere adattata in qualsiasi momento alla luce dell'esperienza acquisita nella sua attuazione e/o qualora il livello di protezione offerta dai principi e dalle FAQ sia superato dai requisiti della legislazione degli Stati Uniti. La Commissione valuta in ogni caso l'applicazione della presente decisione tre anni dopo la sua notifica agli Stati membri sulla base delle informazioni disponibili e comunica qualsiasi riscontro al comitato istituito dall'articolo 31 della direttiva 95/46/CE, fornendo altresì ogni indicazione che possa influire sulla valutazione relativa all'adeguata salvaguardia offerta dalla disposizione di cui all'articolo 1 della

presente decisione, ai sensi dell'articolo 25 della direttiva 95/46/CE, nonché di eventuali applicazioni discriminatorie della decisione stessa.
2. La Commissione, se necessario, presenta progetti di opportuni provvedimenti in conformità alla procedura di cui all'articolo 31 della direttiva 95/46/CE».
8 L'allegato I della decisione 2000/520 così recita:
«Principi di approdo sicuro (safe harbor) del dipartimento del commercio degli Stati Uniti, 21 luglio 2000
(...)
(...) il Dipartimento del commercio sta provvedendo a pubblicare sotto la propria autorità statutaria questo documento e le Frequently Asked Questions ("i principi") al fine di incoraggiare, promuovere e sviluppare il commercio internazionale. I principi sono stati messi a punto in consultazione con l'industria e con il grande pubblico per facilitare gli scambi commerciali fra Stati Uniti ed Unione europea. Essi sono destinati unicamente ad organizzazioni americane che ricevono dati personali dall'Unione europea, al fine di permettere a tali organizzazioni di ottemperare al principio di "approdo sicuro" ed alla presunzione di "adeguatezza" che esso comporta. Giacché questi principi sono stati concepiti esclusivamente a tal fine una loro estensione ad altri fini può non risultare opportuna. (...)
La decisione di un'organizzazione di qualificarsi per l'approdo sicuro è puramente volontaria, e la qualifica può essere ottenuta in vari modi. (...)
L'adesione a tali principi può essere limitata: a) se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia; b) da disposizioni legislative o regolamentari ovvero decisioni giurisdizionali quando tali fonti comportino obblighi contrastanti od autorizzazioni esplicite, purché nell'avvalersi di un'autorizzazione siffatta un'organizzazione possa dimostrare che il mancato rispetto dei principi da parte sua si limita a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione; oppure c) se la direttiva o la legislazione degli Stati membri rendono possibili eccezioni o deroghe, a condizione che tali eccezioni o deroghe si applichino in contesti comparabili. Coerentemente con l'obiettivo di una maggiore tutela della sfera privata le organizzazioni devono fare il possibile per attuare detti principi integralmente ed in modo trasparente, specificando nelle rispettive politiche in materia di tutela della sfera privata in quali casi saranno regolarmente applicate le eccezioni ammesse dal punto b). Per lo stesso motivo, quando i principi e/o la legislazione statunitense consentono tale scelta, le organizzazioni sono tenute a scegliere, per quanto possibile, la protezione più elevata.
(...)».

9 L'allegato II della decisione 2000/520 è redatto come segue:
«Domande più frequenti (FAQ)
(...)
FAQ 6 – Autocertificazione
D: Come può un'organizzazione autocertificare la propria adesione ai principi dell'approdo sicuro?
R: Un'organizzazione usufruisce dei vantaggi dell'approdo sicuro dalla data in cui autocertifica al Dipartimento del commercio o ad una persona (fisica o giuridica) da esso designata l'adesione ai relativi principi, seguendo le indicazioni sotto riportate.
Per autocertificare l'adesione all'approdo sicuro un'organizzazione può fornire al Dipartimento del commercio o ad una persona (fisica o giuridica) da esso designata una lettera, firmata da un proprio funzionario in nome dell'organizzazione che intende aderire all'approdo sicuro, contenente almeno le seguenti informazioni:
1) denominazione dell'organizzazione, indirizzo postale, indirizzo di posta elettronica, numero di telefono e fax;
2) descrizione delle attività dell'organizzazione in rapporto alle informazioni personali pervenute dall'UE;
3) descrizione della politica perseguita dall'organizzazione in merito a dette informazioni personali, che precisi tra l'altro: a) dove il pubblico può prenderne conoscenza; b) la data della loro effettiva applicazione; c) l'ufficio cui rivolgersi per eventuali reclami, richieste di accesso e qualsiasi altra questione riguardante l'approdo sicuro; d) lo specifico organo statutario competente ad esaminare i ricorsi contro l'organizzazione relativi a possibili pratiche sleali od ingannevoli e a violazioni delle norme legislative e regolamentari che disciplinano la tutela della sfera privata (ed elencati nell'allegato ai principi); e) il nome dei programmi concernenti la tutela della sfera privata cui partecipa l'organizzazione; f) il metodo di verifica (per esempio all'interno della società, effettuata da terzi) (...) e g) il meccanismo di ricorso indipendente disponibile per indagare sui reclami non risolti.
Le organizzazioni che intendono estendere i benefici dell'approdo sicuro alle informazioni riguardanti le risorse umane trasferite dall'UE per usi nel contesto di un rapporto di lavoro possono farlo qualora esista un organo statutario competente ad esaminare i ricorsi contro l'organizzazione relativi ad informazioni riguardanti le risorse umane, elencato nell'allegato "Principi di approdo sicuro". (...)
Il Dipartimento (o la persona da esso designata) conserverà un elenco di tutte le organizzazioni che inviano queste lettere, assicurando così la disponibilità dei vantaggi legati all'approdo sicuro, ed aggiornerà tale elenco in base alle

lettere annuali ed alle notifiche ricevute secondo le modalità precisate nella FAQ 11. (...)
(...)
FAQ 11 – Risoluzione delle controversie e modalità di controllo dell'applicazione (enforcement)
D: Come si applicano le norme derivanti dal principio della garanzia di applicazione (enforcement) per la risoluzione delle controversie, e come si procede se un'organizzazione continua a non rispettare i principi?
R: Il principio della garanzia di applicazione (enforcement) stabilisce le norme per l'applicazione dell'approdo sicuro. Le modalità di applicazione delle norme di cui al punto b) di tale principio sono illustrate nella domanda sulla verifica (FAQ 7). La presente domanda interessa i punti a) e c), che prescrivono l'istituzione di dispositivi indipendenti di ricorso. Tali dispositivi possono assumere forme diverse, ma devono soddisfare le prescrizioni formulate nel contesto delle garanzie d'applicazione. Un'organizzazione può adempiere a tali prescrizioni nei modi seguenti: 1) applicando programmi di riservatezza elaborati dal settore privato nei quali siano integrati i principi dell'approdo sicuro e che contemplino dispositivi di attuazione efficaci, del tipo descritto dal principio delle garanzie d'applicazione; 2) uniformandosi a norme giurisdizionali o regolamentari emanate dalle corrispondenti autorità di controllo, che disciplinino il trattamento di reclami individuali e la soluzione delle controversie; oppure 3) impegnandosi a cooperare con le autorità di tutela dei dati aventi sede nella Comunità europea o loro rappresentanti autorizzati. Quest'elenco è fornito a titolo puramente esemplificativo e non limitativo. Il settore privato può indicare altri meccanismi di applicazione, purché rispettino il principio delle garanzie d'applicazione e le FAQ. Si noti che le citate garanzie d'applicazione si aggiungono a quelle di cui al paragrafo 3 dell'introduzione ai principi, in forza delle quali le iniziative di autoregolamentazione devono avere carattere vincolante in virtù dell'articolo 5 del Federal Trade Commission Act o analogo testo di legge.
Meccanismi di ricorso:
I consumatori dovrebbero essere incoraggiati a presentare gli eventuali reclami all'organizzazione direttamente interessata, prima di rivolgersi ai dispositivi indipendenti di ricorso. (...)
(...)
Attività della Commissione federale per il commercio (Federal Trade Commission, FTC):
La Commissione federale per il commercio (FTC) si è impegnata ad esaminare in via prioritaria i casi trasmessi da organizzazioni di autoregolamentazione in materia di riservatezza (quali BBBOnline e TRUSTe) e dagli Stati membri

dell'UE per denunciare la presunta non conformità ai principi dell'approdo sicuro, al fine di stabilire se vi siano state violazioni della sezione 5 del FTC Act, che vieta azioni o pratiche sleali od ingannevoli nel commercio. (...)
(...)».
10 Ai sensi dell'allegato IV della decisione 2000/520:
«Tutela della riservatezza e risarcimento danni, autorizzazioni legali, fusioni e acquisizioni secondo la legge degli Stati Uniti
Il presente documento risponde alla richiesta della Commissione europea di chiarimenti sulla legge statunitense per quanto riguarda a) risarcimento dei danni per violazione della sfera privata (privacy), b) le "autorizzazioni esplicite" previste dalla legge degli Stati Uniti per l'uso di dati personali in modo contrastante con i principi "approdo sicuro" (safe harbor), c) l'effetto delle fusioni e acquisizioni sugli obblighi assunti in base a tali principi.
(...)
B. Autorizzazioni legali esplicite
I principi "approdo sicuro" contengono un'eccezione qualora atti legislativi, regolamenti o la giurisprudenza "comportino obblighi contrastanti od autorizzazioni esplicite, purché nell'avvalersi di un'autorizzazione siffatta un'organizzazione possa dimostrare che il mancato rispetto dei principi da parte sua si limita a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione". È ovvio che quando la legge statunitense impone un'obbligazione conflittuale, le organizzazioni statunitensi, che aderiscano o no ai principi "approdo sicuro", devono osservare la legge. Per quanto riguarda le autorizzazioni esplicite, sebbene i principi "approdo sicuro" intendano colmare le differenze tra il sistema americano e quello europeo relativamente alla tutela della privacy, siamo tenuti al rispetto delle prerogative legislative dei legislatori eletti. La limitata eccezione al rigoroso rispetto dei principi "approdo sicuro" cerca di stabilire un equilibrio in grado di conciliare i legittimi interessi delle parti.
L'eccezione è limitata ai casi in cui esiste un'autorizzazione esplicita. Tuttavia, come caso limite, la legge, il regolamento o la decisione del tribunale pertinenti devono esplicitamente autorizzare una particolare condotta delle organizzazioni aderenti ai principi "approdo sicuro". In altre parole, l'eccezione non verrà applicata se la legge non prescrive nulla. Inoltre, l'eccezione verrà applicata soltanto se l'esplicita autorizzazione è in conflitto con il rispetto dei principi "approdo sicuro". Anche in questo caso, l'eccezione "si limita a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione". Ad esempio, se la legge si limita ad autorizzare un'azienda a fornire dati personali alle pubbliche autorità, l'eccezione non verrà applicata. Al contrario, se la legge autorizza espressamente l'azienda a fornire dati

personali ad organizzazioni governativ[e] senza il consenso dei singoli, ciò costituisce una "autorizzazione esplicita" ad agire in contrasto con i principi "approdo sicuro". In alternativa, le specifiche eccezioni alle disposizioni relative alla notifica al consenso rientrerebbero nell'ambito dell'eccezione (dato che ciò equivarrebbe ad una specifica autorizzazione a rivelare informazioni senza notifica e consenso). Ad esempio, una legge che autorizzi i medici a fornire le cartelle cliniche dei loro pazienti agli ufficiali sanitari senza il previo consenso dei pazienti stessi potrebbe consentire un'eccezione ai principi di notifica e di scelta. Tale autorizzazione non permetterebbe ad un medico di fornire le stesse cartelle cliniche alle casse mutue malattie o ai laboratori di ricerca farmaceutica perché ciò esulerebbe dall'ambito degli usi consentiti dalla legge e dunque dall'ambito dell'eccezione (...). L'autorizzazione in questione può essere un'autorizzazione "autonoma" a fare determinate cose con i dati personali ma, come illustrato negli esempi di cui sopra, è probabile che si tratti di un'eccezione a una legge generale che proscrive la raccolta, l'uso o la divulgazione dei dati personali.
(...)».

La comunicazione COM(2013) 846 final

11 Il 27 novembre 2013 la Commissione ha adottato la comunicazione al Parlamento europeo e al Consiglio, intitolata «Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA» [COM(2013) 846 final; in prosieguo: la «comunicazione COM(2013) 846 final»]. Tale comunicazione era corredata di una relazione, parimenti datata 27 novembre 2013, contenente le «conclusioni dei copresidenti dell'UE del gruppo di lavoro ad hoc UE-USA sulla protezione dei dati personali» («Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection»). Tale relazione era stata elaborata, come indicato dal suo punto 1, in cooperazione con gli Stati Uniti d'America in seguito alle rivelazioni dell'esistenza, in tale paese, di diversi programmi di controllo che comprendevano la raccolta e il trattamento su larga scala di dati personali. Detta relazione conteneva, segnatamente, un'analisi dettagliata dell'ordinamento giuridico statunitense per quanto attiene, in particolare, alle basi giuridiche che autorizzano l'esistenza di programmi di controllo, nonché la raccolta e il trattamento di dati personali da parte delle autorità americane.

12 Al punto 1 della comunicazione COM(2013) 846 final, la Commissione ha precisato che «[g]li scambi commerciali sono oggetto della decisione [2000/520]», aggiungendo che tale decisione «fornisce una base giuridica per il trasferimento dei dati personali dall'UE a società stabilite negli Stati Uniti che hanno aderito ai principi d'Approdo sicuro». Inoltre, sempre al punto 1, la Commissione ha messo in evidenza l'importanza sempre maggiore dei flussi di dati personali, legata segnatamente allo sviluppo

dell'economia digitale, il quale ha effettivamente «portato a una crescita esponenziale nella quantità, qualità, diversità e natura delle attività di trattamento dei dati».

13 Al punto 2 di tale comunicazione, la Commissione ha osservato che «le preoccupazioni sul livello di protezione dei dati personali dei cittadini dell'[Unione] trasferiti agli Stati Uniti nell'ambito del principio dell'Approdo sicuro sono aumentate», e che «[l]a natura volontaria e dichiarativa del regime ha difatti attirato grande attenzione sulla sua trasparenza e sulla sua applicazione».

14 Inoltre, essa ha indicato, in questo stesso punto 2, che «[i] dati personali dei cittadini dell'[Unione] inviati negli USA nell'ambito [del] regime [dell'approdo sicuro] possono essere consultati e ulteriormente trattati dalle autorità americane in maniera incompatibile con i motivi per cui erano stati originariamente raccolti nell'[Unione] e con le finalità del loro trasferimento agli Stati Uniti», e che «[l]a maggior parte delle imprese Internet americane che risultano più direttamente interessate [dai] programmi [di controllo], sono certificate nell'ambito del regime Approdo sicuro».

15 Al punto 3.2 della comunicazione COM(2013) 846 final, la Commissione ha rilevato l'esistenza di un certo numero di carenze quanto all'attuazione della decisione 2000/520. Da un lato, essa ha ivi menzionato il fatto che talune imprese americane certificate non rispettavano i principi di cui all'articolo 1, paragrafo 1, della decisione 2000/520 (in prosieguo: i «principi di approdo sicuro») e che dovevano essere apportati miglioramenti a tale decisione concernenti «i punti deboli strutturali relativi alla trasparenza e all'applicazione, i principi sostanziali dell'Approdo sicuro e il funzionamento dell'eccezione per motivi di sicurezza nazionale». Dall'altro, essa ha osservato che l'«Approdo sicuro funge inoltre da interfaccia per il trasferimento di dati personali di cittadini dell'UE dall'[Unione] europea agli Stati Uniti da parte di imprese che sono tenute a consegnare dati ai servizi di intelligence americani nell'ambito dei programmi di raccolta statunitensi».

16 La Commissione ha concluso, a questo stesso punto 3.2, che, se, «[t]enuto conto dei punti deboli individuati, il regime Approdo sicuro non può continuare ad essere applicato secondo le attuali modalità, (…) abrogarlo nuocerebbe [tuttavia] agli interessi delle imprese che ne sono membri, nell'[Unione] e negli USA». Infine, sempre a detto punto 3.2, la Commissione ha aggiunto che essa intendeva cominciare «col discutere con le autorità americane i punti deboli individuati».

La comunicazione COM(2013) 847 final

17 Sempre il 27 novembre 2013, la Commissione ha adottato la comunicazione al Parlamento europeo e al Consiglio sul funzionamento del regime "Approdo sicuro" dal punto di vista dei cittadini dell'UE e delle società

ivi stabilite [COM(2013) 847 final; in prosieguo: la «comunicazione COM(2013) 847 final»]. Come risulta dal suo punto 1, tale comunicazione si basava, segnatamente, sulle informazioni ricevute nell'ambito del Gruppo di lavoro ad hoc Unione europea-Stati Uniti e faceva seguito a due relazioni di valutazione della Commissione, pubblicate, rispettivamente, nel 2002 e nel 2004.

18 Il punto 1 di tale comunicazione precisa che il funzionamento della decisione 2000/520 «si basa sugli impegni assunti dalle imprese che vi aderiscono e sulla loro auto-certificazione» e aggiunge che «[l]'adesione è volontaria, ma [che] una volta sottoscritta le norme sono vincolanti».

19 Inoltre, emerge dal punto 2.2 della comunicazione COM(2013) 847 final che, al 26 settembre 2013, 3 246 imprese, facenti parte di numerosi settori dell'economia e dei servizi, erano certificate. Tali imprese fornivano, principalmente, servizi sul mercato interno dell'Unione, in particolare nel settore di Internet, e una parte di esse erano imprese dell'Unione con controllate negli Stati Uniti. Alcune di queste imprese trattavano i dati relativi ai loro dipendenti in Europa e li inviavano in tale paese a fini di gestione delle risorse umane.

20 Sempre al punto 2.2, la Commissione ha sottolineato che «[o]gni insufficienza a livello di trasparenza o di applicazione da parte americana [aveva] l'effetto di far ricadere la responsabilità sulle autorità per la protezione dei dati europee e sulle imprese che si avvalgono del regime in oggetto».

21 Si evince, segnatamente, dai punti da 3 a 5 e 8 della comunicazione COM(2013) 847 final che, nella prassi, un numero considerevole di imprese certificate non rispettava, o rispettava solo in parte, i principi dell'approdo sicuro.

22 Inoltre, al punto 7 di tale comunicazione, la Commissione ha affermato che «tutte le imprese partecipanti al programma PRISM [programma di raccolta di informazioni su larga scala], e che consentono alle autorità americane di avere accesso a dati conservati e trattati negli USA, risultano certificate nel quadro di Approdo sicuro», e che tale sistema «è diventato così una delle piattaforme di accesso delle autorità americane di intelligence alla raccolta di dati personali inizialmente trattati nell'[Unione]». A tal riguardo, la Commissione ha constatato, al punto 7.1 di detta comunicazione, che «un certo numero di basi giuridiche previste dalla legislazione americana consente la raccolta e il trattamento su larga scala di dati personali conservati o altrimenti trattati da società ubicate negli Stati Uniti» e che «[a] causa dell'ampia entità dei programmi, può accadere che dati trasferiti nell'ambito di Approdo sicuro siano accessibili alle autorità americane e vengano ulteriormente trattati da queste al di là di quanto è necessario e

proporzionato alla protezione della sicurezza nazionale come previsto dall'eccezione di cui alla decisione [2000/520]».

23 Al punto 7.2 della comunicazione COM(2013) 847 final, intitolata «Limitazioni e rimedi», la Commissione ha sottolineato che «i principali beneficiari delle garanzie previste dal diritto americano sono i cittadini statunitensi o le persone che risiedono legalmente negli USA» e che «[n]on vi è inoltre alcuna possibilità, né per gli interessati [dell'Unione] che per quelli americani, di ottenere l'accesso, la rettifica o la cancellazione dei dati, o rimedi amministrativi o giurisdizionali in relazione alla raccolta e all'ulteriore trattamento dei loro dati personali nell'ambito dei programmi di controllo statunitensi».

24 Secondo il punto 8 della comunicazione COM(2013) 847 final, fra le imprese certificate figuravano «[l]e imprese del web come Google, Facebook, Microsoft, Apple, Yahoo», le quali contano «[centinaia di] milioni di clienti in Europa» e trasferiscono dati personali negli Stati Uniti a fini del loro trattamento.

25 La Commissione ha concluso, a questo stesso punto 8, che «l'accesso su larga scala, da parte dei servizi di intelligence, ai dati trasferiti negli USA da imprese certificate nell'ambito di Approdo sicuro solleva altri gravi problemi riguardanti la continuità dei diritti dei cittadini europei in materia di protezione in caso di invio dei loro dati negli Stati Uniti».

Procedimento principale e questioni pregiudiziali

26 Il sig. Schrems, cittadino austriaco residente in Austria, è iscritto alla rete sociale Facebook (in prosieguo: «Facebook») dal 2008.

27 Chiunque risieda nel territorio dell'Unione e desideri utilizzare Facebook è tenuto, al momento della sua iscrizione, a sottoscrivere un contratto con Facebook Ireland, una controllata di Facebook Inc., situata, da parte sua, negli Stati Uniti. I dati personali degli utenti di Facebook residenti nel territorio dell'Unione vengono trasferiti, in tutto o in parte, su server di Facebook Inc. ubicati nel territorio degli Stati Uniti, ove essi sono oggetto di un trattamento.

28 Il 25 giugno 2013 il sig. Schrems ha investito il commissario di una denuncia, con la quale lo invitava, in sostanza, ad esercitare le proprie competenze statutarie, vietando a Facebook Ireland di trasferire i suoi dati personali verso gli Stati Uniti. In tale denuncia egli faceva valere che il diritto e la prassi vigenti in tale paese non offrivano una protezione sufficiente dei dati personali conservati nel territorio del medesimo contro le attività di controllo ivi praticate dalle autorità pubbliche. Il sig. Schrems si riferiva, a tal riguardo, alle rivelazioni fatte dal sig. Edward Snowden in merito alle attività dei servizi di intelligence degli Stati Uniti, e in particolare a quelle della National Security Agency (in prosieguo: la «NSA»).

29 Considerando di non essere obbligato a procedere ad un'indagine sui fatti denunciati dal sig. Schrems, il commissario ha respinto la denuncia in quanto priva di fondamento. Egli ha ritenuto, infatti, che non esistessero prove del fatto che la NSA avesse avuto accesso ai dati personali dell'interessato. Il commissario ha aggiunto che le censure formulate dal sig. Schrems nella sua denuncia non potevano essere fatte valere in maniera utile, in quanto ogni questione relativa all'adeguatezza della protezione dei dati personali negli Stati Uniti doveva essere risolta in conformità alla decisione 2000/520 e che, in tale decisione, la Commissione aveva constatato che gli Stati Uniti d'America assicuravano un livello di protezione adeguato.
30 Il sig. Schrems ha proposto un ricorso dinanzi alla High Court (Corte d'appello) avverso la decisione di cui al procedimento principale. Dopo aver esaminato le prove prodotte dalle parti nel procedimento principale, tale giudice ha dichiarato che la sorveglianza elettronica e l'intercettazione dei dati personali trasferiti dall'Unione verso gli Stati Uniti rispondevano a finalità necessarie e indispensabili per l'interesse pubblico. Tuttavia, detto giudice ha aggiunto che le rivelazioni del sig. Snowden avevano dimostrato che la NSA ed altri organi federali avevano commesso «eccessi considerevoli».
31 Orbene, secondo questo stesso giudice, i cittadini dell'Unione non avrebbero alcun diritto effettivo ad essere sentiti. La supervisione sull'operato dei servizi di intelligence verrebbe effettuata nell'ambito di un procedimento segreto e non contraddittorio. Una volta che i dati personali sono stati trasferiti verso gli Stati Uniti, la NSA e altri organi federali, come il Federal Bureau of Investigation (FBI), potrebbero accedere a tali dati nell'ambito della sorveglianza e delle intercettazioni indifferenziate da essi praticate su larga scala.
32 La High Court (Corte d'appello) ha constatato che il diritto irlandese vieta il trasferimento dei dati personali al di fuori del territorio nazionale, fatti salvi i casi in cui il paese terzo in questione assicura un livello di protezione adeguato della vita privata, nonché dei diritti e delle libertà fondamentali. L'importanza dei diritti al rispetto della vita privata e all'inviolabilità del domicilio, garantiti dalla Costituzione irlandese, implicherebbe che qualsiasi ingerenza in tali diritti sia proporzionata e conforme ai requisiti previsti dalla legge.
33 Orbene, l'accesso massiccio e indifferenziato a dati personali sarebbe manifestamente contrario al principio di proporzionalità e ai valori fondamentali protetti dalla Costituzione irlandese. Affinché intercettazioni di comunicazioni elettroniche possano essere considerate conformi a tale Costituzione, occorrerebbe dimostrare che tali intercettazioni sono mirate, che la sorveglianza su talune persone o taluni gruppi di persone è oggettivamente giustificata nell'interesse della sicurezza nazionale o della

repressione della criminalità, e che esistono garanzie adeguate e verificabili. Pertanto, secondo la High Court (Corte d'appello), qualora il procedimento principale dovesse essere definito sulla base del solo diritto irlandese, occorrerebbe constatare che, alla luce dell'esistenza di un serio dubbio sul fatto che gli Stati Uniti d'America assicurino un livello di protezione adeguato dei dati personali, il commissario avrebbe dovuto compiere un'indagine sui fatti lamentati dal sig. Schrems nella sua denuncia e che il commissario ha erroneamente respinto quest'ultima.

34 Tuttavia, la High Court (Corte d'appello) considera che tale causa verte sull'attuazione del diritto dell'Unione ai sensi dell'articolo 51 della Carta, cosicché la legittimità della decisione di cui al procedimento principale deve essere valutata sulla scorta del diritto dell'Unione. Orbene, secondo tale giudice, la decisione 2000/520 non soddisfa i requisiti risultanti sia dagli articoli 7 e 8 della Carta sia dai principi enunciati dalla Corte nella sentenza Digital Rights Ireland e a. (C-293/12 e C-594/12, EU:C:2014:238). Il diritto al rispetto della vita privata, garantito dall'articolo 7 della Carta e dai valori fondamentali comuni alle tradizioni degli Stati membri, sarebbe svuotato di significato qualora i pubblici poteri fossero autorizzati ad accedere alle comunicazioni elettroniche su base casuale e generalizzata, senza alcuna giustificazione oggettiva fondata su motivi di sicurezza nazionale o di prevenzione della criminalità, specificamente riguardanti i singoli interessati, e senza che tali pratiche siano accompagnate da garanzie adeguate e verificabili.

35 La High Court (Corte d'appello) osserva, inoltre, che il sig. Schrems, nel suo ricorso, ha contestato in realtà la legittimità del regime dell'approdo sicuro istituito dalla decisione 2000/520 e sul quale poggia la decisione di cui al procedimento principale. Pertanto, anche se il sig. Schrems non ha formalmente contestato la validità né della direttiva 95/46 né della decisione 2000/520, secondo tale giudice occorre chiarire se, avuto riguardo all'articolo 25, paragrafo 6, di tale direttiva, il commissario fosse vincolato dalla constatazione effettuata dalla Commissione in tale decisione, secondo la quale gli Stati Uniti d'America garantiscono un livello di protezione adeguato, oppure se l'articolo 8 della Carta autorizzasse il commissario a discostarsi, se del caso, da una siffatta constatazione.

36 È in tale contesto che la High Court (Corte d'appello) ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:

«1) Se, nel decidere in merito a una denuncia presentata a un'autorità indipendente investita per legge delle funzioni di gestione e di applicazione della legislazione sulla protezione dei dati, secondo cui i dati personali sono trasferiti a un paese terzo (nel caso di specie, gli Stati Uniti d'America) il cui

diritto e la cui prassi si sostiene non prevedano adeguate tutele per i soggetti interessati, tale autorità sia assolutamente vincolata dalla constatazione in senso contrario dell'Unione contenuta nella decisione 2000/520, tenuto conto degli articoli 7, 8 e 47 della Carta, nonostante le disposizioni dell'articolo 25, paragrafo 6, della direttiva 95/46.
2) Oppure, in alternativa, se detta autorità possa e/o debba condurre una propria indagine sulla questione alla luce degli sviluppi verificatisi nel frattempo, successivamente alla prima pubblicazione della decisione 2000/520».
Sulle questioni pregiudiziali
37 Con le sue questioni pregiudiziali, che occorre esaminare congiuntamente, il giudice del rinvio chiede, in sostanza, se e in che misura l'articolo 25, paragrafo 6, della direttiva 95/46, letto alla luce degli articoli 7, 8 e 47 della Carta, debba essere interpretato nel senso che una decisione adottata in forza di tale disposizione, come la decisione 2000/520, con la quale la Commissione constata che un paese terzo assicura un livello di protezione adeguato, osti a che un'autorità di controllo di uno Stato membro, ai sensi dell'articolo 28 di tale direttiva, possa esaminare la domanda di una persona relativa alla tutela dei suoi diritti e delle sue libertà con riguardo al trattamento di dati personali che la riguardano, i quali sono stati trasferiti da uno Stato membro verso tale paese terzo, allorché tale persona faccia valere che il diritto e la prassi in vigore in quest'ultimo non assicurano un livello di protezione adeguato.
Sui poteri delle autorità nazionali di controllo ai sensi dell'articolo 28 della direttiva 95/46, in presenza di una decisione della Commissione adottata in forza dell'articolo 25, paragrafo 6, di tale direttiva
38 Occorre rammentare, in via preliminare, che le disposizioni della direttiva 95/46, disciplinando il trattamento di dati personali che possono arrecare pregiudizio alle libertà fondamentali e, segnatamente, al diritto al rispetto della vita privata, devono essere necessariamente interpretate alla luce dei diritti fondamentali garantiti dalla Carta (v. sentenze Österreichischer Rundfunk e a., C-465/00, C-138/01 e C-139/01, EU:C:2003:294, punto 68; Google Spain e Google, C-131/12, EU:C:2014:317, punto 68, nonché Ryneš, C-212/13, EU:C:2014:2428, punto 29).
39 Risulta dall'articolo 1, nonché dai considerando 2 e 10 della direttiva 95/46, che essa è intesa a garantire non solo una tutela efficace e completa delle libertà e dei diritti fondamentali delle persone fisiche, e segnatamente del diritto fondamentale al rispetto della vita privata con riguardo al trattamento dei dati personali, ma anche un livello elevato di protezione di tali libertà e diritti fondamentali. L'importanza sia del diritto fondamentale al rispetto della vita privata, garantito dall'articolo 7 della Carta, sia del diritto

fondamentale alla tutela dei dati personali, garantito dall'articolo 8 della stessa, è inoltre sottolineata nella giurisprudenza della Corte (v. sentenze Rijkeboer, C-553/07, EU:C:2009:293, punto 47; Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punto 53, nonché Google Spain e Google, C-131/12, EU:C:2014:317, punti 53, 66 e 74 e la giurisprudenza ivi citata).

40 Per quanto attiene ai poteri di cui dispongono le autorità di controllo nazionali quanto al trasferimento di dati personali verso paesi terzi, si deve rilevare che l'articolo 28, paragrafo 1, della direttiva 95/46 obbliga gli Stati membri ad istituire una o più autorità pubbliche incaricate di controllare in piena indipendenza l'osservanza delle norme dell'Unione relative alla tutela delle persone fisiche con riguardo al trattamento di tali dati. Detto obbligo risulta altresì dal diritto primario dell'Unione, segnatamente dall'articolo 8, paragrafo 3, della Carta e dall'articolo 16, paragrafo 2, TFUE (v., in tal senso, sentenze Commissione/Austria, C-614/10, EU:C:2012:631, punto 36, e Commissione/Ungheria, C-288/12, EU:C:2014:237, punto 47).

41 La garanzia d'indipendenza delle autorità nazionali di controllo è diretta ad assicurare che il controllo del rispetto delle disposizioni in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali sia efficace e affidabile e deve essere interpretata alla luce di tale finalità. Essa è stata disposta al fine di rafforzare la protezione delle persone e degli organismi interessati dalle decisioni di tali autorità. L'istituzione, negli Stati membri, di autorità di controllo indipendenti, costituisce quindi, come rilevato dal considerando 62 della direttiva 95/46, un elemento essenziale del rispetto della tutela delle persone con riguardo al trattamento dei dati personali (v. sentenze Commissione/Germania, C-518/07, EU:C:2010:125, punto 25, nonché Commissione/Ungheria C-288/12, EU:C:2014:237, punto 48 e la giurisprudenza ivi citata).

42 Al fine di garantire tale protezione, le autorità nazionali di controllo devono, segnatamente, assicurare un giusto equilibrio fra, da un lato, il rispetto del diritto fondamentale alla vita privata e, dall'altro, gli interessi che impongono una libera circolazione dei dati personali (v., in tal senso, sentenze Commissione/Germania, C-518/07, EU:C:2010:125, punto 24, e Commissione/Ungheria C-288/12, EU:C:2014:237, punto 51).

43 A tal fine, dette autorità dispongono di un'ampia gamma di poteri e questi, elencati in maniera non esaustiva all'articolo 28, paragrafo 3, della direttiva 95/46, costituiscono altrettanti mezzi necessari all'adempimento dei loro compiti, come sottolineato dal considerando 63 di tale direttiva. In tal senso, dette autorità godono, segnatamente, di poteri investigativi, come quello di raccogliere qualsiasi informazione necessaria all'esercizio della loro funzione di controllo, di poteri effettivi d'intervento, come quello di vietare a

titolo provvisorio o definitivo un trattamento di dati o, ancora, del potere di promuovere azioni giudiziarie.

44 È vero che si evince dall'articolo 28, paragrafi 1 e 6, della direttiva 95/46 che i poteri delle autorità nazionali di controllo riguardano i trattamenti di dati personali effettuati nel territorio del loro Stato membro, cosicché esse non dispongono di poteri, sulla base di tale articolo 28, con riguardo ai trattamenti di siffatti dati effettuati nel territorio di un paese terzo.

45 Tuttavia, l'operazione consistente nel far trasferire dati personali da uno Stato membro verso un paese terzo costituisce, di per sé, un trattamento di dati personali ai sensi dell'articolo 2, lettera b), della direttiva 95/46 (v., in tal senso, sentenza Parlamento/Consiglio e Commissione, C-317/04 e C-318/04, EU:C:2006:346, punto 56) effettuato nel territorio di uno Stato membro. Infatti, tale disposizione definisce il «trattamento di dati personali» alla stregua di «qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali» e menziona, a titolo di esempio, «la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione».

46 Il considerando 60 della direttiva 95/46 precisa che i trasferimenti di dati personali verso i paesi terzi possono aver luogo soltanto nel pieno rispetto delle disposizioni prese dagli Stati membri in applicazione di tale direttiva. A tal riguardo, il capo IV di detta direttiva, nel quale figurano gli articoli 25 e 26 della medesima, ha predisposto un regime che mira a garantire un controllo da parte degli Stati membri sui trasferimenti di dati personali verso i paesi terzi. Tale regime è complementare al regime generale attuato dal capo II di questa stessa direttiva, riguardante le condizioni generali di liceità dei trattamenti di dati personali (v., in tal senso, sentenza Lindqvist, C-101/01, EU:C:2003:596, punto 63).

47 Poiché le autorità nazionali di controllo sono incaricate, ai sensi dell'articolo 8, paragrafo 3, della Carta e dell'articolo 28 della direttiva 95/46, di sorvegliare il rispetto delle norme dell'Unione relative alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, ciascuna di esse è quindi investita della competenza a verificare se un trasferimento di dati personali dal proprio Stato membro verso un paese terzo rispetti i requisiti fissati dalla direttiva 95/46.

48 Riconoscendo al contempo, al suo considerando 56, che i trasferimenti di dati personali dagli Stati membri verso paesi terzi sono necessari allo sviluppo degli scambi internazionali, la direttiva 95/46 pone come principio, al suo articolo 25, paragrafo 1, che siffatti trasferimenti possano avere luogo soltanto se tali paesi terzi garantiscono un livello di protezione adeguato.

49 Inoltre, il considerando 57 di detta direttiva precisa che i trasferimenti di dati personali verso paesi terzi che non offrono un livello di protezione adeguato devono essere vietati.
50 Al fine di controllare i trasferimenti di dati personali verso i paesi terzi in funzione del livello di protezione ad essi accordato in ciascuno di tali paesi, l'articolo 25 della direttiva 95/46 impone una serie di obblighi agli Stati membri e alla Commissione. Risulta, segnatamente, da tale articolo, che la constatazione se un paese terzo assicuri o meno un livello di protezione adeguato può essere effettuata, come rilevato dall'avvocato generale al paragrafo 86 delle sue conclusioni, vuoi dagli Stati membri vuoi dalla Commissione.
51 La Commissione può adottare, sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46, una decisione che constata che un paese terzo garantisce un livello di protezione adeguato. Conformemente al secondo comma di tale disposizione, una siffatta decisione ha come destinatari gli Stati membri, i quali devono adottare le misure necessarie per conformarvisi. Ai sensi dell'articolo 288, quarto comma, TFUE, essa ha un carattere vincolante per tutti gli Stati membri destinatari e si impone pertanto a tutti i loro organi (v., in tal senso, sentenze Albako Margarinefabrik, 249/85, EU:C:1987:245, punto 17, e Mediaset, C-69/13, EU:C:2014:71, punto 23), nella parte in cui produce l'effetto di autorizzare trasferimenti di dati personali dagli Stati membri verso il paese terzo da essa interessato.
52 Pertanto, fintantoché la decisione della Commissione non sia stata dichiarata invalida dalla Corte, gli Stati membri e i loro organi, fra i quali figurano le loro autorità di controllo indipendenti, non possono certo adottare misure contrarie a tale decisione, come atti intesi a constatare con effetto vincolante che il paese terzo interessato da detta decisione non garantisce un livello di protezione adeguato. Infatti, gli atti delle istituzioni dell'Unione si presumono, in linea di principio, legittimi e producono pertanto effetti giuridici, finché non siano stati revocati o annullati nel contesto di un ricorso per annullamento ovvero dichiarati invalidi a seguito di un rinvio pregiudiziale o di un'eccezione di illegittimità (sentenza Commissione/Grecia, C-475/01, EU:C:2004:585, punto 18 e la giurisprudenza ivi citata).
53 Tuttavia, una decisione della Commissione adottata sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46, come la decisione 2000/520, non può impedire alle persone i cui dati personali sono stati o potrebbero essere trasferiti verso un paese terzo di investire le autorità nazionali di controllo di una domanda, ai sensi dell'articolo 28, paragrafo 4, di tale direttiva, relativa alla protezione dei loro diritti e delle loro libertà con riguardo al trattamento di tali dati. Analogamente, una decisione di tale

natura non può, come rilevato dall'avvocato generale, segnatamente, ai paragrafi 61, 93 e 116 delle sue conclusioni, né elidere né ridurre i poteri espressamente riconosciuti alle autorità nazionali di controllo dall'articolo 8, paragrafo 3, della Carta, nonché dall'articolo 28 di detta direttiva.

54 Né l'articolo 8, paragrafo 3, della Carta né l'articolo 28 della direttiva 95/46 escludono dall'ambito di competenza delle autorità nazionali di controllo il controllo dei trasferimenti di dati personali verso paesi terzi che sono stati oggetto di una decisione della Commissione in forza dell'articolo 25, paragrafo 6, di tale direttiva.

55 In particolare, l'articolo 28, paragrafo 4, primo comma, della direttiva 95/46, il quale dispone che «[q]ualsiasi persona (...) può presentare [alle autorità nazionali di controllo] una domanda relativa alla tutela dei suoi diritti e libertà con riguardo al trattamento di dati personali», non prevede alcuna eccezione a tal riguardo nel caso in cui la Commissione abbia adottato una decisione in forza dell'articolo 25, paragrafo 6, di tale direttiva.

56 Inoltre, sarebbe contrario al sistema predisposto dalla direttiva 95/46, nonché alla finalità degli articoli 25 e 28 della stessa se una decisione della Commissione adottata in applicazione dell'articolo 25, paragrafo 6, di detta direttiva avesse come effetto di impedire ad un'autorità nazionale di controllo di esaminare la domanda di una persona relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento dei suoi dati personali che sono stati o potrebbero essere trasferiti da uno Stato membro verso un paese terzo interessato da tale decisione.

57 Al contrario, l'articolo 28 della direttiva 95/46 si applica, per la sua stessa natura, a ogni trattamento di dati personali. Pertanto, anche in presenza di una decisione della Commissione adottata sulla base dell'articolo 25, paragrafo 6, di tale direttiva, le autorità nazionali di controllo investite da una persona di una domanda relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento dei dati personali che la riguardano, devono poter verificare, in piena indipendenza, se il trasferimento di tali dati rispetti i requisiti fissati da detta direttiva.

58 Se così non fosse, le persone i cui dati personali sono stati o potrebbero essere trasferiti verso il paese terzo di cui trattasi sarebbero private del diritto, garantito all'articolo 8, paragrafi 1 e 3, della Carta, di investire le autorità nazionali di controllo di una domanda ai fini della protezione dei loro diritti fondamentali (v., per analogia, sentenza Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punto 68).

59 Una domanda, ai sensi dell'articolo 28, paragrafo 4, della direttiva 95/46, con la quale una persona i cui dati personali sono stati o potrebbero essere trasferiti verso un paese terzo fa valere, come nel procedimento principale, che il diritto e la prassi di tale paese non assicurano, nonostante quanto

constatato dalla Commissione in una decisione adottata in base all'articolo 25, paragrafo 6, di tale direttiva, un livello di protezione adeguato, deve essere intesa nel senso che essa verte, in sostanza, sulla compatibilità di tale decisione con la protezione della vita privata e delle libertà e dei diritti fondamentali della persona.

60 A tal riguardo, occorre richiamare la giurisprudenza costante della Corte secondo la quale l'Unione è un'Unione di diritto, nel senso che tutti gli atti delle sue istituzioni sono soggetti al controllo della conformità, segnatamente, ai Trattati, ai principi generali del diritto nonché ai diritti fondamentali (v., in tal senso, sentenze Commissione e a./Kadi, C-584/10 P, C-593/10 P e C-595/10 P, EU:C:2013:518, punto 66; Inuit Tapiriit Kanatami e a./Parlamento e Consiglio, C-583/11 P, EU:C:2013:625, punto 91, nonché Telefónica/Commissione, C-274/12 P, EU:C:2013:852, punto 56). Le decisioni della Commissione adottate in forza dell'articolo 25, paragrafo 6, della direttiva 95/46 non possono pertanto sfuggire ad un siffatto controllo.

61 Ciò premesso, la Corte è competente in via esclusiva a dichiarare l'invalidità di un atto dell'Unione, quale una decisione della Commissione adottata in applicazione dell'articolo 25, paragrafo 6, della direttiva 95/46; la natura esclusiva di tale competenza ha lo scopo di garantire la certezza del diritto assicurando l'applicazione uniforme del diritto dell'Unione (v. sentenze Melki e Abdeli, C-188/10 e C-189/10, EU:C:2010:363, punto 54, nonché CIVAD, C-533/10, EU:C:2012:347, punto 40).

62 Per quanto i giudici nazionali siano effettivamente legittimati ad esaminare la validità di un atto dell'Unione, come una decisione della Commissione adottata in forza dell'articolo 25, paragrafo 6, della direttiva 95/46, essi non sono tuttavia competenti a constatare essi stessi l'invalidità di un siffatto atto (v., in tal senso, sentenze Foto-Frost, 314/85, EU:C:1987:452, punti da 15 a 20, nonché IATA e ELFAA, C-344/04, EU:C:2006:10, punto 27). A fortiori, in sede di esame di una domanda, ai sensi dell'articolo 28, paragrafo 4, di tale direttiva, avente ad oggetto la compatibilità di una decisione della Commissione adottata in forza dell'articolo 25, paragrafo 6, di detta direttiva con la protezione della vita privata e delle libertà e dei diritti fondamentali della persona, le autorità nazionali di controllo non sono competenti a constatare esse stesse l'invalidità di una siffatta decisione.

63 Alla luce di tali considerazioni, qualora una persona i cui dati personali sono stati o potrebbero essere trasferiti verso un paese terzo che è stato oggetto di una decisione della Commissione in forza dell'articolo 25, paragrafo 6, della direttiva 95/46, investa un'autorità nazionale di controllo di una domanda relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento di tali dati e contesti, in occasione di tale domanda, come nel

procedimento principale, la compatibilità di tale decisione con la protezione della vita privata e delle libertà e dei diritti fondamentali della persona, incombe a tale autorità esaminare detta domanda con tutta la diligenza richiesta.

64 Nel caso in cui detta autorità pervenga alla conclusione che gli elementi addotti a sostegno di una siffatta domanda sono privi di fondamento e, per questo motivo, la respinga, la persona che ha proposto detta domanda deve avere accesso, come si evince dall'articolo 28, paragrafo 3, secondo comma, della direttiva 95/46, in combinato con l'articolo 47 della Carta, ai mezzi di ricorso giurisdizionali che le consentono di contestare una siffatta decisione impugnandola dinanzi ai giudici nazionali. Alla luce della giurisprudenza citata ai punti 61 e 62 della presente sentenza, tali giudici devono sospendere la decisione e investire la Corte di un procedimento pregiudiziale per accertamento di validità, allorché essi ritengono che uno o più motivi di invalidità formulati dalle parti o, eventualmente, sollevati d'ufficio siano fondati (v., in tal senso, sentenza T & L Sugars e Sidul Açúcares/Commissione, C-456/13 P, EU:C:2015:284, punto 48 e la giurisprudenza ivi citata).

65 Nell'ipotesi contraria, in cui detta autorità reputi fondate le censure sollevate dalla persona che l'ha investita di una domanda relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento dei suoi dati personali, questa stessa autorità, ai sensi dell'articolo 28, paragrafo 3, primo comma, terzo trattino, della direttiva 95/46, in combinato, segnatamente, con l'articolo 8, paragrafo 3, della Carta, deve poter promuovere azioni giudiziarie. A tal riguardo, incombe al legislatore nazionale prevedere mezzi di ricorso che consentano all'autorità nazionale di controllo di cui trattasi di far valere le censure che essa reputa fondate dinanzi ai giudici nazionali, affinché questi ultimi procedano, qualora condividano i dubbi di tale autorità in ordine alla validità della decisione della Commissione, ad un rinvio pregiudiziale inteso all'esame della validità di tale decisione.

66 In virtù delle considerazioni che precedono, si deve rispondere alle questioni sollevate che l'articolo 25, paragrafo 6, della direttiva 95/46, letto alla luce degli articoli 7, 8 e 47 della Carta, deve essere interpretato nel senso che una decisione adottata in forza di tale disposizione, quale la decisione 2000/520, con la quale la Commissione constata che un paese terzo garantisce un livello di protezione adeguato, non osta a che un'autorità di controllo di uno Stato membro, ai sensi dell'articolo 28 di tale direttiva, esamini la domanda di una persona relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento di dati personali che la riguardano, i quali sono stati trasferiti da uno Stato membro verso tale paese terzo, qualora tale

persona faccia valere che il diritto e la prassi in vigore in quest'ultimo non garantiscono un livello di protezione adeguato.

Sulla validità della decisione 2000/520

67 Come si evince dalle spiegazioni del giudice del rinvio relative alle questioni sollevate, il sig. Schrems fa valere, nel procedimento principale, che il diritto e la prassi degli Stati Uniti non assicurano un livello di protezione adeguato ai sensi dell'articolo 25 della direttiva 95/46. Come rilevato dall'avvocato generale ai paragrafi 123 e 124 delle sue conclusioni, il sig. Schrems esprime dubbi, che tale giudice sembra peraltro condividere nella sostanza, concernenti la validità della decisione 2000/520. In tali circostanze, in virtù delle constatazioni effettuate ai punti da 60 a 63 della presente sentenza, e al fine di fornire una risposta completa a detto giudice, occorre verificare se tale decisione sia conforme ai requisiti risultanti da detta direttiva, letta alla luce della Carta.

Sui requisiti risultanti dall'articolo 25, paragrafo 6, della direttiva 95/46

68 Come è già stato rilevato ai punti 48 e 49 della presente sentenza, l'articolo 25, paragrafo 1, della direttiva 95/46 vieta i trasferimenti di dati personali verso un paese terzo che non garantisce un livello di protezione adeguato.

69 Tuttavia, ai fini del controllo di tali trasferimenti, l'articolo 25, paragrafo 6, primo comma, di tale direttiva, dispone che la Commissione «può constatare (...) che un paese terzo garantisce un livello di protezione adeguato ai sensi del paragrafo 2 [di tale articolo], in considerazione della sua legislazione nazionale o dei suoi impegni internazionali (...), ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona».

70 È vero che né l'articolo 25, paragrafo 2, della direttiva 95/46 né nessun'altra disposizione della medesima contengono una definizione della nozione di livello di protezione adeguato. In particolare, l'articolo 25, paragrafo 2, di detta direttiva si limita ad enunciare che l'adeguatezza del livello di protezione garantito da un paese terzo «è valutata con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati» ed elenca, in maniera non esaustiva, le circostanze che devono essere prese in considerazione in occasione di una siffatta valutazione.

71 Tuttavia, da un lato, come si evince dalla lettera stessa dell'articolo 25, paragrafo 6, della direttiva 95/46, tale disposizione esige che un paese terzo «garantisc[a]» un livello di protezione adeguato in considerazione della sua legislazione nazionale o dei suoi impegni internazionali. Dall'altro, sempre secondo tale disposizione, l'adeguatezza della protezione assicurata dal

paese terzo viene valutata «ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona».

72 In tal modo, l'articolo 25, paragrafo 6, della direttiva 95/46 attua l'obbligo esplicito di protezione dei dati personali previsto all'articolo 8, paragrafo 1, della Carta e mira ad assicurare, come rilevato dall'avvocato generale al paragrafo 139 delle sue conclusioni, la continuità del livello elevato di tale protezione in caso di trasferimento di dati personali verso un paese terzo.

73 È vero che il termine «adeguato» figurante all'articolo 25, paragrafo 6, della direttiva 95/46 implica che non possa esigersi che un paese terzo assicuri un livello di protezione identico a quello garantito nell'ordinamento giuridico dell'Unione. Tuttavia, come rilevato dall'avvocato generale al paragrafo 141 delle sue conclusioni, l'espressione «livello di protezione adeguato» deve essere intesa nel senso che esige che tale paese assicuri effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione delle libertà e dei diritti fondamentali sostanzialmente equivalente a quello garantito all'interno dell'Unione in forza della direttiva 95/46, letta alla luce della Carta. Infatti, in assenza di un siffatto requisito, l'obiettivo menzionato al punto precedente della presente sentenza sarebbe disatteso. Inoltre, il livello elevato di protezione garantito dalla direttiva 95/46, letta alla luce della Carta, potrebbe essere facilmente eluso da trasferimenti di dati personali dall'Unione verso paesi terzi ai fini del loro trattamento in tali paesi.

74 Si evince dalla formulazione espressa dell'articolo 25, paragrafo 6, della direttiva 95/46 che è l'ordinamento giuridico del paese terzo interessato dalla decisione della Commissione che deve garantire un livello di protezione adeguato. Anche se gli strumenti dei quali tale paese terzo si avvale, al riguardo, per assicurare un siffatto livello di protezione, possono essere diversi da quelli attuati all'interno dell'Unione al fine di garantire il rispetto dei requisiti risultanti da tale direttiva, letta alla luce della Carta, tali strumenti devono cionondimeno rivelarsi efficaci, nella prassi, al fine di assicurare una protezione sostanzialmente equivalente a quella garantita all'interno dell'Unione.

75 In tali condizioni, in sede di esame del livello di protezione offerto da un paese terzo, la Commissione è tenuta a valutare il contenuto delle norme applicabili in tale paese risultanti dalla legislazione nazionale o dagli impegni internazionali di quest'ultimo, nonché la prassi intesa ad assicurare il rispetto di tali norme; al riguardo, tale istituzione deve prendere in considerazione, in conformità all'articolo 25, paragrafo 2, della direttiva 95/46, tutte le circostanze relative ad un trasferimento di dati personali verso un paese terzo.

76 Analogamente, alla luce del fatto che il livello di protezione assicurato da un paese terzo può evolversi, incombe alla Commissione, successivamente all'adozione di una decisione in forza dell'articolo 25, paragrafo 6, della direttiva 95/46, verificare periodicamente se la constatazione relativa al livello di protezione adeguato assicurato dal paese terzo in questione continui ad essere giustificata in fatto e in diritto. Una siffatta verifica è in ogni caso obbligatoria quando taluni indizi facciano sorgere un dubbio al riguardo.
77 Inoltre, come rilevato dall'avvocato generale ai paragrafi 134 e 135 delle sue conclusioni, in sede di esame della validità di una decisione della Commissione adottata in forza dell'articolo 25, paragrafo 6, della direttiva 95/46, occorre anche tenere conto delle circostanze intervenute successivamente all'adozione di tale decisione.
78 A tal riguardo, occorre constatare che, alla luce, da un lato, del ruolo importante svolto dalla protezione dei dati personali sotto il profilo del diritto fondamentale al rispetto della vita privata e, dall'altro, del numero significativo di persone i cui diritti fondamentali possono essere violati in caso di trasferimento di dati personali verso un paese terzo che non assicura un livello di protezione adeguato, il potere discrezionale della Commissione in ordine all'adeguatezza del livello di protezione assicurato da un paese terzo risulta ridotto, cosicché è necessario procedere ad un controllo stretto dei requisiti risultanti dall'articolo 25 della direttiva 95/46, letto alla luce della Carta (v., per analogia, sentenza Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punti 47 e 48).
Sull'articolo 1 della decisione 2000/520
79 La Commissione ha considerato, all'articolo 1, paragrafo 1, della decisione 2000/520, che i principi di cui all'allegato I della medesima, applicati in conformità agli orientamenti forniti dalle FAQ di cui all'allegato II di detta decisione, garantiscono un livello adeguato di protezione dei dati personali trasferiti dall'Unione a organizzazioni aventi sede negli Stati Uniti. Risulta da tale disposizione che sia tali principi sia tali FAQ sono stati pubblicati dal Dipartimento del commercio degli Stati Uniti.
80 L'adesione di un'organizzazione ai principi dell'approdo sicuro avviene sulla base di un sistema di autocertificazione, come si evince dall'articolo 1, paragrafi 2 e 3, di tale decisione, in combinato disposto con la FAQ 6 figurante all'allegato II a detta decisione.
81 Sebbene il ricorso, da parte di un paese terzo, ad un sistema di autocertificazione non sia di per sé contrario al requisito previsto dall'articolo 25, paragrafo 6, della direttiva 95/46, secondo il quale il paese terzo di cui trattasi deve garantire un livello di protezione adeguato «in considerazione della (...) legislazione nazionale o [degli] impegni internazionali» di tale

paese, l'affidabilità di un siffatto sistema, con riferimento a tale requisito, poggia essenzialmente sulla predisposizione di meccanismi efficaci di accertamento e di controllo che consentano di individuare e sanzionare, nella prassi, eventuali violazioni delle norme che assicurano la protezione dei diritti fondamentali, e segnatamente del diritto al rispetto della vita privata, nonché del diritto alla protezione dei dati personali.
82 Nella specie, in forza dell'allegato I, secondo comma, della decisione 2000/520, i principi dell'approdo sicuro sono «destinati unicamente ad organizzazioni americane che ricevono dati personali dall'Unione europea, al fine di permettere a tali organizzazioni di ottemperare al principio di "approdo sicuro" ed alla presunzione di "adeguatezza" che esso comporta». Tali principi sono dunque applicabili soltanto alle organizzazioni americane autocertificate che ricevono dati personali dall'Unione, mentre dalle autorità pubbliche americane non si esige il rispetto di detti principi.
83 Inoltre, ai sensi dell'articolo 2 della decisione 2000/520, quest'ultima «dispone soltanto in merito all'adeguatezza della protezione offerta negli Stati Uniti, in base ai principi [dell'approdo sicuro] applicati in conformità alle FAQ, al fine di quanto prescritto dall'articolo 25, paragrafo 1, della direttiva [95/46]», senza tuttavia contenere le constatazioni sufficienti quanto alle misure tramite le quali gli Stati Uniti d'America assicurano un livello di protezione adeguato, ai sensi dell'articolo 25, paragrafo 6, di tale direttiva, in considerazione della loro legislazione nazionale o dei loro impegni internazionali.
84 A ciò si aggiunge che, in conformità all'allegato I, quarto comma, della decisione 2000/520, l'applicabilità di detti principi può essere limitata, segnatamente, «se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia [degli Stati Uniti]», nonché da «disposizioni legislative o regolamentari ovvero decisioni giurisdizionali quando tali fonti comportino obblighi contrastanti od autorizzazioni esplicite, purché nell'avvalersi di un'autorizzazione siffatta un'organizzazione possa dimostrare che il mancato rispetto dei principi da parte sua si limita a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione».
85 A tal riguardo, al titolo B del suo allegato IV, la decisione 2000/520 sottolinea, per quanto attiene ai limiti ai quali è assoggettata l'applicabilità dei principi dell'approdo sicuro, che «[è] ovvio che quando la legge statunitense impone un'obbligazione conflittuale, le organizzazioni statunitensi, che aderiscano o no ai principi "approdo sicuro", devono osservare la legge».
86 In tal modo, la decisione 2000/520 sancisce il primato delle «esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia

[degli Stati Uniti]» sui principi dell'approdo sicuro, primato in forza del quale le organizzazioni americane autocertificate che ricevono dati personali dall'Unione sono tenute a disapplicare senza limiti tali principi allorché questi ultimi interferiscono con tali esigenze e risultano dunque incompatibili con le medesime.

87 Alla luce del carattere generale della deroga figurante all'allegato I, quarto comma, della decisione 2000/520, essa rende pertanto possibili ingerenze, fondate su esigenze connesse alla sicurezza nazionale e all'interesse pubblico o alla legislazione interna degli Stati Uniti, nei diritti fondamentali delle persone i cui dati personali sono o potrebbero essere trasferiti dall'Unione verso gli Stati Uniti. A tal riguardo, poco importa, per accertare l'esistenza di un'ingerenza nel diritto fondamentale al rispetto della vita privata, che le informazioni relative alla vita privata di cui trattasi abbiano o meno un carattere sensibile o che gli interessati abbiano o meno subito eventuali inconvenienti in seguito a tale ingerenza (sentenza Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punto 33 e la giurisprudenza ivi citata).

88 Inoltre, la decisione 2000/520 non contiene alcuna dichiarazione quanto all'esistenza, negli Stati Uniti, di norme statali destinate a limitare le eventuali ingerenze nei diritti fondamentali delle persone i cui dati vengono trasferiti dall'Unione verso gli Stati Uniti, ingerenze che entità statali di tale paese sarebbero autorizzate a compiere laddove perseguano obiettivi legittimi, come la sicurezza nazionale.

89 A ciò si aggiunge il fatto che la decisione 2000/520 non menziona l'esistenza di una tutela giuridica efficace nei confronti delle ingerenze di tale natura. Come rilevato dall'avvocato generale ai paragrafi da 204 a 206 delle sue conclusioni, i meccanismi di arbitrato privato e i procedimenti dinanzi alla Commissione federale per il commercio, i cui poteri, descritti segnatamente nelle FAQ 11 figuranti all'allegato II a tale decisione, sono limitati alle controversie in materia commerciale, riguardano il rispetto, da parte delle imprese americane, dei principi dell'approdo sicuro, e non possono essere applicati nell'ambito delle controversie concernenti la legittimità di ingerenze nei diritti fondamentali risultanti da misure di origine statale.

90 Inoltre, la suesposta analisi della decisione 2000/520 è corroborata dalla valutazione della stessa Commissione quanto alla situazione risultante dall'esecuzione di tale decisione. Infatti, in particolare ai punti 2 e 3.2 della comunicazione COM(2013) 846 final, nonché ai punti 7.1, 7.2 e 8 della comunicazione COM(2013) 847 final, il cui contenuto viene illustrato rispettivamente ai punti da 13 a 16, nonché ai punti 22, 23 e 25 della presente sentenza, tale istituzione ha constatato che le autorità americane

potevano accedere ai dati personali trasferiti dagli Stati membri verso gli Stati Uniti e trattarli in maniera incompatibile, segnatamente, con le finalità del loro trasferimento, e al di là di quanto era strettamente necessario e proporzionato per la protezione della sicurezza nazionale. Analogamente, la Commissione ha constatato che non esistevano, per le persone di cui trattasi, rimedi amministrativi o giurisdizionali che consentissero, segnatamente, di accedere ai dati che le riguardavano e, se del caso, di ottenerne la rettifica o la soppressione.

91 Quanto al livello di protezione delle libertà e dei diritti fondamentali garantito all'interno dell'Unione, una normativa della medesima che comporta un'ingerenza nei diritti fondamentali garantiti dagli articoli 7 e 8 della Carta deve prevedere, secondo la giurisprudenza costante della Corte, regole chiare e precise che disciplinino la portata e l'applicazione della misura de qua e impongano requisiti minimi in modo che le persone i cui dati personali sono interessati dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro dati contro il rischio di abusi nonché contro eventuali accessi e usi illeciti dei suddetti dati. La necessità di disporre di siffatte garanzie è tanto più importante allorché i dati personali sono soggetti a trattamento automatico ed esiste un rischio considerevole di accesso illecito ai dati stessi (sentenza Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punti 54 e 55, nonché la giurisprudenza ivi citata).

92 Inoltre, e soprattutto, la protezione del diritto fondamentale al rispetto della vita privata a livello dell'Unione richiede che le deroghe e le restrizioni alla tutela dei dati personali operino entro i limiti dello stretto necessario (sentenza Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punto 52 e la giurisprudenza ivi citata).

93 In tal senso, non è limitata allo stretto necessario una normativa che autorizza in maniera generale la conservazione di tutti i dati personali di tutte le persone i cui dati sono stati trasferiti dall'Unione verso gli Stati Uniti senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo perseguito e senza che sia previsto alcun criterio oggettivo che permetta di delimitare l'accesso delle autorità pubbliche ai dati e il loro uso ulteriore a fini precisi, rigorosamente ristretti ed idonei a giustificare l'ingerenza che sia l'accesso sia l'utilizzazione di tali dati comporta [v. in tal senso, in relazione alla direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE, (GU L 105, pag.54), sentenza Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punti da 57 a 61].

94 In particolare, si deve ritenere che una normativa che consente alle autorità pubbliche di accedere in maniera generalizzata al contenuto di comunicazioni elettroniche pregiudichi il contenuto essenziale del diritto fondamentale al rispetto della vita privata, come garantito dall'articolo 7 della Carta (v., in tal senso, sentenza Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punto 39).

95 Analogamente, una normativa che non prevede alcuna possibilità per il singolo di avvalersi di rimedi giuridici al fine di accedere a dati personali che lo riguardano, oppure di ottenere la rettifica o la soppressione di tali dati, non rispetta il contenuto essenziale del diritto fondamentale ad una tutela giurisdizionale effettiva, quale sancito all'articolo 47 della Carta. Infatti, l'articolo 47, primo comma, della Carta esige che ogni individuo i cui diritti e le cui libertà garantiti dal diritto dell'Unione siano stati violati abbia diritto ad un ricorso effettivo dinanzi ad un giudice, nel rispetto delle condizioni previste in tale articolo. A tal riguardo, l'esistenza stessa di un controllo giurisdizionale effettivo, destinato ad assicurare il rispetto delle disposizioni del diritto dell'Unione, è inerente all'esistenza di uno Stato di diritto (v., in tal senso, sentenze Les Verts/Parlamento, 294/83, EU:C:1986:166, punto 23; Johnston, 222/84, EU:C:1986:206, punti 18 e 19; Heylens e a., 222/86, EU:C:1987:442, punto 14, nonché, UGT-Rioja e a., da C-428/06 a C-434/06, EU:C:2008:488, punto 80).

96 Come è stato rilevato segnatamente ai punti 71, 73 e 74 della presente sentenza, l'adozione, da parte della Commissione, di una decisione in forza dell'articolo 25, paragrafo 6, della direttiva 95/46 richiede la constatazione, debitamente motivata, da parte di tale istituzione, che il paese terzo di cui trattasi garantisce effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione dei diritti fondamentali sostanzialmente equivalente a quello garantito nell'ordinamento giuridico dell'Unione, come emerge segnatamente dai punti precedenti della presente sentenza.

97 Orbene, occorre rilevare che la Commissione, nella decisione 2000/520, non ha affermato che gli Stati Uniti d'America «garantiscono» effettivamente un livello di protezione adeguato in considerazione della loro legislazione nazionale o dei loro impegni internazionali.

98 Di conseguenza, e senza che occorra esaminare i principi dell'approdo sicuro sotto il profilo del loro contenuto, si deve concludere che l'articolo 1 di tale decisione viola i requisiti fissati all'articolo 25, paragrafo 6, della direttiva 95/46, letto alla luce della Carta, e che esso è, per tale motivo, invalido.

Sull'articolo 3 della decisione 2000/520

99 Si evince dalle considerazioni svolte ai punti 53, 57 e 63 della presente sentenza che, considerato l'articolo 28 della direttiva 95/46, letto alla luce, segnatamente, dell'articolo 8 della Carta, le autorità nazionali di controllo devono poter esaminare, in piena indipendenza, ogni domanda relativa alla protezione dei diritti e delle libertà di una persona con riguardo al trattamento di dati personali che la riguardano. Ciò vale in particolare allorché, in occasione di una siffatta domanda, tale persona sollevi questioni attinenti alla compatibilità di una decisione della Commissione adottata in forza dell'articolo 25, paragrafo 6, di tale direttiva, con la protezione della vita privata e delle libertà e dei diritti fondamentali della persona.
100 Tuttavia, l'articolo 3, paragrafo 1, primo comma, della decisione 2000/520 contiene una disciplina specifica quanto ai poteri di cui dispongono le autorità nazionali di controllo con riferimento ad una constatazione effettuata dalla Commissione in relazione al livello di protezione adeguato, ai sensi dell'articolo 25 della direttiva 95/46.
101 Così, ai sensi di tale disposizione, tali autorità possono, «[f]atto salvo il loro potere di adottare misure per garantire l'ottemperanza alle disposizioni nazionali adottate in forza di disposizioni diverse dall'articolo 25 della direttiva [95/46], (…) sospendere flussi di dati diretti a un'organizzazione che ha autocertificato la sua adesione ai principi [della decisione 2000/520]», a condizioni restrittive che fissano una soglia elevata di intervento. Per quanto tale disposizione non pregiudichi i poteri di dette autorità di adottare misure intese ad assicurare il rispetto delle disposizioni nazionali adottate in applicazione di questa direttiva, cionondimeno essa esclude che le medesime possano adottare misure intese a garantire il rispetto dell'articolo 25 della direttiva medesima.
102 L'articolo 3, paragrafo 1, primo comma, della decisione 2000/520 deve pertanto essere inteso nel senso che esso priva le autorità nazionali di controllo dei poteri che esse traggono dall'articolo 28 della direttiva 95/46, nel caso in cui una persona, in occasione di una domanda basata su tale disposizione, adduca elementi idonei a rimettere in discussione il fatto che una decisione della Commissione che ha constatato, sul fondamento dell'articolo 25, paragrafo 6, di tale direttiva, che un paese terzo garantisce un livello di protezione adeguato, sia compatibile con la protezione della vita privata e delle libertà e dei diritti fondamentali della persona.
103 Orbene, il potere di esecuzione che il legislatore dell'Unione ha attribuito alla Commissione con l'articolo 25, paragrafo 6, della direttiva 95/46 non conferisce a tale istituzione la competenza di limitare i poteri delle autorità nazionali di controllo previsti al punto precedente della presente sentenza.

104 Ciò premesso, occorre constatare che, adottando l'articolo 3 della decisione 2000/520, la Commissione ha ecceduto la competenza attribuitale all'articolo 25, paragrafo 6, della direttiva 95/46, letto alla luce della Carta, e che, per questo motivo, esso è invalido.
105 Poiché gli articoli 1 e 3 della decisione 2000/520 non possono essere separati dagli articoli 2 e 4, nonché dagli allegati alla medesima, la loro invalidità inficia la validità di tale decisione nel suo complesso.
106 Alla luce di tutte le considerazioni che precedono, si deve concludere che la decisione 2000/520 è invalida.
Sulle spese
107 Nei confronti delle parti nel procedimento principale, la presente causa costituisce un incidente sollevato dinanzi al giudice nazionale, cui spetta quindi statuire sulle spese. Le spese sostenute da altri soggetti per presentare osservazioni alla Corte non possono dar luogo a rifusione.
Per questi motivi, la Corte (Grande Sezione) dichiara:
1) L'articolo 25, paragrafo 6, della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, come modificata dal regolamento (CE) n.1882/2003 del Parlamento europeo e del Consiglio, del 29 settembre 2003, letto alla luce degli articoli 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione europea, deve essere interpretato nel senso che una decisione adottata in forza di tale disposizione, come la decisione 2000/520/CE della Commissione, del 26 luglio 2000, a norma della direttiva 95/46 sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «Domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti, con la quale la Commissione europea constata che un paese terzo garantisce un livello di protezione adeguato, non osta a che un'autorità di controllo di uno Stato membro, ai sensi dell'articolo 28 di tale direttiva, come modificata, esamini la domanda di una persona relativa alla protezione dei suoi diritti e delle sue libertà con riguardo al trattamento di dati personali che la riguardano, i quali sono stati trasferiti da uno Stato membro verso tale paese terzo, qualora tale persona faccia valere che il diritto e la prassi in vigore in quest'ultimo non garantiscono un livello di protezione adeguato.
2) La decisione 2000/520 è invalida.

Abstract
Il presente contributo esamina la sentenza della Corte di Giustizia dell'Unione Europea del 06.10.2015, afferente alla causa C-362/14, e le relative conseguenze della pronuncia con la quale la medesima Corte ha

dichiarato invalida la decisione della Commissione Europea che attestava che gli Stati Uniti garantivano un adeguato livello di protezione dei dati personali trasferiti.

The aim of this contribution is to study the decision of the European Court of Justice, relating to Case C-362/14 and the relative consequences of that ruling in which the same Court declared invalid the decision of the European Commission which indicating that the United States had an adequate level of protection for personal data transferred.

1. Introduzione.

La sentenza in commento, pronunciata dalla Corte di Giustizia il 06.10.2015, nella causa C-362/14, si pone lungo la scia di una serie di precedenti provvedimenti, adottati dal medesimo organo giudicante e facenti parte di un emergente filone giurisprudenziale, teso a tutelare adeguatamente il diritto alla *privacy* e la protezione dei dati personali [1].
L'intervento della Corte avviene, poi, nel contesto di un settore, quale quello del trasferimento dei dati personali dall'Unione europea agli Stati terzi ovvero, nello specifico, nel contesto del trasferimento transfrontaliero dei dati verso gli Stati Uniti, sul quale fino ad ora i Giudici di Lussemburgo non avevano avuto ancora la possibilità di pronunciarsi. Tale sentenza sollecita, quindi, una serie di riflessioni in merito alle modalità di salvaguardia dei dati personali trasmessi dall'Unione europea ai Paesi terzi, rilevando, soprattutto l'interpretazione che i Giudici danno della direttiva n. 95/46/CE, informata all'effettiva tutela di dette situazioni giuridiche, in omaggio alle pertinenti disposizioni della Carta di Nizza ed ai principi generali del diritto dell'Unione Europea.

2. La questione all'origine della vicenda.

Il caso sottoposto all'attenzione della Corte di Giustizia traeva origine dalla domanda di pronuncia pregiudiziale, proposta dalla *High Court of Ireland* (Alta Corte di giustizia irlandese o Corte d'appello irlandese) nell'ambito di una controversia insorta tra un cittadino austriaco e il *Data Protection Commissioner* irlandese (commissario per la protezione dei dati).
Nello specifico la suddetta controversia concerneva il rifiuto espresso, da parte del *Data Protection Commissioner*, di istruire la denuncia presentata dal sig. Schrems.
La suddetta vicenda aveva avuto inizio, infatti, con un ricorso con il quale il Sig. Maximillian Schrems, utente di *Facebook*, si lamentava, innanzi al *Data Protection Commissioner* irlandese, del fatto che i propri dati personali, forniti ai fini dell'iscrizione al *social network*, fossero trasferiti dalla filiale irlandese di *Facebook* alla sede principale della medesima negli Stati Uniti dove erano oggetto di trattamento.
A tal riguardo è opportuno premettere che i cittadini Europei che desiderano utilizzare *Facebook* sono tenuti, al momento della loro iscrizione, a sottoscrivere un contratto con *Facebook Ireland* che è una società controllata dalla capogruppo americana *Facebook Inc.* Ciò comporta, immediatamente dopo l'iscrizione al *social network*, il trasferimento in tutto o in parte, dei dati personali degli utenti di *Facebook* residenti nel territorio dell'Unione sui *server* di *Facebook Inc*., ubicati nel territorio degli Stati Uniti.
Tenuto conto di quanto suddetto il sig. Schrems, nella propria denuncia, rilevava come il diritto e la prassi vigenti negli Stati Uniti non offrissero una protezione sufficiente dei dati personali conservati nel territorio americano, stante le attività di controllo, ivi costantemente praticate dalle autorità pubbliche. In particolare, il ricorrente si riferiva, con tale assunto, alle rivelazioni fatte dal sig. Edward Snowden in merito alle attività di sorveglianza di massa condotte dai servizi di *intelligence* statunitensi ovvero dalla *National Security Agency* (NSA), nel contesto dello scandalo c.d. *Datagate*.
Il sig. Schrems chiedeva, quindi, al *Data Protection Commissioner*, di esercitare, alla luce delle predette motivazioni, le proprie competenze statutarie, vietando a *Facebook Ireland* di trasferire i dati personali negli Stati Uniti a causa dell'inadeguatezza dell'ordinamento giuridico americano di impedire forme di controllo indiscriminato sui medesimi dati.
La problematica delle c.d. "intercettazioni di massa", era una questione nota già da tempo. Basti pensare che nel 2003 si iniziò a parlare dell'attività di sorveglianza condotta da parte del Governo degli Stati Uniti mediante

l'utilizzo di un sistema d'intercettazione globale per le comunicazioni private ed economiche c.d. *Echelon* [2].
Risale, poi, al 25 luglio del 2010 la notizia che *WikiLeaks* aveva svelato ai quotidiani *New York Times e The Guardian* e al settimanale *Der Spiegel* il contenuto di alcuni documenti riservati dai quali emergevano aspetti nascosti della guerra in Afghanistan.
Infine nel 2013 scoppiava lo scandalo c.d. *Datagate* e venivano divulgate dal sig. Edward Snowden notizie relative all'attività di sorveglianza di massa e di controllo svolte dai servizi di *intelligence* statunitensi, in particolare dalla *National Security Agency* (NSA) [3].
Nonostante le predette argomentazioni, però, il *Data Protection Commissioner* irlandese, respingeva il ricorso. La decisione del garante si basava sostanzialmente sulla seguente considerazione: l'Autorità irlandese non era obbligata a procedere ad un'indagine sui fatti denunciati dal sig. Schrems visto che, da un lato non vi era prova che la *National Security Agency* (NSA) avesse avuto accesso ai dati personali dell'interessato e dall'altro l'adeguatezza del trasferimento dei dati verso gli Stati Uniti era stata già determinata sulla base della decisione n. 2000/520/CE della Commissione Europea.
Le censure formulate dal sig. Schrems, ad opinione del *Data Protection Commissioner*, non potevano, quindi, essere fatte valere in maniera utile, in quanto ogni questione relativa all'adeguatezza della protezione dei dati personali negli Stati Uniti doveva essere comunque risolta in conformità alla decisione n. 2000/520/CE visto che, proprio mediante tale provvedimento, la Commissione Europea, aveva già constatato che gli Stati Uniti d'America assicuravano un livello di protezione adeguato dei dati.
La legittimità del comportamento di *Facebook* era, quindi, garantita dal provvedimento della Commissione Europea ovvero dall'adesione della società americana ai principi di cui all'accordo di c.d. *Safe Harbor* che consentiva di autorizzare automaticamente il trasferimento di dati verso gli stati Uniti, senza bisogno di alcun ulteriore intervento e/o indagine condotta da parte delle Autorità Europee.
In seguito alla suddetta decisione il sig. Schrems impugnava il provvedimento del *Data Protection Commissioner* innanzi alla *High Court of Ireland* che a sua volta, dopo aver esaminato le prove prodotte dalle parti nel procedimento principale, dichiarava che la sorveglianza elettronica e l'intercettazione dei dati personali trasferiti dall'Unione verso gli Stati Uniti rispondevano a finalità necessarie e indispensabili per l'interesse pubblico.
Detto giudice, però, contemporaneamente evidenziava come le rivelazioni del sig. Snowden avessero dimostrato che la *National Security Agency* (NSA) ed altri organi federali americani di fatto accedessero in maniera generalizzata

ai dati personali ubicati sul territorio degli Stati Uniti senza che tali comportamenti fossero in alcun modo giustificati dall'interesse della sicurezza nazionale e/o dalla necessità di reprimere le attività criminali.
La Corte d'appello irlandese osservava, altresì, che la supervisione sull'operato dei servizi di *intelligence* americani veniva, peraltro effettuata, nell'ambito di un procedimento segreto e non contraddittorio.
Quindi, sostanzialmente una volta che i dati personali dei cittadini europei erano trasferiti verso gli Stati Uniti, la *National Security Agency* (NSA) e gli altri organi federali potevano accedervi nell'ambito dello svolgimento delle rispettive attività di sorveglianza, condotte su larga scala senza che alla base di tali attività vi fosse alcuna giustificazione oggettiva.
Ciò, ad opinione dell'organo giudicante, oltre a porsi in contrasto con i principi della costituzione Irlandese, era contrario ai principi stabiliti dalla Carta dei diritti fondamentali dell'Unione Europea ovvero al diritto al rispetto della vita privata, garantito dall'articolo 7, al diritto alla protezione dei dati di carattere personale di cui all'articolo 8 e ai valori fondamentali comuni alle tradizioni degli Stati membri.
Orbene, secondo i giudici dalla *High Court of Ireland*, la stessa decisione n. 2000/520/CE della Commissione europea, consentendo tale prassi si poneva in contrasto con i principi dell'Unione. La questione, quindi, verteva, sull'attuazione del diritto dell'Unione e la stessa legittimità della decisione di cui al procedimento principale doveva essere valutata sulla scorta dei principi di matrice europea.
Tali principi, infatti, si sarebbero svuotati di significato qualora i pubblici poteri americani fossero stati autorizzati ad accedere alle comunicazioni elettroniche su base casuale e generalizzata, senza alcuna giustificazione oggettiva che si fondasse su motivi di sicurezza nazionale o di prevenzione della criminalità, specificamente riguardanti i singoli interessati, ovvero senza garanzie adeguate e verificabili che accompagnassero tali pratiche.
La *High Court of Ireland* osservava, poi, come stesso il sig. Schrems, nel suo ricorso, in realtà avesse proprio contestato la legittimità del regime dell'approdo sicuro istituito dalla decisione 2000/520/CE della Commissione Europea, sulla quale si poggiava, come già accennato, il provvedimento di cui al procedimento principale.
Secondo tale giudice, quindi, era più che mai necessario chiarire se, avuto riguardo all'articolo 25, paragrafo 6, della direttiva 95/46/CE, l'Autorità irlandese fosse stata vincolata dalla constatazione effettuata dalla Commissione Europea nella predetta decisione, oppure se, viceversa l'articolo 8 della Carta autorizzasse la medesima Autorità a discostarsi, se del caso, da una siffatta constatazione.

In tale contesto la *High Court of Ireland*, decise, pertanto, di sospendere il procedimento principale per sottoporre le questioni di cui sopra al vaglio della Corte di Giustizia.
In particolare, le pregiudiziali, oggetto della suddetta domanda, vertevano sull'ambito dei poteri delle autorità nazionali indipendenti di controllo dei dati, istituite *ex* articolo 28 della direttiva 95/46/CE, in rapporto, in particolare, alla decisione n. 2000/520/CE della Commissione Europea, adottata in base all'articolo 25, paragrafo 6, della medesima direttiva. Quindi, sostanzialmente, ci si interrogava sulla validità della decisione 2000/520/CE della Commissione Europea che aveva introdotto il sistema di c.d. "Approdo sicuro".

3. Il quadro normativo dell'Unione Europea.

Prima di procedere con l'esame dei principali passaggi della sentenza adottata dalla Corte di Giustizia, in seguito al rinvio pregiudiziale di cui sopra, occorre soffermarsi preliminarmente sulle disposizioni attualmente vigenti nel quadro normativo europeo in materia di protezione dei dati personali, visto che le stesse costituiscono il presupposto della medesima decisione.
Il principale strumento giuridico dell'Unione Europea in materia di protezione dei dati personali è costituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (direttiva sulla protezione dei dati).
L'art. 1 della direttiva 95/46/CE, stabilisce che «*Gli Stati membri garantiscono, conformemente alle disposizioni della presente direttiva, la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali*». Risulta, poi, sia dall'articolo 1, che dai considerando 2 e 10 della direttiva, che essa è intesa a garantire non solo una tutela efficace e completa delle libertà e dei diritti fondamentali delle persone fisiche, e segnatamente del diritto fondamentale al rispetto della vita privata con riguardo al trattamento dei dati personali, ma anche un livello elevato di protezione di tali libertà e diritti fondamentali.
Ai sensi della medesima direttiva si intende per: «*dati personali*»: *qualsiasi informazione concernente una persona fisica identificata o identificabile (persona interessata); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica,*

culturale o sociale; «trattamento di dati personali» («trattamento»): qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione; «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali. Quando le finalità e i mezzi del trattamento sono determinati da disposizioni legislative o regolamentari nazionali o comunitarie, il responsabile del trattamento o i criteri specifici per la sua designazione possono essere fissati dal diritto nazionale o comunitario (art. 2).

Per quanto concerne, poi, specificamente il trasferimento dei dati verso un paese terzo l'articolo 25 della dir. 46/95/CE prevede un generale divieto di trasferire dati personali al di fuori dell'Unione europea salvo che ciò non avvenga nel rispetto delle circostanze sancite stesso dal medesimo articolo 25 e dal successivo articolo 26.

In particolare l'articolo 25, paragrafo 1, stabilisce che il «*trasferimento verso un paese terzo di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento* [...] *possa aver luogo soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato, fatte salve le misure nazionali di attuazione delle altre disposizioni della presente direttiva*». Il paragrafo 2 recita, inoltre, che: «*l'adeguatezza del livello di protezione garantito da un paese terzo è valutata con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati; in particolare sono presi in considerazione la natura dei dati, le finalità del o dei trattamenti previsti, il paese d'origine e il paese di destinazione finale, le norme di diritto, generali o settoriali, vigenti nel paese terzo di cui trattasi, nonché le regole professionali e le misure di sicurezza ivi osservate*».

La normativa europea, quindi, sostanzialmente non consente il trattamento dei dati dei cittadini europei da parte di aziende che operano sotto la giurisdizione di paesi con norme non equivalenti (cioè con tutela inferiore per i diritti dei cittadini) a quelle europee.

Il trasferimento, verso un paese terzo, di dati personali oggetto di un trattamento, è consentito, infatti, solo se è stata preventivamente accertata l'adeguatezza della protezione dei medesimi dati presso il destinatario (art. 25). Il concetto di adeguatezza sta a significare che i principi fondamentali

dell'Unione Europea in materia di protezione dei dati sono stati effettivamente introdotti nel diritto nazionale di detto paese.
A norma sempre dell'articolo 25, paragrafo 6, della direttiva, la Commissione Europea è l'organo competente a svolgere la valutazione del livello di protezione dei dati in paesi stranieri e la stessa si esprime sul punto mediante l'adozione di decisioni di adeguatezza che si basano, altresì, sulle consultazioni condotte con il Gruppo di lavoro *ex* articolo 29 per la protezione dei dati [4].
Le decisioni di adeguatezza, adottate in seguito al predetto *iter*, sono vincolanti. Quindi se la Commissione Europea pubblica una decisione di adeguatezza per un determinato paese sulla Gazzetta ufficiale dell'Unione europea, tutti gli Stati membri ed i relativi organismi sono tenuti ad ottemperare alla decisione e ciò comporta che i dati personali oggetto del trasferimento possono circolare verso il paese terzo senza ulteriori procedure di verifica e/o di autorizzazione presso le autorità nazionali.
Talvolta le decisioni di adeguatezza adottate dalla Commissione Europea per i trasferimenti dei dati verso paesi terzi si basano su veri e propri accordi conclusi fra l'Unione europea e gli Stati stranieri. Una prassi più recente nel trasferimento di dati basata su accordi speciali fra l'Unione Europea ed i paesi terzi evidenzia, inoltre, come l'esigenza di decisioni di adeguatezza venga meno proprio in presenza di specifici accordi conclusi con i paesi terzi, presumendosi che l'accordo stesso offra un adeguato livello di protezione dei dati.
Il trasferimento di dati personali oggetto di un trattamento verso un paese terzo che, contrariamente a quanto disposto nell'articolo 25, paragrafo 2, non garantisce un livello di tutela adeguato dei dati, può, poi, essere consentito solo laddove ciò risulti necessario per interessi specifici dell'interessato o per prevalenti interessi legittimi altrui, in particolare per interessi pubblici rilevanti (art. 26, comma 1).
Gli interessi dell'interessato possono giustificare la libera circolazione dei dati se è soddisfatta almeno una delle seguenti condizioni: l'interessato ha espresso il proprio consenso inequivocabile al trasferimento dei dati; l'interessato ha stipulato – o si accinge a stipulare – un contratto che richieda chiaramente il trasferimento dei dati verso un destinatario all'estero; è stato concluso un contratto fra il titolare del trattamento e un terzo nell'interesse dell'interessato; il trasferimento è necessario per la salvaguardia dell'interesse vitale dell'interessato; il trasferimento avviene a partire da un registro pubblico, ossia si è in presenza di un caso di interessi prevalenti della popolazione in generale che consiste nel fatto di poter accedere a informazioni conservate in registri pubblici.

Gli interessi legittimi altrui, invece, possono ugualmente giustificare la libera circolazione transfrontaliera dei dati se ciò è necessario: per la salvaguardia di un interesse pubblico rilevante, diverso dalla sicurezza nazionale o pubblica, dato che questi settori non sono coperti dalla direttiva sulla tutela dei dati; oppure per rivendicare, esercitare o difendere un diritto per via giudiziaria.
Merita sottolineare, però, come i casi succitati debbano sempre essere intesi come delle deroghe, da interpretate in senso restrittivo, alla regola generale secondo la quale il libero trasferimento di dati verso paesi terzi richiede sempre e comunque una valutazione circa l'adeguatezza del livello di protezione dei medesimi dati nel paese destinatario.
L'articolo 26, comma 2, della dir. 46/95/CE, prevede, poi, anche un'altra ipotesi di trasferimento dei dati verso paesi terzi, in deroga al suddetto divieto, di cui all'articolo 25. In particolare, in questa circostanza, è consentito il trasferimento dei dati verso paesi terzi che non posseggono nel proprio ordinamento giuridico principi simili a quelli di matrice europea in materia di protezione dei dati, purché ciò avvenga sulla base dell'utilizzo di strumenti contrattuali in grado di sopperire a tale mancanza offrendo garanzie adeguate [5].
Ciò significa che prima di trasferire i dati verso paesi terzi che non garantiscono un adeguato livello di protezione, il titolare del trattamento può essere tenuto a sottoporre il flusso dei dati all'esame delle autorità di controllo che a loro volta sono tenute in primo luogo a valutare l'esistenza di una base giuridica per il trasferimento di tali dati verso il destinatario e, poi, ad accertare la presenza di misure atte a garantire un'adeguata tutela dei dati presso il destinatario.
Sul punto può intervenire anche la Commissione Europea, che, ai sensi dell'articolo 26 comma 4, è competente ad adottare decisioni nelle quali può stabilire che determinati strumenti contrattuali consentono di trasferire dati personali verso paesi terzi [6].
Al fine di garantire una completa attuazione dei principi di cui sopra l'articolo 28, della direttiva 95/46/CE obbliga gli Stati membri ad istituire una o più autorità pubbliche incaricate di controllare in piena indipendenza l'osservanza delle norme dell'Unione relative alla tutela delle persone fisiche con riguardo al trattamento dei dati personali. Detto obbligo risulta altresì dal diritto primario dell'Unione, segnatamente dall'articolo 8, paragrafo 3, della Carta e dall'articolo 16, paragrafo 2, del TFUE.
Le autorità di controllo, secondo quanto previsto nella direttiva, dispongono, inoltre, di poteri investigativi, di poteri effettivi d'intervento, del potere di promuovere azioni giudiziarie in caso di violazione delle disposizioni nazionali di attuazione della presente direttiva ovvero di adire per dette

violazioni le autorità giudiziarie. Qualsiasi persona può, poi, chiedere ad un'autorità di controllo di verificare la liceità di un trattamento quando si applicano le disposizioni nazionali adottate a norma dell'articolo 13 della presente direttiva [7].

3.1 La decisione della Commissione europea n. 2000/520/CE sul c.d. "Approdo sicuro".

Tra le decisioni di adeguatezza, adottate dalla Commissione Europea, sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46/CE, la più nota è quella del 26 luglio del 2000, che non riguarda in realtà un insieme di disposizioni giuridiche, ma norme molto simili ad un codice di condotta note come principi di approdo sicuro in materia di riservatezza (c.d. principi di *Safe Harbor*).
Più specificamente la suddetta decisione era un provvedimento con cui la Commissione Europea aveva accertato l'adeguatezza della protezione dei dati offerta dai principi del c.d. *Safe Harbor* ("approdo sicuro"), quale condizione per il trasferimento di dati personali dall'Unione Europea verso gli Stati Uniti.
Il c.d. *Safe Harbor* altro non era che un vero e proprio accordo fra gli Stati Uniti e l'Unione Europea in base al quale le aziende americane che volevano trattare dati dei cittadini europei dichiaravano di rispettare *standard* di tutela equivalenti a quelli europei. Tali principi erano stati, infatti, messi a punto proprio al fine di garantire alle imprese commerciali statunitensi la possibilità di trasferire liberamente oltre oceano i dati personali dei cittadini europei.
Per il trasferimento di dati dall'Unione Europea agli Stati Uniti, quindi, il livello di adeguatezza era raggiunto, laddove le imprese si fossero conformate ai "principi dell'approdo sicuro in materia di riservatezza" (*The Safe Harbor Privacy Principles*), nonché alle "domande più frequenti" (*Frequently Asked Questions*), pubblicate dal governo degli Stati Uniti in data 21 luglio 2000, che fornivano indicazioni per l'attuazione dei principi stessi.
La conformità ai predetti principi veniva acquisita mediante un impegno volontario, che l'impresa assumeva tramite una dichiarazione rilasciata dinanzi al dipartimento per il Commercio statunitense, il quale documentava, poi la predetta dichiarazione in un elenco pubblicato dallo stesso dipartimento. Poiché uno degli elementi più importanti dell'adeguatezza è dato dall'effettiva attuazione della tutela dei dati, l'accordo sull'approdo sicuro prevedeva anche un certo livello di supervisione statale: potevano aderire ai principi di approdo sicuro solo le imprese soggette alla vigilanza della Commissione federale per il commercio degli Stati Uniti. Una volta che l'impresa aderiva al programma, doveva, poi, rinnovare la certificazione ogni

12 mesi al fine di ottenere e mantenere i vantaggi risultanti dall'approdo sicuro.
E' opportuno evidenziare che la maggior parte dei principi stabiliti nel programma *Safe Harbor* rispecchiava pedissequamente quanto statuito nella direttiva europea in materia di protezione dei dati personali [8].
L'adesione ai suddetti principi, però, poteva subire delle limitazioni se ciò si fosse reso necessario per soddisfare esigenze di sicurezza nazionale, interessi pubblici o esigenze di amministrazione della giustizia. Ulteriori limitazioni potevano, poi, derivare, altresì, dalle disposizioni legislative o regolamentari ovvero da decisioni giurisdizionali qualora tali fonti avessero comportato obblighi contrastanti. Più nel dettaglio il venir meno dell'obbligo di rispettare i principi dell'approdo sicuro poteva, parimenti essere dovuto, all'adozione da parte del Governo americano, di autorizzazioni esplicite, purché, l'impresa beneficiaria, nell'avvalersi di un'autorizzazione siffatta, fosse stata in grado di dimostrare che, il mancato rispetto dei principi da parte sua, si sarebbe limitato a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione.

3.1.1. Il Quadro normativo Italiano.

Occorre preliminarmente accennare anche alle principali disposizioni vigenti in Italia in materia di protezione dei dati personali, così da poter cogliere a pieno i mutamenti e l'evoluzione della medesima disciplina in seguito all'adeguamento con i principi contenuti nel provvedimento giurisdizionale oggetto del presente commento.
In Italia è stata data attuazione alla direttiva 95/46/CE mediante la c.d. legge sulla privacy (legge n. 675/1996) che ha istituito, inoltre, il Garante per la protezione dei dati personali. Oggi tale disciplina si trova racchiusa nel Codice in materia di protezione dei dati personali di cui al D.lgs. n. 196/2003.
L'Autorità Garante italiana, in seguito alla decisione della Commissione Europea n. 2000/520/CE, considerato che gli Stati membri europei sono tenuti ad adottare le misure necessarie per conformarsi alle decisioni della Commissione, al fine di allinearsi con quanto previsto a livello comunitario, aveva a sua volta autorizzato i trasferimenti di dati personali dal territorio italiano verso organizzazioni aventi sede negli Stati Uniti.
Tale autorizzazione si basava essenzialmente sul fatto che i trasferimenti dei dati personali fossero stati eseguiti nel rispetto di quanto stabilito dalla Commissione Europea ovvero nel rispetto dei "Principi di approdo sicuro in materia di riservatezza" applicati in conformità alle "Domande più frequenti"

e all'ulteriore documentazione allegata alla decisione della Commissione europea sul regime di "Approdo sicuro" [9].
Il Garante si riserva, però di svolgere, in conformità alla normativa comunitaria, alla legge n. 675/1996, all'art. 3 della Decisione della Commissione e all'allegata FAQ. n. 5, i necessari controlli sulla liceità e correttezza dei trasferimenti e delle operazioni di trattamento anteriori ai trasferimenti medesimi, nonché sul rispetto dei predetti Principi.
Lo strumento del *Safe Harbor* consentiva, quindi, a moltissime aziende con sede negli Stati Uniti ed operanti anche nell'Unione europea ed in Italia, in particolare, di procedere al trasferimento dei dati sulla base di una semplice autocertificazione così come prevista dall'accordo siglato tra l'Unione Europea e gli Stati Uniti.

4. La sentenza della Corte di Giustizia: il potere delle autorità garanti nazionali di controllare il rispetto dei requisiti posti dalla direttiva 95/46 in materia di trasferimenti transfrontalieri di dati.

Stante le questioni pregiudiziali, sottoposte al vaglio della Corte di Giustizia dell'Unione Europea ed il quadro normativo vigente in materia di protezione dei dati, occorre ora procedere con l'esame della ricostruzione della vicenda così come compiuta dai Giudici di Lussemburgo.
Con la sentenza pronunciata il 06.10.2015, nella causa C-362/14, la Grande Sezione della Corte di Giustizia dell'Unione europea ha preliminarmente sancito che, anche in presenza di una decisione della Commissione Europea che dichiari che un paese terzo garantisce un livello di protezione adeguato dei dati personali trasferiti, tale circostanza non può sopprimere e neppure ridurre i poteri di cui dispongono le autorità nazionali di controllo in forza della Carta dei diritti fondamentali dell'Unione europea e della direttiva 46/95/CE.
In particolare i Giudici di Lussemburgo sono giunti a tale conclusione valorizzando i poteri e l'indipendenza delle autorità garanti nazionali seguendo, altresì, su tale scia le conclusioni dell'avvocato generale Bot.
Per prima cosa, i Giudici, hanno reputato opportuno stabilire se le autorità garanti nazionali avevano il potere di controllare che il trasferimento dei dati personali dall'Unione Europea verso gli Stati terzi garantisse un adeguato livello di tutela degli stessi, e, poi, in un secondo momento, sono passati ad accertare se le medesime autorità disponessero di tale potere anche nel caso in cui la Commissione europea, in virtù del paragrafo 6 dell'articolo 25 della direttiva 95/46/CE, avesse adottato sul punto una decisione di adeguatezza autorizzando il trasferimento dei dati personali verso quest'ultimo sistema giuridico (punti 50-66).

A fondamento della sussistenza dei poteri delle autorità garanti nazionali, i giudici di Lussemburgo, richiamavano, come accennato precedentemente, il diritto alla protezione dei dati personali garantito dalla Carta dei diritti fondamentali dell'Unione europea e la missione di cui sono investite le autorità nazionali di controllo in forza della Carta medesima e della dir. 46/95/CE. Le autorità nazionali di controllo, alla luce delle predette disposizioni, sono, infatti, incaricate di sorvegliare il rispetto delle norme dell'Unione relative alla tutela delle persone fisiche con riguardo al trattamento dei dati personali.
Ad opinione delle Corte, poi, nessuna disposizione della direttiva 46/95/CE ostava, a che le autorità nazionali controllassero i trasferimenti di dati personali verso paesi terzi anche laddove tali trasferimenti fossero stati oggetto di una precedente decisione della Commissione Europea.
Ad avvalorare tale assunto la Corte, evidenziava, altresì, che «*se così non fosse, le persone i cui dati personali sono stati o potrebbero essere trasferiti verso il paese terzo di cui trattasi sarebbero private del diritto, garantito all'articolo 8, paragrafi 1 e 3, della Carta, di investire le autorità nazionali di controllo di una domanda ai fini della protezione dei loro diritti fondamentali*» [10].
Pertanto, rimarcavano i Giudici, pur in presenza di una decisione di adeguatezza della Commissione Europea le autorità nazionali, investite di un ricorso da parte di un cittadino, dovevano comunque poter esaminare in piena indipendenza se un trasferimento di dati personali verso un paese terzo rispetti i requisiti sanciti dalla direttiva ovvero previsti dalla normativa dell'Unione.
I Giudici, poi, soffermandosi sull'articolo 3, paragrafo 1, della decisione n. 2000/520/CE della Commissione Europea rilevavano che se era vero che tale disposizione faceva salvo il potere delle autorità di controllo di porre in essere attività che garantissero il rispetto delle normative nazionali adottate in base alla direttiva 46/95/CE, era parimenti vero che la predetta disposizione di fatto escludesse la possibilità di siffatte autorità di assicurare l'osservanza dell'articolo 25 della direttiva medesima.
Stante quanto suddetto la Corte sosteneva che, la Commissione Europea, per il tramite dell'articolo 3 della decisione n. 2000/520/CE, aveva, dunque, ecceduto i poteri che le erano stati conferiti ai sensi dell'articolo 25 della direttiva 46/95/CE, visto che tale articolo non le attribuiva la competenza di limitare i poteri delle autorità nazionali di controllo (punti 99-104 della sentenza).
Nella medesima circostanza, la Corte coglieva, altresì, l'occasione di precisare che solo lei stessa è competente a dichiarare invalida una decisione della Commissione Europea, così come qualsiasi altro atto dell'Unione.

Pertanto, qualora un'autorità nazionale o un individuo avesse reputato invalida una decisione della Commissione, sarebbe stato necessario rivolgersi ai giudici nazionali affinché, nel caso in cui anche questi ultimi avessero nutrito dubbi sulla validità della decisione della Commissione, essi stessi potessero con un rinvio pregiudiziale rimettere l'esame della validità della decisione alla Corte di Giustizia.
Dunque, in ultima analisi, la Corte sottolineava l'importanza della propria funzione che si esplicava non solo sotto forma di organo deputato a garantire la corretta ed uniforme interpretazione del diritto dell'Unione ma anche quale autorità competente a determinare la validità degli atti adottati ai sensi del diritto dell'Unione dalle sue istituzioni.

4.1. La sentenza della Corte di Giustizia: L'invalidità della decisione sul c.d. "Approdo sicuro".

Sebbene il rinvio pregiudiziale effettuato dalla Corte irlandese fosse volto principalmente ad ottenere l'interpretazione di talune norme della direttiva 95/46/CE, i giudici di Lussemburgo, invocando la necessità di fornire una risposta completa alla giurisdizione di rinvio, hanno scelto di spingersi oltre il quesito pregiudiziale, accertando anche la validità della decisione "Approdo sicuro".
La Corte, infatti, dopo le questioni precedentemente esaminate passava a verificare la validità della decisione della Commissione europea sul *Safe Harbor* analizzando, in particolare, le modalità mediante le quali la Commissione Europea era giunta ad adottare la medesima decisione con cui aveva, peraltro, accertato l'effettiva adeguatezza della protezione garantita ai dati personali trasferiti negli Stati Uniti. In tale contesto, i giudici di Lussemburgo sottoponevano a critica il provvedimento della Commissione per una serie di ragioni che verranno di seguito esposte.
In primo luogo, i Giudici ritenevano che la Commissione Europea fosse tenuta a constatare effettivamente che gli Stati Uniti garantissero, in considerazione della loro legislazione nazionale o dei loro impegni internazionali, un livello di protezione dei diritti fondamentali, sostanzialmente equivalente a quello garantito nell'Unione Europea a norma della direttiva, interpretata alla luce della Carta dei Diritti Fondamentali dell'Unione europea.
In seguito alle suddette considerazioni emergeva che la Commissione Europea nel compiere le valutazioni di cui sopra, non aveva proceduto ad una constatazione del genere, limitandosi, invece, al contrario ad esaminare in cosa consistesse il regime del c.d. "approdo sicuro".
La Corte di Giustizia rilevava, poi, che il sistema del *Safe Harbor* era applicabile esclusivamente alle imprese americane che lo sottoscrivevano,

mentre le autorità pubbliche degli Stati Uniti non vi erano in alcun modo assoggettate [11].
Le imprese americane, inoltre, in base alla Decisione *de qua* erano di fatto tenute a disapplicare, senza limiti, i principi dell'approdo sicuro laddove tali norme di tutela fossero entrate in conflitto con le esigenze di sicurezza nazionale, ovvero con degli interessi pubblici rilevanti. Il regime americano del *Safe Harbor*, finiva, quindi, ad opinione dei Giudici, per rendere in questo modo possibili delle ingerenze notevoli da parte delle autorità pubbliche americane nei diritti fondamentali delle persone.
Nonostante ciò, rilevava Corte di Giustizia, la decisione adottata dalla Commissione europea, non faceva alcuna menzione dell'esistenza, negli Stati Uniti, di norme intese a limitare queste eventuali ingerenze, né tanto più dell'esistenza, sempre negli Stati Uniti, di una tutela giuridica efficace contro tali possibili ingerenze.
Ad opinione della Corte la suddetta prassi, sarebbe stata tutt'al più giustificata, solo in presenza di regole chiare e precise in grado di disciplinare la portata e l'applicazione della misura *de qua* imponendo anche dei requisiti minimi di modo che le persone, i cui dati personali erano oggetto di trattamento, potessero disporre di garanzie sufficienti contro il rischio di abusi nonché contro eventuali accessi e usi illeciti dei suddetti dati. La protezione del diritto fondamentale al rispetto della vita privata a livello dell'Unione richiedeva, infatti, che le deroghe e le restrizioni alla tutela dei dati personali operassero solo ed esclusivamente entro i limiti dello stretto necessario [12].
Ebbene, stante quanto suddetto, una normativa che autorizzava in maniera generalizzata la conservazione di tutti i dati personali di tutte le persone i cui dati erano trasferiti dall'Unione verso gli Stati Uniti senza operare alcuna differenziazione, limitazione o eccezione in funzione dell'obiettivo perseguito e senza che fossero stati preventivamente fissati criteri oggettivi intesi a circoscrivere l'accesso delle autorità pubbliche ai dati e la loro successiva utilizzazione si poneva in contrasto con la protezione del diritto fondamentale al rispetto della vita privata.
Parimenti una normativa che non prevedeva alcuna facoltà per il singolo di esperire rimedi giuridici per accedere ai dati personali che lo riguardavano o ad ottenerne la rettifica o la cancellazione violava il contenuto essenziale del diritto fondamentale ad una tutela giurisdizionale effettiva. Tale facoltà, osservavano sempre i Giudici, è connaturata all'esistenza di uno Stato di diritto.
Merita rilevare, inoltre, come, nelle propria ricostruzione di cui sopra, la Corte abbia tenuto in considerazione anche le due comunicazioni che la Commissione Europea aveva adottato sul punto nel corso del 2013 [13]. Da

tali provvedimenti si evinceva, segnatamente, che le autorità degli Stati Uniti potevano accedere ai dati personali trasferiti dagli Stati membri verso tale paese e trattarli in modo incompatibile, in particolare, con le finalità del loro trasferimento, effettuando un trattamento in eccesso rispetto a ciò che era strettamente necessario e proporzionato alla tutela della sicurezza nazionale.
Analogamente, sempre la Commissione Europea, aveva, nella medesima circostanza, dichiarato che i soggetti interessati, di fatto non disponevano dei rimedi amministrativi o giurisdizionali intesi a garantire l'accesso ai dati che gli riguardavano e, se necessario, ad ottenerne la rettifica o la cancellazione.
Dal momento che nella Decisione n. 2000/520/CE la Commissione Europea non aveva stabilito che gli Stati Uniti, in considerazione della loro legislazione nazionale o dei propri impegni internazionali, garantissero effettivamente una adeguata tutela dei dati, i Giudici, dunque, rilevavano, l'incompatibilità dell'articolo 1 di detta decisione con i requisiti richiesti dall'all'articolo 25, paragrafo 6, della direttiva 46/95/CE.
In seguito alle risultanze di causa la Corte, quindi, dichiarava, l'invalidità della decisione della Commissione Europea del 26 luglio del 2000.

5. Conseguenze della pronuncia della Corte di Giustizia.

La suddetta pronuncia ha comportato come principale conseguenza quella di rimettere l'esame della denuncia del sig. Schrems dinanzi all'autorità irlandese di controllo la quale risulta tenuta a svolgere, pertanto, le rispettive indagini con tutta la diligenza necessaria e solo dopo ciò la medesima autorità sarà, parimenti tenuta ad adottare una decisione sul punto.
La pronuncia della Corte di Giustizia presenta, però ulteriori aspetti di particolare rilevanza tra cui in *primis* il fatto che tale provvedimento servirà sicuramente come stimolo ad una più attenta disciplina verso il trattamento dei dati dei cittadini europei trasferiti negli Stati Uniti, pur non costituendo, tuttavia la base giuridica per ritenere aprioristicamente invalidi i trasferimenti di dati personali verso i *server* statunitensi.
Merita, infatti, sottolineare come la predetta pronuncia non determini né il blocco automatico di tutti i trasferimenti di dati personali dall'Unione europea agli Stati Uniti né tanto meno il sopraggiungere di un obbligo in capo alle imprese operanti negli Stati Uniti di trasferire i propri *server* nell'Unione europea.
Piuttosto, prima di trasferire i dati verso gli Stati Uniti, il titolare del trattamento, potrà essere tenuto a sottoporre il flusso di dati in questione all'esame delle autorità di controllo, avendo la decisione della Corte, fornito

alle autorità garanti il potere di verificare se il trasferimento di dati personali degli utenti tra nazioni è sicuro.
Le autorità garanti nazionali potranno, quindi, adottare i provvedimenti necessari laddove dovessero ritenere che i trasferimenti di dati verso gli Stati Uniti non rispettino la normativa sulla *privacy*.
L'innovatività di questo *dictum* risiede, infatti, non tanto e non solo nella enunciazione dei poteri conferiti alle autorità di controllo dei dati quanto piuttosto nella loro estensione ai casi di trasferimenti dei dati dall'Unione europea agli Stati terzi. In tal modo, la Corte di Giustizia mostra una particolare sensibilità verso la tutela della *privacy* degli individui coinvolti e conseguentemente una decisa volontà di riconoscere tutele equivalenti dei dati personali trattati in Europa con quelli che vengono, invece, trasferiti in uno Stato terzo.
La sentenza in commento contribuisce, quindi, da un certo punto di vista, all'articolazione dei poteri tra le autorità pubbliche, nazionali ed europee, nel contesto dell'attuazione delle previsioni contenute nella direttiva 94/46/CE. In particolare, tale pronunciamento, eliminando il monopolio esclusivo della Commissione europea in relazione alla valutazione dell'adeguatezza del livello di protezione dei dati offerto dai Paesi terzi, finisce per riconoscere, in tale ambito, un importante potere discrezionale alle autorità di controllo.
Ci si chiede, però, se ciò possa contribuire a determinare contemporaneamente anche delle complicazioni dovute alla nascita di un mosaico di decisioni potenzialmente contradditorie adottate da parte delle autorità garanti nazionali [14]. L'eccessivo spezzettamento tra 28 garanti suscita, infatti, non poche perplessità tra cui in primo luogo il fatto che le imprese, stante quanto suddetto, saranno tenute a verificare i contratti in essere con le proprie controparti statunitensi per renderli conformi alla pronuncia della Corte.

5.1. La posizione del Garante italiano in merito alla pronuncia della Corte di Giustizia.

In considerazione della suddetta pronuncia anche l'autorità Garante italiana per la protezione dei dati personali ha deciso di prendere posizione sulla vicenda del trasferimento dei dati dall'Europa agli Stati Uniti, disponendo, pertanto la decadenza dell'autorizzazione precedentemente adottata [15].
Più specificamente con il suddetto provvedimento il Garante ha determinato la caducazione della delibera n. 36 del 10 ottobre 2001, vietando, altresì, ai sensi degli artt. 154, comma 1, lett. d) e 45 del Codice, ai soggetti esportatori di trasferire, sulla base di tale delibera e dei presupposti indicati

nella medesima, i dati personali dal territorio dello Stato verso gli Stati Uniti d'America.
Venendo meno la decisione della Commissione Europea sul c.d. regime di *Safe Harbor*, veniva meno, contemporaneamente, anche il presupposto di legittimità dei trasferimenti di dati personali posti in essere dal territorio nazionale verso le organizzazioni aventi sede negli Stati Uniti d'America.
Merita osservare, però, come il provvedimento del Garante sia stato adottato alla luce della importante considerazione secondo cui i trasferimenti dei dati personali verso un paese non appartenente all'Unione europea possono comunque essere effettuati sulla base di ulteriori presupposti di liceità, così come previsto negli artt. 43 ("Trasferimenti consentiti in Paesi terzi") e 44 ("Altri trasferimenti consentiti") del Codice Privacy.
Tali articoli, altro non sono, poi, che la trasposizione a livello nazionale dei principi sanciti nella direttiva 95/46/CE.
Impedire il flusso dei dati oltre oceano determinerebbe, infatti, non solo la paralisi per molte imprese, quanto piuttosto anche un potenziale isolamento commerciale per l'Europa.
Il Garante nella predetta deliberazione ha tenuto, altresì, conto delle osservazioni formulate dal Gruppo di lavoro istituito dall'art. 29 della direttiva 95/46/CE, nello «*Statement of the Article 29 Working Party*» del 16 ottobre 2015 [16], in merito agli effetti della sentenza della Corte di giustizia sui trasferimenti dei dati effettuati, in virtù della decisione della Commissione europea del 26 luglio 2000 n. 2000/520/CE, dal territorio dell'Unione europea verso gli Stati Uniti d'America.

5.2. Le linee guida adottate dalla Commissione Europea in seguito alla pronuncia della Corte di Giustizia.

Ad un mese esatto dall'adozione della sentenza della Corte, stante il venir meno dell'autorizzazione generale, di cui alla decisione n. 2000/520/CE, la Commissione europea ha ritenuto opportuno pubblicare delle linee guida in materia di trasferimento dei dati personali dei cittadini europei negli Stati Uniti, al fine di fare chiarezza sul regime di migrazione dei dati oltre oceano [17].
Nella predetta comunicazione la Commissione ha esordito precisando che l'accordo sull'approdo sicuro non può più costituire la base giuridica per i trasferimenti dei dati personali negli Stati Uniti ed a fronte della sua invalidazione il trasferimento dei dati personali verso il territorio americano può in ogni caso avvenire sulla base dell'utilizzo di strumenti giuridici alternativi. Nella comunicazione che ha accompagnato la presentazione delle linee guida la Commissione ha affermato, infatti, che le aziende dovranno

"*conformarsi alla sentenza e avvalersi di eventuali strumenti alternativi per il trasferimento dei dati*".
Nelle linee guida la Commissione ribadisce, inoltre, che troveranno applicazione le regole generali in materia di trasferimento transfrontaliero dei dati, di cui alla dir. 95/46/CE, che si basano sulla chiara distinzione tra, i trasferimenti di dati verso paesi terzi che garantiscono un adeguato livello di tutela (art. 25) e i trasferimenti dei dati verso paesi terzi che non garantiscono, viceversa, un adeguato livello di protezione dei medesimi dati (art. 26).
In particolare il trasferimento transfrontaliero dei dati, laddove gli stessi siano diretti verso paesi terzi che non garantiscono un livello di protezione adeguato, ai sensi dell'articolo 25, paragrafo 2, potrà essere comunque effettuato da parte delle imprese che si avvalgono, nello svolgimento di tali attività, dei seguenti strumenti giuridici alternativi: clausole contrattuali *standard* e *Binding Corporate Rules.*
Per quanto concerne la prima ipotesi, le clausole contrattuali *standard*, possono essere inserite nei contratti che coinvolgono imprese che non appartengono al medesimo gruppo societario e, tali clausole, devono prevedere specifici obblighi, quali ad esempio, misure di sicurezza, informazione dell'interessato, misure di salvaguardia nel caso del trasferimento di dati sensibili e così via. Le medesime clausole, essendo incorporate in un contratto utilizzato per il trasferimento dei dati, garantiscono all'esportatore di compensare, in questo modo, l'assenza, nell'ordinamento giuridico destinatario dei dati, di una normativa equivalente a quella Europea, assicurando, parimenti che il trattamento dei dati avvenga in modo conforme ai principi stabiliti nella direttiva 95/46/CE.
Merita rilevare, inoltre, come il diritto dell'Unione Europea, anche prima del suddetto intervento della Commissione Europea, citasse esplicitamente le clausole contrattuali stipulate fra il titolare del trattamento che trasferisce i dati e il destinatario nel paese terzo come possibile mezzo per garantire un livello sufficiente di protezione dei dati presso il destinatario.
A livello Europeo, infatti, proprio la Commissione Europea, con l'ausilio del Gruppo di lavoro *ex* art. 29, aveva già elaborato, precedentemente rispetto all'intervento i discussione, apposite clausole contrattuali ufficialmente certificate mediante una sua decisione. Tali clausole riguardavano, in particolare i trasferimenti da un titolare del trattamento ad un altro titolare del trattamento [18] e i trasferimenti da titolare del trattamento a responsabile del trattamento [19]. Più specificamente nella prima ipotesi di cui sopra, il titolare del trattamento ha a disposizione la possibilità di scegliere tra due set differenti di clausole tipo, mentre, invece, nella seconda

circostanza esiste un unico set di clausole contrattuali tipo da poter utilizzare [20].
Nelle linee guida che la Commissione Europea ha adottato in seguito alla pronuncia della Corte di Giustizia, la stessa, richiama esplicitamente proprio tali set di clausole *standard*.
Occorre, poi, sottolineare che, poiché le decisioni della Commissione Europea, come ribadito più volte nel corso della presente trattazione, sono vincolanti in ogni loro parte negli Stati membri, le autorità nazionali di controllo dei flussi transfrontalieri di dati devono riconoscere la validità di tali clausole contrattuali tipo nei propri procedimenti. Pertanto, se il titolare del trattamento che trasferisce i dati e il destinatario nel paese terzo concordano e sottoscrivono tali clausole, l'autorità di controllo dovrebbe avere già a disposizione una prova sufficiente dell'esistenza di garanzie adeguate.
L'esistenza di modelli *standard* di clausole contrattuali nel quadro giuridico dell'Unione Europea non vieta, però, ai titolari del trattamento di formulare anche altre clausole contrattuali ad *hoc* purché le stesse garantiscano il medesimo livello di tutela offerto dalle clausole contrattuali tipo [21]. Ovviamente, precisa la Commissione Europea, in questo caso tali clausole dovranno essere sottoposte al vaglio preventivo dell'autorità nazionale di controllo (art. 26, comma 2, dir. 95/46/CE).
Altro strumento, menzionato dalla Commissione Europea, nelle suddette linee guida per il trasferimento di dati personali dal territorio dello Stato verso Paesi terzi, è quello delle *Binding Corporate Rules* ovvero delle norme di condotta vincolanti per i trasferimenti di dati all'interno dello stesso gruppo societario di imprese. Le norme vincolanti d'impresa si concretizzano sostanzialmente in un documento contenente una serie di clausole (*rules*) che fissano i principi vincolanti (*binding*) al cui rispetto sono tenute tutte le società appartenenti ad uno stesso gruppo (*corporate*). Le *Binding Corporate Rules* costituiscono, quindi, un meccanismo in grado di semplificare gli oneri amministrativi a carico delle società di carattere multinazionale con riferimento ai flussi intra-gruppo dei dati personali.
Merita rilevare, però, che le norme vincolanti d'impresa traggono la loro efficacia da una preventiva autorizzazione rilasciata dalle autorità di protezione dei dati in ciascuno Stato membro da cui la multinazionale intende trasferire i dati.
Molto spesso, le predette *Binding Corporate Rules* finiscono, quindi, per coinvolgere contemporaneamente diverse autorità di controllo europee ed affinché siano approvate è richiesto il rispetto di una serie di passaggi.
In particolare come primo *step* del procedimento volto alla approvazione delle norme vincolanti d'impresa, il progetto relativo alle stesse, dev'essere

trasmesso unitamente ai moduli di domanda standardizzati all'autorità capofila. Quest'ultima è tenuta, poi, ad informare, in un secondo momento, tutte le altre autorità di controllo in cui sono stabilite le affiliate del gruppo, sebbene la loro partecipazione al processo di valutazione delle norme sia facoltativa. Pur non essendo obbligatorio, tutte le autorità di controllo interessate dovrebbero, poi, inserire i risultati della valutazione condotta sulle norme nelle proprie procedure formali di autorizzazione. Ovviamente, stante quanto suddetto, quante più filiali ha il gruppo che intende trasferire i dati tante più saranno le autorità nazioni di controllo a dover essere coinvolte nel predetto procedimento.
Per quanto riguarda il contenuto delle norme vincolanti d'impresa, il testo generalmente riprende i principi fondamentali in materia di protezione dei dati personali, di cui alla dir. 95/46/CE. Più specificamente viene fatto riferimento: ai principi di correttezza e legittimità del trattamento, di finalità, necessità e proporzionalità dei dati, all'obbligo del titolare di rilasciare idonea informativa all'interessato, ai diritti dell'interessato, alle misure di sicurezza prescritte dalla legge, al diritto dell'interessato ad ottenere il risarcimento del danno connesso al mancato rispetto delle norme vincolanti d'impresa da parte di una delle società del gruppo (c.d. clausola del terzo beneficiario).
Il gruppo multinazionale che usufruisce delle norme vincolanti d'impresa deve, inoltre, essere in grado di garantire tutta una serie di circostanze accessorie ovvero: la predisposizione di un programma di *training* del personale in materia di protezione dei dati personali, l'implementazione di un meccanismo di gestione del contenzioso e delle segnalazioni connesse alle medesime norme vincolanti d'impresa, la conduzione periodica di *audit* al fine di verificare il rispetto delle regole da parte delle società del gruppo, la creazione di un *network* di *privacy officers* o di uno *staff* che si occupi di monitorare il rispetto delle norme e di gestire le segnalazioni degli interessati.
Va rilevato, inoltre, che gli orientamenti adottati dalla Commissione Europea al fine di fare chiarezza sul regime di trasferimento transfrontaliero dei dati, prevedono anche delle deroghe al regime suddetto. Tali eccezioni consistono sostanzialmente nelle medesime deroghe di cui all'articolo 26 comma 1 della direttiva 95/46/CE. In particolare, viene fatto esplicito riferimento alla possibilità, attribuita alle imprese, di non avvalersi degli strumenti giuridici alternativi per il trasferimento dei dati, laddove ciò sia necessario per la conclusione o l'esecuzione di un contratto (ivi incluse le situazioni precontrattuali, ad esempio è consentito il trasferimento dei dati personali per prenotare un volo o una camera d'albergo negli Stati Uniti); per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; nel caso

in cui vi sia il consenso libero e informato dell'interessato, in assenza di altre motivazioni.
Le predette linee, chiarisce sempre la Commissione europea non pregiudicano in alcun modo l'indipendenza delle autorità di protezione dei dati e la loro facoltà di esaminare la legittimità dei trasferimenti transfrontalieri dei dati.
Infine, la Commissione Europea non può fare a meno di sottolineare con il suddetto intervento anche la necessità comunque di proseguire e concludere i negoziati volti a determinare un nuovo quadro normativo per i trasferimenti transatlantici di dati personali.

5.3. Verso un nuovo accordo c.d. *Privacy Shield*.

Come auspicato da più parti il vuoto creato dall'annullamento della decisione sull' "Approdo sicuro" dovrebbe essere colmato da un intervento tempestivo sul punto. Tale esigenza trova riscontro, peraltro, nei negoziati che, subito dopo la pronuncia della Corte di giustizia, sono stati intrapresi tra le autorità europee e quelle statunitensi proprio al fine del raggiungimento di tale obiettivo. Occorre, però, rilevare che, nonostante si sia parlato, nel corso dei mesi precedenti, del raggiungimento di un accordo tra la Commissione Europea ed il Governo degli Stati Uniti, formalmente ciò non esiste ancora perché per il momento manca un testo vero e proprio su cui discutere.
Nei suddetti negoziati si è fatto più che altro riferimento all'adozione di un c.d. "scudo" per proteggere i diritti dei milioni di utenti europei di Internet e garantire l'operatività delle migliaia di aziende che dipendono dalla possibilità di trasferire dati personali tra l'Europa e gli Stati Uniti. Il dialogo tra l'Europa e gli Stati Uniti si può dire che abbia contribuito, piuttosto, alla nascita di un'intesa politica, che per quanto importante ed auspicabilmente condivisa, attende comunque di essere tradotta in un autentico provvedimento.
Per il momento scarseggiano ulteriori dettagli sul punto ed inoltre i Garanti europei attendono di valutare se tale soluzione compromissoria risponda effettivamente alle preoccupazioni sollevate dalla sentenza della Corte di Giustizia per quanto riguarda i trasferimenti internazionali di dati personali.

6. Conclusioni.

Alla luce delle considerazioni che precedono emergono vari aspetti rilevanti della sentenza in commento. In primo luogo, come già accennato nel corso della presente trattazione, la decisione della Corte di Giustizia ha una valenza

notevole in termini politico-discrezionali, visto che determina un bilanciamento graduale dei diritti fondamentali coinvolti.
Con la sentenza oggetto della presente analisi, infatti, i Giudici di Lussemburgo, decidendo l'invalidità del sistema di c.d. *Safe Harbour*, finiscono, per chiudere il cerchio, ergendosi a custodi della tutela della *privacy* e dei dati personali in Europa. Mediante tale provvedimento, inoltre, essi affermano, in definitiva, la necessità che i trasferimenti delle informazioni personali tra Unione europea e Stati Uniti siano informati alla effettiva osservanza dei principi della normativa europea, primaria e secondaria, risolvendo, altresì, il problema politico posto dall'eccezione della sicurezza nazionale o pubblica rispetto alla protezione generalmente accordata ai dati personali [22].
Occorre, poi, sottolineare come la pronuncia in esame, stante quanto suddetto, produca degli effetti, non solo a livello europeo, quanto piuttosto a livello extraeuropeo, visto che coinvolge l'Europa e gli Stati Uniti, comportando, pertanto, anche la nascita di un dialogo in termini di regolazione politica tra le due sponde dell'Atlantico.
Il confronto tra l'Europa e gli Stati Uniti avviene sulla base di un delicato equilibrio che deve essere in grado di evitare la sorveglianza di massa garantendo al contempo il rispetto dei diritti fondamentali. Più specificamente la Corte, come suddetto, interviene sulla questione del bilanciamento dei diritti coinvolti ovvero sulla necessità di garantire da un lato, una protezione efficace ed equilibrata del diritto alla *privacy* ed al trattamento dei dati personali, mentre dall'altro lato, contemporaneamente sussiste l'esigenza del diritto alla sicurezza pubblica che i Governi hanno il dovere di garantire [23]. Quest'ultima esigenza quanto mai attuale stante le continue minacce terroristiche nei confronti del mondo occidentale.
Per quanto riguarda, poi, gli effetti estrinseci della sentenza della Corte di Giustizia, merita rilevare come la stessa contribuisca ad una potenziale accelerazione della riforma della normativa europea sulla protezione dei dati. La ridefinizione delle modalità di trasferimento dei dati personali dall'Unione europea agli Stati Uniti mediante l'adozione di una nuova soluzione condivisa è un'esigenza che merita di essere risolta quanto prima.
Ciò alla luce soprattutto del fatto che, sebbene lo strumento del *Safe Harbor* non sia l'unico meccanismo legittimante i trasferimenti transfrontalieri dei dati, non si può sottacere che l'utilizzo, da parte delle imprese, degli strumenti giuridici alternativi per i trasferimenti oltre oceano di tali dati, comporti, in termini economici, costi ben più ingenti. Tali costi, inoltre, sarebbero ancora più alti, laddove ad operare il trasferimento dei dati siano delle imprese di piccole dimensioni ovvero delle *start up*. La predetta circostanza si potrebbe, quindi, tradurre, in un meccanismo disincentivante

del flusso dei dati transfrontalieri, cosa che, peraltro, rischierebbe di determinare un potenziale isolamento dell'Europa.
La predisposizione di un accordo, inteso a disciplinare, nonché a ridurre, le divergenze tra l'Unione Europea e gli Stati Uniti, potrebbe, quindi, costituire una soluzione adeguata delle predette problematiche, a patto che lo stesso sia in grado di garantire una tutela "equivalente" dei dati personali rispetto a quella offerta dall'ordinamento giuridico dell'Unione Europea.

Note:
[*] Il presente contributo è stato preventivamente sottoposto a referaggio anonimo affidato ad un componente del Comitato di Referee secondo il Regolamento adottato da questa Rivista.
[1] Si vedano sul punto le seguenti pronunce della Corte di Giustizia: C-131/12, Google Spain SL e Google Inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González.; C-288/12, Commissione europea contro Ungheria; C-293/12 e C-594/12 Digital Rights Ireland Ltd.
[2] Il sistema Echelon è era un sistema software che controllava il download e la diffusione della intercettazione di comunicazioni via satellite. La Rete Echelon venne portata, per la prima volta, all'attenzione pubblica dal direttore dell'Omega Foundation, Steve Wright, quando firmò il rapporto della STOA (Scientific and Technologies Options Panel of the European Parliament) sull'argomento, dal titolo Prison technologies: An Appraisal of the Technologies of Political Control. Da quel momento indagini del Parlamento europeo, e non solo, intervennero sul punto estendendo la ricerca sull'argomento.
[3] Con il termine divulgazioni sulla sorveglianza di massa si fa riferimento ad una serie di inchieste giornalistiche pubblicate nel mese di giugno del 2013 e volte a rivelare dettagli sulle operazioni di sorveglianza e compromissione di massa, messe in atto dall'Agenzia per la Sicurezza Nazionale statunitense (NSA) in complicità con servizi di intelligence di altri paesi. Tali inchieste sono iniziate alla fine del 2012, quando il sig. Edward Snowden ha iniziato a mettere a disposizione di alcuni giornalisti numerosi documenti top secret collezionati durante la sua attività per l'NSA. I primi documenti riservati sono stati pubblicati il 6 giugno 2013 dai quotidiani The Washington Post e The Guardian attirando una notevole attenzione da parte del pubblico e del resto dei media.
[4] Il Gruppo di lavoro ex art. 29 o Data Protection Working Party è un organo consultivo indipendente dell'Unione europea, istituito dall'art. 29 Direttiva n. 95/46/CE, che si occupa di monitorare l'applicazione della direttiva europea

sulla privacy e di fornire linee di indirizzo e suggerimenti per l'evoluzione della disciplina e della sua applicazione.
[5] Cfr. art. 26, comma 2: «Salvo il disposto del paragrafo 1, uno Stato membro può autorizzare un trasferimento o una categoria di trasferimenti di dati personali verso un paese terzo che non garantisca un livello di protezione adeguato ai sensi dell'articolo 25, paragrafo 2, qualora il responsabile del trattamento presenti garanzie sufficienti per la tutela della vita privata e dei diritti e delle libertà fondamentali delle persone, nonché per l'esercizio dei diritti connessi; tali garanzie possono segnatamente risultare da clausole contrattuali appropriate».
[6] Cfr. art. 26, comma 4: «Qualora la Commissione decida, secondo la procedura di cui all'articolo 31, paragrafo 2, che alcune clausole contrattuali tipo offrono le garanzie sufficienti di cui al paragrafo 2, gli Stati membri adottano le misure necessarie per conformarsi alla decisione della Commissione».
[7] Cfr. articolo 13 comma 1: «Gli Stati membri possono adottare disposizioni legislative intese a limitare la portata degli obblighi e dei diritti previsti dalle disposizioni dell'articolo 6, paragrafo 1, dell'articolo 10, dell'articolo 11, paragrafo 1 e degli articoli 12 e 21, qualora tale restrizione costituisca una misura necessaria alla salvaguardia: a) della sicurezza dello Stato; b) della difesa; c) della pubblica sicurezza; d) della prevenzione, della ricerca, dell'accertamento e del perseguimento di infrazioni penali o di violazioni della deontologia delle professioni regolamentate; e) di un rilevante interesse economico o finanziario di uno Stato membro o dell'Unione europea, anche in materia monetaria, di bilancio e tributaria; f) di un compito di controllo, ispezione o disciplina connesso, anche occasionalmente, con l'esercizio dei pubblici poteri nei casi di cui alle lettere c), d) ed e); g) della protezione della persona interessata o dei diritti e delle libertà altrui. E comma 2. Fatte salve garanzie legali appropriate, che escludano in particolare che i dati possano essere utilizzati a fini di misure o di specifiche decisioni che si riferiscono a persone, gli Stati membri possono, nel caso in cui non sussista manifestamente alcun rischio di pregiudizio alla vita privata della persona interessata, limitare con un provvedimento legislativo i diritti di cui all'articolo 13 qualora i dati siano trattati esclusivamente ai fini della ricerca scientifica o siano memorizzati sotto forma di dati personali per un periodo che non superi quello necessario alla sola finalità di elaborazione delle statistiche».
[8] I principi di c.d. Safe arbor facevano esplicito riferimento alle seguenti circostanze: gli utenti dovevano essere avvertiti sulla raccolta e l'utilizzo dei propri dati personali; ciascuno doveva essere libero di rifiutare la raccolta dei dati e il loro trasferimento a terzi; i dati potevano essere trasferiti solo a

organizzazioni che seguivano principi adeguati di protezione dei dati; le aziende dovevano fornire garanzie contro il rischio che i dati venissero smarriti; dovevano essere raccolti solo i dati rilevanti ai fini della rilevazione; gli utenti avevano il diritto di accedere ai dati raccolti ed eventualmente a correggerli o cancellarli se sono inesatti; le regole dovevano essere efficacemente attuate.

[9] Si veda la delibera del 10 ottobre 2001 n. 36 con la quale il Garante Privacy ha autorizzato a sua volta, ai sensi dell'art. 44, comma 1, lett. b) (già art. 28, comma 4, lett. g) della legge 31 dicembre 1996, n. 675), i trasferimenti di dati personali dal territorio dello Stato verso organizzazioni aventi sede negli Stati Uniti effettuati nel rispetto dei "Principi di approdo sicuro in materia di riservatezza", applicati in conformità alle "Domande più frequenti" e all'ulteriore documentazione allegata alla decisione della Commissione europea del 26 luglio 2000 n. 2000/520/CE sul regime di "Approdo sicuro".

[10] Cfr. par. 58 della sentenza della Corte di Giustizia del 6 ottobre del 2015. Il ruolo centrale delle autorità di controllo nel sistema Unione Europea di protezione dei dati personali non solo è espressamente richiamato all'articolo 8, paragrafo 3, della Carta UE, ma è anche alla base della precedente sentenza della Corte di Giustizia: Digital Rights Irland ltd (8 aprile 2014, C-293/12 e C-594/12). In tale pronuncia, i giudici di Lussemburgo hanno dichiarato invalida la direttiva 2006/24 sulla raccolta, la conservazione e l'utilizzo dei dati di una persona fisica residente nell'Unione mediante comunicazioni telefoniche o elettroniche da parte di un'autorità pubblica di uno degli Stati membri (GUUE L 105 del 13 aprile 2006) proprio in quanto essa non stabiliva regole chiare, limiti o eccezioni all'accesso e all'uso dei dati personali da parte delle autorità pubbliche dei paesi membri in grado di ridurre il rischio di abusi o usi illeciti dei dati raccolti e conservati, sui quali i garanti nazionali avrebbero dovuto vigilare. La mancanza di regole chiare sull'uso da parte delle autorità pubbliche nazionali dei dati raccolti e conservati nell'Unione avrebbe di fatto reso impossibile il controllo su tale uso da parte delle autorità indipendenti. Tale operazione, riprendendo le parole della stessa Corte, «costituisce un elemento essenziale del rispetto della tutela delle persone riguardo al trattamento dei dati personali».

[11] La Commissione europea, nella propria decisione n. 2000/520/CE, specificava, peraltro, che l'applicazione del Safe Harbor poteva conoscere dei limiti, quali ad esempio la tutela della sicurezza nazionale o dell'ordine pubblico, ovvero limitazioni dovute ad interventi legislativi, regolamentari o giurisprudenziali.

[12] Secondo i giudici della Corte di Giustizia norme che consentono all'autorità pubblica di avere accesso su base generalizzata al contenuto delle

comunicazioni elettroniche compromettono l'essenza del diritto fondamentale al rispetto della vita privata.
[13] Cfr. Comunicazione della Commissione al Parlamento europeo e al Consiglio, intitolata «Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA» COM(2013) 846 final, 27 novembre 2013 e Comunicazione della Commissione al Parlamento europeo e al Consiglio sul funzionamento del regime «approdo sicuro» dal punto di vista dei cittadini dell'UE e delle società ivi stabilite COM(2013) 847 final, 27 novembre 2013.
[14] Si veda sul punto quanto affermato dall'eurodeputato Renato Soru il quale afferma che: «il rischio è quello di un ritorno a un sistema frammentato, con 28 soluzioni differenti in materia di trasferimento dei dati personali, che potrebbe creare degli ostacoli alle imprese europee operanti nel settore determinando un ritardo di competitività. Occorre pertanto colmare il gap legislativo e accelerare la conclusione della riforma della normativa europea sulla protezione dei dati personali, cosi come dare nuovo impulso alle negoziazioni per la decisione Safe Harbor II». http://www.renatosoru.eu/notizie/privacy-digitale-subito-una-normativa-europea-sulla-protezione-dei-dati-personali/
[15] Cfr. delibera n. 564 del 22 ottobre 2015.
[16] Si veda il link http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf
[17] Si veda la comunicazione della Commissione Europea del 6.11.2015, COM(2015), disponibile al seguente link: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf
[18] La serie I è contenuta nell'allegato alla decisione 2001/497/CE della Commissione, del 15 giugno 2001, relativa alle clausole contrattuali tipo per il trasferimento di dati a carattere personale verso paesi terzi a norma della direttiva 95/46/CE, GU L 181 del 4.7.2001; la serie II è contenuta nell'allegato alla decisione 2004/915/CE della Commissione, del 27 dicembre 2004, che modifica la decisione 2001/497/CE per quanto riguarda l'introduzione di un insieme alternativo di clausole contrattuali tipo per il trasferimento di dati personali a paesi terzi, GU L 385 del 29.12.2004.
[19] Decisione 2010/87/UE della Commissione, del 5 febbraio 2010, relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, GU L 39 del 12.2.2010.
[20] Occorre rilevare al riguardo che nelle linee guida la Commissione Europea fa riferimento anche in questa circostanza a due set di clausole:

quelle di cui alla decisione 2002/16/CE del 27 dicembre 2001 e quelle di cui alla decisione della nota precedente. La decisione 2002/16/CE, essendo stata abrogata dalla successiva decisione 2010/87/UE, continua a trovare applicazione solo per i contratti conclusi prima del 15 maggio 2010.

[21] Le caratteristiche più importanti che le clausole ad hoc devono avere sono: la presenza di una clausola relativa a una terza parte beneficiaria che consenta agli interessati di esercitare diritti contrattuali anche se non sono parte del contratto; il destinatario o l'importatore dei dati accetta, in caso di controversia, di essere sottoposto ai procedimenti dell'autorità di controllo nazionale e/o dei tribunali del titolare del trattamento che trasferisce i dati.

[22] cfr. U. Pagallo, la tutela della Privacy negli Stati Uniti d'America e in Europa. Modelli giuridici a confronto, Giuffrè editore, 2008, pagg. 234-236. Si veda sul punto anche http://www.dirittoegiustizia.it/news/17/0000075890/Le_conseguenze_pratiche_dell_annullamento_della_decisione_Safe_Harbour_gli_altri_presupposti_di_liceita_per_il_trasferimento_dei_dati_personali_negli_USA.html

[23] La problematica è stata recentemente affrontata in un convegno, promosso dall'Università Europea di Roma e dall'Accademia Italiana del Codice di Internet nell'ambito del PRIN, dal titolo: "La regolamentazione giuridica delle Tecnologie dell'Informazione e della Comunicazione (TIC) quale strumento di potenziamento delle società inclusive, innovative e sicure", tenutosi a Roma 9 dicembre 2015. Di particolare rilievo l'intervento del Prof. Alberto Gambino, Presidente dell'Accademia, il quale ha disegnato il quadro entro il quale si colloca il dibattito: "Come realizzare una protezione efficace ed equilibrata dei diritti fondamentali in un'epoca contrassegnata da un ritorno prepotente del fenomeno terroristico? Le risposte si collocano tra due poli: mantenere inalterata la tutela dei diritti umani nella loro massima portata ed estensione o all'opposto sospendere, nel prevalente interesse pubblico della sicurezza, alcune delle garanzie costituzionali, con compressione o svuotamento del contenuto di quel catalogo di diritti che costituisce il patrimonio delle democrazie liberali". La versione integrale dell'intervento è disponibile online sulla Rivista Diritto Mercato e Tecnologia al seguente link http: http://www.dimt.it/2015/12/11/safe-harbour-2-0-i-nodi-da-sciogliere-per-un-nuovo-equilibrio-tra-privacy-e-sicurezza-nel-convegno-con-joe-cannataci/

QUADERNI DI
DIRITTO MERCATO TECNOLOGIA

Numero 4 - 2015
Anno V
www.dimt.it

ISSN (Online edition): 2239-7442