CHALLENGE
Liberty & Security

Research Paper No. 7
December 2007

The Changing Landscape of European Liberty and Security

Rival Freedoms in terms of Security: The Case of Data Protection and the Criterion of Connexity

Nicolas Scandamis, Frantzis Sigalas & Sofoklis Stratakis

Abstract

The analysis of the present paper is based on two axes: one is that of the rivalry between different freedoms in a liberal regime, as well as the security restrictions to the concept of liberty. The other axis is that of the rivalry between the different forms of governing, governance and government in the EU, as articulated in the *connexity criterion* – a concept proposed and explored in this paper. The case study of the data protection regime in the EU demonstrates the tension between the individual right to data protection, economic freedoms and political freedoms and how that right is redefined by security necessities and the 'principle of availability'. The *connexity criterion* between governance and government is employed in the analysis of the Passenger Name Record judgement of the European Court of Justice.

An Integrated Project Financed by
the Sixth EU Framework Programme

ISBN-13: 978-92-9079-746-3

Available for free downloading from the CEPS website (http://www.ceps.eu)

Contents

RIVAL FREEDOMS IN (TERMS OF) SECURITY: THE CASE OF DATA PROTECTION AND (THE CRITERION OF) CONNEXITY

NICOLAS SCANDAMIS, FRANTZIS SIGALAS & SOFOKLIS STRATAKIS*

1. Introduction

The research conducted in the framework of the CHALLENGE programme has investigated a variety of aspects of the *problematique* surrounding the relationship between liberty and security. The tensions involved in this relationship could also be said to exist as far as the relationship between freedoms themselves is concerned: the notion of *Rival Freedoms* represents a significant aspect of the paradigm of *European governance* as a liberal regime.

While it is true that it is in the relationship between individuals and the state (as *government*) and within the framework of liberal regimes that the notion of rivalry acquires its essence and meaning, European governance is arguably to equally appropriate, as a liberal regime, for the examination of rivalry.[1]

As has been emphasised in the research conducted by the University of Athens, the European Union, and the paradigm it constitutes, is characterised by a specific articulation of the relationship between governance and government. On the one hand, *EC governance*, as exemplified in the Community method of the first pillar, refers to a functional mode of exercising power on European populations, with a view to establishing the framework of the Single Market. On the other hand, *State government*, involving organic patterns of power, located at the national level and based on the concept of sovereignty, persists and interplays alongside governance, as the continued use of the intergovernmental method suggests (for an overview, see Scandamis & Boskovits, 2006).

Thus, it is particularly important to examine the articulation of the relationship of rivalry in the framework of European governance, as an evolving institutional scheme drawing from both governance and government. Such an examination is also analytically useful for the examination of the terms of the relationship between liberty and security, which is the primary objective of CHALLENGE.

The present paper attempts to include, within the analytical framework of Rival Freedoms, the challenges posed by security practices – arguably also characterised as 'illiberal practices' – to liberal regimes. The case study of *Data Protection* was selected as a characteristic field in which the argument of rivalry could be adequately made, since the protection of personal data of individuals involves a tension both with other freedoms, notably market freedoms, as well as with security practices.

Thus, at a first stage, the Data Protection Regime will be examined and placed within the broader framework of freedoms/liberties in Europe, so that the argument of rivalry among freedoms can be made. At the second stage, the paper will deal specifically with the

---

* Nicolas Scandamis is Professor of European Law at the University of Athens. Frantzis Sigalas and Sofoklis Stratakis are doctoral students at the University of Athens.

[1] To quote Foucault, this rivalry is inherent within liberalism, since control and constraints constitute the counterpart and the counterbalance of liberties ("…la formidable extension des procédures de contrôle, de contrainte, de coercition qui vont constituer comme la contrepartie et le contrepoids des libertés") (Foucault, 2004: 68).

contribution to the examination of the relationship between liberty and security, which the right to data protection can make, while emphasis will be placed, in this context, on the implications of this rivalry for the tensions between governance and government, as the primary feature of European governance.

An important analytical thread proposed and examined in this paper consists of the notion of the *criterion of connexity*, as already illustrated in the title. Connexity functions as a sort of switch mechanism, it is suggested, which enables the approach of rivalry in terms of the analytical schemes of either governance or government. The function of this criterion and the specific terms of its articulation are aptly illustrated in the well-known recent judgement of the European Court of Justice on the transfer of PNR data to the US public authorities, as will be argued further in this paper.

2. The right to data protection in rivalry with freedoms in the framework of European governance

2.1 The establishment of Data Protection in EU governance

The proliferation of data protection legal instruments at an international level in the last two decades has undoubtedly been influenced by technological advances that facilitate the usage of a great variety of personal information for diverse purposes. This assumption of a "data explosion" (European Commission, 2003: 4) in the Information Age was without doubt a major incentive behind the establishment of the so-called *European Data Protection Regime* (Andenas & Zleptnig, 2003: 771). However, it should also be emphasised that this regime was essentially developed as a corollary of the acceleration of the Single Market in the European Union project and the challenge posed thereby to the protection of data. As is argued below, the relationship of the European Data Protection Regime to market freedoms, together with the distinct and explicit recognition of the right to data protection as a freedom in itself, renders their analysis important for the approach of Rival Freedoms, in the framework of European governance as a liberal regime. This is especially pertinent when the terms imposed by Security (concerns and practices) are added to the *problematique* of Rival Freedoms.

2.1.1 The Data Protection Regime and the European Economic Constitution

Before proceeding to the analysis of the specificities of data protection in European governance that are relevant for our research, the *establishment* of this data protection regime and its rationale are worth emphasising, in order to better highlight our argument.

It is therefore in a different framework, that of the Council of Europe as a distinct international organization, that the initial legislative instruments were adopted for the *specific* purpose of data protection beyond national legal jurisdictions. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (so-called Convention 108), adopted in 1981, was the first legally-binding international instrument on data protection (Andenas & Zleptnig, 2003: 777; Cannataci & Mifsud-Bonnici, 2005: 6). On the other hand, the European Convention of Human Rights is also said to serve the purpose of data protection, by means of the establishment of the right to private life (see also below), thus asserting the pioneering role of the Council of Europe in this respect.

Despite its legally binding nature and its influence on the European Data Protection Regime, in establishing a *common core of principles* (Maiani, 2002: 286; see also below), the Council of Europe legal framework was deemed to be insufficient for the purposes of data protection in the

European Union. The argument for the adoption of *Directive 95/46/EC (hereinafter referred to as Data Protection Directive)*[2] was twofold: the achievement of an Internal Market, in this case by the specific means of the free movement of personal information, as well as the protection of fundamental rights and freedoms of individuals (European Commission, 2003: 3).

It is our argument, however, that the creation of the Data Protection Regime in the first place, should primarily – though not exclusively – be regarded as a structural element of the Single Market and, by extension, of the *European Economic Constitution.* This concept (see, e.g., Gerber, 1998: 245) reflects the role of *Ordoliberal* thought in the process of European Integration, since it is used by this intellectual tradition in order to denote the special relationship between the Economy and the legal system. In the European Community, this relationship is reflected in Competition Law as well as in Free Movement rules in the EC Treaty. These legal rules gain a constitutional status, since they are targeted towards the objective of *market integration,* conceived as establishing, or constructing, a market at the European level.

It is furthermore evident that this process, that reached its peak with the abolition of internal frontiers and the establishment of the Internal Market, had to take into account the "substantial increase in cross-border flows of personal data between all those involved in a private or public capacity in economic and social activity in the Member States" (5th Recital of the Data Protection Directive).

However, the differences that had existed as to the level of protection of personal data in individual member states could put these flows at considerable risk, since this divergence could impose obstacles to the transmission of data from one member state to the other and consequently to the circulation of goods and services, to which circulation of information is inextricably linked (Maiani, 2002: 287). Indeed, prior to and following the formal establishment of the Internal Market, member states held "considerably different views upon the nature of personal data privacy" (Charlesworth, 2000: 256). Thus, whereas some countries emphasised the human rights element in their data protection legislation, others advocated the achievement of minimum standards of protection or even had no data protection legislation at all (ibid.).

Consequently, what was truly at risk was the ultimate goal of the establishment of the Single Market, for which the harmonisation of the level of protection of data was perceived as vital (8th Recital of the Data Protection Directive). This is the most crucial aspect of the rationale behind the creation of the Data Protection Regime, and, arguably, it had priority over rights-related concerns.

2.1.2 The Data Protection Regime as an instrument at the service of negative and positive integration in EU governance

The above-mentioned assertion should enable us to consider data protection, for analytical purposes, as primarily embedded in "*negative integration*", and serving, at least initially, as an instrument for the attainment of its objectives. The concept of negative integration refers to "the process through which barriers to cross-border economic activity within Europe are removed" (Fligstein & Stone Sweet, 2002: 1209). Originally coined by Fritz Scharpf (e.g. Scharpf, 1996), the concept is used to emphasise the establishment of the Single Market as an integrated economic area within which legal and administrative restrictions against the free movement of goods, capital, and the mobility of persons were removed, as well as the elimination of restrictions on free competition. According to this line of thought, governmental intervention is

[2] Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/3.

unnecessary or even harmful, with the dismantling of barriers to trade being the only intervention worth pursuing.

Following the 'periodisation' of European Integration suggested by Fligstein and Stone Sweet (ibid.), negative integration was given priority in the period from 1970 up to the adoption of the Single European Act in 1986. Indeed, from a macropolitical viewpoint, it is during this period that the development of the four Freedoms of Movement reached its full potential, akin to their constitutional status. Data protection was established in the subsequent period, in which EC legislation was primarily directed towards "*positive integration*"; this term denotes the process through which common public policies, e.g. environment and employment policies, are made and enforced, i.e. the replacement of disparate regulatory regimes with harmonised, EC regulatory frameworks (ibid.: 1216).

Nevertheless, as a consequence of the fact that the primary objective of the Data Protection Directive was the promotion and facilitation of the unhindered exercise of the freedoms of movement, its establishment could be argued to constitute an example of a measure directed towards the achievement of negative integration.

On the other hand, the subsequent evolution of the European Data Protection Regime, that emphasised the potential of a (fundamental) freedom, i.e. as the right to data protection, guaranteed at a Europe-wide level, by processes akin to those of harmonised supranational frameworks, may also strengthen arguments for the contribution of this regime to positive integration. Thus, the argument could be that, although the initial goal was to provide minimum standards of data protection, with a view to promoting the goals of the Single Market, data protection subsequently came to contribute to the process of positive integration. It could therefore be considered to lie at the *interface* of the two processes.

2.2 The development of Data Protection in European governance, as a freedom in a state of rivalry with other freedoms

In view of the above, the rationale behind the establishment of the Data Protection Regime should not be taken to denote an understatement of the importance of the "right to data protection" as a fundamental freedom in itself, within both the national and the European legal orders. However, it helps us to better conceptualise the dynamics behind its establishment. The subsequent development, both in legislation and in case law, of this same right, however, points to a distinct dynamics, as suggested above, namely that of a fundamental freedom, that inevitably gives rise to rivalry with other freedoms; this latter point deserves further analysis at this point.

2.2.1 The right to data protection and its elevation to the status of fundamental freedom

At the foundations of the European Data Protection Regime lies the recognition of a right to data protection. The position of this right in the framework of both national and international legal instruments for the protection of human rights is, however, ambiguous what is more, data protection has only relatively recently been construed as a distinct right/freedom and has been elevated to this status.

Indeed, data protection had at a first stage been considered to constitute an aspect of the right to private life. In the framework of the Council of Europe, the European Convention of Human Rights (ECHR) expressly recognizes, in its Article 8, the right of the person to respect for his/her private and family life, home and correspondence. The breadth of this provision was argued to encompass protection of personal data as an important element, that was thereby fundamentally linked to the notion of privacy and the associated right (Maiani, op. cit.; Adam, 2006: 416). Furthermore, the adoption of Convention 108 in the framework of the Council of

Europe (see above) was argued to encapsulate a "common core of principles" that were embodied in national laws concerning data protection (Maiani, op. cit). This rationale is most clearly expressed in the Data Protection Directive itself: in its 10th recital an explicit reference is made to the protection "notably of the right to privacy" as being the "object of the national laws on the processing of personal data".

Nevertheless, this extension of the right to privacy so as to include data of a personal nature was not undisputed: already in national legislation of the 1970s and especially after a landmark decision by the German Federal Constitutional Court in 1983, the predominance of the privacy discourse in data protection is gradually abandoned, in favour of an autonomous conceptualisation of the right. The notion of "informational self-determination" ("informationelle Selbstbestimmung"), meaning the capacity of the individual to determine himself/herself the processing of his/her own personal data, has considerably influenced this shift in the discourse (see, e.g., Bygrave, 2004: 323). Furthermore, the broad interpretation of Article 8 ECHR by the European Court of Human Rights also confirmed the trend to guarantee data protection as a distinct right. In a series of recent judgements of the Strasbourg Court, notably *Rotaru v. Romania* (Application number 28341/1995-judgement of May 4, 2000), *Amann v. Switzerland* (Application number 27798/95 – judgement of February 16, 2000), and *P.G. and J.H. v. the United Kingdom* (Application number 44787/98 – judgement of September 25, 2001), the wide scope of Article 8 ECHR, so as to encompass data protection as a fundamental freedom, was given emphasis.

The shift may additionally be observed in developments subsequent to the adoption of the Data Protection Directive at the level of the European Union, which has since taken the lead in the promotion of the right. On the one hand, this gradual "autonomisation" (Adam, op. cit.) from the right to privacy can be gleaned from the extension of data protection in specific sectors: Directive 1997/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector[3] and Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector[4] are steps towards the extension of the right to data protection itself, i.e. towards the enhancement of its scope and therefore of its legal status, while treating it separately from the right to privacy, as the titles of the Directives suggest.

On the other hand, and parallel to the establishment of the right to data protection as an autonomous and distinct right in the national Constitutions of certain member states, Article 8 of the European Charter of Fundamental Rights marks the most important such development. The explicit reference in this Article to a right that every individual enjoys, i.e. *in addition to* his/her right to private life, emphasises the development of data protection to the status of a fundamental right of individuals (Cannataci & Mifsud-Bonnici, 2005: 10-11).

What is more, an even more radical enhancement of the status of this right, at least at face value (ibid.), lies in its enshrinement in the Treaty for the Constitution of Europe. In Article I-51 thereof, the EU as an institution is committed to providing an adequate level of data protection, by means of appropriate rules, for activities which fall within the scope of Union law. Though the wording of the Article is not unambiguous and could give rise to contestations, the strength of the argument made above, concerning the promotion of the right to a constitutional level, is undisputable.

---

[3] OJ L24/1, 30 January 1998.

[4] OJ L201/37, 31 July 2002.

2.2.2 The right to data protection and its rival relationship with freedoms in the framework of European governance

The evolution of data protection as an autonomous right/freedom is definitely not unproblematic. The relationship with other rights is an issue deserving careful consideration. Before proceeding to the specific terms of the rivalry, it is necessary to shed some light on the background of this analytical perspective.

The concept of "rival freedoms" or, alternatively, "freedoms in rivalry" is drawn from the controversies surrounding the analysis of liberalism in political philosophy. The major point of reference for the contemporary debate lies in the pioneering work of John Rawls (1971) and the extensive commentary and critique it engendered. Rawls' idea of "Justice as Fairness" consists of two principles: namely that all have the greatest degree of liberty compatible with like liberty for all, and that social and economic inequalities be attached to positions open to all under fair equality of opportunity and to the greatest benefit of the least well-off members of society.

It is especially important, in our view, to take account of the critique of liberalism in the research of fundamental freedoms, including data protection. In criticising Rawls' first principle of justice, according to which each person is to have an equal right to the most extensive basic liberty compatible with a similar liberty for others, H.L.A. Hart, as well as other philosophers, accuses this thesis of giving rise to indeterminacy. In support of the same argument, it is notably John Gray who extends this line of thought to reach the position that freedoms within liberalism are essentially rival.[5]

Thus, in *Two Faces of Liberalism*, Gray emphasises that "liberal values prescribe rival freedoms. By so doing they engender dilemmas for which liberal principles have no answer" (Gray, 2000: 104). This alleged "deadlock" is supposed to have its roots in the conflicting and, above all, incommensurable, values that different freedoms simultaneously guarantee and protect.[6]

While the concept of 'Rival Freedoms' in the very specific way it is used by Gray may be of significance, it is argued here that a broader understanding of the concept is analytically more powerful. The concept should extend beyond the critique of liberalism, so as to encompass the wider *problematique* of the relationship between freedoms, which is not necessarily reduced to a conflict between different values and, above all, is not restricted to theoretical accounts of liberalism. It is from such a wider perspective that data protection should be examined, thereby drawing significant conclusions for its conceptualisation as a freedom in the framework of liberal regimes.

Most importantly, it is important to state this conceptualisation in terms of the *paradigm of European governance*. The latter constitutes an example of a liberal regime *par excellence*. It is therefore important to ascertain the specific terms of the rivalry of freedoms in European governance, in which the establishment of the Internal Market and its implications add a crucial dimension.

---

[5] It should be emphasised that although it is Gray who comes up with the concept of 'rival freedoms', our use of the term by no means implies an agreement with this philosopher's general theoretical framework.

[6] As a primary illustration of such a rivalry, an example is given by the same author: Gray mentions the conflict between the basic liberty respecting freedom of speech and the potential liberty not to be subject to hate or racist speech. Most liberal democracies have curbs on the unrestricted freedom of speech, which gives rise to the problem of pluralism again, since legislators are faced with two values that are in conflict so that they have to make hard political choices. For an overview of this argument, see also Kelly (2006: 143-144).

Thus, in the first place, the relationship of data protection with *market freedoms*, in the framework of the Internal Market, is a major issue at stake in EU governance. The central question arising is whether the previously mentioned rationale of the adoption of the Data Protection Directive and the priority given to its "economic background" (Charlesworth, 2000: 258) have a restrictive effect upon the scope of the Directive. Consequently, at issue here is whether the right to data protection, primarily as embodied in the Data Protection Directive, should only be perceived as complementary and subordinate to the freedoms of movement or as having a broader scope instead.

In this respect, it was the European Court of Justice that played a substantial role in elucidating the framework of the relationship between market freedoms and the right to data protection; in so doing, it clarified the scope and the field of application of the Data Protection Directive and put an end to the ambiguities that had arisen.

More specifically, in the *Österreichischer Rundfunk* cases[7] it was emphasised, in line with previous case-law, e.g. the famous *Tobacco Advertising* case, that "recourse to Article 100a of the Treaty as legal basis does not presuppose the existence of an actual link with free movement between Member States in every situation referred to by the measure founded on that basis" (paragraph 41 of the Judgment). Thus, the applicability of the Data Protection Directive "cannot depend on whether the specific situations at issue in the main proceedings have a sufficient link with the exercise of the fundamental freedoms guaranteed by the Treaty" (paragraph 42).

The same finding is reiterated in a subsequent important case, namely *Bodil Lindqvist*:[8] it was again emphasised that "it would *not* be appropriate to interpret the expression 'activity which falls outside the scope of Community law' as having a scope which would require it to be determined *in each individual case whether the specific activity at issue directly affected freedom of movement between Member States*" (paragraph 42 of the Judgement, emphasis added). On the contrary, "the activities mentioned by way of example in the first indent of Article 3(2) of Directive 95/46 are intended to define the scope of the exception provided for there, with the result that *that exception applies only to the activities which are expressly listed there or which can be classified in the same category* (*ejusdem generis*)" (paragraph 44 of the Judgement, emphasis added).

In essence, therefore, the ECJ held that the right to data protection has an extensive field of application, regardless of the relationship that the data processed may have with Community law (Coudray, 2004: 1369). Indeed, the only cases in which data processed do not fall under the Data Protection Regime, are those cases in which the activities undoubtedly concern the so-called second and third pillars of the EU, and are explicitly mentioned in the Directive for this purpose: public security, defence, state security and criminal law.

In light of the above, it could be argued that the clarification of the terms of the rivalry between the two categories of freedoms was achieved by means of an interpretation of the legal instrument itself, i.e. with an appropriate interpretation of its wording, without having recourse to the market rationale in which the establishment of the freedom was embedded. Instead, the Data Protection Regime was found to adequately delineate its own field of application.

The same considerations, i.e. the capacity of the mechanisms of the Data Protection Regime, both European and national – at the level of implementation for the latter – to carry out by

---

[7] Joined Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others* [2003] ECR I-4989.

[8] Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12971.

themselves a satisfactory balancing of freedoms that are in a position of rivalry, are also to be found in the relationship of the right to data protection with the *freedom of expression*.

This was made clear by the Court in *Bodil Lindqvist* (see above) in the evaluation it carried out of data protection and of its compatibility with the general principle of the freedom of expression, enshrined, in particular, in Article 10 ECHR. In this case, the Court found that, notwithstanding the restrictions imposed on this freedom, "the mechanisms allowing those different rights and interests to be balanced are contained, first, in Directive 95/46 itself, in that it provides for rules which determine in what circumstances and to what extent the processing of personal data is lawful and what safeguards must be provided. Second, they result from the adoption, by the member states, of national provisions implementing that directive and their application by the national authorities." (paragraph 82 of the Judgement). In this way, it went on to conclude that "it is for the authorities and courts of the Member States not only to interpret their national law in a manner consistent with Directive 95/46 but also *to make sure they do not rely on an interpretation of it which would be in conflict with the fundamental rights protected by the Community legal order or with the other general principles of Community law, such as inter alia the principle of proportionality*" (paragraph 87 of the Judgement, emphasis added).

Therefore, as the above analysis suggests, the rivalry of data protection with other freedoms, as a major characteristic of their relationship, is confirmed and its specific terms outlined. However, the conflict of values that appeared insolvable by liberal principles themselves, should necessarily be given a certain qualification in light of the preceding analysis.

What is perhaps more significant, furthermore, is the new analytical lens through which the concept of rivalry is examined. Thus, whereas rivalry has traditionally been considered in terms of a conflictual relationship between the values embodied in the different freedoms, in the framework of liberal regimes, it is argued here that a conceptual shift should be attempted. Indeed, the examples given, point towards a specific interpretation of the rivalry, suitable for the paradigm of EU governance. In this way, the concept of rivalry necessarily acquires a dimension that clearly distinguishes it from the philosophical background from which it was derived in the first place, but from which it has become subsequently detached.

3. The right to data protection as defined through security in the framework of European governance and the criterion of connexity

In part I we examined the data protection framework and its implications for the individual's liberties and freedoms. In this part, the Data Protection Regime will be considered in light of security in the framework of EU governance.

Security, in a general sense, is the essence of any type of governance. Without further adjectives (internal/external, national/societal, individual/public), it may be broadly understood that it has no proper content other than the one posed by the threat in question.

Furthermore, it has been argued in our previous research that the significant analytical distinction between *governance* and *government* has important implications for the conceptualisation of security in its various forms: while external security clearly belongs to the realm of so-called state government,[9] it has already been observed by Scandamis and Boskovits (2006), that internal security, on the other hand, falls under the realm of national sovereignty, while at the same time pertaining to the flow of populations. In other words, internal security presents itself as the issue at stake for both state institutions responsible for law and order and

[9] The concept of government means the central political power of the state, which retains the monopoly of force and resources.

EU governance of an "area of freedom, security and justice". In this context, internal security seems to defy any clear-cut distinction between EU governance and state government. Matters relating to internal security are subject to a hybrid institutional framework, marked by the division between the Community method and enhanced forms of co-operation under the third pillar.

Therefore, it is no surprise that the general objective of the establishment of an area of freedom, security and justice has, thus far, led to a rather dubious regime, involving the gradual application of the Community method, alongside with a series of notable exceptions relating to the matters concerned –justice and police cooperation in criminal matters remain under the third pillar- as well as to decision-making and the enforcement procedure, in the form of limits to the participation of the European Commission and the European Parliament and to the jurisdiction of the ECJ.

An analytical distinction should also be made between *security* as conceived in the above-mentioned manner and *safety* as conceived from the perspective of the individual/citizen as a right *(right to safety of the individual).* This latter right draws from Article 5 ECHR to subsequently acquire a much broader content: the right to safety is supposed to include, in this logic, the safe exercise of any (other) right, as well as, most importantly, the right to defend oneself against the discretionary power of the state.

In light of the above, the right to safety could be said to be exercised, at least in some instances, *against* security (as an *interest* of the state). This distinction leads to a conceptualisation of the relationship of the two concepts *(safety and security)* in terms of *restrictions and exceptions, in the same way that security poses restrictions to the exercise of liberties.*

The above-mentioned analysis also enables us to consider the right to data protection as a facet and a specific application of the *right to safety*, which may be conceived as a general right for this purpose.

As far as the Data Protection Regime in the European Union and its relationship with security is concerned, it should be noted that the Data Protection Directive is not applicable in the third pillar, which regulates security in a predominantly intergovernmental framework, since activities such as those provided for by Title VI of the EU treaty, and in any case to processing operations concerning public security, defence, state security and state activities in areas of criminal law, were excluded by virtue of article 3(2) thereof. On the other hand, it is precisely in the third pillar that data protection is of substantial importance, since police and judicial authorities have a strong incentive for easy access to personal data, for the sake of their effective action. Furthermore, the nature of personal data in the third pillar is sensitive and confidential, since they are compiled and exchanged for the sake of law enforcement purposes. It is in order to cover this vacuum that the Commission adopted a proposal for a Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (COM 2005/490), which has undergone a number of revisions without having reached a final form yet.

To recapitulate, in this part of the paper the connection exists between the rights of the individual, such as the right to safety, which, it can be argued, includes the right to data protection, and the interests of society, European and national, such as the security interest (Alder, 2002: 420; Halpin, 1997: 108-114). In general, as Delgado, in his capacity as Deputy Data Protection Supervisor, says: "it has become relatively common to refer to security and data protection as if both concepts were, *by definition*, contraries and incompatibles. In trying to reconcile the application of both principles, it is often argued that it is necessary to find a proper balance between security requirements, on the one hand, and the protection of personal data, on the other" (2006: 1).

3.1 The right to data protection and its relationship with the demands of public security in the EU

3.1.1 Data protection in rivalry with the principle of availability[10]

It is characteristic of the European Community and Union Treaties that no European law enforcement authority is established. The enforcement of European law is a matter for member states, while the authorities of the latter are not normally empowered to take action within other member states' territory. The use of coercive measures remains within the competence of member states themselves and persists as a core feature of national sovereignty. This lack of a central European enforcement system obstructs the effectiveness of EU law (Hijmans, 2006). As a consequence, information-sharing, including exchange of police and judicial information, is seen as a key cooperation tool.[11]

In order to enhance this cooperation[12] actively, the Hague Programme included a new concept, "the principle of availability", meaning that "throughout the Union, a law enforcement officer in one Member State who needs information in order to perform his duties can obtain this from another Member State and that the law enforcement agency in the other Member State which holds this information will make it available for the stated purpose…". The concept is used with the same meaning in the proposal for a Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, in article 1.2 of which it is stated that "Member States shall ensure that the disclosure of personal data to the competent authorities of other Member States is neither restricted nor prohibited for reasons connected with the protection of personal data as provided for in this Framework Decision".

> Sharing available information such as personal data, is already foreseen in existing EU legislation and multilateral Conventions such as the Europol Convention,[13] the Eurojust Decision[14] and finally in the Schengen Convention,[15] although sharing is made on a

---

[10] The term 'principle of availability' is used with the same meaning as the concept of exchange of information, since it was an easy step from the calls for the exchange of information and intelligence to the 'principle of availability'. The Prüm treaty does not use the term 'principle of availability', preferring 'exchange of information' instead.

[11] The Europol Convention and the Eurojust Council Decision are directed to that end and include exchange of information. The other major information systems which have been set up are the Schengen Information System, which is currently governed by the Schengen Convention, the Eurodac, which was set up under Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention, the Visa Information System (VIS) that is to be set up by virtue of the proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between member states on short-stay visas (COM (2004) 835 final). The Convention drawn on the basis of Article K.3 of the treaty on European Union, on the use of information technology for customs purposes. A common feature of all these existing data information systems in the area of freedom, security and justice is that the member states are responsible for their functioning and they do not have an autonomous European structure. The Eurodac and the Visa Information System belong to the first pillar while the Europol and Eurojust databases fall entirely within the third pillar.

[12] According to Hijmans (ibid.), there are other instruments as well (apart from the concept of availability) designed to make information available to authorities in other member states, such as the proposed provisions on exchange of information from criminal records. See Council Framework Decision on the organization and content of the exchange of information extracted from criminal records between Member States (COM (2005) 690 final).

[13] OJ C 316, 27.11.1995.

[14] OJ L 63, 6.3.2002.

> voluntary basis. The two legal instruments which render the principle of availability obligatory, are the Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union and the Treaty of Prüm of 27 May 2005. In this way, availability is more than mutual recognition of national legislation since Member State authorities have to provide active cooperation based on mutual trust.[16]

From the preceding analysis, it becomes obvious that the principal aim of the concept of availability, apart from the free flow of law enforcement information, is the improvement of internal security and safety for the citizen by means of facilitating the combat of trans-border crime and the fight against terrorism. The effectiveness of the principle of availability presupposes effectiveness in the respect of the protection of fundamental rights and freedoms of citizen, in particular the rights to privacy and data protection. Mutual trust is not just important in the relationship among authorities, though data subjects also need to be able to rely on their rights not to be infringed when information is shared between member states.

Although the activities falling under Titles V and VI of the EU Treaty are outside the scope of the Data Protection Directive, member states have expanded its scope of application to include the processing of data carried out by police and judicial authorities and apply the general data protection principles, since these principles are also included in the Council of Europe Convention 108. Besides, there also exists the protection provided by Regulation 45/2001.[17] The principles of this Regulation are applied to the European databases, such as the Visa Information System and the second generation of the Schengen Information System. What is noteworthy on the other hand, is that the data protection framework of Europol and Eurojust is based on specific rules and principles.

Apart from the general protection in the EU Data Protection Regime, there is also the principle that data should be collected for explicit and legitimate purposes. The problem is that exceptions and restrictions to the above-mentioned principle are allowed for security reasons, in a context where the principle of availability for the exchange of data primarily serves exactly such security purposes.

More specifically, from an individual's perspective, the question of which data are to be made available and under what circumstances the exchange of data could be allowed, clearly shows the rivalry between the principle of availability and the protection of data. Extra safeguards and additional measures are required especially for the exchange of special categories of data, such as biometric data, for the purposes of law enforcement, since the need for additional checks constantly emerges. Besides, there is also the need for the member states to establish the exact

---

[15] OJ L 239, 22.9.2000.

[16] Mutual trust and mutual recognition are an essential condition for the exchange of law enforcement information. Police and judicial cooperation requires mutual trust. The Constitutional Treaty (I.42) regards promoting mutual confidence between authorities as a foundation stone of AFSJ. The European Court of Justice saw mutual confidence as lying at the heart of the *Gözütok* and *Brügge* judgment concerning the application of the double-jeopardy bar. The Court found it necessary "that the Member States have mutual trust in their criminal justice systems and that each of them recognises the criminal law in force in the other Member States even when the outcome would be different if its own national law were applied" (Joined cases C-187/01 and C-385/01 [2003] ECR I-1345) (Hijmans, 2006). The concept of mutual trust is a foundation stone also for other legal instruments of the third pillar, such as the European Arrest Warrant (case C-303/05).

[17] When personal data is processed by private or public authorities, the data protection principles, as defined in Directive 95/46, will be applicable. When this data is processed either by European institutions or in European data files, the principles of Regulation 45/2001 and/or the applicable specific rules for these files will apply.

competences of judicial authorities and data protection authorities to control data processing and their exchange among Member States, since it is the latter that are principally responsible for the functioning of the databases in the third pillar.

The free movement and exchange of information that enhances the effectiveness of security measures, according to the principle of availability, is therefore in rivalry with individual freedoms and especially with the Data Protection Regime. Their reconciliation should be based on the grounds of a solid legal infrastructure, which would allow controlled and proportionate information sharing, respecting the fundamental freedoms and rights of the individual.

3.1.2 The right to data protection of the individual as defined by public/internal security

As far as the issue of the balance between public security interests and privacy/data protection is concerned, it is crucial to define the legal framework where this conflict of values exists.

As it has already been mentioned, the Data Protection Directive, which is the main instrument for the protection of the right to data protection, does not apply to the third pillar. This is also true for the directive 2002/58/EC on data protection in the communications sector. As a consequence, the protection of privacy[18] and data protection in the third pillar are guaranteed only by the European Convention of Human Rights and the European Charter of Fundamental Rights.[19]

Article 8 of the ECHR protects the individual against arbitrary interference by the public bodies in his/her private life or family life and, in general, offers low protection in the field of personal data protection since it does not provide for more specific and subjective rights, in the way that the Council of Europe Convention 108 (mentioned above), does since it emphasises that data protection implies privacy protection. The main aim of Convention 108 is to grant subjective rights to the data subject, so as to allow the individual control over the information concerning his/her person (right to be informed, right to access, right to rectify etc.) (Poullet, 2006: 215). Convention 108 offers, as a consequence, a more positive approach to the data protection regime than that of Article 8 ECHR, which gives a limited interpretation. The same is true for all the legal instruments examined in the previous part of the paper, which led to the establishment of the right to data protection as a distinct human right.

As far as these latter legal instruments are concerned, therefore: on the one hand, the Charter of Fundamental Rights has not yet become legally binding. On the other hand, the provision of Article 8 of the latter does not specify any security restrictions or exceptions, so that the balance between privacy and security is (presently) determined by the relevant provisions of the ECHR. According to the ECJ case law, these provisions are derived from the common constitutional principles of the member states, with an autonomous interpretation given by the ECJ. The second paragraph of article 8 ECHR stipulates:[20]

---

[18] For the recognition of privacy as a concept worthy of distinct treatment by law, see, in addition to previously mentioned sources, Gunasekara (2007: 4).

[19] Although the Data Protection Directive does not apply to the processing of personal data carried out by enforcement and judicial authorities, its principles could perhaps be used to form the core of a comprehensive European data protection law (*Krakow Declaration*). On the other hand, Europol and Eurojust have autonomous data protection regimes.

[20] The importance of article 8 for the protection of data and the individual' s right of privacy in the third pillar becomes obvious from the *PNR* judgment of the ECJ (Joined Cases C-317/04 and C-318/04, *European Parliament v. Council and Commission*, Judgement of the Grand Chamber of 30 May 2006, [2006] ECR I-4721) where, at the very beginning, in paragraph 3, the first effective paragraph of the judgement, the provision of article 8 of ECHR is mentioned: "To our knowledge it is unprecedented that

> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of rights and freedoms of others

This second paragraph introduces a necessity and proportionality test. When a national measure interferes with the right, it can be justified only if it is in accordance with the law and necessary in a democratic society for a legitimate purpose. The first condition requires that the measure have an adequate basis in national law, and that this law satisfy certain quality criteria: it must be accessible, sufficiently precise and predictable for affected parties. The second condition requires that the measure correspond to a pressing social need, such as security and public order, and conform to the principle of proportionality (Hustinx, 2006a). This means that the national measure should be designed to achieve, on the one hand, effective enforcement and, on the other hand, a minimum interference with privacy. As the European Data Protection Supervisor stresses (ibid.), "the European Court of Human Rights allows a margin of appreciation, depending on the nature and the purpose of interference but not unlimited discretion, not even in highly sensitive areas". The same rationale was followed by the ECJ in the *Österreichischer Rundfunk* case (see above), which was its first judgement concerning the application of the Data Protection Directive, in such a way that the application of the latter would comply with the requirements imposed in Article 8 ECHR.

Even if it is admitted that the necessity and proportionality principles, as they are interpreted by the European Court of Human Rights and the ECJ, offer an adequate protection of the fundamental rights of the individual, it must also be mentioned, however, that it is disputed whether the proposed Framework Decision (see above) will eventually apply to national security matters. There is a broad consensus that processing of personal data in connection with national security purposes, should remain beyond its scope in all cases. What is more, the draft Framework decision does not apply to the Europol and Eurojust databases, which possess an autonomous institutional framework.

In light of the above, the fragmented regime of data protection in the third pillar, which is characterised by the exceptions of security and public order, demonstrates that the state government factor has a strong presence in this field, thus affecting the individual's right to data protection and to privacy.

The threats to the individual's privacy are multiplied where law enforcement authorities possess biometric data of the individual, which are a special category of data in need of additional safeguards. The dangers posed to biometric data derive from the fact that biometric characteristics are not readable by the human eye and they almost never change throughout a person's life, which means that this type of data is permanent. The use of biometric data entails that surveillance becomes indivisible and the presumption of innocence, as derived from the right to safety, is at stake. This is the reason that this type of data-processing should be accompanied by procedures of constant check, which have to take the form of a specific individual right provided by data protection law.

As Hustinx additionally pointed out (2006b), the advisory role of data protection authorities under the present arrangements is unsatisfactory: "The European Commission has confirmed that it feels bound by article 28(2) of Regulation (EC) 45/2001 to consult the European Data

---

the European Court of Justice, the court of the European Union, commences one of its judgments with a reference not to the law of the EU but to an international human rights agreement to which the EU is not even a party" (Guild & Brouwer, 2006: 3).

Protection Supervisor (EDPS) when it adopts a proposal for legislation with an impact on the protection of personal data, but [in the third pillar] its right of legislative initiative is shared with Member States not bound by such an obligation. Arrangements for a systematic input from national data protection authorities are even less adequate" (ibid.: 2).

3.2 The European Data Protection Regime between governance and government and the connexity criterion

3.2.1 The significance of the PNR judgement

The duality of forms of governing, i.e. governance and government, is reproduced within the whole EU framework and determines the rationale of every policy measure, including the Data Protection Regime examined here.

As we have already seen in our previous research, what pertains to economic life, crucial under normal circumstances, is governed by the original and paradigmatic Community method, which draws basically from governance. The Community method pertains to the economic field, being based on a synergy and complex forms of networking between supranational and intergovernmental elements.

In the absence of EU institutions primarily responsible for the maintenance of order and the incomplete 'communautarisation' of the AFSJ, one may not speak of an EU government in the field of security, but of EU governance acting in support of State government.

In general, it is unclear where the border between the first and the third pillar lies and this ambiguity influences the distinction between governance and government. On the other hand, as the Advocate General Léger has held, [21] for the European pillar structure "the choice of the appropriate legal basis has constitutional significance. Since the Community has conferred powers only, it must tie [the international agreement concerned] to a Treaty provision which empowers it to approve such a measure".

The most important example of the way in which the Data Protection Regime lies between governance and government, is arguably the recent so-called PNR judgement of the Court.[22] In this judgement, the Court ruled on a Council Decision and a Commission Decision requiring European airlines to pass on passenger data to US customs authorities, or even to give those authorities access to their databases, when flying to, from or over the United States of America.

As De Leon (2006: 322) summarises: "Several European airlines contended that the disclosure of sensitive PNR data would be violating EU data protection rules and human rights which are governed by Human Rights conventions. European human rights protect: -the right of privacy; -the right of protection of personal data; -the right of people to travel anonymously".

The Court based its judgement on the first indent of article 3(2) of the Data Protection Directive. Under this provision, the scope of the Directive excludes the processing of personal data in the course of an activity that falls outside the scope of Community law, such as activities provided for by Titles V and VI of the treaty on European Union, and in any case to processing operations concerning public security, defence, state security and state activities in areas of criminal law. The Court went on to find that processing of passenger data for the US authorities "…constitutes processing operations concerning public security and the activities of the State in

---

[21] Opinion of Advocate General Léger, 22 November 2005, Case C-317/04, *European Parliament v. Council of the European Union*, paragraph 127.

[22] Joined Cases C-317/04 and C-318/04, *European Parliament v. Council and Commission*, Judgement of the Grand Chamber of 30 May 2006, [2006] ECR I-4721. For an analysis see, e.g., De Leon (2006).

areas of criminal law" (paragraph 56 of the judgement). Thus, it concluded that "While the view may rightly be taken that PNR data are initially collected by airlines in the course of an activity which falls within the scope of Community law…the data processing which is taken into account in the decision on adequacy is, however, quite different in nature…that decision concerns not data processing necessary for a supply of services, but data processing regarded as necessary for safeguarding public security and for law-enforcement purposes" (paragraph 57 of the judgement).

According to the judgement, the member states do not cease to be competent in matters of internal security: as a consequence, they are responsible for reconciling the two objectives pursued by agreements of the PNR agreement type, namely that of the fight against terrorism and that of data protection in the framework of the ECHR (Mariatte, 2006: 8). Perhaps this is the reason that from the first effective paragraph of the judgement the Court sets out the provision of the ECHR and especially that of Article 8 (Guild & Brouwer, 2006: 2). The ECJ therefore acknowledges that the fight against terrorism and consequently public security is a government task, coming under government responsibility.

The ECJ thus limited itself to a formalistic approach (Gilmore & Rijpma, 2007: 1081), without answering the crucial pleas, which alleged infringement of the right to protection of personal data and breach of the principle of proportionality. The only matter with which the Court was engaged, was that of the establishment of an appropriate legal basis for an antiterrorist measure, which has taken the form of an international agreement. It was supposedly a matter of competence and of the appropriate use of the pillar structure.

Although it could be argued, on the one hand, that the choice of the first pillar is more suitable for reasons of respect to the *acquis communautaire* and for an implementation of the measures/responsibilities of the PNR agreement by means of Community law, it must be mentioned, on the other hand, that the EU legislation in response to terrorism has been adopted predominantly under the third –intergovernmental- pillar, and, as a consequence the PNR should be examined in this light and not in isolation (ibid.). In any case, what is important and essential for a democratic society based on the principles of accountability and the division of power, is that the choice of a legal basis for a measure must rest on objective factors, amenable to judicial review, which include the aim and the content of the measure (ibid: 1095).

In the same framework, namely that of the legal basis, it should be reminded that the first pillar expanded its implementation field through the concept of conferred or implied powers of Community institutions and through the use of legal bases interpreted broadly, such as Articles 95 (the harmonisation clause for the internal market) and 301 EC (a passerelle clause which is used to impose financial and economic sanctions upon individuals, allowing the Union objectives to be achieved with Community instruments) (ibid: 1081).

Furthermore, different theories have been suggested as to the choice of the appropriate legal basis of a European Community measure. The most important among them is that of the main objective of the measure (the centre of gravity theory), which comes into play when a measure can be based on two different articles of the EC treaty; as a result, application is excluded in the present case under examination. The second theory is that of whether a certain threshold has been crossed, whereby a measure is considered to adequately contribute to the functioning of the internal market (ibid.: 1093-94). Nevertheless, both these theories do not offer an adequate solution to the choice of pillar in the PNR case, since they apply only to the Community pillar.

3.2.2 Data protection and security in the PNR judgement: the connexity criterion.

Most importantly, what is really at stake but still lies beyond a prima facie reading of the PNR judgement is the connection between safety and security and, by extension, between governance

and government, as will be illustrated below. Indeed, by analysing the PNR judgement solely in terms of the legal basis, which implies a restrictive analysis from the perspective of the pillar structure, there is always the danger of missing the essence of the fundamental balances that shape the institutional patterns of European integration. The latter is a process characterised by the duality of the paths of economic and political integration in their various and evolving relations. The essence in the PNR judgement, indeed, lies in the type of governing and its implications for the status of the individual. This is the reason why we need a new analytical approach to this judgement, from the bottom-up this time, according to the proposed **connexity criterion,** so that the duality of types of governing, governance and government, in the European Union, can be better understood.

The proposed criterion thus functions as a sort of *switch mechanism*, which enables the connection (hence the term connexity), in each case of rivalry under examination, with *either* governance *or* government.

The connexity criterion[23] is, furthermore, particularly appropriate in the European context, since it permits, in ambiguous situations, an approach to the distinction between governance and government from the perspective of the individual or citizen. It depends on the field in which a measure is applied that its *connexity* with a certain type of governing will be established – governance or government – and, most importantly, the kind of protection of the individual that is required in the framework of the European regime of governance.

In our case, the question posed, according to the connexity criterion, is the following: is the exchange of data required by the PNR agreement more closely connected to the right to safety of the individual, conceived as the safe exercise of economic freedoms, with the latter being effectively guaranteed by the PNR agreement? Or, instead, whether the exchange of data is in closer connection to security, with the PNR agreement having primarily a security-related objective, such as the fight against terrorism. This question boils down to determining whether it is in the field of governance or, instead, that of government, that this practice should be placed, with all the implications flowing from this latter characterisation.

Although the judgement of the Court did not make any explicit reference to such a criterion of connexity, it can be argued to have followed implicitly this logic in its *ratio decidendi*.

Thus, in the PNR judgement, the Court introduced a number of elements on which the connexity criterion is implicitly based. These elements can be traced in the following passages of the judgement:

"While the view may rightly be taken that PNR data are initially collected by airlines in the course of an activity which falls within the scope of Community law, namely sale of an aeroplane ticket which provides entitlement to a supply of services, the data processing which is taken into account in the decision on adequacy is, however, quite *different in nature*. As pointed out in paragraph 55 of the present judgment, that decision concerns not data processing *necessary for* a supply of services, but data processing regarded as *necessary for* safeguarding public security and for law-enforcement purposes…The Court held in paragraph 43 of *Lindqvist*, which was relied upon by the Commission in its defence, that the activities mentioned by way of example in the first indent of Article 3(2) of the Directive are, in any

[23] The connexity criterion is also used in constitutional theory to examine whether the provisions and measures implemented are directly related to the causes that support the declaration of the State of Emergency. Besides, it is used as a means to treat rights equally which are not constitutionally guaranteed, but are inseparably linked with those fundamental rights that are guaranteed by the Constitution (see Jàcome, 2003). The present conceptualisation of connexity is substantially different, however.

event, activities of the *State or of State authorities* and unrelated to the fields of activity of individuals. However, this does not mean that, because the PNR data have been collected by *private operators for commercial purposes* and it is they who arrange for their transfer to a third country, the transfer in question is not covered by that provision. *The transfer falls within a framework established by the public authorities that relates to public security* (paragraphs 57 and 58 of the judgement, emphasis added).

The argument can be made that the Court implicitly derived two elements that serve the purpose of defining the criterion of connexity: a) the *purpose (objective)* and b) the *agent*. These elements are closely linked in the case under consideration, so that they could be said to have a cumulative effect.

Thus, the first element of the connexity criterion lies in the "*difference of nature"* between data processing activities: when such activities are *necessary for* a supply of service, or, more generally, for a market-related purpose, they should be included in the framework of governance. Whereas when the nature of data-processing is orientated towards the objective of public security and law enforcement, it should be conceptualised as falling in the framework of government.

What is most important, in addition, is the second element of the connexity criterion, introduced in the above-mentioned passage of the judgement, which concerns the *type of agent* responsible for the data processing operation: the Court appears to abandon its finding in the *Lindqvist* judgement, namely that it is only the state or its authorities that determine the characterisation of data processing as connected with government. Instead, it opts for a *functional* conceptualisation of the agent, by means of dissociating the agent initially responsible for the data collection and the commercial, i.e. market-related, purposes pursued, from the subsequent processing of the same data, which takes place in a framework that has been established for public security purposes and is conducted by public authorities themselves.

Consequently, in security matters the Court does not examine the agent who is charged with the responsibility of the execution of the relevant task, but the agent who holds the decisive power. In this case, it is irrelevant that it was private companies that were responsible for the collection of the PNR data; the essence of the matter, according to the Court, is that the processing is a prerogative of the US public authorities, which have the decisive authority in respect of the data processing.

Thus, the PNR judgement is notable in that the Court combined, on the one hand, the objective ("necessary for…") of the activity under consideration, with a functional approach to the type of the agent that is responsible, on the other.

The above-mentioned elements, which were combined in a Court judgement for the first time, are used for the establishment of the connexity criterion: in this case, the criterion takes the form of a substantial examination of the contested activities, in order to determine the type of governing which is applicable.

However, it should be underlined that, whereas the European Court of Justice did formulate the elements for the establishment of the connexity criterion, at least implicitly, it is equally important that this formulation was articulated in essentially political terms. In other words, the Court did not establish these elements by means of legal reasoning, but rather in a substantially abstract manner.

The implications of this observation are important: the connexity criterion, at least in the way it was approached by the ECJ in the PNR case, reveals an orientation towards the distinction between governance and government, which is political in nature. Therefore, it may also be

argued that the content of the criterion remains vague and cannot be adequately conceptualised in legal terms.

The contribution, then, of this judgement was, on the one hand, the abstract determination of criteria for the choice between the two types of governing -governance/government- as well as the level of protection afforded to the individual's fundamental rights in the framework of each type of governing. On the other hand, it has been made clear from the above, that the choice of legal basis and consequently the choice of pillar were significant but were not the primary issue at stake.

Further, the annulment of the PNR agreement on the grounds of the lack of Community competence, and the subsequent finding that the exchange of data in the framework of this agreement falls outside the field of (European Community) governance, does not mean, on the other hand, that this exchange belongs exclusively to the realm of government, in the way a traditional security measure in the field of external security does. This is due to the hybrid nature of internal security matters, which lie between governance and government. The latter is one more reason that explains the importance of the criterion of connexity.

Data of a personal nature should also be protected in the field of internal security and the individual should definitely not be left in a legal vacuum. The reference to the ECHR at the beginning of the judgement indicated, in this respect, the lack of competence of the European Community and its inadequacy to provide a *comprehensive* data protection regime for EU citizens. Indeed, beyond the first pillar, no instruments of a legal nature equal to that of Directive 95/46 exist and the jurisdiction of the Court in such matters is very limited. On the other hand, data protection rules and provisions do exist in the constitutional framework of member states (state government), even if they are fragmented and not harmonised, while it is also rules of public international law (ECHR) that are primarily applicable. The mention of article 8 ECHR also serves the purpose of showing that the exchange of data in the field of security complies with specific rights guaranteed by the ECHR, and especially the right to privacy and the right to safety.

It is also important to note the relevance of the above-mentioned elements of the connexity criterion for the principle of availability, so that it can be determined under which conditions the information will freely move from one member state to the other. In this way, it will be determined when the free movement of information will be subjected to the Data Protection Regime of European governance and in which cases it will be treated under the fragmented data protection rules of the different databases in the field of internal security.

In the realm of state government, the fact is that the information circulating among the law enforcement authorities is ruled by secrecy while, on the other hand, the individual does not acquire a sufficient level of protection with appropriate legal remedies and procedural rights (right of access, rectification, erasure or blocking) against the discretionary power of the law-enforcement agencies in the field of security.

This is the reason why the EDPS has suggested, in this context, the introduction of a fundamental principle, that of the "continuity of safeguards", which means that the existing protection and safeguards of one member state should be preserved when information is being passed to other member states, according to the principle of availability (Hustinx, 2006a).

It is, in light of the above, an issue of concern, in general terms, for the EU citizen/individual, that the institutional scheme of the EU, as exemplified in the concept of governance, cannot provide adequate safety and a solid legal framework for its citizens, against the demands of security involved in government, notably by granting an effective *right of access to court*. What is considered to belong to the realm of government, is characterised as *arcana imperii*, and normally lies beyond the jurisdiction of judicial authorities, thus leaving the individual

unprotected. This concern is intensified in the case of the PNR: the PNR judgement made clear the rivalry and the tension which exists between the right to safety, as fully guaranteed in the field of European Community governance, on the one hand, and Security in the field of State government, on the other.

In this way, the Court also made clear that the individual's right to data protection in relation to the PNR agreement is more closely connected to personal safety and public security as a matter of common concern for the EU, and not so much with the rivalry that exists between the economic freedoms and the right to privacy with the free flow of information. In line with the connexity criterion, the PNR judgement is clearly an instance of conflict of the freedoms of the individual with the demands of government, rather than merely a rivalry between freedoms themselves.

4. Concluding remarks

The creation of an internal market without frontiers and the free movement of persons leads to an increasing flow of personal data, so that any obstacle to the flow of data on the grounds of their protection would indirectly impede the functioning of the market (governance).

The harmonisation of the legal framework in the field of data protection, leads to a uniform European regime, which allows personal data to circulate freely and this facilitates free movement of persons and the smooth functioning of the Internal Market. This approach acknowledges that the primary objective behind the establishment of data protection is Internal Market considerations. In this context, it is clear that data protection is not an objective *per se* but is an instrument that aims at ensuring free movement. On the other hand, as has been indicated, the right to data protection has gradually acquired an autonomous protection as a fundamental right.

The concept of rivalry, drawn from political philosophy but acquiring a distinct meaning in legal terms and in our research framework, is the other important variable; this rivalry is inherent in the relationship between different freedoms in the framework of liberalism. The terms of the rivalry between data protection and other freedoms, notably market freedoms and the freedom of expression, were examined. Most importantly, the paradigm of EU governance arguably constitutes, given its historic novelty, a major illustration of this concept of rivalry.

In this framework, the importance of the PNR judgement of the European Court of Justice was highlighted and analysed. This judgement illustrated the significance of the connexity criterion as a switch mechanism between governance and government. The importance of this criterion is demonstrated by the fact that the elements that the Court implicitly argued that connexity is based upon, namely the objective of the activity and the functional approach to the agent, are capable of being scrutinised by the Court.

Nevertheless, it should be noted that this scrutiny is made in abstract terms, characteristic of a reasoning of a political nature, rather than in the specific manner an essentially legal reasoning would imply: this observation may render the use of the connexity criterion problematic.

Furthermore, the implementation of the connexity criterion in the field of the rights of the individual indicates that although the protection of fundamental rights is taken into account by the European institutions, the European Union legal system has not provided for an effective legal instrument to ensure that protection. By transferring the PRN agreement from the field of Community governance to a state between governance and government in security matters, the Court created a loophole in the right of data protection of the individual. In this state of "mixed governance" (between governance and government). The real problem is the access of the individual to the ECJ, which is problematic. The connexity criterion demonstrates that even the

eventual abolition of the pillar framework would not by itself be adequate. While it would bring any future PNR decision within the first pillar and would thus subject it to the Data Protection Directive, as the Court stated, the exceptions of public security, defence, state security and activities of the state in areas of criminal law would still apply, so that the individual might still not be subject to data protection.

Consequently, the communautarisation of the third pillar is not a panacea. The problem is not so much that of a choice of pillar but of the kind of institutional protection.

As a final note, it should be said that the only possible adequate protection of individuals, from a European perspective, would perhaps be the *legally binding nature of the European Charter of Fundamental Rights,* which would also form a *common constitutional framework* for the European institutional structure.

Bibliography

Adam, A. (2006), "L'échange de données à caractère personnel entre l'Union Européenne et les Etats-Unis: Entre souci de protection et volonté de coopération", *Revue Trimestrielle de Droit Européen*, 42(3): 411-437.

Alder, J. (2002), *General Principles of Constitutional and Administrative Law*, Basingstoke: Palgrave.

Andenas, M. and S. Zleptnig (2003), "Surveillance and Data Protection: Regulatory Approaches in the EU and Member States", *European Business Law Review*, 14(6):765-813.

Bygrave, L.A. (2004), "Privacy Protection in a Global Context – A Comparative Overview", *Scandinavian Studies in Law*, 47: 319-348.

Cannataci, J.-A. and J.-P. Mifsud-Bonnici (2005), "Data Protection Comes of Age: The Data Protection Clauses in the European Constitutional Treaty", *Information and Communications Technology Law*, 14(1): 5-15.

Charlesworth, A. (2000), "Clash of the Data Titans? US and EU Data Privacy Regulation", *European Public Law*, 6(2): 253-274.

Coudray, L. **(**2004), "Case C-101/01, *Bodil Lindqvist*", *Common Market Law Review*, 41, pp. 1361-1376.

Delgado, J.B. (2006), "Towards the Creation of a European Area of Freedom, Security and Justice: Where Security and Data Protection Go Hand-in Hand", speech delivered at the First International Conference on Data Protection in Plurinational and Federal States in Barcelona, Spain, 4-5 October.

European Commission (2003), *First report on the implementation of the Data Protection Directive*, COM (2003) 265 final, Brussels.

Fligstein, N. and A. Stone Sweet (2002), "Constructing Polities and Markets: An Institutionalist Account of European Integration", *American Journal of Sociology*, 107(5): 1206-1243.

Foucault, M. (2004), *Naissance de la biopolitique, Cours au Collège de France (1978-1979)*, Paris: Seuil/Gallimard.

Gerber, D.J. (1998), *Law and Competition in Twentieth Century Europe: Protecting Prometheus*, Oxford: Oxford University Press.

Gilmore, G. and J. Rijpma (2007), "Joined cases C-317/04 and C-318/04", *Common Market Law Review*, 44, pp. 1081-1099.

Gray, J. (2000), *Two Faces of Liberalism*, New York: The New Press.

Guild, E. and E. Brouwer (2006), *The political life of data: The ECJ Decision on the PNR Agreement between the EU and the US*, CEPS Policy Briefs, No. 109, Centre for European Policy Studies, Brussels.

Gunasekara, G. (2007), "The 'final' privacy frontier? Regulating trans-border data flows", *International Journal of Law and Information Technology*, 15.

Halpin, A. (1997), *Rights and Law Analysis Theory*, Oxford: Hart Publishing.

Hijmans, H. (2006), *The third pillar in practice: coping with inadequacies. Information sharing between Member States*, discussion paper for the meeting of the Netherlands Association for European Law (NVER).

Hustinx, P.J. (2006), *Human Rights and Public Security: Chance for a Compromise, or Continuity of safeguards?*, Conference on Public Security and Data Protection, Warsaw, May (Hustinx, 2006a).

Hustinx, P.J. (2006), *A Framework in Development: Third Pillar and Data Protection*, "Personal Data Protection Yesterday, Today, Tomorrow", Warsaw (Hustinx, 2006b).

Jàcome, J.G. (2003), "The political and legal struggle for the determination of economic, social and cultural rights: the Colombian and International contexts", *Universitas* 106 (www.javeriana.edu.co/Facultades/C_Juridicas/pub_rev/documents/3GonzalezJacome.pdf).

Kelly, P. (2006), "The Social Theory of Anti-Liberalism", *Critical Review of International Social and Political Philosophy*, 9(2): 137-154.

De Leon, P.M. (2006), "The fight against terrorism through aviation: Data protection versus data production", *Air and Space Law*, 31: 320-330.

Maiani, F. (2002), "Le cadre réglementaire des traitements de données personnelles effectués au sein de l'Union européenne", *Revue Trimestrielle de Droit Européen*, 38(2): 283-309.

Mariatte, F. (2006), "La sécurité intérieure des États Unis…ne relève pas des compétences externes des Communautés", *Europe*, July, 4-8.

Poullet, Y. (2006), "The Directive 95/46/EC: Ten Years After", *Computer Law and Security Report*, 22: 206-217.

Rawls, J. (1971), *A Theory of Justice*, Cambridge, Massachusetts: Belknap Press of Harvard University Press.

Scandamis, N. and K. Boskovits (2006), *Governance as security*, Athens: Ant. No. Sakkoulas-Bruylant.

Scharpf, F. W. (1996), "Negative and Positive Integration in the Political Economy of European Welfare States", in G. Marks, F. Scharpf, P. Schmitter and W. Streeck (eds), *Governance in the European Union*, London: Sage.

About CHALLENGE

The familiar world of secure communities living within well-defined territories and enjoying all the celebrated liberties of civil societies is now seriously in conflict with a profound restructuring of political identities and transnational practices of securitisation. CHALLENGE (Changing Landscape of European Liberty and Security) is a European Commission-funded project that seeks to facilitate a more responsive and responsible assessment of the rules and practices of security. It examines the implications of these practices for civil liberties, human rights and social cohesion in an enlarged EU. The project analyses the illiberal practices of liberal regimes and challenges their justification on the grounds of emergency and necessity.

The objectives of the CHALLENGE project are to:

- understand the convergence of internal and external security and evaluate the changing character of the relationship between liberty and security in Europe;
- analyse the role of different institutions in charge of security and their current transformations;
- facilitate and enhance a new interdisciplinary network of scholars who have been influential in the re-conceptualising and analysis of many of the theoretical, political, sociological, legal and policy implications of new forms of violence and political identity; and
- bring together a new interdisciplinary network of scholars in an integrated project, focusing on the state of exception as enacted through illiberal practices and forms of resistance to it.

The CHALLENGE network is composed of 21 universities and research institutes selected from across the EU. Their collective efforts are organised under four work headings:

- *Conceptual* – investigating the ways in which the contemporary re-articulation and disaggregation of borders imply a dispersal of practices of exceptionalism; analysing the changing relationship between new forms of war and defence, new procedures for policing and governance, and new threats to civil liberties and social cohesion.
- *Empirical* – mapping the convergence of internal and external security and transnational relations in these areas with regard to national life; assessing new vulnerabilities (e.g. the 'others' targeted and critical infrastructures) and lack of social cohesion (e.g. the perception of other religious groups).
- *Governance/polity/legality* – examining the dangers to liberty in conditions of violence, when the state no longer has the last word on the monopoly of the legitimate use of force.
- *Policy* – studying the implications of the dispersal of exceptionalism for the changing relationship among government departments concerned with security, justice and home affairs, along with the securing of state borders and the policing of foreign interventions.

The CHALLENGE Observatory

The purpose of the CHALLENGE Observatory is to track changes in the concept of security and monitor the tension between danger and freedom. Its authoritative website maps the different missions and activities of the main institutions charged with the role of protection. By following developments in the relations between these institutions, it explores the convergence of internal and external security as well as policing and military functions. The resulting database is fully accessible to all actors involved in the area of freedom, security and justice. For further information or an update on the network's activities, please visit the CHALLENGE website (www.libertysecurity.org).

An Integrated Project Financed by
the Sixth EU Framework Programme