1. Introduction

Since the Paris terrorist attacks of January 2015, counter-terrorism issues have reached the top of the political agenda, both in the Member States most concerned and at EU level.

At the same time, the rapid technological developments, which allow personal data to be processed on an unprecedented scale, and the need to assure an high level of protection of the fundamental rights, such as the right to respect for private life and the right to the protection of someone's personal data, called for the adoption of a common general framework at the European level. Among the main measures under debate are the creation of an EU-wide system which would enable Passenger Name Records (PNR) data transfer to law enforcement agencies and the reform of the EU data protection system. The objectives of the latter are to ensure that personal data of victims, witnesses and suspects of crimes are duly protected and to facilitate cross-border cooperation in the fight against crime and terrorism.

Before the Treaty of Lisbon came into force, fragmentation, lack of adequate independent oversight and monitoring as well as lack of intra-agency data protection cooperation were the characteristics which emerged from the general picture of supervision over data protection, when it came to personal data processing in the law enforcement and criminal area in the EU. The most relevant development in EU data protection pursuant the Lisbon Treaty is Article 16 TFEU, which replaces and expands on the old Article 286 EC, establishing an independent individual right to data protection. The second novelty introduced by the Treaty of Lisbon pertains to the data protection regime for police and judicial cooperation in criminal matters as provided for by Article 87(2)(a), of the TFEU. This new provision now allows for adoption, by means of ordinary legislative procedure, of measures concerning the collection, storage, processing, analysis and exchange of relevant information, except where such data is processed in the context of operational police cooperation.

Using Article 16, Article 87(2)(a) and Article 82(1)(1) TFEU as legal bases, the European legislator adopted a Regulation and a Directive on the so-called EU data protection package

and the EU Passenger Name Record (PNR) Directive, which were published in the EU Official Journal on 4 May 2016. The aim of this contribution is to further the legal debate on the balance between the rights of data protection and the security needs in the fight against terrorism and other serious crimes. Based on an initial analysis of the two directives mentioned above this contribution will examine the questions at issue and underline the shortcomings that still exist.

2. Legislative background

The EU data protection reform package, comprising the Data Protection Regulation (for some considerations see Bottino, in this *Review*) and the Directive for the criminal and justice sector, was envisaged for the first time as early as 2009 with the release of a public consultation by the Commission that led to the first Commission position paper published in 2010. Subsequently the Commission released its first drafts on the Data Protection Regulation and the Directive for data protection in the police and justice sectors in early 2012. Over the following years their text was processed by the Council and the Parliament. The final compromise text of the Directive for data protection in the police and justice sectors was published on 15 December 2015, as approved by the Parliament. On 14 April 2016, at its Plenary meeting, the European Parliament announced the approval of the Council's first readings. The President of the Parliament and the Dutch Minister of Justice, on behalf of the Council, signed the legal instruments on 27 April 2016, formally adopting them. The Data Protection Regulation will enter into force on 24 May 2016, but shall apply as of 25 May 2018. The Directive for data protection in the police and justice sectors enters into force on 5 May 2016 and EU Member States have to transpose it into their national laws by 6 May 2018.

The Data Protection Regulation will replace the current Data Protection Directive, dating back to 1995.It regulates all personal data processing activities and is designed to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States. The new Directive for data protection in the police and justice sectors replaces the

2008 Framework Decision and lays down a harmonised legal framework to facilitate the free flow of personal data between competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties within the Union and the transfer of such personal data to third countries and international organisations, while ensuring a high level of protection of personal data. Before the adoption of the Directive for data protection in the police and justice sectors fragmentation was the main characteristic of the legal framework in the criminal justice and law enforcement area. Protection of personal data was regulated differently depending on the policy area concerned – based on whether the policy area concerned lay within the competence of the Community or not. The general legal framework formulated in Directive 95/46/EC, was complemented by other regimes valid for specific sectors, such as Regulation (EC) No 45/2001 that regulates the data processing by the European Union institutions and bodies and Directive 2002/58/EC that regulates privacy in the electronic communications sector.

The 2008 Framework Decision was also adopted for regulating the processing of personal data in the European space. The data protection within the ambit of criminal law was also regulated by Council Decision 2008/616/JHAconcerning, in particular, the deepening of the cross-border cooperation in the fight against terrorism and cross-border criminality, and by Council Framework Decision 2006/960/JHA, which aimed at simplifying the exchange of information between the repressive services of the Member States.

Numerous other texts relating to data protection and information exchange were promulgated in the European penal sector; reference is made, in particular, to the Council Decision 2005/876/JHA on the exchange of information extracted from criminal records and to the Decision 2007/413/JHA**,** as well as to different regulations pertaining to the Schengen Information System or the Visa Information System. In addition to this multitude of texts regulating personal data processing and protection in the European criminal field, the numerous EU agencies operated, in practice, under their own, individual frameworks with little regard for harmonization among their personal data processing practices. The basic text which supposedly set the common standards in the criminal justice and enforcement

area, the 2008 Data Protection Framework Decision, could not be considered a satisfying general framework. Its scope was substantially restricted, as it only applied to the exchanges of data between the investigative authorities of the Member States and not to the processing of data in the repressive domain occurring within their national territories. The Commission itself has expressly acknowledged that the limited scope of the 2008 Data Protection Framework Decision already leads to legal and practical shortcomings in the protection of personal data at EU level as well as to different levels of data protection in different Member States, creating legal uncertainty. In addition, the fact that it was essentially a pre-Lisbon Council instrument that had to achieve unanimity among Member States and conform to the pillar system, was also of relevance considering that its principles were worded almost to the point of voluntary application. Finally, the protection of individual rights, such as the right to information, access, rectification or erasure of personal data, was inadequate and gave unbalanced priority to the needs of security-related processing. As will be discussed below, the Directive for data protection in the police and justice sectors aims at remedying all these deficiencies.

On 14 April 2016 the Parliament also adopted at first reading the proposal for a Directive on European Passenger Name Records (PNR). The idea is not new: the possibility of having an EU-wide PNR scheme has been discussed since 2007, when the Commission proposed a Council Framework Decision on this issue. However, following the Lisbon Treaty's entry into force on 1 December 2009, the Commission proposal, which had not been adopted by the Council by that date, became obsolete. Subsequently the Commission replaced the proposal for a framework decision with one for a Directive on European Passenger Name Records (PNR). The legislative procedure became blocked when the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) rejected the proposal in April 2013, questioning its necessity and proportionality. However, the Parliament's plenary in 2013 and the Council in 2014 decided to move forward with it. On 21 April 2016 the Council endorsed the Parliament's position adopted at first reading, thus concluding the legislative procedure on this proposal and, finally, on 27 April 2016 the Directive on European Passenger Name Records (PNR) was signed by the President of the Parliament, and by Dutch Minister of Defence on behalf of the Council. The Member States are required to

transpose the Directive on European Passenger Name Records (PNR) by 25 May 2018.

The Directive on European Passenger Name Records (PNR) sets out harmonised rules on collection and processing of PNR data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. In accordance with the Directive on European Passenger Name Records (PNR), the airlines will be obliged to provide EU countries with their passengers' data in order to help the authorities to fight terrorism and serious crime, taking fully into consideration the right to the protection of personal data and the right to non-discrimination. The Directive on European Passenger Name Records (PNR) is to apply to "extra-EU flights", but Member States may also extend it to "intra-EU" ones, provided that they notify the Commission.

3. Contents of the Directive for data protection in the police and criminal justice sectors

The Directive for data protection in the police and justice sectors has been adopted in order to ensure a high level of data protection while improving cooperation in the fight against terrorism and other serious crime. After the Treaty of Lisbon came into effect, the protection of natural persons in relation to the processing of personal data is expressly recognized as a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union ('the Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her. However, Declaration 21, annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon, acknowledges that the specific nature of the security field merits special legislative treatment. According to the European institutions' approach, processing in the police and criminal justice context should be differentiated from all other personal data processing. The European legislator has *prima facie* differentiated between the fields by choosing two different types of legal instruments (regulation and directive). The protection and free movement of data processed by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties has been regulated

by a directive, allowing Member States a certain level of flexibility while incorporating it into their respective national laws, whereas a regulation was adopted for regulating general processing of personal data. In this way the EU acknowledged a two-speed process in the effort to harmonise all EU personal data processing.

One of the main differences between Data Protection Regulation (regulating data protection in general) and Directive for data protection in the police and justice sectors (regulating data protection within the ambit of criminal law) lies essentially in the rights of information and of access to personal data. If such rights provided for in the Data Protection Regulation were exercised to the fullest possible extent within the ambit of criminal law, it would effectively make criminal investigations impossible. That is why special security-related needs have to be accommodated in the text of the Directive for data protection in the police and justice sectors. The Directive for data protection in the police and justice sectors aims at balancing the data protection objectives with the security policy objectives and, while certainly contributing to the creation of a less fragmented general framework, it doesn't solve all the shortcomings which had emerged before its adoption.

The Directive for data protection in the police and justice sectors comprises ten chapters. The first five chapters describe the scope of the Directive, the general principles relating to processing of personal data, the rights of the data subject, the obligations of the controllers and the processors, the technical and organisational measures to ensure security of personal data, which have to be adopted by them, and, finally, the regulation of transfer of personal data to third countries or international organisations. The second part of the Directive for data protection in the police and justice sectors (from chapter VI to chapter VIII – the final two chapters are about implementing acts and final provisions) regulates the status, tasks and powers of the independent supervisory authorities and establishes the right to lodge a complaint with a supervisory authority, the right to an effective judicial remedy against a controller or processor and the right to compensation for any person who has suffered material or non-material damage as a result of an unlawful processing of personal data.

As far as the scope of the Directive for data protection in the police and justice sectors is concerned, despite the apparent broad approach of the Directive for data protection in the police and justice sectors, its actual scope is more limited than it seems at first glance. First, its scope is restricted to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, not covering personal data processing in the context of criminal court proceedings. In other words, where the personal data are processed in the course of a criminal investigation and court proceedings in criminal matters, Member States may provide for the exercise of the right to information, access and rectification or erasure of personal data to be carried out in accordance with their national law (Recitals 20, 49 and 107 and Article 18). In this respect, therefore, the real added value of the Directive for data protection in the police and justice sectors depends on its implementation in national law and the willingness of national courts to ensure that the Directive for data protection in the police and justice sectors is applied in a uniform manner across the EU. Second, the Directive for data protection in the police and justice sectors does not regulate the processing of data in the course of an activity which falls outside the scope of Union law (Article 2(3)). That provision has been interpreted (Recital 14) as relating to activities concerning national security, activities of agencies or units dealing with national security issues and the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU. The formulation of that provision is therefore partially contradictory with the inclusion within the purposes set out in Article 1 of safeguarding against and the prevention of threats to public security. Even if it is not defined in the text, the concept of activities concerning public security seems to include the activities of safeguarding against and prevention of threats to public security. Until the Court of Justice interprets it, the scope of the Directive for data protection in the police and justice sectors depends again on the interpretation that national courts will give to the expression “activity which falls outside the scope of Union law” and of the way the Member States decide to implement the Directive for data protection in the police and justice sectors. Finally, the Directive for data protection in the police and justice sectors does not apply to the processing of personal data by the Union institutions, bodies, offices and agencies. In other words, the data processing by the European institutions and

bodies will continue to be governed by Regulation n. 45/2001, which has not been amended yet. Unlike the 2008 Framework Decision, the Directive for data protection in the police and justice sectors will actually regulate processing of personal data by Member States and not only intra-Member States exchanges of data, but it is still far from ensuring maximum harmonization of data processing in the criminal field. That is confirmed by Article 1(3), which states that the Directive for data protection in the police and justice sectors shall not preclude Member States from providing higher safeguards than those established in the Directive for the protection of the rights and freedoms of the data subject.

Having established the scope of the Directive for data protection in the police and justice sectors, our analysis will now turn to the different articles on data protection and connected rights covered by the Directive for data protection in the police and justice sectors. Several principles relating to processing of personal data are the same as those enshrined in the Data Protection Regulation. However, because of the peculiarity of the field, while the basic data protection principles are included in its text, some of those set out in the Data Protection Regulation are not included in the Directive for data protection in the police and justice sectors. For example, as far as the characteristics the data should have in order to be processed by the competent authorities are concerned, it may be observed that not all the conditions required by the Data Protection Regulation in order to consider the data processing lawful and fair need to be met. The consent of the data subject, for instance, is not a necessary condition for processing personal data by the competent authorities when they order natural persons to comply with requests made in order to perform the tasks of preventing, investigating, detecting or prosecuting criminal offences (Recital 35). Where the data subject is required to comply with a legal obligation, the data subject has no genuine and free choice, so that the reaction of the data subject could not be considered to be a freely given indication of his or her wishes. Whether the correct balance between individual data protection and the interests of the police and criminal justice process is respected depends once again on how Member States implement the exemptions contained in the Directive for data protection in the police and justice sectors. The latter also includes limitations on the rights to information, access and rectification thus attempting to strike a balance between the individual right to data protection and the processing interests and

concerns of the police and other law enforcement-related agencies; if exercised to their fullest extent these rights would undermine much of the work done by the police and the competent authorities within the criminal justice system. The level of flexibility accorded to this end depends once more on the breadth of national legislative measures implementing the Directive for data protection in the police and justice sectors, which can restrict, wholly or partly, the data subject's right in order to assure the due performance of investigations and protect national security, as set out in Article 15.

The final important element of the EU data protection model refers to the establishment of an independent supervisory authority entrusted with the task of monitoring the application of data protection law within the respective Member State. The Directive for data protection in the police and justice sectors permits assignment of this role to the authority established for similar purposes under the Data Protection Regulation. Data Protection Authorities, as independent supervisory authorities, have been already introduced by Directive 95/46 and have become the basic mechanism for enforcement and monitoring of data protection in the EU today. An ostensibly significant change brought by the EU data protection reform package to the EU data protection systems concerns the replacement of the old Article 29 Data Protection Working Party by the European Data Protection Board. The Board will replace the Article 29 Working Party but, as far as the Directive for data protection in the police and justice sectors is concerned, only apparently since it will essentially retain the same powers as. In this respect it should be noted that, while in the Data Protection Regulation the EU legislator assigned a central role to the Board, especially in the consistency mechanism, no such role is provided for in the Directive for data protection in the police and justice sectors. However, in the police and criminal justice context conflicts pertaining to processing of personal data may arise between the Data Protection Authority and the judicial authorities in order to determine if Data Protection Authority may monitor processing done by judicial authorities. The Directive for data protection in the police and justice sectors, in order to limit the discretionary power of the Member States, provides that the processing of data by judicial authorities must not be affected by its provisions when acting within their judicial capacity. In spite of that it should be noted that Article 1 permits Member States to maintain a higher level of data protection which could ultimately be a

cause of problems.

With regard to the transfer of personal data to third countries or international organisations the Directive for data protection in the police and justice sectors requires that personal information be allowed to be transmitted by an EU Member State to a third country only if the Commission has decided that the recipient ensures an "adequate" level of protection. The concept of adequate level of protection has been defined by the Court of Justice in the *Schrems case* (ECLI:EU:C:2015:650, para 73; see Crespi's case-note in this Review), as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union. The Court of Justice has also stated that the Commission's discretion as to the adequacy of the level of protection ensured by a third Country should be limited,considering, first, the important role played by the protection of personal data in the light of the fundamental right to respect for private life and, secondly, the large number of persons whose fundamental rights are liable to be infringed where personal data is transferred to a third country without ensuring an adequate level of protection (*Scherms*, para 78, and*Digital Rights Ireland and Others* (ECLI:EU:C:2014:238), paras 47 and 48)**.** In that respect it should be underlined that data processing in the police and criminal justice context was a field left until now outside EU law; that's why practically all Member States have bilateral agreements with third countries permitting the exchange of personal data for law enforcement related purposes, notwithstanding any "adequacy" finding in respect of the recipients' data protection safeguards. Therefore, here again the Directive for data protection in the police and justice sectors had to maintain a careful balance between, on the one hand, the requirements of police and criminal justice work and existing bilateral agreements and, on the other, the requirement for an increased level of personal data protection. The Directive for data protection in the police and justice sectors does little to affect bilateral agreements already in place. Admittedly this wording automatically turns all bilateral agreements into definite term ones, in need of amendment to match the Directive's standards immediately when the first opportunity arises. However, if Member States – that are called upon, but not obliged to actively seek to amend bilateral agreements in the foreseeable future – do not take

action, the prolonged existence of those bilateral agreements which apply lower standards than the Directive for data protection in the police and justice sectors could undermine the whole international data transfer edifice. The regulation of profiling deserves a separate mention. As we shall see in the next section when examining the Directive on European Passenger Name Records (PNR), profiling is especially problematic in the police and criminal justice context, because if profiles are misused they can lead to stressful situations for individuals, who could be put under surveillance or arrested on the grounds of automated processing of personal data. The compatibility with the presumption of innocence can be questioned. It is necessary to underline here that in this regard the Directive for data protection in the police and justice sectors provides substantial and procedural safeguards. Member States are prohibited from providing for a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject. The Directive also stresses that profiling resulting in discrimination against natural persons shall be prohibited (Article 11).

4. Contents of the Directive on European Passenger Name Records (PNR)

The Directive on European Passenger Name Records (PNR) aims at regulating the transfer of passenger name record (PNR) data of passengers of extra-UE flights from air carriers to the Member States, as well as the processing of such data, including its collection, use, retention and its exchange between Member States. The Directive on European Passenger Name Records (PNR) establishes that the scope is limited to the PNR data collected for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. As far as the definitions of serious crimes is concerned, it should be highlighted that the list of offences contained in the Annex II is broad and much wider than the list of serious crimes set out in Article 83(1) TFEU. The choice of Articles 82(1)(d) and 87(2)(a) TFEUas legal bases for the adoption of the Directive on European Passenger Name Records (PNR) is a clear sign of the EU legislator’s willingness to harmonise Member States’ provisions concerning the retention of certain data which are generated or processed by air carriers to

enhance the cooperation between police and judicial authority and to ensure that the data would be available for the purpose of the investigation, detection and prosecution of terrorist offences and serious crime.

The lack of any mention of the protection of fundamental rights in the Directive on European Passenger Name Records (PNR) raises concerns as to its impact on fundamental rights and questions whether such scheme is indeed indispensable to effectively address serious crime and terrorism. The rights at stake include the right to privacy (Article 7 of the Charter), the right to data protection (Article 8 of the Charter), the right to non-discrimination (Article 21 of the Charter), with indirect discrimination being more likely than direct discrimination given the prohibition on processing sensitive data under the Directive on European Passenger Name Records (PNR), and, in case of extension of the Directive on European Passenger Name Records (PNR) to intra-EU flights, the right to free movement, which may be restricted only on grounds of public policy or public security, provided that the restrictions comply with the principle of proportionality. Recently, fundamental rights and, in particular, the principles of proportionality and necessity, have been debated in the context of the judgment of the Court of Justice in *Digital Rights Ireland*. The Court formulated a series of requirements, arguably valid for all security measures interfering with the protection of personal data, especially if they provide for data retention. In particular it stated that the retention of and access by the competent authorities to data represents an interference with the right to privacy and the right to protection of personal data set out in Articles 7 and 8 of the Charter. The Court also affirmed that, in order to respect Article 52 of the Charter, the limitations to the aforementioned rights must be provided for by law, respect the essence of those rights and, subject to the principle of proportionality, must be necessary and genuinely meet objectives of general interest recognised by the Union. It must be held that the retention of data for the purpose of allowing the competent national authorities to have possible access to those data, as required by Directive on European Passenger Name Records (PNR), satisfies an objective of general interest. The fact that the fight against international terrorism in order to maintain international peace and security constitutes an objective of general interest is apparent from the case-law of the Court (see *Kadi* (ECLI:EU:C:2008:461), para 363, and *Al-Aqsa*

(ECLI:EU:C:2012:711), para 130). The same is true of the fight against serious crime in order to ensure public security (*Tsakouridis* (ECLI:EU:C:2010:708), paras 46 and 47). However, in order to ascertain whether the limitations to fundamental rights included in the Directive on European Passenger Name Records (PNR) are lawful or not it is necessary to evaluate if they are necessary and proportionate. Consequently, the Directive on European Passenger Name Records (PNR) must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data (*Digital Rights Ireland*, para 54; see, by analogy, as regards Article 8 of the ECHR, *Liberty and Others v. the United Kingdom*(Appl. No. 58243/00, 2008), paras 62 and 63, *Rotaru v. Romania* (Appl. No 28341/95, 2000), paras 57 to 59, and *S. and Marper v. the United Kingdom* (Appl. Nos 30562/04 and 30566/04, 2008), para 99). In this regard it should be noted that, in spite of the fact that Recital 7 of the Directive on European Passenger Name Records (PNR) states that the creation and application of assessment criteria should be limited to terrorist offences and serious crime for which the use of processing of PNR data is relevant, the Directive covers, in a generalised manner, all persons as well as extensive personal data on each and every passenger of extra-EU flights. It affects all passengers of extra-UE flights, even when there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. This kind of "mass surveillance tool" (De Hert and Papakonstantinou) creates doubts about the respect for the principle of presumption of innocence, considering that each passenger is presumed a criminal suspect unless his or her profile hints at the opposite. Another problem with the EU Directive on European Passenger Name Records (PNR) is that it is silent on how profiling is done. The Directive on European Passenger Name Records (PNR) clarifies for how long passenger data can be kept and by whom they may be kept, but the criteria for these delicate profiling operations performed in respect of the data are not set out in the Directive on European Passenger Name Records (PNR). Similarly, the concrete measures that law enforcement agencies are allowed to take on the basis of the results are not adequately specified.

One cause for concern is legal redress, which is also required under Article 16 TFUE. The Directive on European Passenger Name Records (PNR) only refers to the general means of redress laid down "in Union and national law and in implementation of Article 17, 18, 19 and 20 of the Framework Decision 2008/977/JHA" (Article 13), without indicating any specific means of redress. In that regard, it should be noted that, while before the adoption of the Directive for data protection in the police and justice sectors no adequate judicial remedy in case of personal data breaches existed, today the reference to the Directive for data protection in the police and justice sectors ensures the possibility to obtain redress and, where appropriate, compensation in case of infringement of the provisions pursuant to this Directive. Finally, the absence of clear and precise rules on data retention period is evident with regard to the data retention period. Article 12 of Directive on European Passenger Name Records (PNR) requires that data be retained for a period of at least six months, after which it should be made accessible by stripping off the elements, such as name, address and contact details that may lead to the identification of individuals; in this respect no distinction is made on the basis of its possible usefulness for the purposes of the objective pursued or according to the persons concerned. Furthermore, it is indicated that the PNR data should be retained for a period of five years, without a possibility to vary the period of retention based on objective criteria in order to ensure that the period is limited to what is strictly necessary.

Despite the above mentioned critical issues, it should be highlighted that, unlike the Data Retention Directive annulled by the Court, the Directive on European Passenger Name Records (PNR) contains substantive and procedural safeguards relating to the access and subsequent use of the data retained. PNR data should be transferred, stored and analysed only by a specifically created entity, the Passenger Information Unit, and the results of the PNR processing will be transferred to law enforcement authorities only under strict conditions. The choice for the "push" method, under which air carriers transfer ("push") the required PNR data to the authority requesting them, thus allowing air carriers to retain control over what data is provided, instead of the "pull" method, under which the competent authorities of the Member State requiring the PNR data can access the air carrier's reservation system and extract ("pull") a copy of the required PNR data, is another indicator

of the attempt made by the EU legislator to provide procedural safeguards for the data protection.

5. Final remarks

Two important questions arise from the above: does the new Directive for data protection in the police and justice sectors really provide a general data protection framework in the context of criminal law? Is the Directive on European Passenger Name Records (PNR) – in view of the decisions by the Court of Justice – a legitimate instrument to fight terrorism and other serious crimes?

As to the former question, it should be noted that the Directive for data protection in the police and justice sectors seems to have two faces. On the one hand, it is innovative as its scope is now intended to cover all personal data processing undertaken in the context of police and judicial cooperation in criminal matters, regardless of whether the processing takes place within or outside national borders. Criminal law enforcement authorities, therefore, will no longer have to apply different sets of data protection rules depending on the origin of the personal data. Yet, on the other hand, the scope of the Directive for data protection in the police and justice sectors does not cover personal data processing in the context of criminal court proceedings, it does not apply to the processing of personal data by the Union institutions, bodies, offices and agencies. As underlined above, what is meant by criminal court proceedings is not always clear. It depends on Member States (national) policies. The expression “activity which falls outside the scope of Union law” remains likewise unclear. The term can receive different interpretations and does not provide for a clear delimitation of the tasks of the police within the scope of the Directive for data protection in the police and justice sectors. Moreover, the fact that the EU agencies operating within the EU criminal justice and enforcement area are not subject to the rules laid down in the Directive for data protection in the police and justice sectors creates a problem of coordination between the rules established in the Directive for data protection in the police and justice sectors and those contained in each individual legal constitutive text. Thus the real added value of the Directive for data protection in the police and justice

sectors will depend on its implementation in national law and the willingness of the national courts, as well as of the Court of Justice, to ensure that the Directive for data protection in the police and justice sectors contributes to the enhancing of data protection in the EU. That problem arises because of the architecture of the reform package on data protection itself: the establishment of a Regulation and a Directive. The level of protection in the Directive for data protection in the police and justice sectors is much lower than the one laid down in the Data Protection Regulation. The option of a regulation also covering the area of criminal law enforcement was apparently unacceptable for most Member States; that is why finally it was decided to adopt a Directive with the same substance as the Regulation, but subject to the relevant limitations and exceptions, and leaving more space for domestic implementation.

In relation to the first question we can conclude that the Directive for data protection in the police and justice sectors does not provide for a general data protection framework in the context of criminal law because of the nature of the type of act – a directive – chosen, and because the Directive for data protection in the police and justice sectors only contains minimum harmonisation rules which leave wide discretion to the Member States.

Turning our attention towards the second question, it will be recalled that Article 52 of the Charter foresees that any limitation on the rights under Articles 7 and 8 of the Charter must be provided for by law and may be made only if the limitations are necessary and genuinely meet objectives of general interest. In this respect, the jurisprudence of the Court of Justice of the European Union and of the European Court of Human Rights confirms that the law must be sufficiently precise to indicate to citizens in what circumstances and on what terms the public authorities are empowered to gather information on their private lives and make use of it. Such information should "be accessible to the person concerned and foreseeable as to its effects", which means that it must be "formulated with sufficient precision to enable any individual – if need be with appropriate advice – to regulate his conduct". The analysis of the content of the Directive on European Passenger Name Records (PNR) shows that, although some procedural safeguards to protect personal data are introduced, the absence of rules regulating the method of processing data and the fact that are retained

PNR data of even those passengers of extra-EU flights for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crimes, raise questions about the compatibility of the Directive on European Passenger Name Records (PNR) with the respect for human rights. The European Data Protection Supervisor (Opinion of 25 March 2011, para 19) has recalled that the development of such a system raises serious transparency and proportionality issues and that it might lead to a move towards a surveillance society (Opinion of 20 December 2007, para 35). The risk of infringement of several fundamental rights is evident and has not been eliminated by the final text of the Directive on European Passenger Name Records (PNR). It is now up to the Court of Justice to rule on the consistency of the Directive on European Passenger Name Records (PNR) with the fundamental rights enshrined in the Charter.

To conclude, it should be underlined that the right balance between security and data protection can be attained only by establishing a common framework of reference, in a regulation, for the data protection system in the criminal field. The risk of infringement of data protection rules is higher when there are 28 different implementing national systems. Respect for data protection principles affirmed by the Court of Justice becomes more difficult in that situation.

Considering that Member States turned down the possibility of adopting such unified rules in a regulation, we should consider if the Member States are willing to adopt such a regulation in a field so strictly connected with State sovereignty as criminal law. It can be hoped that the inadequacies of the directives considered herein will make the EU legislator take this step forward.