Data protection policies in EU justice and home affairs: A multi-layered and yet unexplored territory for legal research

Chapter · November 2017

CITATIONS
2

READS
161

2 authors:

Paul De Hert
Vrije Universiteit Brussel
395 PUBLICATIONS **3,976** CITATIONS
SEE PROFILE

Vagelis Papakonstantinou
Vrije Universiteit Brussel
100 PUBLICATIONS **1,238** CITATIONS
SEE PROFILE

14

DATA PROTECTION POLICIES IN EU JUSTICE AND HOME AFFAIRS

A multi-layered and yet unexplored territory for legal research

Paul De Hert and Vagelis Papakonstantinou

Introduction

Data protection is a EU law field that has undergone substantial if not groundbreaking change over the past few years. In April 2016, a five-year law-making process finally came to an end with the formal adoption of the General Data Protection Regulation (Regulation 679/2016/EU) and the Police and Criminal Justice Data Protection Directive (Directive 680/2016/EU). Each one is aimed at replacing the legal instruments already in effect in their respective fields. In particular, the General Data Protection Regulation (the 'GDPR') is intended to replace Directive 95/46/EC; it will find immediate application across the EU on May 25, 2018. On the other hand, the Police and Criminal Justice Data Protection Directive (the 'Directive') is intended to replace Framework Decision 977/2008/JHA; it was also released on the same day as the GDPR, on April 27, 2016, but, being a Directive, it gives member states unti May 6, 2018 to harmonize their national laws with its provisions.

This chapter will focus on the Directive, its subject matter being directly related to the EU justice and home affairs field. The Directive is an ambitious text, aiming at assuming the data protection standard-setting role within this field: all and any personal data processing in the law enforcement field undertaken by member states should observe its provisions. Nevertheless, space for exemptions is provided for. Most significantly, personal data processing performed by EU law enforcement agencies and bodies (Europol, Eurojust, OLAF, the European Border and Coast Guard Agency – Frontex, SIS II, VIS, CIS, Eurodac), is set to follow its own rules and not those of the Directive. At this EU level, the role of the standard-setting text is to be assumed by Regulation 45/2001/EC. Early in 2017, the Commission released its draft proposal for a Regulation replacing it (COM(2017) 8 final). Currently, virtually every EU agency or body active in this field profits from its own particular data protection provisions. In early 2017 these were found at various levels of completion: for example, while Europol and Eurojust are having their respective legal frameworks updated, and the European Public Prosecutor Office (EPPO) is in the process of being newly established, other EU agencies and bodies follow data protection developments in a more passive manner.

It is exactly the interplay of the above legal instruments (the Directive, Regulation 45/2001 or its successor, and agency-specific data protection provisions) that poses the main data protection policy challenge in the EU field of justice and home affairs today. The legal architecture in

the field matters in terms of policy-setting, legal clarity, straightforwardness, and ultimately, accountability and adequate protection of the individual right to data protection (De Hert and Papakonstantinou 2014). In particular, the basic question here is whether the cumulative effect of the provisions of all the above instruments that are applicable each time is sufficient in protecting individuals and their right to data protection.

Because the field is currently undergoing substantial legal change, for the time being this is still an open, ongoing discussion. Attention should be given both to the applicable legal framework, meaning the interplay of the above instruments in each particular case, and also to application practices by the actors themselves (member state and EU law enforcement bodies) and data protection supervisors: Data Protection Authorities (DPAs) at the member state level and the European Data Protection Supervisor (the EDPS) at the EU level.

This chapter will first attempt to map the data protection field within the EU justice and home affairs region (sections 1 to 4). This is a not a straightforward task given the multitude of legal documents currently in various stages of the lawmaking process, as well as the multitude of legal layers with agency-specific legal provisions that frequently apply in parallel with general-scope texts (under a *lex specialis/lex generalis* relationship). The first section will discuss EU primary law (the Treaty of Lisbon) and the two basic data protection instruments regulating data processing by police and criminal justice actors in member states before and after Lisbon, the 2008 Framework Decision and the 2016 Police and Criminal Justice Data Protection Directive. The second section looks at some loose ends in this area that co-exist with the Framework Decision and the Directive. Examples that come to mind are bilateral PNR data exchange agreements with the USA, Australia and Canada, each containing specific data protection measures.

In the third section we discuss Regulation 45/2001, a document with general standards for data processing done at the level of the EU, but with remarkably little attention focused on what is happening at the EU level in the justice and home affairs field. In a subsequent section we will highlight instruments aimed at regulating agencies working at the EU level. We will then discuss briefly the (new) 2016 Europol Regulation and the proposed regulations for Eurojust and the European Public Prosecutor's Office.

These descriptions are followed by an analysis of the lack of research in this area and possible main legal and non-legal research issues in order to provide readers with some guidance as to research avenues that are currently open or are likely to be opened in the near future. Finally, some speculation on possible future scenarios with regard to the protection of individuals, which is ultimately the reason why data protection applies in the field, will be attempted in the concluding section.

The general regulatory instruments within the EU justice and home affairs field: from a decision to a directive after Lisbon (layer 1)

The ratification of the Treaty of Lisbon back in 2009, Article 16 in particular, constitutes a turning point in the relationship between data protection and the EU justice and home affairs field (Hijmans and Scirocco 2009). Up until that time the field was largely fragmented, lacking coherence. Directive 95/46/EC expressly excused itself from undertaking the role of the common text of reference. Article 3 excluded from the scope of the Directive all processing of personal data in areas related to justice and home affairs, public security, defense and state security. Framework Decision 977/2008/JHA, which saw the light of day many years later, was a first attempt to regulate data protection in the EU justice and home affairs field, but only with modest outcomes. One could hardly speak of a common reference text for the field in view of

the many exceptions and the limited scope of the instrument (De Hert and Papakonstantinou 2009). Some of the regulative work was done through several sector-specific legal instruments (for example, the Data Retention Directive on electronic communications data or the Passenger Name Records agreements with the USA, Australia and Canada on travel data) introduced particularly in the aftermath of terrorist attacks in the USA (9/11) and Europe. Some of these instruments were proven to be short-lived, as was the case with the EU Data Retention Directive (Directive 24/2006/EC) which was annulled by the CJEU in April 2014 (Joined Cases C-293/12 and C-594/12). Member states were therefore largely left alone to implement their own personal data processing practices at national level. They did so at multiple paces: some experimented enthusiastically in the field through the introduction of specialized legislation at the national level; others were more or less indifferent to it, as perhaps evidenced by their choice to apply their general data protection legislation (as affected by Directive 95/46) also to related personal data processing.

The ratification of the Treaty of Lisbon in November 2009 brought change. Article 16 states:

> [E]veryone has the right to the protection of personal data concerning them. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

The precise consequences of this important provision remain unclear (De Hert 2015), but the wordings imposed change in the field and seemingly better mandate the EU to regulate data protection more thoroughly in less traditional areas. Nevertheless, Article 16 should be read together with Declaration 21 of the TFEU:

> [T]he Conference acknowledges that specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 of the Treaty on the Functioning of the European Union may prove necessary because of the specific nature of these fields.

In other words, the individual right to data protection is not unreservedly protected within the law enforcement field, or, at least, not in the same unrestricted manner as is the case with all other personal data processing. The Treaty of Lisbon, through Declaration 21, ensured that explicit differentiation is made between the two categories of personal data processing (general purpose, as opposed to that carried out by law enforcement agencies) so as to accommodate the special needs of the law enforcement sector.

As a consequence of the ratification of the Lisbon Treaty, the Police and Criminal Justice Data Protection Directive was introduced on April 27, 2016. Perhaps most importantly, the Directive addresses the main shortcoming of the Framework Decision it replaces, meaning its scope of self-limitation to cross-border processing, by declaring itself applicable to all processing undertaken at member state level (in Article 2). It also strengthens individual rights and adapts novelties introduced by the GDPR into the law enforcement field whenever and wherever applicable (see, for example, the cases of data protection impact assessments or data protection

by design and by default). Supervision is granted to member state DPAs. Overall, it constitutes a text moving in the right direction, meaning that of providing adequate protection to individuals while striking a correct balance with law enforcement's personal data processing needs. On the other hand, the Directive leaves outside of its scope the processing performed by EU law enforcement actors (in Article 60), an inevitable choice given that a Directive cannot regulate EU agencies.

The introduction of the Police and Criminal Justice Data Protection Directive concludes an almost ten-year effort by the Commission (work on the Framework Decision began in 2006) to regulate the personal data processing of law enforcement agencies at the member state level according to common data protection standards. However, while harmonization at the member state level is indeed expected to be achieved through the Directive, at the EU level this remains an open issue.

The specific regulatory state within the EU justice and home affairs field: loose ends and umbrellas (layer 2)

In addition to the foregoing, a multitude of texts and initiatives exist in the field with more specific aims. Examples that come to mind are EU texts on Passenger Name Records collection (EU PNR) and EU bilateral agreements with third countries. Because an examination of each one of these cases largely exceeds the purposes of this chapter, this section will mention them only briefly. Directive 681/2016 (the so-called 'EU PNR Directive') was introduced on May 4, 2016 obliging airlines to hand over their passengers' data in order to help the authorities fight terrorism and serious crime. The EU PNR Directive organizes the more systematic collection, use and retention of PNR data (data collected during reservation and check-in procedures) on air passengers, thus affecting their right to data protection. This directive came after years of elaboration that included a long period, during which it was assumed it was abandoned, as a reply to recent terrorist attacks across Europe – the recent attacks in Paris weighing heavy in this regard. Its introduction, despite its best intentions to comply with the proportionality principle and to apply adequate data protection safeguards, raised a number of data protection concerns; for example, concerning expansive passenger blacklisting or profiling (De Hert and Papakonstantinou 2015).

Long before the EU PNR Directive was introduced, the EU entered bilateral PNR data exchange agreements with the USA, Australia and Canada. Each of these agreements has a long history of multiple versions, court disputes, and long and complex negotiations (Argomaniz 2009; Hornung and Boehm 2012). Attention should therefore be given to each case separately; here it will only be noted that, by early 2017, the EU had effective bilateral PNR Agreements with the United States (since 2012), Canada (since 2006) and Australia (since 2012). In the same context, the EU has also entered bilateral agreements with the USA, namely the Terrorist Finance Tracking Programme (TFTP) in 2010 regulating the transfer of financial messaging data as well as the so-called 'EU–US Umbrella Agreement' which, once formally adopted, will supposedly provide a comprehensive high-level data protection framework for EU–US law enforcement cooperation.

The regulatory state at the high, standard-setting EU level: Regulation 45/2001 (layer 3)

At the EU level, personal data processing is regulated through a two-step process: Regulation 45/2001, or its successor, sets general standards. At the same time each actor in the field also

benefits from its own, ad hoc data protection legal regime that should be read in combination with the provisions of Regulation 45/2001. Supervision tasks are awarded to the European Data Protection Supervisor (EDPS).

A number of problems are caused by this policy option. Those originating from Regulation 45/2001 itself are of an interim nature. The Regulation was introduced back in 2001 in order to apply, for the first time, data protection standards upon processing performed at the EU level. It also established the EDPS to supervise the application of these standards across EU institutions. However, Regulation 45/2001 kept away from the processing performed in the justice and home affairs sector, being applicable only to the processing of EU personnel files (through Article 46), but not to their case files. Despite this self-restrained approach, over the years several law enforcement EU actors voluntarily submitted themselves to the supervision powers of the EDPS. In effect, at the time of drafting this text, this has been the case with all EU actors in the field apart from Eurojust and Europol (a situation that, at least for Europol, is about to change). However, these actors were permitted an inexplicable, and unjustifiable, selective submission: while they accepted EDPS supervision, they did not resign from the substantive data protection law and submit themselves only to the provisions of Regulation 45/2001, which after all provide the terms of reference for the EDPS. Instead, each one was allowed to keep its ad hoc data protection regime, and only vest supervision upon the EDPS. The EDPS is therefore entrusted with the nearly impossible legal task of applying different substantive data protection rules to each actor it supervises.

A further problem connected to Regulation 45/2001 is the vagueness of its provisions. They were simply not written to regulate law enforcement personal data processing. Because the Regulation was released as a general-purpose (then first pillar) instrument to regulate all types of personal data processing, it does not cater specifically to the needs of processing undertaken by law enforcement actors. Nevertheless, substantial differences exist between these two types of personal data processing that justified the release of two different instruments to accommodate each one: the GDPR and the Directive. In the previous section we discussed the policy decision reached by the EU and member states about one legal instrument being unable to regulate all personal data processing; hence the co-existence of a general text (GDPR) and a specific text for justice and home affairs (the Police and Criminal Justice Data Protection Directive). What is self-evident at the member state level should also be reflected at the EU level; however, this has not been the case until today, with Regulation 45/2001 striving to hold a catch-all role.

In early 2017, the Commission made available its proposal for a new regulation, replacing Regulation 45/2001. The new regulation will supposedly address shortcomings of the past, taking into account 'the results of enquiries and stakeholder consultations, and the evaluation study on its application over the last 15 years'. While it is too early to assess its provisions, it should be noted that the above two problems are not addressed in its text. Again, a single text is expected to cover both general and law enforcement personal data processing at the EU level, maintaining an inexplicable differentiation between EU and member state personal data processing. Moreover, as far as substantive law is concerned, legal confusion is expected to continue because the Commission proposal prefers to leave the ad hoc data protection regime of each actor intact, merely asking for 'consistency' with the Directive's provisions (in par. 9 of the Preamble).

While the above developments with regard to Regulation 45/2001 and its successor describe change at a high, standard-setting EU level, developments have also been noted at the agency level over the past few years.

The regulatory state at the EU agency level (layer 4)

A multitude of EU actors (agencies, bodies and IT systems) are active in the justice and law enforcement field today. For the time being, each one benefits from its own ad hoc data protection regime as far as substantive data protection law is concerned. On the other hand, data protection supervision tasks are now almost unanimously granted to the EDPS.

With regard to Europol, a new Europol regulation, Regulation 794/2016, was published on May 11, 2016. As far as its substantive data protection regime is concerned, the Regulation includes an ad hoc one that is influenced by Regulation 45/2001, but is also carefully worded so as not to submit itself to its provisions (see, e.g., Recital 40). Accordingly, the Europol ad hoc data protection legal framework is laid down in Articles 17 to 50. On the other hand, as far as data protection supervision is concerned, the EDPS will replace the Europol Joint Supervisory Body (JSB) previously entrusted with this task.

Eurojust is awaiting an amendment to its legal framework. The Commission released its proposal for a regulation for Eurojust on July 17, 2013 (COM 0535 final), together with a proposal for a Council regulation on the establishment of the European Public Prosecutor's Office (COM 0534/final). Both regulations have yet to be finalized. The Commission's approach with regard to their substantive data protection law is to refer directly to Regulation 45/2001 and to its provisions as applicable to all processing operations at Eurojust and the EPPO. As far as supervision is concerned, it is suggested that the EDPS be made responsible for supervision of all personal data processing, thus replacing Eurojust's Joint Supervisory Body (JSB) currently carrying out these tasks.

All other actors in the field benefit from ad hoc, substantive data protection provisions that complement and particularize the provisions found in Regulation 45/2001. While each needs to be examined separately, it is briefly noted here that this is the case for Frontex or the European Border and Coast Guard (through Regulation 1168/2011), Eurodac (through Regulation 603/2013), the EU Visa Information System (through Regulation 767/2008), the EU Customs Information System (through Regulation 515/1997) and the Schengen Information System (through Regulation 1987/2006).

An important point for clarification refers to EU and member state cooperation. Because EU law enforcement actors most likely do not themselves collect the data found in their databases, but instead rely on member states for this task, data protection cooperation and coordination is of crucial importance. However, in practice this distinction between datasets increases regulatory complexity. Essentially, two different sets of data protection rules apply on the same individual file when processed at the member state and EU level. When processed at the member state level, local rules apply; once transmitted to a EU agency, EU rules apply. Cooperation between the two agencies is warranted through 'coordinated supervision' between the two data protection supervisory authorities involved, namely national data protection authorities at the respective member state level and the EDPS for processing at the EU level.

Why so little academic attention in the past?

Although research interest in the broader data protection field has witnessed an unprecedented, exponential growth over the past few years, attention has mostly focused either on general-purpose personal data processing governed by the 1995 Directive (now) or the 2016 GDPR (upcoming), in particular to such issues as internet social networks, cloud computing, the Internet of things, biometric data, drones and other technologies dominating the field, or to novelties in the text of the GDPR (e.g., the right to be forgotten or data protection impact assessments).

In relation to its glamorous sibling, the 2016 Police and Criminal Justice Data Protection Directive has mostly remained in the shadows of legal research, despite its very important subject matter. The same has been the case both with regard to its predecessor, the 2008 Framework Decision, and agency-specific data protection regimes. At least three reasons may have caused this neglect.

First, the lawmakers' approach itself: even during the long negotiations leading to the adoption of the EU data protection reform package, attention was disproportionately awarded to the GDPR. The Directive has always been under the assumption that it would be easier to adopt once the GDPR was concluded and that, in any event, its provisions would have to follow those of its sibling wherever possible. This phenomenon is after all also demonstrable in the Commission's recent proposal for a regulation replacing Regulation 45/2001: while the GDPR is repeatedly acknowledged and referred to, the Police and Criminal Justice Data Protection Directive only receives passing mention in its provisions.

Another reason for the limited interest of legal research in the field may be explained by its subject matter. The processing of personal data for law enforcement purposes gained in importance only relatively recently, after terrorist attacks across the world brought forward this type of personal data processing as an indispensable tool in the 'war against terror'. The majority of relevant legal initiatives have a history of no more than ten years – admittedly, a relatively short period for new legal research to emerge. In addition, the legal framework is in constant flux: at the time of the drafting of this text, the Eurojust and the EPPO draft regulations, as well as the successor to Regulation 45/2001, await finalization. On the other hand, political scientists have approached the field from a different angle, focusing mainly on institutional dynamics in the adoption of data protection laws (Argomaniz 2009; Bellanova and Duez 2012; Ripoll Servent and MacKenzie 2012; Ripoll Servent 2013).

Finally, the inherent difficulty of keeping up with the field should not be overlooked. The complex legal architecture described in the previous chapter affects legal research as well: anyone interested in the field would have to keep up both with general and intra-agency data protection developments. In addition, these would have to be complemented by member state law that, given the lack of the requirement for harmonization until at least May 2018, is at best multi-speed across the EU. As stated by the EDPS as early as 2008 in the context of EU frontier databases, 'the sheer number of these proposals and the seemingly piecemeal way in which they are put forward make it extremely difficult for the stakeholders (European and national Parliaments, data protection authorities including EDPS, civil society) to have a full overview' (EDPS 2008). His views were shared by O'Neill two years later (O'Neill 2010). Consequently, the formulation of a complete picture would have to be performed on an agency-specific level. In addition, the limited information that the agencies themselves (or the EDPS, for the same purposes) make available to the public further hinders legal research in the field.

Main scholarly debates and future research avenues (first series of questions)

Notwithstanding the difficulties mentioned above, or perhaps precisely because of them, the field is currently faced with some very interesting legal questions. First and foremost, the relationship between its basic legal instruments, namely the Directive and Regulation 45/2001 or its successor, is an issue of crucial importance. Disappointingly, the current Commission's draft updating Regulation 45/2001 leaves the issue unaddressed through mere indirect and brief mention in its preamble.

This may well change in the Regulation's final text. The main question here is whether the alignment of two essentially different texts (the Directive being aimed at law enforcement and

Regulation 45/2001 at general processing), which somehow need to co-exist, is at all possible. Once this issue is addressed, their relationship with each agency-specific data protection legal regime will have to be clarified – a far from straightforward issue. For example, with regard to Europol, Cocq (2016) has already noted the difficulties of attempting to align the data protection provisions of its new regulation with those of the Directive in terms of definitions or scope and objectives. Taking into account that supervision will be undertaken by the EDPS, regulated by Regulation 45/2001, the importance of consistency becomes obvious.

At the same high level, the relationship between the GDPR itself and the Directive may also give rise to interesting legal questions. The line separating processing under the GDPR or under the Directive may at times become extremely thin. For example, a police station anywhere in the EU may soon discover that it has to apply both legal instruments: the GDPR while processing personnel or non-law enforcement-related files, and the Directive for the detection, prevention and combatting of crime. In the past, this distinction line, which corresponded broadly to the then first and third pillars respectively, remained blurred. González and Paepe (2008) characterized their relationship as 'conflictive'. In the cases of the first-generation EU PNR bilateral agreement and in the ultimately annulled Data Retention Directive, the Court was called upon to make the necessary adjustments (in joining cases C-317/04 and C-318/04, and Case C-301–06 respectively). In the future, given the intertwining of these two legal instruments, disputes and cases of conflict are expected to increase and will need to be addressed by sound theoretical analysis.

If viewed from a non-*stricto sensu* legal research point of view, the field of EU justice and home affairs is evidently faced with the fundamental contemporary question of reconciling privacy and security (Van Lieshout *et al*. 2013). Terrorist attacks across EU capitals have increased lawmaking efforts towards warranting security to EU citizens. These initiatives unavoidably conflict with the protection of fundamental rights and the right to data protection is found at the epicenter of this debate. As noted by McGinley and Parkes (2007), as early as 2007, 'the international exchange of information (both raw data and intelligence) has become a cornerstone of efforts to combat internal security threats faced by EU Member States'. The validity, however, of the relevant underlying assumption need not remain unchallenged: legal research could focus on evidencing whether data protection indeed constitutes a constraint upon effective security (combatting crime and counter-terrorism) policy or not. In any event, as given in Article 16 TFEU, the balance between adequate data protection and security needs to be struck carefully. This task is often far from straightforward. González (2012) notes that security has played different roles in EU personal data protection law, functioning both as a limit of its scope of application, whereby data processing concerning 'national security' is expressly excluded, and as a means to justify legitimate restrictions or modulations of otherwise basic data protection law. In the same context, the use of surveillance technologies for crime prevention and investigation purposes may lead to a 'perilous double shift' effect. As noted by Cocq and Galli (2013), surveillance technologies introduced in relation to 'serious crime' are increasingly used for the purpose of preventing and investigating 'minor' offenses, while at the same time surveillance technologies originally used for public order purposes in relation to 'minor' offenses are increasingly guided in the context of prevention and investigation of serious crime.

Main scholarly debates and future research avenues (second series of questions)

Agency-specific research in the field is always welcome – and should be considered interesting at all times, especially if placing all actors in the field under a common axis of analysis, as performed by Gutierrez Zarza (2015). In particular Europol and Eurojust already have a rich data

protection history; important changes are under way and critical questions may arise with regard, for example, to supervision by the EDPS or their new substantive data protection regime. While other EU actors in the field may attract less attention, also given their sector-specific type of processing, the question of the adequacy of their data protection regime when compared to the Directive should provide an interesting field for legal research. Research findings in the recent past have not been encouraging in this regard. Boehm (2012: 256, 318) has duly noted the existence of a 'fragmented' and 'stagnating' data protection framework in the field versus increasing 'powers of the AFSJ agencies and OLAF and functionalities of the EU Information Systems'. This led her to highlight the need for a 'central supervisory authority' (Boehm 2012: 394). However, while external supervision is of course important, it would be equally important for legal research to focus on internal supervision as well: what, if anything, will replace the Europol and Eurojust internal Joint Supervisory Bodies when the new regime abolishes them?

In the same context, Article 16 TFEU requires that not only the ad hoc substantive data protection legal regime for each actor in the field be formulated and assessed, but also that this be done from the perspective of data subjects. The means of recourse in the event that one of the EU actors in the field infringes the right to data protection of individuals must become visible and accessible. When the law does not provide such clarity, as is the case today in the field, legal research should take over.

At member state level, it will evidently be interesting for legal researchers to examine how the Directive is implemented in their respective jurisdictions. As is the case also with the GDPR, the Directive allows for significant space for member state differentiation. Although inadvisable because it would ultimately contradict the Directive's own purpose to achieve harmonization across the EU, data protection history has shown that different approaches across the EU are in fact possible and attributable to different legal systems and cultures. However, legal research and the Commission should keep an open mind, so as to identify differences that go beyond the permitted level of local differentiation.

Finally, the specific data protection legal topics within the EU justice and home affairs field frequently provide fruitful areas of legal research. This is the case both with subject-specific new legal instruments, such as the EU PNR Directive, or, in the past, the Data Retention Directive, and with the EU's bilateral agreements with third countries in the field. Special topics such as profiling for law enforcement purposes (Custers *et al.* 2013) or the accessing of private sector data by law enforcement agencies (Goemans-Dorny 2012) also come to mind in this regard. The cooperation between the EU and the USA that spans several modalities in the EU justice and home affairs field in particular should provide a continuous and interesting topic for further research by data protection scholars. Despite the frequent lack of materials that may be characterized as restricted and therefore not be accessible to the public, there is always a lively interest in any new insight in a field that affects a great number of individuals, but which up until today remains largely undocumented.

While possible research topics of immediate use and concern are described above, the field will reach its research maturity once the legal framework has been firmly established and should be considered as settled, at least for the foreseeable future. Only then will researchers be able to finally focus on its actual application. Today, in essence, legal research struggles to formulate a clear and coherent picture with regard to the legal framework applicable each time; it is only reasonable that much less interest is vested in how exactly this legal framework is to be applied in practice. Once these issues have been resolved, legal researchers in the field may finally embark upon the perhaps more interesting questions that their colleagues focusing on the GDPR are already dealing with, meaning the use of new technologies in the field. The same new technologies referred to above with regard to the GDPR (Internet social networks, cloud

computing, drones, the Internet of things) are also being used in the law enforcement context. However, up until today they have attracted very limited legal research interest. It is the authors' belief that once issues of the applicable legal framework have been addressed, legal research will be free to indulge itself in these, and, perhaps more relevant (from the data subjects' perspective), future research avenues.

Concluding remarks: data protection in the EU justice and home affairs field as a yet unexplored territory for legal research

The main understanding one derives after closer examination of the EU data protection policies in EU justice and home affairs is that this is a field in constant flux. It gained exponentially in importance following terrorist attacks across Europe. For more than fifteen years it never ceased to develop and change, either centrally or in its constituting parts. At the central level, the need for a standard-setting text was identified as early as 2008, but is hopefully only now on course to be achieved through the interplay of the Police and Criminal Justice Data Protection Directive and the successor of Regulation 45/2001. The relationship between these two instruments is expected to give rise to interesting research and perhaps even disputes and case law. As regards the constituting parts of the EU justice and home affairs field, a basic distinction needs to be made between EU and member state personal data processing. The former is faced with an incomprehensible, unjustifiably complex architecture whereby each single EU agency and body active in the field profits from its own data protection substantive law. Some harmonization is expected to be achieved at the member state level after May 2018, as per the Directive's requirements.

While what is mentioned above may illustrate a complex and fragmented legal environment that actively discourages legal research or even mere interest in the field, the authors wish to see the glass half-full: to their mind, the past fifteen years have been a fast-track process, from the birth of a new type of personal data processing at the national level towards, admittedly, a reluctant EU harmonization. Personal data processing for law enforcement purposes, at least as it is known today, was conceived following 9/11. Member states experimented with it, each at its own pace and with its own idiosyncrasies. Once it was established that this new type of processing was here to stay, the EU intervened and attempted to assume the central monitoring and rule-setting role. The legal ambiguity that we are perhaps still living in today is the hopefully short-term result of this worthy – at least to our mind – effort.

Bibliography

Argomaniz, J. (2009). When the EU is the 'Norm-taker': The Passenger Name Records Agreement and the EU's Internalization of US Border Security Norms. *Journal of European Integration*, 31(1), pp. 119–136.

Bellanova, R. and Duez, D. (2012). A Different View on the 'Making' of European Security: The EU Passenger Name Record System as a Socio-technical Assemblage. *European Foreign Affairs Review*, 17 (Special Issue), pp. 273–288.

Boehm, F. (2012). *Information Sharing and Data Protection in the Area of Freedom, Security and Justice*. New York: Springer.

Cocq, C. (2016). EU Data Protection Rules Applying to Law Enforcement Activities: Towards a Harmonised Legal Framework? *New Journal of European Criminal Law*, 7(3), pp. 263–276.

Cocq, C. and Galli, F. (2016). The Catalysing Effect of Serious Crime on the Use of Surveillance Technologies for Prevention and Investigation Purposes. *New Journal of European Criminal Law*, 4(3).

COM (2013a). 0534: Proposal for a Council Regulation on the Establishment of the European Public Prosecutor's Office.

COM (2013b). 0535: Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Criminal Justice Cooperation (Eurojust).

Custers, B., Calders, T., Schermer, B. and Zarsky, T. (eds) (2013). *Discrimination and Privacy in the Information Society Data Mining and Profiling in Large Databases*. New York: Springer.

De Hert, P. (2015). The Right to Protection of Personal Data. Incapable of Autonomous Standing in the Basic EU Constituting Documents? *Utrecht Journal of International and European Law*, 31(80), pp. 1–4.

De Hert, P. and Papakonstantinou, V. (2009). The Data Protection Framework Decision of 27 November 2008 Regarding Police and Judicial Cooperation in Criminal Matters – Modest but not the Data Protection Text Everybody Expected. *The Computer Law & Security Review*, Vol. 25. Elsevier.

De Hert, P. and Papakonstantinou, V. (2014). The Data Protection Regime Applying to the Inter-agency Cooperation and Future Architecture of the EU Criminal Justice and Law Enforcement Area. European Parliament, Committee on Civil Liberties, Justice and Home Affairs.

De Hert, P. and Papakonstantinou, V. (2015). Repeating the Mistakes of the Past will do little Good for Air Passengers in the EU – The Comeback of the EU PNR Directive and a Lawyer's Duty to Regulate Profiling. *New Journal of European Criminal Law*, 6(2), pp. 160–165.

EDPS (2008). Preliminary Comments on COM(2008) 69 final, COM(2008) 68 final, COM(2008) 67 final.

Goemans-Dorny, C. (2012). Accessing Private-sector Data: The Need for Common Regulations for the Police. Data Protection in the Area of European Criminal Justice Today, ERA, Trier.

González Fuster, G. (2012). Security and the Future of Personal Data Protection in the European Union. *Security and Human Rights*, 4, pp. 331–342.

González Fuster, G. and Paepe, P. (2008). Reflexive Governance and the EU Third Pillar: Analysis of Data Protection and Criminal Law Aspects, in Guild, E. and Geyer, F., *Security versus Justice? Police and Judicial Cooperation in the European Union*. Farnham: Ashgate.

Gutierrez Zarza, A. (2015*). Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe*. New York: Springer.

Hijmans, H. and Scirocco, A. (2009). Shortcomings in EU Data Protection in the Third and the Second Pillars, Can the Lisbon Treaty Be Expected to Help? *Common Market Law Review*, 46, 1485–1525.

Hornung, G. and Boehm, F. (2012). Comparative Study on the 2011 Draft Agreement between the United States of America and the European Union on the Use and Transfer of Passenger Name Records (PNR) to the United States Department of Homeland Security. Passau/Luxemburg, March 14.

McGinley, M. and Parkes, R. (2007). *Data Protection in the EU's International Security Cooperation: Fundamental Rights vs. Effective Cooperation?* SWP Research Paper No. 5. Berlin: Stiftung Wissenschaft und Politik.

O'Neill, M. (2010). The Issue of Data Protection and Data Security in the (Pre-Lisbon) EU Third Pillar. *Journal of Contemporary European Research*, 6(2), pp. 211–235.

Ripoll Servent, A. (2013). Holding the European Parlament Responsible: Policy Shift in the Data Retention Directive from Consulation to Codecision, *Journal of European Public Policy*, 20(7), pp. 972–987.

Ripoll Servent, A. and MacKenzie, A. (2012). The European Parliament as a 'Norm Taker'? EU–US Relations after the SWIFT Agreement. *European Foreign Affairs Review*, 17 (Special Issue), pp. 71–86.

Van Lieshout, M., Friedewald, M., Wright, D. and Gutwirth, S. (2013). Reconciling Privacy and Security. *Innovation: The European Journal of Social Science Research*, 26, pp.1–2.