Notification, an important safeguard against the improper use of surveillance – finally recognized in case law and EU law

Franziska Boehm [1] and Paul de Hert [2] [3]

Cite as:

Abstract:

According to the European Court of Human Rights, the notification of individuals of surveillance measures is both an essential safeguard against the abuse of monitoring powers and an important part of the right to an effective remedy before the courts. However, the right of an individual to be informed that the police or the secret service is collecting data about them, or that particular surveillance measures have been carried out (telephone tapping, visual or video surveillance, covert installation of monitoring software on a computer etc.) is not harmonised in the EU. National regulatory controls in this area thus vary between Member States and there is a lack of regulatory cohesion at the EU level. This article analyses the current provisions within both the EU and Council of Europe regulatory frameworks concerning notification requirements after data have been collected and after surveillance has been carried out. It also examines future regulation in this field including the EU Commission's proposals to revise the current Data Protection Directive 95/46/EC and the Framework Decision 2008/977/EC for data processing concerning police and judicial co-operation.

1. Introduction

The surveillance of individuals and the resulting collection of information are regarded by the security community as an effective tool to locate terrorists and other criminals. In addition to the establishment of crime-fighting databases, the travel behavior of citizens is recorded, and telecommunication and internet data are required to be retained for possible use in investigations.[4] Databases and information systems containing such data exist at both national and EU levels. Personal data are increasingly collected, analyzed and interlinked.
This article examines the importance of the right of citizens to be informed that their data has been collected, or that they have been the subject of surveillance, by reference to current laws. It first provides a brief overview of the increasing surveillance measures at EU level, then analyzes the current notification requirements existing in EU, and discusses the right of notification in the framework of the Council of Europe and the case-law of the ECtHR. With the proposed changes to EU data protection law in mind, an overview of potential future regulation in this field is then essayed.

2. Increased surveillance at EU level

Before discussing existing and potential notification rules, a brief impression of the current databases and systems of surveillance within the EU is instructive. Post 9/11 policy concepts, such as proposed in the Hague and the Stockholm programme led to an increase of systems developed to control various parts of our daily life. [5] Surveillance thereby takes place at

different levels: On the initiative of the EU, Member States implement the data retention directive to reinforce their police and secret service activities. At EU-level, so called anti-terrorism measures are increasingly often initiated: travelers are comprehensively checked when they enter EU territory and EU databases and information systems serving multiple purposes are installed to collect and analyze information (see further, Boehm 2012). In addition to databases serving police purposes (the Europol Information System (EIS), the Schengen Information System (SIS) and the Customs Information System (CIS)), databases initially installed to facilitate border control such as the Visa Information System (VIS) and Eurodac are increasingly used for surveillance purposes.[6] In fact, almost all existing databases have multiple functionalities. The SIS for instance is a database in the framework of law enforcement and immigration control and collects data of third state and EU nationals. The CIS serves customs control purposes but also contains personal data of individuals suspected of illicit trafficking activities. The VIS serves the purpose of the exchange of visa data and entails information of third state nationals who apply for a visa to enter the EU. Plans to give law enforcement access to the VIS are under consideration. Eurodac stores fingerprint data of asylum seekers and should prevent that asylum seekers make multiple asylum applications in different Member States of the EU. The EIS and Eurojust's database entail data of criminals, but also of suspects, victims and witnesses. Frontex is the EU's border agency and collects data of third state nationals trying to pass the external borders.

The rise of techniques and databases developed in recent years touches therefore on different aspects of the daily life of citizens. Not only traditional criminals are targeted by such measurers, but also individuals not suspected of having committed a crime. A shift towards the preventive entry of citizens in databases serving police but also other purposes can be observed. The rights of individuals affected by such measures do not always keep up with this fast developing field of different surveillance techniques (Van Brakel & De Hert 2011).

The cooperation in terms of crime prevention with third states, in particular with the US is additionally increasing. Flight passenger and bank data of EU citizens are transferred to the US in the framework of the PNR and the TFTP agreements.[7] Only recently the EU signed an agreement with Australia to forward flight passenger data. As the Parliament asked the Commission in May 2010 to review the existing PNR agreements, the agreement with Canada is currently in the renegotiation process. A new PNR agreement with the US was concluded in April 2012. In consequence, there are various actors involved in surveillance and data collection at EU level and beyond. An enhanced cooperation between these actors takes place. Law enforcement agencies and EU information systems exchange data amongst each other and transfer them also to third states. All these actors have different data protections regimes to the effect that individuals concerned are faced with various applicable legal sources.

In view of these developments, it is important to understand the consequences and effects on the citizens and the society as a whole. Many questions arise. From a legal point of view, it is essential that the different interests at stake are balanced and that safeguards against the misuse of governmental powers exist. In addition to other safeguards, a basic prerequisite to assure that the rights of individuals are respected in this context is the possibility to control the legality of the mentioned measures. One important question in this respect is whether the individuals should be informed after they have been subjected to such surveillance measures. This would allow them to control *a posteriori*. So far, rules at national as well as at EU level reflect a certain ambiguity in the regulation of this issue. However, the jurisprudence of the European Court of Human Rights shows a clear tendency towards the establishment of a right to be informed. Already in 1987, the Council of Europe issued Recommendation R (87) 15

requiring the notification of individuals after they had been subject of surveillance measures. The rationale of the notification duty in the framework of the Council of Europe is therefore discussed later. EU instruments, analyzed in the next paragraph, are more reluctant in this regard.

3. Current notification requirements in EU instruments

In EU law, the notification of individuals about the processing of their personal data is one tenet of the Data Protection Directive 95/46/EC.[8] In ordinary data protection law, the information provided to the data subject constitutes an important element of a fair processing of personal data. Controllers (those who process data) have to inform the data subjects about the data they collect and store about them. Knowing that one's personal data are processed guarantees transparency and enables the person concerned to assess its own position and to adapt its behavior to a given situation. (Damman & Simitis 1997: Art.10 para 1; Ehmann & Helfrich 1999: Art.10 paras 25-28) Foreseeability and the control of the use of personal information play an essential role in this context. Although, due to the former pillar structure, Directive 95/46/EC does not apply to security related data processing and therefore not to surveillance measures, it illustrates the general data protection standard applicable to ordinary data processing activities.[9]

Directive 95/46/EC distinguishes two situations with regard to information rights: first, data which have been obtained from the data subject and second, data which have been obtained by other means.[10] In both cases, information has to be provided irrespective of whether the individual applies for access to the data.[11] The information includes (a) the identity of the controller and of his representative, (b) the purposes of the processing for which the data are intended and (c) any further information, including information on the right to access and to rectify, in so far as such further information is necessary having regard to the specific circumstances in which the data are collected and to guarantee fair processing in respect of the data subject.[12] As the individual concerned has not itself taken part in the process of data collection (Dammann & Simitis 1997: Art 11, para.4), information on the categories of data must be additionally provided in the case that the information is not obtained from the data subject.[13]

Derogations exist in the event of processing for statistical purposes, historical or scientific research.[14]

In the second scenario, when the information is not obtained from the data subject, the information need not be given, if the 'provision of such information proves impossible or would involve a disproportionate effort, or if recording or disclosure is expressly laid down by law'.[15] Although the provision on the disproportionate effort allows for a certain discretion, Member States must nonetheless provide appropriate safeguards in these cases. Another important exception exists with regard to the freedom of expression. Article 9 of the Directive 95/46/EC allows to provide for exceptions and derogations for the processing of personal data for journalistic purposes or the purposes of artistic or literary expression, but, 'only if they are necessary to reconcile the right to privacy with the rules governing the freedom of expression'.[16]

Directive 95/46 does not, however, apply to police and judicial related data processing. These matters are covered by Framework Decision 2008/977 (FDPJ).[17] In contrast to Directive 95/46/EC, a clear obligation to provide the data subject with information is not found in the

Framework Decision. Recital (26) FDPJ mentions that '…' it may be necessary to inform data subjects regarding the processing of their data '…'. Article 16 FDPJ further details that 'Member States shall ensure that the data subject is informed regarding the collection or processing of personal data by their competent authorities, in accordance with national law'.[18] As the European Data Protection Supervisor notes, the wording of the provisions relating to notification of the data subject suggests it is a possibility rather than an obligation.[19] Member States may additionally ask another Member State not to inform the data subject about data transferred from this first Member State to the other.[20]

In consequence, in the framework of police and judicial related work, Member States themselves decide about the introduction of the notification duty. By certain Member States the information of the individual is regarded as an obstacle to effective police work. Actors involved proceed on the assumption that the notification of persons concerned may hamper investigations. However, other Member States, for example Germany and Belgium, have nonetheless introduced a notification requirement in their criminal procedures. Article 101 (4) of the German Criminal Code does not only lay down a duty to inform the person under surveillance, but also other individuals who might have also been concerned by the surveillance measures. The notification duty includes traditional forms of surveillance (e.g. telephone tapping, acoustical observation of private premises, or surveillance through undercover agents) as well as newer surveillance techniques such as the use of 'international mobile subscriber identity (IMSI) catchers' or profiling methods. The duty to notify in German law is thus part of the classical criminal procedure and an essential legal requirement to be respected in the aftermath of surveillance measures. In Belgium, the Constitutional Court came recently to the conclusion that intelligence itself must actively inform the person concerned as soon as it is possible without compromising the intelligence work.[21] The different approaches in the Member States may be an explanation for the missing notification requirement in the FDPJ.

Thus, whereas the notification of individuals in the EU is left to the Member States in police and judicial related activities, it is established in ordinary EU data protection law since 1995 and constitutes an important element of Directive 95/46/EC. Transparency is regarded as 'a fundamental condition for enabling individuals to exercise control over their own data and to ensure effective protection of personal data'.[22] With regard to future developments in this field, it is interesting to note that within the upcoming revision process of Directive 95/46/EC, it is planned to increase the transparency for individuals by establishing a general transparency principle which goes beyond the current, above mentioned, information duties of Directive 95/46/EC (compare section V).

4. The right of notification at the CoE

The foregoing shows an unsatisfactory image of the duty to notify in the area of police, justice and secret service and in the FDPJ. Should it be a starting point or not: In this paragraph we will broaden the analyses by looking at development at policy level and human rights level.

The Council of Europe has a long recognized tradition in the protection of individual rights against surveillance measures ordered by states. The Council has produced various relevant policy documents and is also responsible for the 1959 Court of Human Rights (ECtHR) that has set the framework for the functioning of the ECJ. Starting with the case *Klass v. Germany* in 1978, the ECtHR continuously developed important criteria restricting the power of the states to enact surveillance measures by referring to the protection offered by the right to the

protection of private life stipulated in Article 8 European Convention on Human Rights (ECHR) over the last 30 years. Since then, the ECtHR issued a number of cases identifying the rules to be respected by states when they want to enact security and surveillance legislation. The criteria developed so far relate to the following minimum standards: The law permitting the surveillance measures must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances in which authorities are empowered to resort to any measures of secret surveillance and collection of data.[23] Moreover, 'because of the lack of public scrutiny and the risk of abuse intrinsic to any system of secret surveillance, the following minimum safeguards should be set out in statute law to avoid abuses: the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law'.[24] More recently, in addition to the mentioned safeguards, the ECtHR increasingly often insists on the right to be informed of surveillance measures. We will refer to a case against Bulgaria later.

At the level of policy making, already in 1987, the Council of Europe recognized the importance of the information of the individual. Principle 2.2. of the 1987 Recommendation R (87) 15 regulating the use of personal data in the police sector requires the notification of the individual concerned when data about him have been collected and stored without his knowledge, as soon as the object of the police activities is no longer likely to be jeopardized.[25] It should guarantee a way of independent *ex post* control to enable individuals subjected to surveillance measures to retrospectively enact infringement proceeding to challenge the lawfulness of the measure. Although all EU Member States are also members of the Council of Europe, this important principle was however not introduced in most of them. While Recommendation R (87) 15 is not binding upon the Member States, other instruments of the CoE, for instance Convention No. 108 for the protection of individuals with regard to automatic processing of personal data, have a different character. The binding nature of Convention No. 108 might be one of the reasons why this instrument is silent on this matter.

In addition to Principle 2.2. of Recommendation R (87) 15, the case-law of the ECtHR in relation to the protection of individuals in police related activities also plays an important role for the development of the notification requirement at CoE level. Cases such as *Klass*, *Weber and Saravia*, *Ekimdzhiev*, *Kennedy* and *Uzun* showed a continuous development towards to the right to be informed. [26] (de Hert & Boehm, Yearbook of the Digital Enlightenment Forum) Already in 1978 in *Klass v. Germany* the ECtHR recognized a passive way of informing individuals of surveillance measure by demanding adequate and effective guarantees against abuse.[27] The Court insists that one important safeguard against abuse constitutes the possibility to obtain a remedy in cases of misuse. In the view of the ECtHR, the notification guarantees the possibility to have recourse to the courts to be able to challenge the legality of the surveillance measures retrospectively and to ensure against abuses in this way.[28] To be able to claim a possible violation of the rights, an individual must be aware of the fact that he was the subject of surveillance measures. The Court puts much emphasis on this possibility and therefore links the question of notification to the possibility of independent control (at least *a posteriori*) and effective remedies before courts:

> As regards review *a posteriori*, it is necessary to determine whether judicial control, in particular with the individual's participation, should continue to be excluded even after surveillance has ceased. Inextricably linked to this issue is the question of subsequent notification, since there is in principle little scope for recourse to the courts by the

individual concerned unless he is advised of the measures taken without his knowledge and thus able retrospectively to challenge their legality.'[29]

Whereas in *Klass* the Court did not directly require the notification of the persons concerned – being satisfied with the solution found by the German legislator which provided for a notification – in more recent cases the Strasbourg Court increasingly insists on the notification duty. One example is the case *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* of June 2007.[30]

---

[1] Professor Franziska Boehm holds a chair (junior professorship) at the University of Münster, Institut für Informations-, Telekommunikations- und Medienrecht - Zivilrechtliche Abteilung -, Germany, (franziska.boehm@uni-muenster.de).

[2] Professor Paul de Hert holds a chair at the Vrije Universiteit Brussel as well as at the Tilburg University (paul.de.hert@vub.ac.be).

[3] A first version of this article was presented at the 2011 conference of the University of Leeds 'Human Rights in the Digital Era' and is published in: Yearbook of the Digital Enlightenment Forum ('The Rights of Notification After Surveillance is Over: Ready for Recognition?'), pp. 19-40.

[4] Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, [2006] OJ L 105/54.

[5] Political goals of the EU Treaties are practically enforced by the adoption of multi-annual work programmes (the Vienna (1998), the Tampere (1999), the Hague (2004) and the Stockholm programme (2009)), which establish general priorities and political objectives in this area. Although multi-annual work programmes are not as such binding instruments, these programmes set different political goals, which are subsequently legally implemented by the instruments available to the European legislator, primarily by way of Directives, Regulations and Council Decisions. As a result thereof, these programmes have a substantial effect on the future institutional policy and often directly influence legislative actions in this area, compare: Boehm, F. (2012), Information sharing and data protection in the Area of Freedom, Security and Justice.

[6] The Commission recently presented its 'smart border package' which provides for a comprehensive strategy to control the external border of the EU COM 2011 (680) final, http://ec.europa.eu/home-affairs/news/intro/docs/20111025/20111025-680%20en.pdf.

[7] See the agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Unites States Department of Homeland Security (DHS), [2007] OJ L 204/18; similar plans to establish a comparable system allowing for the analyses of European flight passengers exist also at EU level: Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2011) 32 final Brussels, 2.2.2011 and the TFTP (Terrorist Finance Tracking Programme) agreement from 28 June 2010.

[8] Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] OJ L 281/31.

[9] Art. 3, Dir. 95/46/EC.

[10] Arts. 10 & 11, Dir. 95/46/EC.

[11] Arts. 10 & 11, Dir. 95/46/EC.

[12] Arts. 10(1) & 11(1), Dir. 95/46/EC.

[13] Art. 11(1), Dir. 95/46/EC. Reg. 45/2001/EC, which regulates the processing of personal data by the EU institutions and bodies, additionally adds three/four pieces of information that has to be notified: the legal basis of the processing operation for which the data are intended, the time-limits for storing the data and the right to have recourse at any time to the European Data Protection Supervisor and the origin of the data, except where

In the *Ekimdzhiev* case, the omission of a notification by the authorities of *Ekimdzhiev* after surveillance measures have been carried out was regarded as a violation of Articles 8 and 13 ECHR. The ECtHR was faced with the Bulgarian 'Special Surveillance Means Act' (SSMA). The legislation granted far reaching surveillance rights to the police and the Bulgarian secret service, but did not entail sufficient safeguards against abuse. One of the essential requirements missing in the SSMA related to independent control of the surveillance measures. The Court noted in this case that safeguards must not only exist during the initial stage of a surveillance measure, but also after the end surveillance activities.[31] Nevertheless, Bulgarian law did not provide for any notification of the individual.[32] It even explicitly prohibited the disclosure of information that a person had been subjected to surveillance, or that warrants had been issued for this purpose. In view of this, the ECtHR recognized that 'the

---

the controller cannot disclose this information for reasons of professional secrecy in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected and to guarantee fair processing in respect of the data subject, see Art. 12(1)(f) Regulation 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, [2001] OJ L 8/1.

[14] Arts. 10(2) & 11(2), Dir. 95/46/EC; Arts. 11(2) & 12(2), Reg. 45/2001/EC.

[15] Art. 11(2), Dir. 95/46/EC; Art.12(2), Reg. 45/2001/EC.

[16] Art. 9, Dir. 95/46/EC.

[17] Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, [2008] OJ L 350/60: hereafter FDPJ.

[18] Art. 16(1) FDPJ.

[19] Opinion of the European Data Protection Supervisor on the Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, [2007] OJ C 139/1, para 37.

[20] Art. 16(2) FDPJ.

[21] Belgium Constitutional Court, Case No. 145/2011, 22 September 2011, paras 88 and 92.

[22] Communication from the Commission to the European Parliament, the Council, the Social Committee and the Committee of the Regions on 'A comprehensive strategy on data protection in the European Union', COM(2010) 609 final of 4 November 2010, para 2.1.1, p. 6.

[23] *Shimovolos v Russia* Application No 30194/09, Merits, 21 June 2011, para 68.

[24] *Shimovolos*, para 68.

[25] Principle 2.2. of Recommendation R (87) 15: 'Where data concerning an individual have been collected and stored without his knowledge, and unless the data are deleted, he should be informed, where practicable, that information is held about him as soon as the object of the police activities is no longer likely to be prejudiced.'

[26] ECtHR cases *Klass v Germany*, A 28 (1978), 2 EHRR 214; *Weber and Saravia v Germany*, Application No 54934/00, Admissibility, 29 June 2006; *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* Application No 62540/00, Merits, 28 June 2007; *Kennedy v the United Kingdom* Application No 26839/05, Merits, 18 May 2010; *Uzun v Germany* Application No 35623/05, Merits, 2 September 2010 at paras 41-53.

[27] *Klass v Germany*, A 28 (1978), 2 EHRR 214, para 50, hereafter *Klass.*

[28] *Klass*, paras 56-57.

[29] *Klass*, para 57.

[30] *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* Application No 62540/00, Merits, 28 June 2007, hereafter *Ekimdzhiev*.

fact that persons concerned by such measures are not apprised of them while the surveillance is in progress or even after it has ceased' is in line with the case law of the ECtHR 'as it is the very unawareness of the surveillance which ensures its efficacy'.[33] However, the Court then adds with reference to the *Klass* case that 'as soon as notification can be made without jeopardising the purpose of the surveillance after its termination, information should be provided to the persons concerned'.[34]

The Court observed that in the current Bulgarian regime persons under surveillance had no opportunity to discover that they have been subjected to surveillance measures, unless they were subsequently prosecuted on the basis of the information collected during the surveillance or if there was a leak of information.[35] As a consequence they were unable to claim redress for possible intrusions with their rights stemming from Article 8 ECHR.[36] With regard to the missing information, the ECtHR explicitly notes that 'Bulgarian law thus eschews an important safeguard against the improper use […] of surveillance.'[37]

In addition to the violation of Article 8 ECHR caused by the missing notification duty, the Court also found an infringement of a procedural right for the purpose of Article 13 ECHR. Due to the lack of information of the surveillance measure, the applicants were deprived of the possibility to challenge the violation of their rights before a court. With regard to Article 13 ECHR, the court stipulated:

> It is obvious that when surveillance is ordered and while it is under way, no notification of the persons concerned is possible, as such notification would jeopardise the surveillance's effectiveness. They are therefore of necessity deprived of the possibility to challenge specific measures ordered or implemented against them. However, this does not mean that it is altogether impossible to provide a limited remedy – for instance, one where the proceedings are secret and where no reasons are given, and the persons concerned are not apprised whether they have in fact been monitored – even at this stage.[38]

Although the ECtHR recognizes the difficulty of notifying a person during an ongoing surveillance measure, it clearly insists on the possibility to seek redress in respect of the use of secret surveillance measures in their aftermath.[39]
As the applicant was unable to claim his rights in front of courts because Bulgarian law excluded the notification of the surveillance measure, the ECtHR additionally found a violation of Article 13 ECHR:

> As regards the availability of remedies after the termination of the surveillance, the Court notes that, unlike the legislation in issue in *Klass and Others*, and *Weber and*

31 *Ekimdzhiev*, para 84.

32 *Ekimdzhiev*, para 90.

33 *Ekimdzhiev*, para 90.

34 *Ekimdzhiev*, para 90.

35 *Ekimdzhiev*, para 91.

36 *Ekimdzhiev,* para 91.

37 *Ekimdzhiev,* para 91.

38 *Ekimdzhiev*, para 100.

39 *Ekimdzhiev*, paras 100-101.

> *Saravia*, '…', the SSMA does not provide for notification of the persons concerned at any point in time and under any circumstances. On the contrary, in two judgments of 12 February and 15 May 2004 the Supreme Administrative Court held that the information whether a warrant for the use of means of secret surveillance had been issued was not to be disclosed. The second judgment stated that such information was classified '…'. It thus appears, that, unless criminal proceedings have subsequently been instituted or unless there has been a leak of information, a person is never and under no circumstances apprised of the fact that his or her communications have been monitored. The result of this lack of information is that those concerned are unable to seek any redress in respect of the use of secret surveillance measures against them.[40]

In brief, the Court held in the *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* case that the missing notification of the individual after surveillance has ended does not only violate Article 8 ECHR, but also Article 13 ECHR. The legal protection of the individual in surveillance cases and the obligation to be notified is thus considerably strengthened by the possibility to invoke Article 13 ECHR in addition to Article 8 ECHR. Due to the status of Article 13 ECHR as a procedural right, this possibility remains however limited to cases where the individuals concerned started subsequent legal proceedings.

The clear recognition of an (active) notification duty after surveillance measures have ended in the *Ekimdzhiev v. Bulgaria* case constitutes a remarkable development in the framework of the safeguards against abuse which are necessary in surveillance cases.

5. Planned changes at EU level

Given the foregoing discussion, a recent development in EU data protection law will very likely considerably influence the right to be informed of data collection and surveillance measures. Directive 95/46/EC and the Framework Decision 2008/977 for data processing in police and judicial related contexts should be replaced by a new Regulation and a Directive respectively. This would mean that EU data protection law would be more effectively harmonised than ever before: if adopted, the Regulation would apply directly in the Member States and the Directive would be binding to the result to be achieved (Article 288 TFEU). The planned revision of the two instruments explicitly foresees provisions providing for more transparency including the rules on police and judicial related activities. The proposals were presented in January 2012. Their possible impact on the notification right will be briefly illustrated in the following. It should be noted that the scope of the instruments relates to data processing of the Member States and not to the data processing carried out by EU institutions, agencies and bodies. Following the example of Directive 95/46/EC and Framework Decision 2008/977, the two-fold approach (one instrument for economic related data processing and another one for data processing for police and judicial purposes) is upheld. Before discussing the consequences of this separation and the restriction of the scope in a police and judicial context (5.2), the new provisions relating to the notification requirement in the new regulation are briefly illustrated (5.1).

5.1 Notification in the new regulation replacing Directive 95/46/EC

[40] *Ekimdzhiev*, para 101.

In contrast to Directive 95/46/EC, the right to information of the data subject is now intended to be regulated in one single article. Draft Article 14 establishes in a first paragraph rules applying to the controller notwithstanding whether the data have been obtained from the data subject or not. Compared to Articles 10 and 11 of Directive 95/46/EC, the information which has to be given to the data subject is much more comprehensive and entails, in addition to the details required already due to Directive 95/46/EC (identity of the controller, purposes of processing and other information if necessary), more specific information.

Article 14 (1) of the draft regulation for instance obliges the controller to provide the data subject with its contact details including the contact details of its data protection officer. If the processing is necessary for the performance of a contract, the contract terms and general conditions have to be given to the data subject. In case the data are processed for the purposes of the legitimate interests pursued by the controller, the legitimate interests have to be communicated as well. Further information such as the contact details of the responsible data protection authority, and, if applicable, the intention to transfer the data to a third country or an international organisation must also be given to the data subject. In this context, details to the level of protection afforded by the third state and information relating to the potential access to the data within the third country have to be included in the information.

Similar to the current provisions in Directive 95/46/EC, where the data are not collected from the data subject, the controller should indicate the source of the data.[41] If the data are collected from the data subject, the controller shall inform the data subject of the fact whether the collection of data is obligatory or voluntary as well as the possible consequences of the failure to provide such data.[42] Exemptions only apply in three situations: (a) the data subject is already in possession of the information, (b) the provision of the information is impossible or would involve a disproportionate effort in case the data are not collected from the data subject or (c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law.

Taking the aforesaid into account, an important improvement compared to the current Articles 10 and 11 of Directive 95/46/EC relates to the obligation to communicate information concerning the recipients or categories of recipients of the data, the existence of the right of access to and the right to rectify the data. Whereas in Directive 95/46/EC such information is subject to the condition that the information 'is necessary having regard to the specific circumstances in which the data are collected […]', the proposed provisions refrain from this condition and oblige the controller to communicate such details in any case. [43]

All in all, when comparing the current information duty of Directive 95/46/EC with the proposed provisions of the regulation, the rights of the data subject have been increasingly extended to the effect that more detailed information has to be given to the data subject. Moreover, to specify the criteria stipulated in the proposed articles the Commission should be entitled to adopt delegated acts.

5.2 Notification in the police and justice Directive replacing Framework Decision 2008/977

[41] Art. 14(3), Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25 January 2012, COM (2012) 11 final, hereafter, PGDPR COM (2012) 11 final.

[42] Art. 14(2), PGDPR COM (2012) 11 final.

[43] See above, Arts. 10(1) & 11(1), Directive 95/46/EC.

In addition to the changes with regard to Directive 95/46/EC, the current Framework Decision 2008/977 in police and judicial cooperation is intended to be replaced by a directive.[44]

As mentioned before, the notification of individuals in the framework of police and judicial related activities is currently left to the Member States and not stipulated in form of an obligation in Framework Decision 2008/977. Article 11 of the draft directive would fundamentally change this and would require Member States to inform individuals concerned when personal data about them have been collected. According to this article and very similar to the planned provisions of the draft regulation, previously discussed, information about the identity and the contact details of the controller including the data protection officer, the purposes of the processing, the storage period, the existence of the right to request from the controller access to and rectification or erasure of the data, the right to lodge a complaint to the supervisory authority and the recipients of the data have to be given to the person concerned.[45] Where relevant, the individual has the right to be informed about intended transfers to a third country or international organization, about the level of protection afforded by that third country or international organization and the potential access to the data transferred by authorities to that third country or international organisation under the rules of that third country or international.[46]

Like in the draft regulation, if the data are collected from the data subject, the controller is obliged to inform about the fact whether the provision of personal data is obligatory or voluntary, as well as the possible consequences of failure to provide such data. The individuals should be informed at the time of recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected.[47]

To recognize the specifics in police and judicial related data processing, the draft directive provides for exemptions. Article 11 (4) of the draft directive allows for 5 derogations from the information duty. Member States are allowed to adopt legislative measures restricting or delaying the information right 'to the extent that and as long as such partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the person concerned' in the following cases: (a) to avoid obstructing official or legal inquiries, investigations or procedures; (b) to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or for the execution of criminal penalties; (c) to protect public security; (d) to protect national security and (e) to protect the rights and freedoms of others. These are at a first glance, relatively far reaching exemptions and Member States have the possibility to establish categories of data processing which may wholly or partly fall under the exemptions.[48]

---

[44] Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, 25 January 2012, COM (2012) 10 final, hereafter PDPJP, COM (2012) 10 final.

[45] Art. 11, PDPJP COM (2012) 10 final.

[46] Art. 11, PDPJP COM (2012) 10 final. In addition, 'any further information in so far as such further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected' have to be given.

[47] Art. 11(3), PDPJP COM (2012) 10 final.

[48] Art. 11(5), PDPJP COM (2012) 10 final.

When comparing the current Framework Decision 2008/977 with the draft directive, a first important change relates to the scope of the latter which would include data processing by the national authorities. The current Framework Decision 2008/977 is only applicable in transnational matters and is, among others, therefore subject to criticism (Hijmanns & Scirocco 2009). The new directive would apply to all national authorities 'competent for the prevention detection and investigation of criminal offences' or the execution of criminal penalties and would therefore close the gap produced by Framework Decision 2008/977.[49] Excluded from the scope would however remain the data processing in national security matters and by EU institutions, bodies, offices and agencies.[50] While national security matters do not fall within the scope of EU law, data processing regarding EU institutions, bodies, offices and agencies is, according to the explanatory memorandum of the Commission, 'subject to Regulation 45/2001 and of specific legislation'.[51]

5.3 Notification by EU institutions

While it is perfectly clear that a directive is only applicable to the Member States, it is nonetheless astonishing that the draft directive does not specify the aspect of EU institutions, bodies and agencies in more detail. More specifically, as a consequence of the inapplicability of the rules to EU institutions, bodies, offices and agencies, the fragmented data protection system within the former third pillar at EU level will be maintained.

The Commission's argument that Regulation 45/2001 is applicable in this context can not hide the fact that the specific rules of the former third pillar bodies (e.g. Europol, Eurojust, SIS, CIS) remain applicable as a consequence. Regulation 45/2001 was established to cover the data processing of the Community institutions only under the former first pillar and therefore does not entail specific rules for data processing carried out in a police and judicial related context. In relation to former first pillar institutions, the General Court stated in 2007 in the case *Nikolaou v. Commission* that the rule of law demands that a person targeted by an investigation must be informed as soon as possible of the existence of it, as long as the information does not prejudice the ongoing investigation.[52] One could now argue that the Commission plans to propose a new regulation for the not yet covered former third pillar context at later stage, but this is neither mentioned in the draft directive, nor the draft regulation.

As a result, different data protection regimes with different levels of protection would be created. Regarding the notification requirement, this would have remarkable consequences: As none of the specific rules for the former third pillar (Europol, Eurojust, SIS, CIS) entail the obligation to inform the individual, only the Member States would be obliged to introduce such a requirement. Eurojust even argues that it would have counter-productive effects to require such a requirement because the notification of, for instance, contact persons after surveillance measures have ended 'could have [a] substantially negative impact on the reputation of that person [the person under surveillance], even if the investigation did not have

---

[49] Arts. 1(1) and 3(14), PDPJP COM (2012) 10 final.

[50] Art. 2 (3)(b), PDPJP COM (2012) 10 final.

[51] Explanatory Memorandum , PDPJP COM (2012) 10 final, p. 7, para 3.4.1.

[52] Compare T-259/03, *Nikolaou v. Commission* of 12 September 2007 in paras 263–264, more information in: Boehm, F. (2012), Information sharing and data protection in the Area of Freedom, Security and Justice, p. 231.

any judicial consequence for the person as such.' (Alonso Blas 2010: 243) When following this argument, the missing notification duty would have as a consequence that the notification is excluded especially in sensitive cases in which the state never enacted judicial proceedings (and thus in cases in which the person under surveillance is innocent). This however would run against the basic idea of the notification requirement which intends to enable individuals subjected to surveillance measures to enact infringement proceeding challenging the lawfulness such measures, at least *ex-post*.

This example shows how sensitive the topic of notification is regarded at EU level. Currently, EU agencies and bodies seem to be satisfied with the non-existent obligation to inform the person who has its data introduced in EU databases and systems. The latter however collect and store an increasing significant amount of personal data each year, for example, Eurojust registered 1,372 new cases in 2009 (Eurojust 2009: 50), and Europol had 88,419 objects stored in the EIS and initiated 8,377 cases in 2008 (Europol 2008: 33–35). In absence of the notification duty, EU agencies and databases such as Eurojust, Europol, the SIS and the CIS can therefore collect data and even enact surveillance measure against persons without ever fearing that their measure will be subject to independent control in the future. Therefore, the need for clarifying and harmonized rules also in this context is worth mentioning. Further efforts to reform and harmonize EU related texts (in particular Regulation 45/2001) concerning the notification duty are required.

6. Conclusion

This article has shown a development of the duty to inform persons concerned about the collection and use of their personal data in general and also in the delicate police and judicial related environment. The analysis of the existing and future instruments in this field clearly indicates a tendency towards the obligation to notify individuals to guarantee them an impartial examination of the lawfulness of data collection or surveillance measure and the access to courts to obtain, if relevant, an effective remedy. At CoE as well as at EU level, the information of individuals seems to become an important right in view of the increased instruments and databases established to monitor different parts of the daily life of EU citizens. Whereas currently this right is not yet entailed in the respective EU instruments, the plans to amend Framework Decision 2008/977 include relatively comprehensive provisions in this regard.

Data processing in the framework of the EU databases and information systems is however not yet affected by this development. Individuals concerned do not profit from the protection (soon) offered to them at national level, although the entry in a EU database may have even more wide ranging consequences. The contribution wanted to stress the need for regulation also in this field.

Bibliography

Alonso Blas, D. (2010) 'Ensuring data protection in the field of police and judicial activities: some considerations to achieve security, justice and freedom', *ERA Forum* 11(2): 233-250.

Boehm, F. (2012) *Information sharing and data protection in the Area of Freedom, Security and Justice*, (Heidelberg: Springer)

Dammann and Simitis (eds), *EG-Datenschutzrichtline*, Commentary to Directive 95/46 (Baden-Baden: Nomos Verlag, 1997),

De Hert, P. & Boehm, F. 'The Rights of Notification After Surveillance is Over: Ready for Recognition?' in: Yearbook of the Digital Enlightenment Forum, pp. 19-40.

Ehmann and Helfrich (eds), *EG Datenschutzrichtlinie – Kurzkommentar* (Köln: Verlag Dr. Otto Schmidt, 1999).

Eurojust, *Annual Report 2009* [last accessed 22 June 2012] http://www.eurojust.europa.eu/doclibrary/corporate/Pages/annual-reports.aspx

Europol, *Annual Report 2008* [last accessed 22 June 2012] https://www.europol.europa.eu/sites/default/files/publications/annual_report_2008.pdf

Hijmanns, H. & 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.

Van Brakel R. & De Hert, P. (2011) 'Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies', *Journal of Police Studies* 20(3): 163 - 192.