DE GRUYTER OPEN
International Conference KNOWLEDGE-BASED ORGANIZATION
Vol. XXIII No 2 2017

A NEW DATA PROTECTION DEVELOPMENT IN THE EU JUDICIAL AND CRIMINAL AREA

Gabriela BELOVA, Gergana GEORGIEVA

"Neofit Rilski" South-West University Blagoevgrad, Bulgaria
gbelova@law.swu.bg, georgieva@law.swu.bg

Abstract: *The following article is dedicated to a new data protection regime in the European Union, in particular the Directive (EU) 2016/680 of the European Parliament and the Council on the protection of natural persons regarding processing of personal data by authorities aiming at prevention, investigation, detection and prosecution of crime offences, including execution of criminal penalties. For this purpose, the authors look first at the data protection within the Prüm framework as well as at the relevant provisions of Lisbon Treaty. The important cases of the European Court of Human Rights are analyzed. Whereas in 2014 EU Member states focused on the question whether or not to retain data, the 2016 conclusion was that in some aspects data retention is the most efficient measure to ensure national security, public safety and fighting across serious crimes. The terrorist attacks in Paris and Brussels call to better equip security authorities. The EU legislature made significant progress on the Data Protection regime. The Directive (EU) 2016/680, the so called the 'Police and Criminal Justice Directive', repeals the Council Framework Decision 2008/977/JHA and will enter into force on 6 May 2018.*

Keywords: Prüm framework, DNA, data protection, new Police and Criminal Justice Directive.

1. Introduction

Handing over vital personal information and transferring vast amounts of data across borders on a daily basis could often fall into the wrong hands. Under European Union Law, personal information can be collected legally under strict conditions and for a legitimate purpose and each person has the right to personal data protection. However, contradictory data protection rules in various countries would disrupt international exchanges. Since individuals may be reluctant to transfer their data to a foreign country if they doubt the level of protection in other states, common rules of the European Union have been established to guarantee the protection of one's personal data allowing complaints as well as obtaining redress if the data has been misused within the EU. The ever-increasing necessity to enhance collaboration in combatting terrorism, cross-border related crimes and illegal migration has led to signing the so called Prüm Treaty. It was signed on 27th May 2005 by seven Member States of the European Union (Belgium, Spain, Germany, Austria, France, Luxemburg, and the Netherlands). The data obtained by comparing information should open up new investigative approaches for Member States and as the Treaty states: "**a new dimension in crime fighting**". [2]

On 23 June 2008 the most important aspects of the Treaty were transferred into EU law by the two Framework Decisions, namely Council Decision 2008/615/JHA as well as Council Decision 2008/616/JHA. The manner in which Prüm became a part of EU *acquis* has been harshly condemned by a number of commentators, including

DOI: 10.1515/kbo-2017-0103

the European Data Protection Supervisor who claimed that it was performed in a way permitting just 'limited margin of manoeuvre'. [11]

2. Transformation of Prüm Treaty into a part of EU law

At this time there are three possibilities for the content of Prüm Treaty to become a part of EU law:

- Ratification by MS;
- Enhanced co-operation mechanism;
- Council Framework Decisions.

Under the German Presidency states that are contracting ones avoided the substantive requirements of enhanced cooperating. The Treaty of Prüm only partially became *acquis communautaire* because Council Decisions comprise no provisions related to 'air marshals' and illegal migration.

There are four main elements that are present in the Prüm decisions. The first one is automatic search and comparison of data from national data in the area of DNA, dactyloscopic and vehicle registration data. The second one is related to information exchange for the prevention of offences in the context of some main events concerning a cross-border dimension and regarding possible terrorist offences. This element is followed by police co-operation and the last one is dedicated to the operational chapters being underpinned by Data Protection rules. [6]

3. Prüm's Goal

The major aim of Prüm is to get over long bureaucratic procedures through the creation of automatic exchange of information. [8] An evaluation of the Polish Presidency inferred that the procedure is "complex, technically fraught and expensive". [9] Nevertheless the Prüm Decisions make it possible for MS to look for other MS fingerprints and DNA databases through an automated system within the frameworks of obligatory response times: DNA – 15 minutes; Fingerprints – 24 hours; Vehicles – 10 seconds.

By August 1st 2011 every Member State had to configure their DNA database, which did not actually happen. At present 22 countries are connected within the Prüm network or DNA data exchange, 18 states regarding fingerprints exchange and 19 countries – vehicles exchange. [4]

Its target is the European Union Member States' accreditation of forensic laboratories to one and the same standard, i.e. EN ISO/IEC 125. The aim is the outcomes of their activities, respectively dactyloscopic data and DNA profiles, to be first recognized, then treated as identically dependable in the rest of the Member States of the European Union.

4. DNA Profile

A forensic DNA profile might be obtained from cell material in bodily fluids such as blood, saliva and semen, and - less often - from biological material such as nails, skin flakes and bones. A DNA profile consists of a set of numbers that indicate which genetic markers (or alleles) appear at 10 to 15 places (called loci) that are chosen for their great variability (called polymorphy) across human beings and are located on the 23 pairs of chromosomes which could be found in the nucleus of most human cell types. Chromosomes are composed of long strings of four paired chemical compounds or building blocks, that is T or thymine, A that stands for adenine, C meaning cytosine and G - guanine, arranged in the form of a double helix and constitute the individual's so called genotype or genetic make-up. The numbers in the DNA profile represent the repetitions of sequences of – typically – four such paired building blocks or base pairs, e.g., TACG-TACG-TACG etc., with T always pairing with A, and G with C. [2]

The **first conviction that was based on DNA profiling evidence** happened in England in 1987. Colin Pitchfork received a sentence of life imprisonment for raping and murdering two females. To begin with, a police investigation led to the wrong person, whose name is Richard Buckland.

He was a 17-year-old boy who deceitfully admitted he committed one of the crimes. After an exceptional mass screening of five thousand people with the usage of pioneering "DNA profiling" technology, in the end, Pitchfork was captured. Firstly, Pitchfork had escaped justice by convincing one of his colleagues to take the test instead of him. In April 2016 the first killer caught by DNA has been refused parole.

The UK set up the **first DNA database** in the world in 1995. The United States of America has the biggest database - more than 5 million profiles. Great Britain has the most profiles as a percentage of its population - 4 million, representing 6% of those living on the island.

DNA has played a significant role in crime investigations: helping to convict criminals and acquit innocent people. Genetic profiles could exist on clothes and other items for decades, even centuries, making it possible for police to dig deep into the past in order to deal with "cold cases".

The implementation of the Prüm Treaty involves two types of technical regulations, in particular Inclusion Rules and Matching Rules. In 2011 the European Standard Set (ESS) was extended from six to twelve loci. The Amelogenin locus, which marks for gender, may also be specified but it is not included in the number of matching loci. There could be **full match** - two profiles share all alleles on at least six loci and **near match** - when they share all alleles but one on at least seven loci. [4]

It should be noted that the DNA profile exchange process essentially amounts to sending encrypted (anonymous or pseudonymised data) DNA profiles between the national Prüm (identification numbers) which are not traceable to an individual.

Only if a match is detected, is an encrypted message sent to the custodians of both databases to find the person whom the hit refers to.

The national Prüm database of an MS is a virtual database within or separate from the national forensic database. [3]

5. Prüm Decisions - benefits and concerns

There are numerous *benefits* with regard to Prüm Decisions such as simplified processes to request information and/or data; efficiency gains in international searching; increase in resolution of unsolved crimes; improved response to requests for information associated with crime and terrorism; detection of volume crime as well as serious crimes – can help reveal crime trends and patterns; enhanced crime and terrorism intelligence picture.

The main *concern* related to the Prüm system of exchange of data represents **'rising risk of false positives'** owing to the manner DNA profiles are thought to be the so called 'hit'. [3,7]

The risk of false positives grows bigger since a larger number of MS join the network. It would be justifiable to say that the risk of false positives occurring from using the Automated Fingerprint Identification System 'has not been sufficiently investigated'. Access to DNA samples and profiles can allow unethical abuses (categorisation of individuals as 'risky' based on genetic data). In various aspects, the Prüm arrangements point out to sensitiveness towards the bioethical considerations. [5]

6. DNA, Data protection and HR

The ECtHR in contemplating on the preservation of DNA or fingerprints for forensic usage sounded a cautionary note for states that are in the forefront of technological innovation:

"…any State claiming a pioneer role in the development of new technologies bears special responsibility for **striking balance** between the use of modern scientific techniques in the criminal justice system and important private life interests". (*S & Marper v. the UK*) [12]

The Strasbourg Court in *X. v the Netherlands* case [1978] recognised the following: submitting to a blood test does not make a presumption of blame. This contradicts Article 6 (2) of the European Convention for the Protection of Human Rights and Fundamental Freedoms (1950). [1]

Presently the most typical samples taken for investigative purposes is the collection of saliva or hair samples.

There are obvious disparities between the different national legislations with regard to the suspects under 18. Commonly, there should be an agreement of the minor and their parents, defence lawyer or guardian.

In the UK there are samples that are taken counting on the **gravity of offence** not on the age of the suspect. [1] It looks like the creation of a special database of minors' profiles would be the best option.

In *S & Marper v United Kingdom* [2008] ECtHR acknowledges that storing cellular material is far more perilous for the right to privacy compared to storing the DNA profile. This is so because an analysis of cellular material could display a lot more personal data. [12]

Unrestricted retention of these data is not justifiable; the outcome is a breach of the right to privacy.

7. A Road to a New Data Protection Regime

On 25 January 2012, based on Art.16 TFEU, the European Commission accepted a proposal for the so called General Data Protection Regulation, including a suggestion for the so called Police and Criminal Justice Directive. It has been pointed that a few aspects of the Commission's Draft have had a critical outcome on behalf of the European Data Protection Supervisor. [1] Concerns have been voiced by the European Parliament as well. As far as the European Data Protection Supervisor's say on the data protection reform package is concerned, the Draft Data Protection Directive is not as strong as the Draft Data Protection Regulation. There are non-affected or without any justification certain acts, particularly the rules for Eurojust, Europol, as well as data exchange according to Council Decision 2008/615/JHA. [10] In the following years a lot of recommendations have been tailored.

7.1. New Data Protection Package

The adoption of the new Data Protection Package took place on 27 April 2016 via two secondary legislation acts:

1) Regulation (EC) 2016/ 679 or the General Data Protection Regulation of the European Parliament as well as the Council. It is connected with: protecting persons regarding the processing and free movement of personal data, repealing Directive 95/46 / EC. It shall apply from 25th May 2018. (OJ L119 / 1, 04.05.2016);

2) Directive (EU) 2016/680 of the European Parliament and of the Council. This second act is related to: protecting persons regarding the personal data's processing by the qualified bodies for the aims of preventing, prosecuting, investigationg of penal offenses or the enforcement of crime sanctions. The free movement of this data as well as repealing Council Framework Decision 2008/977/JHA also apply here (OJ L 119 89 04.05.2016). The binding nature of this secondary legislation will certainly make EU Member States comply with established data protection standards.

7.2. New Data Protection Directive (EU) 2016/680

The new Data Protection Directive (EU) 2016/680 is actually the so-called Police and Criminal Law Directive. It has a dual purpose, which is to protect personal data as well as provide exchanges among authorities at national level. [1] It makes a connection between the legislative gap between Directive 95/46/EC, which is the present European Data Protection Law, and Framework Decision 2008/977/JHA.

What the Directive does is harmonise Member States' laws as regards the information exchange among judicial bodies and police. It leaves discretion in

particular fields, e.g. penalties for violation of the Directive in order to respect the various Member States' legal established practices.

Analysts think that the directive is some leaps ahead of Council Framework Decision 2008/977 / JHA since: it concerns both the cross-border and national processing of personal data and aims to improve Member States' mutual work in the combat against terrorism and other criminal offenses in the EU; it ensures that personal data transmitted from outside the EU by law enforcement bodies of criminal law should be adequately protected; it covers the genetic data exchange; it provides that the agreements by the Member States are to be revised in accordance with the Directive's provisions; it sets major principles for the processing of personal data, just when it is needed, in a proportionate manner and in accordance with a particular objective [1].

The processing of personal data in the framework of judicial cooperation in criminal matters as well as police cooperation is characterised by the processing of data with the relation to various categories of data subjects.

This ought not to be an obstacle for the implementation of the right to a presumption of innocence assured by the Charter and the European Court of Human Rights as it has been interpreted in the Court of Justice's case-law and the ECHR.

Thus, where possible, there should be made a differentiation between personal data of varied categories of data subjects. For instance, these could be individuals guilty of a crime; victims; witnesses; individuals holding relevant information or contacts; suspects; suspects' associates as well as criminals that have been found guilty, that is Recital 31.

8. Conclusion

Whereas in 2014 EU Member states focused on the question whether or not to retain data, the 2016 conclusion was that in some aspects data retention is the most efficient measure to ensure national security, public safety and fighting across serious crime. The terrorist attacks in Paris and Brussels call to better equip security authorities [13].

Despite all the innovations, the Data Protection Directive does not include each and every area of freedom, security plus justice. For now the 'old' Data protection regime will apply until the coming into force of the Directive – a period during which the Commission needs to assess and decide upon the necessity to align the provisions of other acts with the ones of the abovementioned Directive. Further progress is envisaged to be observed when Member States apply the Directive's provisions since 6th May 2018.

References

[1] Helena Soleto Muñoz, Anna Fiodorova 'DNA and Law Enforcement in the European Union: Tools and Human Rights Protection' Utrecht Law Review, Volume 10, issue 1 (January 2014), http://www.utrechtlawreview.org

[2] M. D. Taverne , A.P.A. Broeders: The light's at the end of the funnel! Evaluating the effectiveness of the transnational exchange of DNA profiles between the Netherlands and other Prüm countries, University of Leiden, Institute of Criminal Law and Criminology, November 2015

[3] Carole I. McCartney & Tim J. Wilson & Robin Williams 'Transnational Exchange of Forensic DNA: Viability, Legitimacy, and Acceptability' European Journal on Crime Policy and Research, Volume 1, N0 4, 2011

[4] Van der Beek, C.P. Forensic DNA Profiles Crossing Borders in Europe (Implementation of the Treaty of Prüm). [Internet] 2011. Available from: http://worldwide.promega.com/resources/
[5] Prüm Business and Implementation Case, Report of the Home Office, November 2015, presented to the Parliament by the Secretary of State for the Home Department, Cm 9149
[6] Rocco Bellanova "The Prüm Process": The Way Forward for EU Police Cooperation and Data Exchange? Security v. Justice
[7] Helen Wallace 'The UK DNA database and the European Court of Human Rights; Lessons India can learn from UK mistakes', www.genewatch.org
[8] Eric Töpfer, 'Europe's emerging web of DNA databases' http://database.statewatch.org/article.asp?aid=30566
[9] Chris Jones "Complex, technologically fraught and expensive" – the problematic implementation of Prüm Decision, Statewatch analysis
[10] European Data Protection Supervisor, Report 2012/C 192/05, OJ C 192, 30.6.2012, pp. 13-15.
[11] Opinion of the European Data Protection Supervisor on the Initiative of the Federal Republic of Germany, with a view to adopting a Council Decision on the implementation of Decision 2007/…/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (2008/C 89/01)
[12] *S. and Marper v. the United Kingdom*, Applications nos. 30562/04 and 30566/04, Judgment of 4 December 2008.
[13] Белова Г., Марин Н. Многовекторни измерения на сигурността в Черноморския регион, сп. Международна политика, бр. 1/2016, с. 81-91