UDC 336.7:340.5(043.2)

Pika Šarf, Junior Researcher
at the Institute of Criminology at the Faculty of Law, Ljubljana
PhD candidate at the University of Ljubljana Faculty of Law, Slovenia

INTEROPERABILITY OF INFORMATION SYSTEMS IN THE AREA OF FREEDOM, SECURITY AND JUSTICE: A SURVEILLANCE NIGHTMARE FOR THIRD COUNTRY NATIONALS

An American author writing about the impact of then newly adopted EU Data Protection Directive [1] on trans-Atlantic relations observed in 2002 that "*to the extent that Europeans feel vulnerable as a result of terrorism, they may shift their emphasis away from data privacy and toward protective anti-terrorist surveillance programs"* (Salbu, 2002)" In the early days of 2000's, his dystopian prediction could not feel more ill-suited: data protection regime was for the first time harmonised on the EU level due to the implementation of the Data Protection Directive by the Member States. In 2000 the EU introduced data protection rules for its own institutions and organs [2]. Data protection was gaining its momentum. However, around the same time EU began a rather different and less publicly discussed process towards generalised surveillance of third country nationals (TCNs) in the fight against terrorism and serious crime. This was conducted by granting law enforcement access to the existing information systems in the Area of Freedom, Security and Justice (AFSJ), establishing new databases "in order to fill the information gaps", and finally, interconnecting all previously separated databases with the adoption of two interoperability regulations. This article will look into EU's data gathering practices in the fight against terrorism by focusing on the most recent development in the field, namely the interoperability of the information systems in the AFSJ.

In order to ensure high level of security EU has in the past 25 years established legal basis for six large-scale centralised information systems: Schengen Information System (SIS II), Visa Information System (VIS), European Asylum Dactyloscopy Database (Eurodac), European Travel Information and Authorisation System (ETIAS), Entry-Exit System (EES) and European Criminal Records Information Exchange System for Third Country Nationals (ECRIS-TCN). SIS II, VIS and Eurodac are already fully operational, however EES, ETIAS and ECRIS-TCN are still under development and are expected to become functional in the next couple of years. A plethora of information systems closed the information gaps by storing personal data of tens of millions of TCNs effectively capturing almost the entire non-EU population present on the Schengen territory or even just trying to enter the Union (Vavoula, 2019). Even more importantly, the data gathered for an entirely different purpose gradually became available to law enforcement

agencies and Europol as a measure in the fight against terrorism and serious crime therefore blurring the line between migration control and law enforcement in the EU (Quintel, 2018; Blasi Casagran, 2017).

With the introduction of additional three systems, the information exchange landscape in the AFSJ became difficult to navigate due to its complexity and fragmentation (COM(2016) 205 final, 2016). In order to overcome this shortcoming, in 2016 the Commission proposed [3] to make all of the information systems in the AFSJ interoperable. The terrorist attacks in Paris and Brussels, coupled with the unprecedented challenges posed by the migrant crisis, forced the EU to re-think its policy towards border management, migration control and law enforcement, while creating an environment prone to security-oriented solutions, which was confirmed when the two interoperability regulations were swiftly adopted in 2019 [4]. Interoperability is defined as "*the ability of information systems to exchange data and to enable the sharing of information*" (COM(2016) 205 final, 2016) and consists of four components:

1. *European Search Portal* (ESP) would allow competent Member State authorities and Union agencies to simultaneously search multiple EU information systems (SIS, VIS, Eurodac, EES, ETIAS, ECRIS-TCN), Europol data and Interpol databases;
2. *Shared Biometric Matching Service* (shared BMS) would enable search and comparison of biometric data (fingerprints and facial images) contained in all of the AFSJ information systems with the exception of ETIAS;
3. *Common Identity Repository (CIR)* would create and store an individual file composed of biographical and biometric data of every person included in VIS, Eurodac, EES, ETIAS or ECRIS-TCN;
4. *Multiple Identity Detector (MID)* would establish and store identity confirmation files of TCNs.

Although the names used to describe the interoperability components - "matching service", "repository", "identity detector" - try to conceal their true nature, they cannot change the fact that they *de facto* entail the establishment of three additional databases (BSM, CIR, MID), which inevitably raises questions relating to the right to private life and protection of personal data enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. Although both the right to privacy and protection of personal data are not absolute rights and can be limited subject to conditions stipulated in Article 52 of the Charter, it is hard to argue the requirements are fulfilled in the present case. Wide-ranging, untargeted surveillance extending even to individuals whose activity is in no way associated with serious crime or terrorism does not meet the conditions of necessity and proportionality established in the jurisprudence of the CJEU (Digital Rights Ireland, 2014; Tele2 Sverige, 2016). Interoperability not just facilitates, but entirely bypasses strict rules of access to the data stored in each information system for law enforcement purposes and enables national law enforcement agencies as well as Europol routine access to

the data of millions of third country nationals, including biometric data such as fingerprints and facial images. Access to sensitive data of innocent individuals regardless of their behaviour is particularly troublesome and could additionally lead to infringement of protection against discrimination pursuant to Article 21 of the Charter (Opinion 1/15, 2017).

Interoperability does not just complicate the whole structure of information sharing and data protection in the Area of freedom, security of justice, but even further blurs the lines between border and immigration control on one hand and the fight against terrorism and serious crime on the other. Moreover, the newly adopted measures could implicate that EU is following the path taken by the US in the fight against terrorism by conducting mass surveillance on third country nationals and moving away from its traditional stance on universal application of human rights by affording third country nationals lower standard of protection. The author mentioned in the introduction was not so wrong after all.

References

1. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50.

2. Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 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 OJ L 8, 12.1.2001, p. 1–22.

3. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) COM/2017/0794 final; Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226 COM/2017/0793 final.

4. Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA, OJ L 135, 22.5.2019; Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816, OJ L 135, 22.5.2019, p. 85–135.