

Uniwersytet Śląski w Katowicach

Wydział Prawa i Administracji

mgr Aleksandra Kacała-Szwarczyńska

Promotor: dr hab. Joanna Nowakowska-Małusecka, prof. UŚ

SUMMARY OF THE DOCTORAL DISSERTATION
PROFILING ON THE INTERNET
TO COUNTER TERRORISM
STUDY ON EUROPEAN LAW

The aim of this study was to investigate the legal aspects of profiling potential terrorists with the use of the Internet. The author conducted an analysis of whether, and if so, how profiling violates or restricts human rights. As a result of the research, an attempt was made to evaluate this tool, as well as to create a catalogue of situations and conditions in which it is permissible.

In the first chapter, author explores the general introductory issue. The history of the emergence of the Internet and the information society was discussed. The social and technological context of the subject of the dissertation was presented. The next part of this chapter analyses the basic concepts used at work, namely profiling and terrorism. Legal regulations concerning these issues were also discussed. Legal norms have been divided into general sources and sources of broadly understood European law (European Union and Council of Europe law).

Then, the second chapter examines the scope and principles that should apply to profiling. It also explains what data may be processed in accordance with European Union law, and indicates which entities may perform such data operations. This chapter also discusses the issues of automatic profiling, the most important aspect of which is automatic decision making. Then, the admissibility of data transfer to third countries was analysed. Data transfer in view of the cross-border nature of the Internet is an important tool for profiling and countering international terrorism. It was also noted that European standards for the protection of personal data set strict rules, the compliance of which by third countries often causes many difficulties, in particular in relation to the more liberal United States of America in this respect.

The third chapter is devoted to the guarantees of human rights protection. It analyses the admissibility of excluding guarantees or limiting human rights. Next, it was considered whether and under what circumstances the terrorist threat could constitute a premise for the

restriction of human rights. The rights that individuals, in the event of profiling, have been investigated successively. The rights of an individual that enable the protection of their data include the right to access data, the right to rectify or delete personal data and limit their processing. The obligations of data controllers, which include creating lists of categories of processing activities and records of processing operations, have also been analysed. Then, the reasons justifying the exclusion of protection of individual rights were indicated. Restrictions on rights motivated by reasons of state security have shown the ineffectiveness of the protective mechanisms that are formally available to individuals. Finally, the institutional guarantees for the protection of personal data were analysed. The scope of duties and principles of operation of data supervision inspectors and state supervisory authorities were examined.

Chapter four deals with the risks associated with profiling. The analysis covered errors and lack of transparency, risk of discrimination, violations of the right to privacy, and the right to be forgotten. In theory, it is possible to exclude these risks, thanks to precise legislation and ensuring appropriate technical standards. Complete automation of these kinds of processes is not desirable. Human should be present at every stage of processing - system design, data collection, data processing and decision making.

The subject of the last - fifth - chapter is profiling in practice. First, it examined whether surveillance programs are used in the fight against terrorism. In view of the positive answer to this question, an analysis was made of how the European Union and the Council of Europe relate to mass surveillance programs in their activities. Finally, the internal regulations of Belgium, France, Germany, Poland and the United Kingdom were analysed in relation to surveillance programs. These countries had legislation that allowed the use of surveillance tools, despite the well-established jurisprudence of the CJEU and the ECtHR in this regard. In the course of work on this hearing, proceedings against these countries, apart from Poland, were conducted before the CJEU aimed at establishing the compliance of internal regulations with EU law. The judgments in these cases indicate trends in the development of further anti-terrorist law with regard to personal data in the EU Member States, including Poland.

At the end of the hearing, the thesis was confirmed that the existing legal provisions do not fully effectively protect data subjects in relation to the use of mass surveillance tools by states, such as profiling in the security sector. The research questions and hypotheses were also addressed. *De lege ferenda* postulates were formulated in the field of profiling carried out in the public sector in order to counteract terrorism in Polish law.