Identity, Race and Ethnicity in Constitutional Law Working Paper Series No. 5

MTA Law Working Papers
2025/16

Ethnic Data and Law Enforcement — A Brief Insight into the Hungarian Context

Kovács Szitkay, Eszter

ISSN 2064-4515
http://jog.tk.mta.hu/mtalwp
Társadalomtudományi Kutatóközpont – MTA Kiválósági Kutatóhely
Eötvös Loránd Kutatási Hálózat
Centre for Social Sciences – MTA Centre of Excellence
Eötvös Loránd Research Network

Ethnic Data and Law Enforcement — A brief insight into the Hungarian context

Eszter Kovács Szitkay[*]

Abstract. The chapter explores the relationship between ethnicity and data protection regulation and practice from a Hungarian context. Its aim is to outline a problem-posing line of thought on the recurring appearance and disappearance of ethnic data in law enforcement work. In a country such as Hungary, where in principle the collection of such data is subject to very tight and strict regulation, the trajectory of such data can be partially traced, but many of its parts are obscured, a feature worthy of attention not only for its regulatory solutions, but also for its implications for criminology and ethnic profiling, for example. The dilemma is clear: we are dealing with highly sensitive data in an environment that could easily leave the subjects concerned in a vulnerable position; hence, knowledge of the practical steps of the procedure is crucial. As the regulation presented in this chapter indicates, beyond the dilemmas mentioned above, the practice must also face up to its inconsistency and contradictory nature. In order to unravel this emergent and vanishing dynamics of ethnic data, the chapter adopts the following thematic approach: first, it clarifies its concept and legal framework in the Hungarian context, including regulation at the European level, followed by a presentation of examples from the spectrum of law enforcement work, and finally concluding with the findings.

Keywords: ethnic data, law enforcement, data collection and process, Hungary

1. Introduction

The debate surrounding the concept, collection and process of ethnic data have long been of concern to both theorists and practitioners, not to mention legislators—how to capture it, what the pros and cons of its collection are, what it should be used for, and ultimately how it relates to human rights; ethnic data collection is "a complex issue, particularly because of the great variety of stakeholders whose consensus it presupposes: minority communities, statisticians, data protection agencies, equality bodies and policymakers."[1] Practices in this area also vary within the European Union,[2] given the different interpretations of international and European legislation by national authorities;[3] some take a more restrictive,[4] others a more pro-

[*] Junior research fellow, HUN-REN Centre for Social Sciences Institute for Legal Studies; PhD student, University of Public Service Doctoral School of Law Enforcement, kovacs.szitkay.eszter@tk.hu.
The research was carried out in the framework of No. 134962 Hungarian National Research and Innovation Office Grant. The research was carried out and the journal Special Issue was published in the framework of No. 134962 Hungarian National Research and Innovation Office Grant on Legal approaches to operationalize nationality and ethnicity.

[1] Farkas (2017) 6.

[2] "Research on national practices shows that there is great discrepancy among Member States regarding the terminology, methodology, format of questions and sources used to collect data on racial or ethnic origin, if they do so at all." Van Caeneghem (2019) 163.

[3] Van Caeneghem (2019) 171.

[4] "Research shows, however, that many EU Member States interpret data protection legislation restrictively, thereby hindering data collection for anti-discrimination purposes." Van Caeneghem (2019) 172. In footnote 112, Van Caeneghem points at the ENAR Shadow Report. which—among other countries—mentions Hungary which follows the before-mentioned interpretation.

collection stance, with appropriate regulation and objectives.[5] Two major camps emerge: one view is that the collection of ethnic data essentializes ethnic groups and contributes to racial discrimination, while others see "migration, language, education level and poverty data are not effective proxies for measuring discrimination based on racial and ethnic origin."[6] Thus, their collection and process may arise in many areas, even indirectly,[7] and in terms of their purpose, referring back to the previous sentence, equality and anti-discrimination efforts are strongly marked.[8]

Ethnic data—i.e., information on ethnicity (I am using "race" and "nationality" as synonyms, although they can mean different things in terms of content[9])—when it arises in the course of law enforcement activity, presents a complex and difficult-to-follow picture in the Hungarian context. The (personal) data can be any information relating to the data subject, who is or can be identified from any piece of information.[10] In principle, it can be encountered in several places in the course of law enforcement activities: it appears as a factual element in the context of hate crimes, it appears in the list of prejudice indicators defined in ORFK Order No. 30/2019, 18 July of the Chief of the National Police on the implementation of police tasks related to the handling of hate crimes, or in ORFK Order No. 22/2011, 21 October on cooperation and liaison between the body established for the performance of general police tasks and the Roma minority self-governments, but it also appears in ORFK Order No. 27/2011, 30 December on police measures in multicultural environments. The question under examination is whether all this produces data in a procedural, documentary sense, either from the side of the person concerned or in a concrete or aggregated form, and how this is reflected in law enforcement activity? The chapter seeks to capture a snapshot of the status of this data in a particular segment of law enforcement activity, and to formulate critical reflections that point to the inconsistencies that arise from the regulation. My aim is not to provide a "literature review," but rather, through the presentation of the literature, to highlight anomalies and contribute to the ongoing professional discourse on this issue.

At the outset, it is important to point out that, contrary to appearances, the processing of ethnic data is intended to facilitate the achievement of legislative objectives and the efforts to eliminate institutional discrimination.

The chapter has the following structure: after a brief introduction of the Hungarian legal environment, I will present the practice of the collection and processing of ethnic data, pointing out examples from the field of law enforcement practice, and conclude with critical problem statements.

2. The legal embeddedness of ethnic data

[5] For country practices, see Balestra – Fleischer (2018).

[6] Farkas (2017) 6.

[7] See e.g. van Bekkum – Zuiderveen Borgesius (2023) 3.

[8] Balestra – Fleischer (2018) 12.

[9] "*Race* is a controversial category. In the social science literature, it is widely understood to be a social construct rather than a biological trait (in the biological sense, the entirety of humanity constitutes one single race) without a theoretically or politically uniform definition" (italic in original text) Pap (2015) 33. Regarding nationality, we can rely on the term set out in Recommendation 1201(1993) of the European Council: "For the purposes of this Convention (1) The term 'Convention' in this text refers to the Convention for the Protection of Human Rights and Fundamental Freedoms., the expression 'national minority' refers to a group of persons in a state who: a. reside on the territory of that state and are citizens thereof; b. maintain longstanding, firm and lasting ties with that state; c. display distinctive ethnic, cultural, religious or linguistic characteristics; d. are sufficiently representative, although smaller in number than the rest of the population of that state or of a region of that state; e. are motivated by a concern to preserve together that which constitutes their common identity, including their culture, their traditions, their religion or their language."

[10] Infoact, Article 3 (1) and (2).

2.1. Briefly about the relevant regulation at the European level[11]

At the European level, the Council of Europe 1981 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data and Protocols (Convention 108(+)) and Regulation (EU) 2016/679 Of The European Parliament And Of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR) apply. Basically, the rules on the processing of ethnic data are discussed in the context of sensitive data, as "Personal data revealing racial or ethnic origin are among the special categories of data the processing of which may lead to a violation of data subjects' rights, including the right to privacy, because of their specific nature."[12]

According to Article 6.1-2. Convention 108(+): "1. The processing of: [...] personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life, shall only be allowed where appropriate safeguards are enshrined in law, complementing those of this Convention. 2. Such safeguards shall guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination." But the existence of these safeguards is often interpreted by states as a kind of prohibition in practice.[13]

While Convention 108(+) is more permissive, the GDPR prohibits[14] the processing of sensitive data, including ethnic data, Article 9.1.: "Processing of personal data revealing racial or ethnic origin [...] shall be prohibited." But it also includes a list of cases that are exempt: Articles 9.2–9.3 GDPR. "The extensive list of exemptions included in the GDPR gives Member States a margin of manoeuvre in relation to the lawful processing of sensitive data. This opens the door for the adoption of legal frameworks for equality data processing."[15]

It is important to note that they do not address the definition of ethnicity either.

2.2. National law

Ethnic data is defined in Act CXII of 2011 on the right to informational self-determination and on the freedom of information (Infoact) as Article 3 (3) "personal data revealing racial or ethnic origin", which is categorised as personal data that is also considered sensitive data.[16] This regulation does not in itself shed light on what ethnicity or the related conceptualisation problematic means, so for a clearer conceptual framework I will take the approach of Andras L. Pap, who foresees that the imprecision and inconsistency in the application of the concepts causes many problems. On the concept of "race," we learn that there is in fact a scientifically proven existence of one race, i.e. humanity belongs to one race, and that different "racial characters" do not refer to different races; and that "ethnicity" "refers to social groups whose members are linked by a common origin, tradition, ancestry, language or culture. Accordingly, ethnicity may change over time and cannot be clearly established by an outside observer."[17]

[11] For more information, see Van Caeneghem (2019) chapters 3.5.1–3.5.2.

[12] Van Caeneghem (2019) 213.

[13] Van Caeneghem (2019) 214.

[14] Van Caeneghem (2019) 216.

[15] Van Caeneghem (2019) 218.

[16] Infoact, Article 3 (2) and (3).

[17] M. Tóth – Pap (2012) 244.

Concerning data protection, the law lays down strict rules to protect personal data, especially sensitive data. Accordingly, if the personal data is also considered as sensitive data, its processing is authorised as follows according Article 5 (2) of the Infoact "Sensitive data (a) as set out in points (c) to (d) of paragraph 1; or (b) may be processed if absolutely necessary and proportionate for the implementation of an international treaty proclaimed by law or if ordered by law in the interests of the fundamental right guaranteed by the Fundamental Law, national security, the prevention, detection or prosecution of criminal offences or in the interests of national defence." Article 5 (1) (c) "except as provided for in point (a), necessary and proportionate for the protection of the vital interests of the data subject or of another person, or for the prevention or elimination of an imminent threat to the life, limb or property of a person; or (d) in the absence of point (a), the personal data have been explicitly disclosed by the data subject and the disclosure is necessary and proportionate for the purpose of the processing."

We can see that there is a strict framework for the treatment of ethnic data. This strictness is a result of the change of regime: until the 1990s it was possible to collect such data; for example, between 1971 and 1989 offenders of a Roma origin were still counted. However, this practice was ended by Act LXIII of 1992 on the Protection of Personal Data and the Disclosure of Data of Public Interest (DPA), which defined ethnic data as sensitive data. Therefore, after that, its recording or disclosure required legal authorisation or the written consent of the data subject.[18]

In the 1990s, the interpretative framework for the protection of personal data changed, and the Constitutional Court now regards it as a right to informational self-determination. In this light, we should mention two Constitutional Court decisions, the principles of which led to the adoption of the DPA and then the Infoact: "The Constitutional Court—continuing its practice according to the Constitutional Court Decision 20/1990—interprets the right to the protection of personal data not as a traditional right of protection, but also taking into account its active aspect, as a right of informational self-determination. Accordingly, the right to the protection of personal data, as guaranteed by Article 59 of the Constitution, has the content that each person has the right to decide for himself whether his personal data are disclosed and used. The collection and use of personal data must therefore be subject to the consent of the person concerned; the entire processing chain must be made transparent and verifiable for everyone, i.e. everyone has the right to know who, where, when and for what purpose their personal data are being used. By way of exception, the law may provide for the mandatory disclosure of personal data and may also prescribe the way in which it is used. Such a law restricts the fundamental right of informational self-determination and is constitutional if it meets the conditions required by Article 8 of the Constitution."[19]

I would add—referring to the legal regulation already set out above—that if there is a legal basis for data processing, then the relevant data can be collected.

Let's see some examples! These include hate crime offences, as well as the ORFK orders mentioned above and the prejudice indicator list, to be explained later, which create a legal basis and obligation for data processing.

3. Ethnic data in criminal justice

It is necessary to briefly look at the link with the criminal justice system. Despite the fact that the strict rules of the Infoact allow room for the processing of sensitive data and in the cases mentioned above it is based on a legal obligation, I have assumed that ethnic data is widely used in the procedure, but the conclusion is the following: such data is not actually

[18] Kerezsi – Gosztonyi (2014) 239–240.

[19] Reasoning of the decision of the Constitutional Court No. 15 of 13 April 1991.

collected by the criminal justice system in any form, even if a legal fact would suggest its presence or other regulators suggest a legal basis for it (e.g. an ORFK order).

To summarise, in the context of law enforcement, the judiciary and the penitentiary system, the ethnicity of persons is not recorded,[20] hence not only individual data but also statistical statements (i.e. not traceable to specific persons) are not produced; neither the various data sheets nor the various registration systems have the IT facilities (a rubric, if you like) to record it.

Typical cases where ethnic data is generated—i.e. not recorded statistically—can be extensive, both in terms of cases and individuals, with the victim, perpetrator and witness all being able to generate such data.

The simplest is when the perpetrator or victim voluntarily declares their ethnicity, which may be relevant to the investigation/ criminal proceedings. In practice, this information is not recorded, it is merely presented as part of the facts in a "free text" way. The next case relates to hate crimes: since the victims may not immediately identify themselves as the victims of such a crime, it is sometimes the case that the competent authority has to carry out a legal reclassification based on the list of indicators laid down in ORFK Order No. 30/2019, 18 July on the implementation of police tasks related to the handling of hate crimes, i.e. from hooliganism to violence against a member of the community, and thus ethnicity is revealed.

Moving away from hate crime, one general area is worth mentioning: characterisation. A witness's description of the perpetrator is recorded by means of the description method, which is also used to search for the person. In this case, for example, although such a description may point to a specific ethnicity—or the witness may make such a statement about the perpetrator—this is not stated *expressis verbis* in the description of the wanted person.

Overall, therefore, no ethnic data will be generated in the criminal proceedings, so we cannot explore the way forward. However, this information is already very important for us, because it will allow making critical observations that will help us to shed light on the anomalous situations that arise from this kind of processing of ethnic data and how that, despite the best intentions, causes problems in practice.

4. Forensic considerations

Personal information about the suspect, with physical attributes being an important component, plays a major role in the detection of crime. The description of the person can be used in criminal proceedings in a number of cases: to locate and identify the perpetrators of crimes, to locate and apprehend suspects in an unknown location, to locate missing persons, to locate unidentified bodies, to identify persons of unknown identity, i.e. persons who cannot or do not want to identify themselves, or for certain tactical methods of criminal investigation and team tactics.[21] All this shows that the uniqueness of a person's external or internal characteristics can be used in many areas. And the description of the person: "a forensic tool for the identification of a person and a corpse or body, which contains differentiated information with regard to the principles and subject of the description of the person: the general human biological characteristics (biological sex, age, height, weight, body composition, type and location of obesity, posture, colour composition); the shape of each part of the body (size, shape, asymmetry, deformity of the face and body parts); functional criteria (gait, speech, behaviour, smell); and other characteristics (tattoos, body jewellery, clothing, etc.), i.e. the description of general characteristics and particularities (special features)."[22]

[20] Kerezsi – Gosztonyi (2014) 240.

[21] Anti (2017) 75–82.

[22] Anti (2017) 65.

We can see the wide range of characteristics that can be recorded in the course of the description of a person, which can be used to give a very accurate picture of the person, but according to previous practice, it is not used for identification but for recognition, it is used for detection, and is only indirectly involved in evidence.[23]

With a special focus on the search for wanted persons, Article 3 (2) c) of Act LXXXVIII of 2013 on the wanted persons registration system and on the search and identification of persons and objects lays down the following—closely related to our topic: "(2) The register of wanted persons shall contain the following data: c) specific data revealing the racial origin, religious beliefs, sexual behaviour or political opinions of the requested person".[24]

How can we interpret these frameworks? On the one hand, we see that person specification provides a wide scope for the detection and description of these attributes, so that the possibility of capturing characteristics that could be said to be specific to an ethnicity by creating a person specification is present. The statutory Article cited only addresses race, but we can treat these concepts as synonymous—which I have explained by explaining the concepts—so presumably the Article is about being able to clearly identify, for example, a person of African-American descent. So we can be careful to indicate that we can find suggested legal basis even in this case. The serious problem, however, is that neither the law nor its explanatory memorandum provides a conceptual framework for what is meant by race—so we cannot know how and in what ways ethnicity is different—and so conceptualisation is lacking. As explained above, this issue is far from clear-cut. The European Union Agency for Fundamental Rights also states, in the context of ethnic profiling, that "The description of the suspect, which is based on the description of the crime victim or witnesses, includes personal information such as skin, hair and eye colour, height and weight, and clothing worn. A good suspect description provided to the police can be used to carry out stop and search operations to take suspects into custody. However, if law enforcement officers are provided with an overly general suspect description that includes racial, ethnic and other similar characteristics, they cannot use it as a basis for actions such as stop and search, as many innocent persons who share these characteristics are likely to be stopped."[25] It is not that this is specifically forbidden, but such a general wording could indeed lead to misleading, discriminatory actions, and therefore it is not appropriate in itself.

An interesting attitude can be detected when, for example, the nicknames of Roma people include the ethnicisation of external characteristics in everyday life: black hair, brown, sooty skin, etc., but in the course of the description of the person, it is still necessary to pretend that society does not use or know them, so that when the person giving the description refers to such characteristics, the authority in charge does not record it in a way that clearly identifies ethnicity. Thus, although the description could indirectly create a legal basis for recording ethnicity, the actual legal provisions do not follow this interpretation.

5. Predictive policing and automated justice

In this subchapter, I will describe the mechanisms that are at the heart of performing operations on data, and I will use this brief description to illustrate the importance of performing operations on data that do not ultimately distort the result. In a broader sense, by this

[23] Anti (2017) 73.

[24] I will only mention here that Act XLVII of 2009 on the criminal records system, on the register of convictions handed down by the courts of the Member States of the European Union against Hungarian nationals and on the register of biometric data in criminal and law enforcement matters, was supposed to provide guidance in the detection of the "road" in question, but in the end it did not provide any relevant information.

[25] European Union Agency for Fundamental Rights (2010) 63.

information gap: "[...] we make it much easier for criminal justice actors: they do not have to face the question of whether there is discrimination in the justice system, and they do not have to do anything about it, because there is no verified information or research data available. So we know little about the drivers of crime, and especially little about its municipal and neighbourhood aspects."[26]

Predictive policing and automated justice are computer methods and software that help law enforcement agencies by using calculations to predict where, when and who will commit criminal offences. It is predictive analytics, so it is not just about collecting masses of data to look for patterns, but also making predictions for the future. Further, it is also necessary to distinguish between predictive policing (which focuses on crime prevention and investigative solutions) and automated justice (which aims to make prosecution and sentencing objective). One of the most important pieces of information for the topic is that in both cases, the data collected on crime and criminality form the database that is processed to achieve the stated objectives.[27] One form of automated decision-making is profiling, the content of which is also laid down in Article 3 (27) of the Infoact: "profiling means any processing of personal data by automated means intended to evaluate, analyse or predict personal aspects relating to the data subject, in particular his or her performance at work, economic situation, state of health, personal preferences or interests, reliability, behaviour, location or movements."

Here we also need to talk about ethnic profiling. Balázs M. Tóth and Andras L. Pap introduce the following concept: "Ethnic profiling occurs when, in the course of law enforcement, law enforcement or other activities where the person acting in an official capacity has the authority to take legally binding action against targeted persons, and the selection of the persons to be targeted is made with at least a minimum of discretion and is based on the ethnicity or colour of the person concerned."[28]

What we can observe with these concepts is that we can see the distortion caused by the lack of recording of ethnic data: since collection is not possible, predictive policing and automated decisions will give us misleading information to guide us[29] and, more importantly, create huge obstacles to preventing acts of discrimination.[30]

It is necessary to mention the recently adopted European Union regulation on artificial intelligence (EU AI Act),[31] as it is a relatively recent development. Contrary to the General Data Protection Regulation (GDPR) of the European Union, which does not apply to "the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data"—since it is regulated by Directive (EU) 2016/680 of the European Parliament and of the Council[32] (GDPR Recital 19)—, the EU AI Act includes a prohibition on predictive identification based solely on profiling or on the assessment of a

[26] Kerezsi – Gosztonyi (2014) 237–238.

[27] Harmati – Szabó (2020) 25–26; see also Kisfonai (2023).

[28] M. Tóth – Pap (2012) 47.

[29] For more on the misleading inferences that can be drawn from data and the importance of the context in which the data were generated, see e.g. Heaven (2020); Grierson (2019).

[30] On a different topic, but on the prevention of discrimination in AI, see van Bekkum – Zuiderveen Borgesius (2023).

[31] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance).

[32] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

person's personality traits and/or characteristics (EU AI Act Article 5 (1) d)). However, there are a number of concerns that can be identified about the effectiveness of its application, at least for the time being, highlighting—according to Jessie Levano—conceptual ambiguities ("profiling" and "assessment of personality traits and characteristics") and the general exemption for national security purposes.[33]

6. ORFK Orders

ORFK Order No. 27/2011, 30 December on police measures in a multicultural environment is also related to the conceptual issue of ethnicity and the legal basis for the collection of ethnic data. In the instruction, we can trace the conceptual confusion to which we have already referred, and despite this confusion, we can still read the groups with regard to which the instruction is interpreted. It considers the objectives to be achievable through minority liaison and working groups, and then refers back to the ORFK order on cooperation and liaison between the police and Roma minority self-governments, which seems an interesting solution, as it seems to remove the multicultural environment that was originally the starting point. Although the directive does not single out the Roma, the specific characteristics of Hungarian society suggest that they are most affected.[34] What is interesting from a data protection point of view is the "identification of ethnicity." When mentioning minority communities, the instruction explicitly mentions only the Roma and refugees, but not other minorities or immigrant groups listed in the Act CLXXIX of 2011 on the Rights of Nationalities (Nationality Act). It considers it essential "the existence of a conflict of values between ethnic, religious or other groups or communities' with different cultural traits, behavioural patterns and values from the majority and the majority society, which is criminal, i.e. to be assessed in the dimension of criminal law (or at least the law of violation of rules)."[35]

From the point of view of the generation and identification of ethnic data, this is interesting because it is able to delimit, on the basis of the aspects indicated (cultural, ethnic, religious traits, etc.), the group that differs from the majority, and if we look at the text as a whole, the naming of the Roma makes this delimitation or identification even clearer. Thus, once again, we see an example of a suggested legal basis for the appearance of ethnic data in the legislative context.

7. Concluding remarks

To date, the collection and processing of ethnic data has been the subject of intense debate among experts and, as we have seen, different levels of regulation and different countries are not in complete agreement. The objectives behind data protection are clear and understandable. The weight of historical experience makes it clear to us that the creation of such databases can be dangerous. However, it is worth considering that databases based on other data (for example, on extreme poverty) could also be used to make discriminatory provisions.[36] In any case, at an international level, various documents have also articulated the need for countries to have information on the situation of minorities in their territories[37] and,

[33] Levano (2024).
[34] Pap (2019) 23–25.
[35] Pap (2019) 23–24.
[36] M. Tóth – Pap (2012) 238.
[37] Kállai – Jóri (2009) 21.

more generally, the need to have the right information available to promote equality and anti-discrimination efforts.

The aim of this chapter was to present the anomalies between theory (regulation) and practice in the Hungarian context. What emerges from the case studies presented is the Murphy’s Law of racism,[38] which aptly captures the problem common to all these cases. A kind of East-Central European phenomenon is the highly contradictory situation in which the perpetrator—if there is a discriminatory intent behind his act—has no definitional problem in determining the identity of his victim’s minority group—or indeed the concept of a minority group—but it is the defenders, practitioners and academics who have a difficulty in identifying it.[39] The extent of the issue is demonstrated by the fact that the phenomenon is not only present in the spectrum of law enforcement work, but is also clearly present in the practice of desegregation litigation.[40]

It should be seen that by banning the collection of ethnic data “we have thrown the baby out with the bath water”[41]. Despite all the good intentions, a counter-productive effect has been achieved: by making the collection of ethnic data subject to such strict rules, the very protective function has not been achieved. The introduction of ethnic data collection has been mooted before: in 2009, the then Data Protection Commissioner (András Jóri) and the Member of Parliament for National and Ethnic Rights (Ernő Kállai) already took the view that it should be introduced for several reasons, notably to help fight discrimination.[42] “The need for data collection is more of a theoretical issue: international documents agree that data collection is an indispensable tool for combating discrimination and for developing truly effective measures and programmes.”[43]

It could be argued that the rigorous data collection framework imposed by the legislature provides a degree of protection for those who might otherwise face a tension between the rules and the reality on the ground. There is a presumed caution on the part of practitioners, who find it easier to claim that they are acting in accordance with the law and are careful with ethnic data. Therefore, despite the existence of arguments and practical proposals aimed at resolving this tension, the data collection principles previously outlined remain in force for the time being. However, it is crucial to emphasise that collaboration from the grassroots level, including the police and the Working Group Against Hate Crime,[44] can also influence the development of legislation and more precise practice.

In conclusion, although the study does not offer solutions to resolve these anomalies, nor does it take a position on the issue of collection/non-collection, but only refers to the professional discourse, the presentation of anomalies that show the clash between “theory” and practice can lead to a further reflection on the issue towards a solution that can ensure legal certainty and adequate access to rights/justice.

[38] Pap (2019) 99.

[39] Pap (2012) 88.

[40] Pap (2012) 100–104.

[41] Kerezsi – Gosztonyi (2014) 237.

[42] M. Tóth – Pap (2012) 235.

[43] Kállai – Jóri (2009) 26.

[44] Website of Working Group Against Hate Crime (Gyűlölet-bűncselekmények Elleni Munkacsoport): https://gyuloletellen.hu.

© Kovács Szitkay Eszter

MTA Law Working Papers

Kiadó: ELTE Társadalomtudományi Kutatóközpont (MTA Kiválósági Kutatóhely

Székhely: 1097 Budapest, Tóth Kálmán utca 4.

Felelős kiadó: Boda Zsolt főigazgató

Felelős szerkesztő: Kecskés Gábor

Szerkesztőség: Hoffmann Tamás, Lux Ágnes, Mezei Kitti

Honlap: http://jog.tk.mta.hu/mtalwp

E-mail: mta.law-wp@tk.mta.hu

ISSN 2064-4515