Case C-57/23

Summary of the request for a preliminary ruling pursuant to Article 98(1) of the Rules of Procedure of the Court of Justice

Date lodged:

2 February 2023

Referring court:

Nejvyšší správní soud (Czech Republic)

Date of the decision to refer:

26 January 2023

Applicant:

JH

Defendant:

Policejní prezidium

Background to the main proceedings

Application to determine whether the performance of identification procedures, the retention of samples and information concerning the applicant, and the subsequent retention of personal data thus obtained in connection with his prosecution for a criminal offence constitute an unlawful interference.

Factual and legal context of the request for a preliminary ruling

Article 267 TFEU

The questions referred

(1) What degree of distinction between individual data subjects is required by Article 4(1)(c) or Article 6 in conjunction with Article 10 of Directive 2016/680? Is it compliant with the obligation to minimise personal data processing, and with the obligation to distinguish between various categories of data subjects, for national law to permit the collection of genetic data in

WORKING DOCUMENT

respect of all persons suspected or accused of having committed an intentional criminal offence?

(2) Is it in accordance with Article 4(1)(e) of Directive 2016/680 if the necessity of continued retention of a DNA profile is assessed, with a reference to the general prevention, investigation, and detection of criminal activity, by Police authorities on the basis of their internal regulations, which frequently means in practice that sensitive personal data is retained for an unspecified period without a maximum limit for the duration of the retention of that personal data being set? If not, by what criteria should the proportionality of the period of the retention of the personal data collected and retained for that purpose be assessed?

(3) In the case of particularly sensitive personal data falling under Article 10 of Directive 2016/680, what is the minimal scope of the substantive or procedural conditions for obtaining, retaining, and deleting such data that must be regulated by a 'provision of general application' in the law of a Member State? Can judicial case-law qualify as 'Member State law' within the meaning of Article 8(2) in conjunction with Article 10 of Directive 2016/680?

Applicable European legislation

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 (OJ 2016 L 119, p. 89) – Articles 4 to 6, 8, and 10.

Applicable national legislation

Zákon č. 273/2008 Sb., o Policii České republiky (Law 273/2008 on the Police of the Czech Republic; the 'Police Law') – Paragraph 65:

'(1) The Police may, in performing their tasks for the purpose of future identification of

(a) A person suspected of having committed an intentional criminal offence or a person who has been informed that he or she is suspected of having committed such a criminal offence,

[…]

WORKING DOCUMENT

take fingerprints, identify physical features, perform measurements of the body, obtain visual, audio, and similar recordings, and take biological samples that make it possible to obtain information about genetic make-up.

[…]

(5) The Police shall delete the personal data obtained pursuant to paragraph 1 as soon as their processing is no longer required for the purpose of the prevention, investigation, and detection of criminal activity or for the prosecution of criminal offences […].“

Paragraph 65 of the Police Law is implemented by means of internal procedural measures of the Police of the Czech Republic, in the form of *pokyny policejního prezidenta (Guidelines of the Police President)*. The contents of those guidelines are not public and access to them is provided to individual applicants. The referring court has not been privy to their contents.

The case-law of the referring court is also of relevance, as, according to it, the lawfulness of the obtaining or retention of personal data requires not only compliance with the conditions set in Paragraph 65 of the Police Law but also the performance of a proportionality test in every particular case.

Facts of the case and original proceedings

1 The Police of the Czech Republic, Department for the Investigation of Corruption and Financial Crime of the Criminal Police and Investigation Group at the Pilsen Office (‘Defendant’) launched criminal prosecution of the applicant on 11 December 2015 for the offence of breach of trust. The offence allegedly consisted of the granting of a subsidy, despite the applicant knowing that the application under assessment does not meet the requirements for the provision of a subsidy.

2 On 13 January 2016, the defendant questioned the applicant in the course of criminal proceedings and ordered identification procedures to be performed. Despite the disagreement voiced by the applicant, the defendant took fingerprints, performed a buccal smear from which it created a DNA profile, took the applicant’s photographs and description, which it then placed in the relevant Czech Police databases (‘the contested interference’).

3 By final judgment of the Městský soud v Praze (Prague City Court) of 15 March 2017, the applicant was convicted of both the offence of a breach of trust and the crime of misconduct in public office. The applicant committed that crime and that offence as Deputy Minister, thereby making use of his significant influence on the decision to approve the subsidy, and he purposefully advanced the approval of a subsidy application for a civil association and the payment of that subsidy despite knowing that the subsidy applicant failed to meet the conditions for the provision

WORKING DOCUMENT

of that subsidy. By those actions, the applicant caused damage to the Czech Republic amounting to a total of CZK 4,500,000.

4 By an application lodged on 8 March 2016, the applicant sought a decision determining the contested interference as unlawful.

5 By judgment of 23 June 2022, Prague City Court granted the application and ruled the contested interference unlawful. Furthermore, it ruled that the retention of the personal data of the applicant thus obtained in databases of the Police of the Czech Republic is also unlawful. Consequently, the Prague City Court ordered that the defendant delete all of the applicant's personal data retained by it from databases of the Police of the Czech Republic.

6 The defendant challenged the judgment of the Prague City Court by an appeal lodged with the referring court.

Basic arguments of the parties to the original proceedings

7 *The defendant* claims that the contested interference was not conducted unlawfully. It claims that the only criterion for the collection of genetic material is, in cases such as the present case, set by Paragraph 65 of the Police Law, which states that the person concerned must be a person accused of an intentional criminal offence or a person who has been informed that he/she is suspected of having committed an intentional criminal offence. That criterion was met in this case. The defendant holds that it was not competent to assess any other criteria.

8 Furthermore, the defendant stresses that it assessed the proportionality of the collection and retention of the applicant's personal data. In doing so, it took into account the factor of recidivism, the potential escalation of the actions, as well as the fact that the applicant had already committed administrative offences on several occasions in the past, i.e., repeatedly committed unlawful conduct. As regards the duration of the retention of the applicant's personal data, the defendant stressed that the Police of the Czech Republic has an established mechanism of regular (internal) review of the necessity of the retention of personal data. Furthermore, it states that criminal proceedings in the applicant's case were completed in 2017, with the imposition of a four-year suspended sentence, i.e., relatively recently. Finally, in view of the alleged insufficient publication of internal police regulations, the defendant stressed that the internal regulations concerned were provided to the public within the framework of the right to information and that legal regulation is always inevitably supplemented by case-law, which is also the case of Paragraph 65 of the Police Law.

9 *The applicant* stressed in his statement, first and foremost, that, at the time of the actions taken by the Police of the Czech Republic, no review of the proportionality of the interference took place. The action was simply conducted automatically by the police authorities, with a reference to Paragraph 65(1)(a) of the Police Law, and the fact that the applicant had been accused of an intentional

WORKING DOCUMENT

criminal offence. The arguments added by the defendant *ex post*, as to the offender having committed other unlawful actions in the form of administrative offences, and that therefore his personal data should continue to be kept in police databases, are unconvincing, just like the abstract and unfounded references to the possibility of recidivism. The applicant expresses his surprise at the fact that, according to the defendant, 5 years after conviction is a period too short for the deletion of that data, when, in some cases, the conviction may be expunged within the same period. Furthermore, the applicant criticises the lack of publication of police guidelines pertaining to the performance of identification procedures in a situation when the publication of legislation is a necessary foundation of the rule of law. In a state respecting the rule of law, all measures that may interfere with fundamental rights must be regulated directly by statute. Internal police organisational rules, which do not constitute legislation, and cannot substitute for such statutory rules.

Summary of the grounds for the order for reference

General remarks

10 The referring court has questions as to the compliance of certain aspects of national legislation concerning the obtaining and retention of personal data for the purpose of future identification, in particular sensitive personal data in the form of a DNS profile, with EU legislation, as well as with the case-law of the Court of Justice and the European Court of Human Rights (ECtHR). In this context, the referring court holds that the interpretation of Directive 2016/680 is key for the decision in the case at hand; however, before elucidating the background to the individual questions referred, the referring court deems it appropriate to mention two general points that are shared by all three questions referred.

11 First: Directive 2016/680 is a relatively new EU legal instrument with respect to which there is no relevant case-law of the Court of Justice. Existing case-law concerning Regulation 2016/679 (‘GDPR’) or its predecessor in the form of Directive 95/46 certainly does provide useful bases for interpreting a number of the issues before the referring court in the present case; however, it is not evident to what extent the GDPR regulation is indeed automatically applicable by analogy to the specific application framework of Directive 2016/680. After all, if both regimes were to be automatically identical, it is not evident why the EU legislator deemed it important to enact a comprehensive and specific legal regulation in the form of Directive 2016/680 as a *lex specialis* in relation to the GDPR. Consequently, it can be assumed that the protection of natural persons with regard to the processing of personal data for the purposes of the prevention, investigation or prosecution of criminal offences is to differ in certain aspects from the general regime of personal data protection. The common denominator of all three questions referred is the effort to discover wherein exactly that difference lies.

WORKING DOCUMENT

12 Second: the case referred concerns the extensive collection of a particularly sensitive type of personal data: genetic material and the DNA profile of persons obtained therefrom. That type of personal data is expressly referred to in Article 10 of Directive 2016/680, which delimits genetic information to the regime of "processing of special categories of personal data" for which it envisages the regime of "strict necessity" of processing, connected with the existence of "appropriate safeguards for the rights and freedoms of the data subject'; however, it is not evident from that legal framework or from existing case-law of the Court of Justice, including that related to the similar regulation under the GDPR, how this "extra-special" framework is to differ in practical terms from the already special framework of Directive 2016/680 and the high level of protection of personal data envisaged therein.

13 It is characteristic of the entire situation that the criteria on the basis of which a decision is made not to carry out identification procedures, or an order is issued to delete personal data already obtained, exist in the form of an exemplary list solely in case-law; however, there is no prototype for them in the law. Furthermore, in practice, the decision about such an interference being (dis)proportionate, made on the basis of many of these criteria, will be made with a considerable delay, by an administrative court. It is not common for a police authority performing identification procedures, typically in the early stages of investigation, to be able to carry out the required type and scope of evaluation, because the information concerned may not even be available to it.

The first question

14 ECtHR case-law has repeatedly formulated a requirement with a view to the protection of the right to privacy pursuant to Article 8 of the European Convention on Human Rights (ECHR), that the national law of an ECHR contractual party distinguish between criminal offences in connection with which DNA samples are collected having regard to their societal gravity. In the opinion of the ECtHR, perpetrators of serious criminal acts, in particular of violent acts, with respect to which the collection and storage of a DNA sample is legitimate, cannot be approached in the same manner as the perpetrators of less serious criminal offences (cf., in particular, judgments of 13 February 2020, *Trajkovski and Chipovski v. North Macedonia*, complaints No 53205/13 and 63320/13; of 13 February 2020, *Gaughran v. the United Kingdom*, complaint No 45245/15; of 22 June 2017, *Aycaguer v. France*, complaint No 8806/12; or of 4 December 2008, *S and Marper v. the United Kingdom*, complaints No 30562/04 and 30566/04).

15 In general the case-law of the Court of Justice also, although in the context of the interpretation of legislation other than Directive 2016/680, insists on the requirement of proportionality between the seriousness of an interference with fundamental rights (in the form of collection of personal data) and the seriousness of the criminal activity – cf., for example, judgments of 6 October 2020, *La Quadrature du Net and Others*, C-511/18, C-512/18 a C-520/18, EU:C:2020:791,

WORKING DOCUMENT

paragraph 140; of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 102; of 2 October 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, paragraphs 56 and 57, or Opinion 1/15 *(PNR Agreement EU-Canada)* of 26 July 2017, EU:C:2017:592, paragraph 149).

16 It remains unclear as to what type of proportionality is envisaged here and to what extent the logic of the building of databases (systemic, legislative proportionality) can automatically be replaced by an assessment of individual proportionality having regard to the specific perpetrator in each individual case (specific, casuistic proportionality). In other words, if the legislator made a sufficient distinction on the legislative level (in terms of the types of criminal offences and in view of their seriousness, and setting additional general, proportionate criteria), would it then still be necessary to assess the proportionality of each individual collection in each individual case?

17 It appears that the national legislator is of the opinion that it has already considered the proportionality of the obtaining of identification details at first hand in Paragraph 65(1) of the Police Law, as it restricted its application solely to intentional criminal offences, whereby it adequately differentiated between individual data subjects. Based on this logic, no further considerations concerning individual proportionality in specific cases are required; however, this line of thinking is deemed inadequate.

18 Hence, the question arises as to the degree of legislative or judicial differentiation expected in this regard from Member States by Directive 2016/680. Article 6 of Directive 2016/680 seems to require only a distinction between the personal data of suspects and convicted persons, on the one hand, and victims and third parties on the other; however, this list is only illustrative (introduced with the words "such as"). The requirement as to the proportionality of the data processed clearly follows from the principles set out in Article 4 of the Directive, as well as from case-law; nevertheless, the specific scope of the provision remains unclear regarding the question at hand.

The second question

19 The second question concerns the proportionate duration of the period of retention of identification data by police authorities. Neither Directive 2016/680 nor applicable national legislation set out a specific timeframe.

20 It follows from Article 4(1)(e) of Directive 2016/680 as well as from general principles and case-law of the Court of Justice merely that personal data are to be kept for no longer than is necessary having regard to the purposes for which they are processed; however, it is not clear how that logic is to be applied in a situation when the declared purpose is the prevention, investigation, and detection of criminal activity, a purpose which is, by its nature, prospective and unlimited in time.

WORKING DOCUMENT

21 In practice, two different types of proportionality, pursuing different objectives, collide in the assessment of the proportionality of the term for which personal data is kept: *structural* on the one hand and *individual* on the other. If the *prevention, investigation, and detection of criminal activity* were accepted as a legitimate objective on a general level, the logical and appropriate means for achieving it would be to retain information about a maximum number of data subjects for a maximum possible period of time. A police database from which an applicant would have to be removed upon request after a certain period would no longer fulfil a meaningful role in the detection of criminal activity.

22 Conversely, in the context of an examination of proportionality in the case of applications for deletion from police databases with regard to *individual* persons or offenders, the continued registration in a police database is seen as a continuation of a type of a punishment, which will, sooner or later, focus on the question of the expiration of a period from the formulation of a suspicion or conviction of the offender and his or her subsequent orderly life, including speculation regarding the risk of recidivism.

23 It is understandable that a periodic internal review by the Police of the Czech Republic of the continued legitimacy of the retention of identification data obtained will lean towards pursuing the structural objective of effective investigation and discovery of criminal activity. Hence, the question arises whether it is compatible with EU law for national law not to set a maximum limit on the period of retention possible, with the understanding that on the basis of periodic internal review by police authorities, DNA profiles obtained will tend to be kept without any time restriction.

24 In this context, the referring court notes that it is familiar with the concept of the ‘right to be forgotten’ embodied in the case-law of the Court of Justice and subsequently codified in Article 17 GDPR. The question arises, however, to what extent that approach and case-law are transferable to the context of police databases and Directive 2016/680, the meaningful functioning and usability of which can only be ensured if those databases – in metaphorical terms – ‘do not forget’.

The third question

25 The referring court has no doubt that the internal police regulations, in the form of the Guidelines of the Police President, do not meet the conditions as to the quality or as to the publication of legislation. They do not constitute legislation and conceptually cannot possess the qualities of ‘law’, within the meaning of Article 8(2) of Directive 2016/680.

26 The provisions of Paragraph 65 of the Police Law undoubtedly have the qualities of “law of a Member State”. However, in itself this provision is not sufficiently certain and detailed as to meet the requirements of Article 8(2) in conjunction with Article 10 of Directive 2016/680. The provisions of Paragraph 65 of the

WORKING DOCUMENT

Police Law do not contain, among other things, any regulation of specific conditions for retention, the types of information that may be obtained from a sample, and in terms of the continued retention of DNA profiles, the conditions subject to which they should be deleted. And it does not contain any of the guarantees required by Article 10 of Directive 2016/680.

27 That statutory regulation is, however, made complete by constitutionally conforming interpretation and case-law. In this regard, recital 33 of Directive 2016/680 stipulates that 'where this Directive refers to Member State law, a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament […]. However, such a Member State law, legal basis or legislative measure should be clear and precise and its application foreseeable for those subject to it […].'

28 It also follows from settled ECtHR case-law that 'law' in the context of a test of the legality of restrictions of fundamental rights includes not only law but also case-law (judgments of 26 April 1979, *Sunday Times v. the United Kingdom (No 1)*, complaint No 6538/74, paragraph 47; of 24 April 1990, *Kruslin v. France*, complaint No 11801/85, paragraph 29, and of 10 November 2005, *Leyla Şahin v. Turkey*, complaint No 44774/98, paragraphs 84-98).

29 More recent case-law of the Court of Justice has been, however, marked in this regard by higher requirements in terms of the quality and publication of the 'law' that restricts fundamental rights. The Court of Justice ruled, for example, that, given the high level of protection in cases of particularly serious restrictions of fundamental rights, 'only a provision of general application could meet the requirements of clarity, predictability, accessibility and, in particular, protection against arbitrariness' (cf., e.g., judgment of 15 March 2017, *Al Chodor*, C-528/15, EU:C:2017:213, paragraph 43). A similar conclusion was reached by the Court of Justice in a number of cases concerning personal data protection, when it insisted on the requirement that legal regulation 'must also lay down the substantive and procedural conditions' governing any use and access to traffic and location data obtained (cf., more recent judgments of 2 March 2021, *Prokuratuur*, C-746/18, EU:C:2021:152, paragraph 49, or of 5 April 2022, *Commissioner of An Garda Síochána and Others*, C-140/20, EU:C:2022:258, paragraph 104).

30 The logic of stricter requirements in terms of the quality of legislation laying down minimum requirements for the obtaining, retention, and destruction of DNA samples and DNA profiles obtained therefrom should probably also apply to the present case. After all, Article 10 of Directive 2016/680 in conjunction with recital 37 of the Directive, which places this personal data in a specific category of data requiring special protection, would support this conclusion. In that case, EU law would require that general legislation lay down at least a general framework for the database, the question of access, a type of use of the DNA information that is more precise, including barriers to their use, but, above all, in line with Article 10, appropriate safeguards for rights and freedoms, including in the form of a clear differentiation of the types of criminal offences in which DNA profiles

WORKING DOCUMENT

may be obtained and the conditions subject to which they must or may be subsequently destroyed.

31 National law applicable to the present case does not, however, regulate any such matters. If similar requirements were to be automatically applied in the case at hand and in other cases before administrative courts on the basis of the present Paragraph 65 of the Police Law, the consequence would necessarily be radical: the court would be obliged to declare the national legal regulation as incompatible with Article 8(2) in conjunction with Article 10 of Directive 2016/680, and any biological DNA samples and DNA profiles obtained on their basis as automatically unlawful.

WORKING DOCUMENT