



Collecting digital personal information in criminal matters

Introduction

The EU has already taken important measures to promote cooperation between judicial and police authorities in criminal matters. This is important because cross-border crime can only be prevented and combated through strong cooperation. Nowadays, society has become digitised to a great extent, and with it, so has criminality. As a result, an unprecedented amount of information is available digitally, including information about criminality. The issue of access to this unprecedented volume of information raises new legal questions.

We, as Member States, must keep pace with this development and establish a general legal framework which allows us to gain access to digitally available information including when that information is related to an identified or identifiable natural person, while respecting the right to a private life and the right to the protection of personal data.

Proposal

- The Netherlands calls for codification of the principles concerning the collection of personal data, on the basis of the essential case law of the EU Court of Justice.

Problem definition using examples

1. The smartphone of a suspect of organized crime will contain information about his criminal actions: communications with co-suspects, photographic and video material about criminal offenses, and information about travel- movements in relation to criminal actions. At the same time, access to the smartphone seriously infringes the private life of the data subject. Because the smartphone will (mostly) also contain information about the private life that allow precise conclusions to be drawn concerning the private life of the data subject.

2. A provider of a communications service that (predominantly) focuses on the criminal market holds information about organized crime. Recent practical examples show that access to that information is necessary to combat serious crime. At the same time, access to that information seriously infringes on the private life of the data subject.

The services of such providers are not limited to a Member State. Nor are users of such a communication service or the smartphone mentioned in the first example limited by national borders.

The Netherlands believes that due to the cross-border dimension of collecting information through digital means, and mutually transferability and admissibility of evidence in the EU, we must further refine cooperation between judicial and police authorities in criminal matters.

Legal questions and draft article

The issue of access to this unprecedented volume of information raises new legal questions. Due to the current lack of a clear uniform framework in the EU, competent authorities and judges in the Member States may have different legal opinions on the issue of collecting digital information. These varying legal opinions block further judicial cooperation in criminal matters.

Access to digital information constitutes a limitation of the data subject's right to respect for private life and the right to protection of personal data. Against the background of the principle of proportionality, access to information should respect the essence of these rights. A balance must be found between the importance of access to information for the investigation of crimes on the one hand and the importance of respecting the rights of the data subject on the other.

Directive 2016/680 provides a general framework for processing personal data for the purposes of law enforcement. A specific framework for the collection of large amounts of personal data is missing. Directive 2014/41 provides a specific framework for the collection of personal data, but its scope is limited to the European Investigation Order. Similarly, Regulation 2023/1543 provides a specific framework, but its scope is limited to the European Production Orders and the European Preservation Orders.

The EU Court of Justice was called upon to rule on the balance between the two aforementioned interests due to the lack of clear EU legislation in the criminal justice field, which does not provide a concrete



starting point for answering legal questions, particularly on the interpretation of the EU charter on the matter of data protection in relation to criminal investigations.

The Netherlands advocates the necessity for the Member States to take their responsibility to stress that the EU legislator establish a general legal framework for the collection of personal data within the framework of the principle of proportionality that accommodates the different legal systems and legal traditions of the Member States. In this light, The Netherlands calls for codification of the principles concerning the collection of personal data, on the basis of the essential case law of the EU Court of Justice.

A suitable framework that does justice to all interests involved can be found within existing EU-law. The Netherlands proposes that the framework for issuing an European Investigation Order under Directive 2014/41 and issuing an European Production Order or European Preservation Order under Regulation 2023/1543 also applies to the collection of personal data under Directive 2016/680. Consequently, there will be no room for a different framework when interpreting Directive 2016/680 against the background of the EU Charter of Fundamental Rights because the EU legislators will have provided an identical framework under Directive 2016/680.

This requires an amendment in Directive 2016/680. The proposed first paragraph is similar to Article 4(2) of Directive 2016/680. The proposed second and third paragraphs are equivalent to Articles 6(1) and 2(c) of Directive 2014/41. The proposed fourth paragraph is equivalent to Article 5(4) of Regulation 2023/1543.

Draft article 4a – to be added in Directive 2016/680

Article 4a

Collection of personal data

1. *The controller may only collect personal data for the purposes set out in Article 1(1), where the following conditions have been met:*
 - (a) *the controller is authorised to collect personal data for such a purpose in accordance with Union or Member State law; and*
 - (b) *the collection of personal data is necessary and proportionate for such a purpose.*
2. *The conditions referred to in paragraph 1 shall be assessed by the controller in each case.*
3. *The controller referred to in paragraph 1 is:*
 - (i) *a judge, a court, an investigating judge or a public prosecutor competent in the case concerned;*
or
 - (ii) *any other competent authority as defined by the Member State which, in the specific case, is acting in its capacity as an investigating authority in criminal proceedings, with competence to order the collection of personal data in accordance with national law. In addition, before it is collected, the collection shall be validated, after examination of its conformity with the conditions for collecting under this Directive, in particular the conditions set out in this Article, by a judge, court, investigating judge or a public prosecutor.*
4. *If the collection of personal data constitutes a serious restriction on the data subject's right to respect for private life and the right to protection of personal data, the collection can only be justified by an Article 1(1) purpose of combating serious crime. Serious crime refers to:*
 - (i) *criminal offences punishable in the Member State by a custodial sentence of a maximum of at least three years; or*
 - (ii) *specific offences which, in accordance with the principle of proportionality, constitute a serious offence under the law of the Union or Member State.*