ECJ Ruled on Police Access to Mobile Phone Data

Thomas Wahl

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

AUTHOR

Thomas Wahl
Senior Researcher
Max Planck Institute for the Study of Crime, Security and Law

Published in
2024, Vol. 19(3) eucrim pp 189 – 191
ISSN: 1862-6947
https://eucrim.eu

On 4 October 2024, the ECJ, sitting as Grand Chamber, delivered an important judgment on the respect for data protection rules if police attempt to access data on a mobile phone. The ECJ laid down parameters for such access under EU law. The ruling concerned scope and limits of the following data protection principles:

- Principle of "data minimisation";
- Prior review by a court or independent administrative authority;
- Information to be made available or given to the data subject.

Facts of the case and questions referred

In the case at issue (C-548/21, *Bezirkshauptmannschaft Landeck*), Austrian customs officers seized a package containing 85 grams of cannabis. Subsequently, in a police investigation relating to narcotics trafficking, two police officers conducted a search of the recipient's (CG's) residence and questioned him regarding the consignor of the package. Following CG's refusal to give access to the police officers to the connection data on his mobile telephone, those officers seized the telephone. Next, an expert of the Landeck District (Austria) police station and – after his failure – experts at the Vienna Bundeskriminalamt (Federal Office of the Criminal Investigation Police) attempted in vain to unlock the telephone in order to access the data contained therein.

The Austrian police did not have an authorisation from the public prosecutor's office or a court, and the attempts to unlock were not documented in the police files. Furthermore, CG was not informed promptly of the attempts to make use of his mobile telephone. He only became aware of the police measures during proceedings before the Landesverwaltungsgericht Tirol (Regional Administrative Court, Tyrol, Austria), the referring court, before which he challenged the lawfulness of the seizure of his mobile telephone.

Given that the criminal investigations only concerned a minor offence (punishable pursuant to the Austrian Law on Narcotics by a term of imprisonment of up to a year only) and recalling the ECJ's judgments in *Ministerio Fiscal* (→ eucrim 3/2018, 155-157) and *Prokuratuur* (→ eucrim 1/2021, 28-30), the Tyrol court sought clarification on the following three issues:

- Constitutes full and uncontrolled access to all the data contained in a mobile telephone so serious an interference with fundamental rights that this access must be limited to fighting serious offences?
- Are national legal rules precluded, pursuant to which the criminal investigation police can gain, without the authorisation of a court or independent administrative body, full and uncontrolled access to all data contained in a mobile telephone?

- Are national legal rules compatible with the right to an effective judicial remedy, in so far as they do not require the police authorities to inform the owner of a mobile telephone of the measures for the digital exploitation of that telephone?

The applicable law

The ECJ first countered arguments against its jurisdiction because the request for preliminary ruling erroneously referred to the e-privacy Directive 2002/58/EC. The judges in Luxembourg confirmed that the Directive is indeed not applicable. If Member States directly implement measures that derogate from the rule that electronic communications are to be confidential, without imposing processing obligations on providers of electronic communications services, the protection of the data of the persons concerned is covered not by Directive 2002/58, but by national law only, subject to the application of the Law Enforcement Data Protection Directive 2016/680. This is the case here because the police attempted to directly access personal data contained in a mobile telephone, without any intervention on the part of a provider of electronic communications services having been sought.

However, the judges in Luxembourg stated that the procedure before the ECJ was lawful when the Court reformulated the questions referred in light of the relevant Directive 2016/680.

Application of Directive 2016/680

The ECJ then rejected arguments put forward by certain governments that Directive 2016/680 is only applicable if personal data contained in a mobile telephone were successfully accessed by law enforcement authorities. The ECJ clarified that an access attempt falls within the scope of Directive 2016/680. This conclusion can be drawn from the wording, context, and objective of Art. 3 no. 2 of the Directive as well as from the principle of legal certainty: if the applicability of Directive 2016/680 were to depend on the success of the attempt to access personal data contained in a mobile telephone, that would create uncertainty incompatible with the principle of legal certainty for both the competent national authorities and individuals.

Requirements for the protection of fundamental rights

With regard to the questions posed by the Austrian court, the ECJ examined whether national legal rules which afford the competent authorities the possibility of accessing data contained in a mobile telephone, for the purposes of the prevention, investigation, detection and prosecution of criminal offences in general, without making reliance on that possibility subject to prior review by a court or an independent administrative body, are compatible with the principle of “data minimisation”, as an expression of the principle of proportionality, enshrined in Art. 4(1)(b) of Directive 2016/680.

In this context, the ECJ pointed out that the limitations which, under Directive 2016/680, can be placed on the right to the protection of personal data (Art. 8 CFR), and on the right to respect for private and family life (Art. 7 CFR), must be interpreted in accordance with the requirements of Art. 52(1) CFR, which include respect for the principle of proportionality. Within this framework, the ECJ makes the following key statements:

- The access sought may relate to a very wide range of data (e.g. messages, photos and internet browsing history), and could thus allow very precise conclusions to be drawn concerning the private life of the data subject. In addition, they may include particularly sensitive data. Therefore, such an interference with the fundamental rights to privacy and the protection of personal data must be regarded as serious, or even particularly serious.

- The seriousness of the offence under investigation is an essential parameter when examining the proportionality of the serious interference. However, to consider that only the fight against serious crime may justify access to such data would unduly limit the investigative powers of the competent authorities. This would result in an increased risk of impunity for criminal offences in general and undermine the objective of achieving an area of freedom, security and justice within the European Union.
- That being said, in order to meet the requirement that any limitation on the exercise of a fundamental right must be "provided for by law"', it is for the national legislature to define with sufficient precision the factors, in particular the nature or categories of the offences concerned, which must be taken into account.
- In order to ensure compliance with the principle of proportionality, where access to personal data by the competent national authorities carries the risk of serious, or even particularly serious, interference with the fundamental rights of the data subject, that access must be subject to a prior review carried out by a court or by an independent administrative body.
- This review must take place prior to any attempt to access the data concerned, except in cases of duly justified urgency, in which case this review must take place within a short time.
- In the context of this review, the court or independent administrative body must be entitled to refuse or restrict an access request falling within the scope of Directive 2016/680 where it finds that the interference with fundamental rights which that access would constitute would be disproportionate.
- Law enforcement authorities must take account of the enhanced level of protection for the processing of sensitive data (as laid down in Art. 10 of Directive 2016/680).

It is now for the referring court to draw the appropriate conclusions from the ECJ's clarifications. However, given that the interference of the attempts to access personal data on the defendant's mobile phone was serious and no prior independent authorisation was issued, the Austrian rules seem not compatible with the requirements by the EU law.

Information rights before data access

Lastly, the ECJ replied to the question whether CG should have been informed of the attempts to access the data contained in his mobile telephone in order to be able to exercise his right to an effective remedy. In this regard, the ECJ interpreted Art. 13 of Directive 2016/680 (information to be made available or given to the data subject), and, Art. 54 of Directive 2016/680 (right to an effective judicial remedy against a controller or processor) in light of Art. 47 CFR (the fundamental right to an effective remedy and to a fair trial).

According to this legal framework, it is for the competent national authorities which have been authorised by a court or an independent administrative body to access stored data to inform the data subjects of the grounds on which that authorisation is based, as soon as such information is no longer liable to jeopardise the investigations carried out by those authorities.

For the present case this means: Given that CG was aware of the seizure of his mobile phone, informing him of the access attempts would not have harmed the investigation; thus, there were no circumstances that justified a limitation of the right to be informed (Art. 13(3) lit. a) and b) of Directive 2016/680). Hence, CG should have been informed beforehand of the attempts to access the data contained in his mobile telephone.

Put in focus

The ruling in "*Landeck*" has been considered "groundbreaking for investigative work and data protection throughout the European Union." In any case, the judgement is an important contribution to the interpretation

of the Law Enforcement Data Protection Directive 2016/680, which is often overshadowed by the General Data Protection Regulation.

The ECJ allows access to cell phone data for all criminal offences, but adds a big “BUT”: Member States must have legislation that respects the proportionality principle. This includes definition of the type or categories of offenses that justify access as well as judicial or independent administrative authorisation *before* police access to the cell phone data to ensure the balance between law enforcement interests and citizens' fundamental rights. The ECJ also stressed that in urgent cases the authorisation cannot be completely waived but should “take place within a short time”.

The ruling gains importance beyond the legal situation in Austria. EU Member States should scrutinize their national law and potentially adapt it to the parameters set by the judges in Luxembourg.

The “Landeck” case may also prompt national debates for legal reforms. National codes of criminal procedure often do not appear to have been prepared for digitalisation.

In Germany, for example, the rules on search and seizure in the Code of Criminal Procedure (StPO) do not currently differentiate between complex digital data carriers and other objects. This means that it is currently solely up to the interpretation practice of the public prosecutor's offices and investigating judges to concretise the principle of proportionality in individual cases. The suspects’ laptops and smartphones are often seized even if the suspicions are tenuous and the vague hope of finding evidence is based solely on experience.

This is why German lawyers recently called for a change to the existing regulations. Like the ECJ, the majority of the members of the “German Jurists' Conference” (Deutscher Juristentag) rejected the blanket exclusion of the seizure of such devices in the case of minor crimes and misdemeanours. However, they demanded that the law should clarify that the court order authorising the search or seizure must already specify the data to be inspected. The judgement of the ECJ confirms this position – an impulse for the German legislator?

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and “criministrative” law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union