COURT OF JUSTICE
OF THE EUROPEAN UNION

PRESS RELEASE No 135/23
Luxembourg, 7 September 2023

Judgment of the Court in Case C-162/22 | Lietuvos Respublikos generalinė prokuratūra

The Directive on privacy and electronic communications precludes the use, in connection with administrative investigations into corruption in the public sector, of data collected for the purpose of combating serious crime

The Directive on privacy and electronic communications covers only criminal prosecutions

A public prosecutor in a Lithuanian public prosecutor's office was dismissed from service by the Lithuanian Prosecutor General's Office. That disciplinary penalty was imposed on him because he had, according to the Prosecutor General's Office, unlawfully provided information to a suspect and to the suspect's lawyer during a pre-trial investigation. He contests that decision before the Lithuanian courts.

The misconduct in office alleged against that public prosecutor was established on the basis of data retained by providers of electronic communications services. According to the public prosecutor, the use of data making it possible to identify the source and destination of telephone communications from a suspect's landline or mobile telephone in cases relating to misconduct in office constitutes unjustified interference with the fundamental rights enshrined in EU law.

Action to combat serious crime may, according to the case-law of the Court on the conditions of access to data relating to electronic communications provided for in the Directive on privacy and electronic communications [1], justify interferences with the fundamental rights enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. In this case, the Supreme Administrative Court of Lithuania, before which the appeal was brought, seeks to ascertain, in essence, whether the use, for the purposes of an investigation into corruption-related misconduct in office, of personal data relating to electronic communications which have been retained by providers of electronic communications services and which have subsequently been made available to the competent authorities for the purpose of combating serious crime, is compatible with that directive.

By today's judgment, the Court rules that **that directive precludes the use, in connection with investigations into corruption in the public service, of personal data relating to electronic communications which have been retained by providers of electronic communications services and which have subsequently been made available to the competent authorities for the purpose of combating serious crime**.

The Court notes in that regard that, in order to combat serious crime, legislative measures may provide for:

— the targeted retention of traffic and location data which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, for a period that is limited in time to what is strictly necessary;

[1] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37).

— the general and indiscriminate retention of IP addresses assigned to the source of an internet connection for a period that is limited in time to what is strictly necessary;

— the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems; and

— recourse to an instruction requiring providers of electronic communications services, by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a specified period of time, the expedited retention of traffic and location data in the possession of those service providers.

The Court also recalls that, in accordance with the principle of proportionality, only action to combat serious crime and measures to prevent serious threats to public security are capable of justifying serious interference with fundamental rights, such as the interference entailed by the retention of traffic and location data. In that regard, the Court states, on the basis of its case-law on the public interest objectives that may justify a limitation on rights, the fight against serious crime and the prevention of serious threats to public security are of lesser importance than the safeguarding of national security, but their importance is greater than that of fighting crime generally.

According to the Court, **traffic and location data retained by providers** pursuant to a measure adopted under Article 15(1) of the Directive on privacy and electronic communications for the purpose of combating serious crime **and made available to the competent authorities** for the purpose of combating serious crime, **cannot subsequently be transmitted to other authorities and used in order to combat corruption-related misconduct in office, which is of lesser importance than combating serious crime**.

NOTE: A reference for a preliminary ruling allows the courts and tribunals of the Member States, in disputes which have been brought before them, to refer questions to the Court of Justice about the interpretation of European Union law or the validity of a European Union act. The Court of Justice does not decide the dispute itself. It is for the national court or tribunal to dispose of the case in accordance with the Court's decision, which is similarly binding on other national courts or tribunals before which a similar issue is raised.

The full text and, as the case may be, the abstract is published on the CURIA website on the day of delivery.

Press contact: Jacques René Zammit ✆ (+352) 4303 3355

Pictures of the delivery of the judgment are available from "Europe by Satellite" ✆ (+32) 2 2964106