ELVINGER HOSS
LUXEMBOURG LAW

CJEU clarifies legality of surveillance legislation for national security

What happened?

Recently, the Court of Justice of the European Union ("**CJEU**") ruled on case C-623/17[1] and the joined cases C-511/18, C-512/18[2] and C-520/18[3] (the "**Joined Cases**") on the lawfulness of national security laws of the United Kingdom, France and Belgium, respectively, which each require electronic communications services providers (the "**Service Providers**") to retain and disclose traffic and location data of their respective users to national authorities for the purpose of combating crime or safeguarding national security. The CJEU provided some important clarifications on the circumstances in which traffic and location data can be collected and retained.

What clarification did the CJEU provide?

National security is within the competence of each EU Member State. However, the CJEU clarified that national legislation requiring Service Providers to retain and disclose users' locations and traffic data to public authority falls within the scope of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 (the "**ePrivacy Directive**"). Consequently, those legislative measures have to comply with the general principles of European Law and the Charter of Fundamental Rights of the European Union (the "**Charter**").

It follows that Member States cannot restrict the scope of the ePrivacy Directive unless such restrictions comply with the general principles of EU law, are proportionate and preserve the fundamental rights guaranteed under the Charter.

Derogation regarding targeted surveillance

However, the Court did formulate certain derogations regarding the scope of the ePrivacy Directive. More precisely, the Court specified that the ePrivacy Directive does not prevent:

- the recourse of a Member State to an order requiring Service Providers to retain traffic and location data generally and indiscriminately, only if that Member State

faces a serious threat to national security that proves to be genuine and present or foreseeable; and

- the recourse of Member States to the targeted retention of traffic and location data (1) limited in time to what is strictly necessary and (2) limited on the basis of objective and non-discriminatory factors, according to the categories of persons concerned, or by using a geographical criterion.

The CJEU framed how targeted surveillance can comply with the ePrivacy Directive and existing EU Laws.

Derogations regarding real-time collection

EU Member States may adopt legislative measures requiring Service Providers to collect traffic and location data in real time provided that the collection is based

- on a genuine and present or foreseeable serious threat to national security; or
- concerns persons suspected of being involved in terrorist activities.

By this recent ruling, the Court clarified a framework under which Member States can adopt laws under which Service Providers are required to retain and disclose traffic and location data to supervisory authorities.

This may also interest you :

- 5G: Opportunities and Legal Challenges
- 5G: Opportunities and Legal Challenges – Part 2. Deployment of 5G in Luxembourg
- Draft Law implementing the European Electronic Communications Code in Luxembourg

> - 1. Privacy International v. United Kingdom.
> - 2. La Quadrature du Net & Others v. France.
> - 3. Ordre des barreaux francophones and germanophones & Other v. Belgium.

Subscribe to EHLO, our dedicated ICT, IP, media and data protection news