



Briefing

On the data protection requirements set out in the CJEU judgment of 6 October 2020 (joined cases C-511/18, C-512/18 and C-520/18) on the automated analysis of communications data

The Europe Section was asked to determine whether the requirements set out by the CJEU in paragraph 177 and the paragraph 2 of the operative part of the *La Quadrature du Net and Others* judgment (joined cases C-511/18, C-512/18 and C-520/18) are transmissible to the automated analysis of communications data, with the consequence that it must be limited to situations in which there is a threat to national security and must not be used permanently to detect criminal offences (e.g. cases of child pornography).

Paragraph 2 of the operative part reads as follows:

‘Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights, must be interpreted as not precluding national rules which requires providers of electronic communications services to have recourse, first, to the automated analysis and real-time collection, inter alia, of traffic and location data and, second, to the real-time collection of technical data concerning the location of the terminal equipment used, where:

–recourse to automated analysis is limited to situations in which a Member State is facing a serious threat to national security which is shown to be genuine and present or foreseeable, and where recourse to such analysis may be the subject of an effective review, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that a situation justifying that measure exists and that the conditions and safeguards that must be laid down are observed [...]

And paragraph 177 states:

‘In that regard, it should be noted that the particularly serious interference that is constituted by the general and indiscriminate retention of traffic and location data, [...], and the particularly serious interference constituted by the automated analysis of that data can meet the requirement of proportionality only in situations in which a Member State is facing a serious threat to national security which is shown to be genuine and present or foreseeable, and provided that the duration of that retention is limited to what is strictly necessary.’

The CJEU’s comments on automated analysis are based indirectly on the following provision of national (French) law, namely Article L. 851-3 of the Internal Security Code (CSI), which states:

‘I. Under the conditions laid down in Chapter I of Title II of this Book, and for the sole purpose of preventing terrorism, the operators and persons referred to in Article L. 851-1 may be required to implement on their networks automated data processing practices designed, within the parameters laid down in the authorisation, to detect links that might constitute a terrorist threat [...]’

(underlining added)

The CJEU therefore only had cause in that context to examine the legality under EU law of the use of automated analysis to prevent acts of terrorism. In this regard, the CJEU states that ‘the importance of the objective of safeguarding national security, read in the light of Article 4(2) TEU, goes beyond that of the other objectives referred to in Article 15(1) of Directive 2002/58, inter alia the objectives of combating crime in general, even serious crime, and of safeguarding public security’ and that ‘the objective of safeguarding national security is therefore capable of justifying measures entailing more serious interferences with fundamental rights than those which might be justified by those other objectives.’¹ This does not necessarily exclude the possibility of automated analysis being considered justifiable under EU law when used to counter other (serious and specific) threats.

The CJEU’s judgment indicates that general automated analysis of traffic and location data constitutes a particularly serious interference with the fundamental rights enshrined in Articles 7, 8 and 11 of the Charter². According to the CJEU, this finding is all the more justified given that the data that is the subject of the automated analysis is likely to reveal the nature of the information consulted online.³

The permanent latent risk that a crime (even of a serious nature) may be committed should not suffice to justify continuous and comprehensive automated analysis. The CJEU therefore only deems automated analysis justifiable under EU law when it is used for limited periods of time⁴ in narrowly defined cases, when there is a particularly serious and imminent threat. The exact wording of legislation is likely to be decisive. The requirement, established in Article 52(1) of the Charter, that any limitation on the exercise of fundamental rights must be provided for by law implies that the legal basis which permits that interference with those rights must itself define the scope of the limitation on the exercise of the right concerned⁵. In addition, in order to meet fully the requirement of proportionality, derogations from the protection of personal data must apply only in so far as in strictly necessary⁶. To guarantee this, the CJEU considers that it is ‘essential that the decision authorising automated analysis be subject to effective review, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that a situation justifying that measure exists and that the conditions and safeguards that must be laid down are observed’⁷.

- Europe Section -

¹ See: Paragraph 136, CJEU Judgment of the 6 October 2020 on joint cases C-511/18, C-512/18 and C-520/18

² See: Paragraph 173 and 174, CJEU Judgment of the 6 October 2020 on joint cases C-511/18, C-512/18 and C-520/18

³ See: Paragraph 174, CJEU Judgment of the 6 October 2020 on joint cases C-511/18, C-512/18 and C-520/18

⁴ See: Paragraph 178, CJEU Judgment of the 6 October 2020 on joint cases C-511/18, C-512/18 and C-520/18: Even in situations in which a Member State is facing a serious threat to national security which is shown to be genuine and present or foreseeable, the CJEU stresses that duration should be limited to what is ‘strictly necessary’.

⁵ See: Paragraph 175, CJEU Judgment of the 6 October 2020 on joint cases C-511/18, C-512/18 and C-520/18.

⁶ See: Paragraph 176, CJEU Judgment of the 6 October 2020 on joint cases C-511/18, C-512/18 and C-520/18.

⁷ See: Paragraph 179, CJEU Judgment of the 6 October 2020 on joint cases C-511/18, C-512/18 and C-520/18.