CJEU on Access and Retention of Traffic and Location Data for National Security

On 6 October 2020, the Court of Justice of the European Union (the ***CJEU or Court***) delivered its judgment in three cases on the compatibility of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (the ***ePrivacy Directive***) with methods for combating terrorism (Case C-623/17, *Privacy International*, Joined cases C-511/18, *La Quadrature du Net and Others* and C-512/18, *French Data Network and Others*, and Case C-520/18, *Ordre des barreaux francophones et germanophone and Others*).

In these cases, various prejudicial questions had been referred to the CJEU on the retention of traffic and location data and the transmission of such data to public authorities for national security and other purposes. After the CJEU had prohibited "general and indiscriminate" retention obligations and invalidated Data Retention Directive 2006/24/EC, Member States felt deprived of using an instrument they deem necessary to safeguard national security and to combat crime and terrorism. Member States therefore updated their rules to maintain this instrument. The national rules were then called into question by NGOs and other organisations. This led to new preliminary questions being referred to the CJEU by the UK Investigatory Powers Tribunal, the Belgian Constitutional Court (*Grondwettelijk Hof / Cour constitutionnelle*) and the French Council of State (*Conseil d'Etat*).

In its answer to these questions, the CJEU confirmed once again that EU law prevents national legislators from imposing broad obligations on providers of electronic communications services to retain or transmit traffic and location data. However, the CJEU judgments also provide guidance on which retention and transmission requirements can be considered to be compatible with EU law and how national (criminal) courts should handle evidence that is collected on the basis of illegal retention and transmission requirements. The judgments are largely in line with the Opinion of the Advocate General in these cases (our article on the Advocate General opinions in these cases can be found here: *VBB on Belgian Business Law Newsletter, Volume 2020, No. 1, at p. 9*).

As a result of these judgments, Member States must review their legislation and practices for compliance with EU requirements to protect the public, its security and fundamental rights. In addition, these CJEU judgments could have an impact on EU-UK transfers post-Brexit.

The Privacy International case

Privacy International, a non-governmental organisation, brought an action before the UK Investigatory Powers Tribunal challenging the UK security and intelligence agencies' (***SIAs***) collection and use of bulk personal data, including communications data acquired from providers of public electronic communications networks. Privacy International's claim is based on the CJEU judgment in Case C-698/15, *Tele2 Sverige and Watson and Others* (*See VBB on Belgian Business Law Newsletter, Volume 2017, No. 1, p. 14*). In this judgment from 2016, the CJEU held that following the *Digital Rights Ireland* case general and indiscriminate retention of all traffic and location data of all subscribers and registered users is disproportionate and incompatible with EU law.

In the *Privacy International* case, the CJEU first determined that a requirement in national legislation for communications service providers to retain data falls within the scope of EU law and specifically the ePrivacy Directive. Indeed, Article 3 of the e-Privacy Directive makes clear that the Directive applies to the activities of communications service providers. As a result,

laws requiring communication service providers to retain and transmit traffic and location data fall within the scope of Article 15 of the ePrivacy Directive since such practices "*necessarily involve the processing, by those providers, of the data and cannot, to the extent that they regulate the activities of those providers, be regarded as activities characteristic of States*". A legislative measure such as section 94 of the UK Communications Act, based on which the competent authority may give the providers of electronic communications services a direction to disclose bulk data to the SIAs by transmission, thus falls within the scope of the ePrivacy Directive. The CJEU thereby rejects arguments that these rules concern public security and therefore would fall outside the scope of EU law.

Having clarified that the relevant rules fall within the scope of EU law, the CJEU pointed out that the purpose of the ePrivacy Directive was to protect users from threats to their privacy arising from new technologies. Therefore, it gave expression to Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (the ***Charter***). However, Article 15(1) of the ePrivacy Directive allows Member States to adopt restrictions to certain rights, provided that such restrictions are "*necessary, appropriate and proportionate*". The Court warned that the exceptions to the obligation to ensure the confidentiality of electronic communications could not be defined so broadly that they would effectively become the rule. This also applies to the prohibition from keeping data longer than necessary for their initial purpose. Restrictions to these fundamental rights must comply with the Charter. Referring to *Schrems II* (See *VBB on Belgian Business Law Newsletter, Volume 2020, No. 7, at p. 8*), the CJEU held that any limitation on the exercise of fundamental rights must be provided for by law. This implies that the legal basis which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned.

Derogations from the protection of personal data and any restriction on confidentiality of communications and traffic data must thus be proportionate, meaning that they may apply only in so far as is *strictly* necessary and "*by properly balancing the objective of general interest against the rights at issue*". Proportionality also requires the legislation to lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards to protect effectively against the risk of abuse. The legislation must ensure that interference with the protection of personal data is limited to what is "strictly necessary". "*Necessity"* means that due account should be taken of the risk at hand. Thereby, the CJEU pointed out that automated processing gives rise to more significant risks. These considerations are more pressing in the context of sensitive data.

The CJEU noted that the transmission of data to SIAs constituted a breach of confidentiality in a general and indiscriminate way. The broad scope of this exception effectively makes disclosure – and not confidentiality – the rule.

Finally, the CJEU distinguished between various objectives set out in the ePrivacy Directive. 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 the ePrivacy Directive (*i.e.*, the objectives of combating crime in general, even serious crime, and of safeguarding public security). While measures safeguarding national security must still comply with Article 52(1) of the Charter, the CJEU considered that the seriousness of threats comprised in "national" security are in principle capable of justifying more intrusive measures on fundamental rights than those which might be justified by the other objectives foreseen in Article 15(1) of the ePrivacy Directive.

On this basis, the CJEU decided that the national legislation requiring providers of electronic communications services to disclose traffic data and location data to the SIAs through general and indiscriminate transmission exceeds the limits of what is strictly necessary. It cannot be justified, within a democratic society, even in the interests of protecting national security.

The full text of the CJEU's judgment can be found here (in English).

The Joined cases La Quadrature du Net and Ordre des barreaux francophones et germanophone

The Joined cases C-511/18, C-512/18 and C-520/18, concern, on one hand, actions brought by *La Quadrature du Net and Others* before the Council of State in France to challenge a French decree related to specialised intelligence services; and, on the other hand, by the *Ordre des barreaux francophones et germanophone and Others* before the Constitutional Court of Belgium to challenge Belgium's legislation on collection and retention of communications data. In particular, the French court asked questions about the collection of live traffic and location data while the Belgian court sought guidance on the use of data obtained in breach of EU law during criminal proceedings. Since the cases concerned similar questions, these cases were joined before the CJEU.

In response to the questions raised by the French and Belgian courts on the general and indiscriminate transmission of traffic data and location data to the security and intelligence agencies to safeguard national security, the CJEU adopted the same reasoning as set out above in the *Privacy International case*. It held that national legislation requiring such measures was precluded under the Charter and Article 15 of the ePrivacy Directive.

In addition, the Belgian and French courts asked the CJEU for clarification on the criteria and purposes for which national law could require traffic and location data to be retained.

The CJEU considered that neither the ePrivacy Directive nor the Charter precludes recourse to an order requiring providers of electronic communications services to retain, generally and indiscriminately, traffic data and location data. This is, however, only the case when the Member State concerned is facing a sufficiently serious threat to national security (*i.e.*, a threat that is genuine and actual or foreseeable). In such a case, data retention must be proportionate, and the retention can only be for a period limited to that which is strictly necessary. If such an order is renewed, it must be for a specified length of time. Additionally, the retained data must be protected by strict safeguards against the risk of abuse. Finally, the CJEU explained that the decision must be subject to effective review by an independent body, whose decision is binding, in order to verify that such a situation exists and that the conditions and safeguards laid down are observed. Again, the CJEU pointed out that the objective of safeguarding national security is capable of justifying measures entailing more serious interferences with fundamental rights than those which might be justified by the objectives foreseen in Article 15(1) of the ePrivacy Directive.

By contrast, the CJEU observed that general and indiscriminate surveillance refers to that which covers virtually the entire population without any differentiation, limitation or exception being made in the light of the objective pursued. It therefore even applies to persons with respect to whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with the objective of combating serious crime and, in particular, without there being any relationship between the data whose retention is provided for and a threat to public security.

Next, the CJEU assessed whether national law could require the retention of IP addresses and data relating to the civil identity of users of electronic communication systems. The CJEU held that IP addresses could be retained preventively in a general and indiscriminate manner subject to a requirement of strict necessity. Further, it considered the different purposes for which identification of users of electronic communication systems could be relevant and held that the ePrivacy Directive does not preclude the retention of data beyond statutory data retention periods when strictly necessary to shed light on serious criminal offences or attacks on national security, or when the offences or attacks have already been established, or if their existence may reasonably be suspected.

Moreover, the CJEU stated that real-time data could be used, for instance when it is limited to people in respect of whom there is a valid reason to suppose that they are involved in terrorist activities. However, the use of such data must be subject to prior review by an independent body to ensure that real-time collection is limited to what is strictly necessary. The CJEU notes that in urgent cases that review should take place promptly.

Finally, the CJEU provided guidance on the legal consequences of the invalidation of national data retention rules. In a statement that may be important for many pending cases, the CJEU considered that the use of evidence obtained on the basis of retention rules that were declared to be illegal could affect the right of a fair trial. Therefore, it held that national criminal courts should *"disregard information and evidence obtained by means of the general and indiscriminate retention of traffic and location data in breach of EU law*" if the suspect is not in a position to defend itself against such data effectively and this could have a significant impact on the case.

The full text of the CJEU's judgment can be found here (in English).

What the judgment means for EU-UK data flows

The UK officially left the EU on 31 January 2020 and there is a transition period until the end of 2020 to allow time to negotiate a new relationship with the EU. During this transition period, EU law continues to apply to the UK. After the transition period, a framework of protection needs to be implemented for data transfers between the EU and the UK since the UK will be considered to be a third-party country. The GDPR foresees the possibility for the European Commission to adopt an adequacy decision which would facilitate such transfers. With such a decision for the UK, the European Commission would recognise that the UK legislation ensures a high level of data protection that is at least similar to the GDPR and personal data can be transferred freely between the EU and UK.

While it is generally expected that the UK legislation, which copies the substantive provisions of the GDPR, should qualify for an adequacy finding, the CJEU's judgments discussed above indicate that such a decision may not be straightforward. UK surveillance law and its provisions for the collection of bulk communications data will need to be assessed by the European Commission in light of these judgments. In the absence of an adequacy finding, organisations transferring personal data between the UK and the EU may need to resort to other means to bring such transfers in line with the GDPR.