The CJEU judgments in Privacy International and La Quadrature du Net and others - the return of the walking dead?

Summary by Alessandra Calvi (VUB/LSTS)

On 19 November 2020, the Brussels Privacy Hub, in cooperation with the **Government&Law Research group of the University of Antwerp** and media partnership with **Privacy Laws & Business**, organised a webinar entitled ***The CJEU judgments in Privacy International and La Quadrature du Net and others - the return of the walking dead?***

The first webinar discussed the judgements rendered by the Court of Justice of the European Union (CJEU) on data interception/retention matters concerning Case C-623/17, Privacy International, and to Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophone and Others (referred to as La Quadrature du Net and Others).

Juraj Sajfert (VUB/University of Luxembourg) hosted the discussion. Invited speakers were **Catherine Van de Heyning** (Antwerp University) and **Christian Wiese Svanberg** (DPO at the Danish National Police, but speaking in a purely private capacity).
During the webinar, the discussants tackled the following three questions:

1. Did the CJEU sufficiently take into account the necessities of fighting crime?
2. Did the CJEU undermine with these judgments the coherence of its data retention case law?
3. How will the balance between fighting crime on the one hand, and privacy rights & data protection on the other look in the future?

The opinions expressed by the speakers and attendees are in their own capacity.

Did the CJEU sufficiently take into account the necessities of fighting crime?

Catherine Van de Heyning argued that it would be incorrect to consider the judgements a clear win for privacy or law enforcement, as they achieve a compromise solution without overruling previous case law. As in Tele2 Sverige, the judgements reiterate the principle that bulk data retention of traffic data and location data for fighting serious crime is not allowed, being only possible targeted retention on suspects. However, whereas in *Tele2* the push was towards privacy, in *La Quadrature du Net and Others*, the balancing is more towards law enforcement. In the latter, the CJEU acknowledges and emphasises the importance of IP addresses to fight crimes as child abuse or trafficking, and to protect public security.

Christian Wiese Svanberg considered the approach towards IP addresses the main element of novelty of *La Quadrature du Net and Others*. By opening to the possibility to retain information about IP addresses and the sources of communication, for a limited period, the CJEU accommodates law enforcement needs. He termed this almost a sort of 'phone book' of IP addresses at the Internet Service Providers level. He pointed out that 17 Member States and the Commission requested the CJEU to nuance Tele2 jurisprudence because of the importance of the general data retention for prosecuting certain crimes and protect victims (e.g. child abduction).

Q&A

On challenges raised by the use of dynamic IP addresses -that may relate to thousands of people- to identify perpetrators of crimes, **Wiese Svanberg** said that combing the information on civil identity (namely subscriber information) with IP addresses of the source of communication, e.g. subscriber

information or IMEI number, may be what is required to enable identification. Questioned about the impact of geographic data retention, **Wiese Svanberg** replied that probably it would not affect the free movement of individuals in the EU but rather lead to some risk of "discrimination" in protecting the public, in so far as prosecuting crimes would be easier in certain areas than in others. Establishing criteria for geographical data retention (e.g. at public border crossing points, airports, schools) is a real dilemma. **Van de Heyning** also reflected on the difficulties to politically justify the criteria grounding geographic data retention and to identify those crimes for which the use of retention may be allowed.

Did the CJEU undermine with these judgments the coherence of its data retention case law?

Juraj Sajfert expressed concerns about the consistency of the CJEU case law after the two judgements were released, calling for the CJEU to revert its jurisprudence. He identified two main turning points of *La Quadrature du Net and Others* comparing with *Tele2*. First, the judgement opens to bulk data retention of traffic and location data for national security purposes (but not for law enforcement ones). Second, that the new approach towards IP addresses and civil identity retention puts online anonymity at stake.

Catherine Van de Heyning admitted that IP addresses have always been categorised as traffic data and classifying them as less sensitive may be juridically problematic. However, she noted that the exception of the CJEU is narrow. IP addresses are deemed necessary for fighting crimes, but there are other traffic data for which retention is not allowed. She considered the public security exception coherent with previous case law, as the CJEU states it is still necessary to justify the retention and that the retention measures may be reiterated but must be limited in time.

Q&A

On the possibility to continuously renew data retention measures, **Van de Heyning** admitted it could be a risk for fundamental rights, but she stressed that the Court expressly states that data retention measures shall be temporary. Otherwise, the necessity and proportionality test and temporary criterion would be circumvented.

It was pointed out that Belgium tried to frame the issue of data retention differently, namely to allow data retention by providers but to limit access to the data by law enforcement authorities. However, this approach was considered unacceptable by the CJEU.

On the Big Brother Watch case pending at the European Court of Human Rights (ECHR), **Sajfert** emphasised that CJEU and ECHR have different perspectives on data retention. For the latter, bulk interception of communications by intelligence agencies is *per se* acceptable, whereas for the former is not. However, strict criteria for the acquisition of a particular dataset from a service provider and its actual use by those authorities shall apply in both cases. **Van de Heyning** wondered which of the two approaches is the most protective for human rights.

How will the balance between fighting crime on the one hand, and privacy rights & data protection on the other look in the future?

Juraj Sajfert stated that the judgements had two different outcomes. In *Privacy International*, the CJEU rules on the scope of EU law, concluding that the exemption *ex* Article 4 TEU (excluding national security from the scope of EU law) must be interpreted narrowly and does not cover the activities of service providers requested to perform data retention. Furthermore, the CJEU rules against the idea of a collective right to security implying a positive action by a State, stating that the right to liberty and security belongs to the *habeas corpus*.

In *La Quadrature du Net and Others*, the CJEU legitimises a hierarchy of categories of data, where the content of communications is more protected than metadata and subscriber data.

After these judgements, it will be probably easier to accept that law enforcement agencies may access e-evidence and EU large scale databases, especially when IP addresses and subscriber data are concerned, although such data may not be reliable.

Christian Wiese Svanberg called for the CJEU to reflect on the value and utility of data in the modern world to combat crime and protect victims also in its future decisions, especially when addressing the pending cases regarding Passenger Name Records (PNR). He appreciated that the CJEU case law nuances data protection, especially the necessity and proportionality test, acknowledging – at least to some extent – the fundamental role of data retention in combating crimes.

Q&A

On the relationship between surveillance and data retention, **Wiese Svanberg** highlighted that traffic and location data are not by default available to law enforcement agencies, but data is retained only by service providers and may only be shared in so far there is a warrant. Also in the case of IP addresses, a bulk transmission to public authorities would not be allowed. **Van de Heyning** pointed out how retention itself is an issue for data security and should be addressed together with transparency.

The question concerning the usability of data in trials, and not just for prosecution, remains open.

Juraj Sajfert closed the event thanking the speakers and the participants for the fruitful debate.