Non-paper WK 7294/2021 – Responses by Germany

I. General remarks

To take the decision on a European instrument governing the retention of data doesn't seem feasible until clarification has been obtained regarding the as-yet unresolved questions arising from the rulings handed down by the Court of Justice of the European Union (ECJ) and, in particular, until general agreement has been reached among the Member States as to whether such a European regulation ought to be developed, and if so, how it should be structured.

This point was emphasised by Germany during the informal meeting of the Ministers of Justice on 11 March 2021. We uphold this assessment.

In light of the proceedings still pending before the ECJ including the referral procedure being pursued by Germany, it is still too early to conclusively evaluate the possibilities and reach of a European solution. Given that, by European standards, the German provisions governing the retention of data have been structured in particularly restrictive fashion, we are proceeding from the assumption that the ECJ will recognise the German provisions as being compliant with European law; in particular, we expect this decision to provide additional insights and to bring clarity to those questions yet to be resolved.

This said, in our view taking a purely national approach to the retention of data seems to be problematic. It is true that such an approach would allow for a high degree of flexibility; as a consequence, it would be possible to take account of the differing national specificities and requirements in greater detail. However, this approach also would give rise to mutually divergent regulations among the individual Member States. This is disadvantageous for cross-border cooperation. But more important in our opinion, such a measure would send the wrong message, given the ever-increasing number of cross-border crimes, not just in the field of cybercrime but also in that of organised crime.

The fact that with the nullified Directive 2006/24/EC an European regulatory instrument already existed, is another consideration prompting us to conclude that a European approach should not be abandoned.

As regards a possible European instrument, it bears noting that the decisions of the ECJ have a bearing on European primary law, i.e. on the way in which the European fundamental rights are interpreted. This means that any new European regulatory instrument on data retention

must be reconcilable with these requirements and thus also with the EU Charter of Fundamental Rights, with which it must specifically comply. For this reason, we are in favour of adopting the approach proposed by the Commission, which is aligned with the categories defined by the ECJ. As Germany sees it, this also means that optionality clauses in the domain of secondary law (such as the e-Privacy Regulation) will not be able to change the legal situation indicated by the Court of Justice. Germany had already stated its opposition to providing for the retention of data as part of the e-Privacy Regulation in February 2021, during the negotiations over the e-Privacy Regulation. As before, we do not endorse providing for data retention in some other legal instrument of secondary law that addresses a different topic.

Finally, we would be open in principle to considering a 'mixed' approach in which only certain aspects would be provided for by a European legal instrument.

II. Remarks on the individual policy approaches proposed by the Commission

- Generalised retention of traffic and location data for national security purposes – Approach 3a

  In light of the delineation of national and EU competences, what are Member States' views on a legislative initiative that would harmonise certain criteria relating to the retention of traffic and location data and related access conditions for national security purposes, for situations that involve private actors (for storage, transmission and providing access to data to relevant competent authorities)?

By its judgments of 6 October 2020 (in the joined cases C-511/18, C-512/18 and C-520/18 '*Quadrature du Net, a.o.*' and C-623/17, '*Privacy International*'), the ECJ ruled that a provision of domestic law permitting a governmental body to require operators of electronic communications services to transmit traffic and location data to the security and intelligence services in order to safeguard national security falls under the applicable scope of EU Directive 2002/58. At the same time, the ECJ made clear that a generalised and undifferentiated retention of traffic and location data is permissible for a narrowly defined period in cases in which a serious threat to national security is given that can be considered to be either genuine and present, or foreseeable.

As regards the applicability of a European regulatory instrument to the sphere of national security, we do have reservations when it comes to Article 4 (2) TEU, also given the reasoning

provided by the ECJ for the aforementioned decisions; this is because we continue to take the view that national security remains the sole responsibility of the Member States. But if a decision in favour of introducing a European regulatory instrument in this domain were to be taken, then we would share the Commission's assessment that the criteria set forth in the working paper would have to serve as prerequisites for a corresponding retention of data.

We wish to point out in this context that German law currently exempts the domain of national security from the retention of data.

- Targeted data retention of traffic and location data for serious crime and serious threats to public security – Approach 3b

  - What are the legal challenges for Member States and the technical challenges for providers to comply with a targeted retention obligation and how could they be overcome? Please be as specific and concrete as possible in your responses.
  - What is the 'objective evidence' (in the case of persons) and what are the 'objective and non-discriminatory factors' (in the case of geographical areas) or other objective criteria that Member States could consider in drawing up a targeted retention framework?
  - Do Member States consider there is merit in revisiting the 'data matrix' exercise initiated by Europol in 2018 to try to find ways to devise a targeted retention system that fulfils the Court's requirements?
  - Do Member States consider there is merit in devising a targeted retention system by developing criteria to limit the means of communication or the number or type of electronic communications service providers subject to retention obligations (e.g. based on size, geographical coverage, number of subscribers, cross-border presence)?
  - Can Member States share their views of what serious threats to public security entails?

The instrument of targeted retention developed by the ECJ – i.e. retention obligations that apply only to a specific group of persons or to a specific geographical area – does not constitute an equally effective alternative to any generalised retention of data.

As a general rule, the public prosecution authorities will not be aware in advance of when, where and by whom a crime is going to be committed, i.e. before an actual offence or an actual threat is suspected. Both Directive 2006/24/EC, which since has been declared invalid, and the domestic regulations on the generalised retention of data respectively in place derive their rationale from the fact that in order to fight serious crime it is impossible to predict in advance which traffic data will be required for which persons, for which region, and for which period.

Serious offences are not limited to specific geographical areas, after all, and often take place in a private setting. Moreover, the key communications activity at issue frequently takes place somewhere other than the location at which the offense occurs or at which a threat manifests itself. Especially when it comes to organised crime, analysing the communications activities in the pro-active phase prior to the deed is of decisive importance for evaluating acts contributing to the principal offence. Concurrently, limiting data retention to a specific geographic area is not particularly useful given the mobility of suspects.

From a legal standpoint, there is also the issue of how such targeted data retention could be performed without discriminating against certain groups of persons in the process. This applies to the targeted retention of the data of a specific person as well as to the delineation of specific geographical areas.

As we see it, an acceptable criterion for retaining the data relating to a specific person (with future effect) in individual cases could at best be the existence of objective evidence and known facts to support the suspicion that a person has committed, is attempting to commit, or has planned to commit a crime that is of serious import even when committed in a single instance, or that a given person poses a significant threat to public security or national security in the context of counter-terrorism. A prior criminal conviction that has become non-appealable, by contrast, would not serve as a suitable criterion in the view taken by Germany, since this would almost certainly lead to the person concerned being labelled ‘guilty’ upon their having been charged.

Moreover, targeted data retention hardly would be feasible in technical terms. Thus, the current state of technology is such that providers are not able to determine which specific radio cells are being used in a particular area, given that other radio cells could also be in use depending on the level of demand being experienced by a person’s network/location. In addition, it would have to be ensured that such data retention terminates the moment a device leaves a certain location, and that it resumes once the device re-enters the area.

Taking account of the sole criteria that the Court of Justice thus far has admitted for the retention of data limited to specific persons or a specific geographical area, respectively, it does not appear purposeful to perform another review of the ‘data matrix’ elaborated by Europol in 2018.

The opposite would be the case, however, if a further criterion for the targeted retention of data in addition to the existing criteria were recognised in addition to the criteria for data retention

limited to specific persons or specific geographical areas named by the Court of Justice as examples, respectively, this being the one the Advocate General brought into play in his final pleading in Case No. C-520/18: The retention of data depending on the categories of data concerned. Inasmuch, we attribute particular importance to the decision by the Court of Justice of the European Union in the German referral procedure, given that such a limitation is applicable in our domestic law, both in terms of the data categories involved as well as of the duration of the retention period.

In developing a system for targeted retention that is geared towards the individual provider's means of communication or its size, respectively, it is to be considered that such a limitation unavoidably would cause suspected offenders to use other means of communication or providers, respectively, without this changing the degree of interference with the rights of other users. At the same time, it would have to be ensured that small enterprises, in particular, are not unduly burdened, meaning that a balance would need to be struck between the interests at stake.

- Expedited retention (quick-freeze) of traffic and location data for serious crime and the safeguarding of public security – Approach 3c

  - Given that a "quick freeze" provision can apply only if there is data available to "freeze", can Member States share any experience relating to the normal period of availability of data, absent a general retention obligation? Can Member States point to any ideas stemming from that experience that may be helpful in this context?
  - Can Member States share any experience relating to the use of expedited retention in their current legislation?
  - Which options do Member States see for operationalising this mechanism to meet its objective to support investigations into serious crime and protection of national security?

By its judgment of 6 October 2020 in the joined cases C-511/18, C-512/18 and C-520/18 '*Quadrature du Net* a.o.,' the ECJ raised the possibility of an expedited retention of data, while making express reference to the Convention on Cybercrime of the Council of Europe of 23 November 2001 (CETS No. 185, aka 'Budapest Convention'). According to the decision handed down by the ECJ, such retention is permissible to fight serious crime and to protect national security, insofar as its scope and duration remain limited to what is strictly necessary.

The German legal system does not provide for a 'quick-freeze' procedure since our domestic provisions on data retention are further-reaching; thus, Germany has seen no need to implement this provision of the Budapest Convention into national law. Against this backdrop, we have no information to share on practical experiences made with the transposition. This said, we do not believe that the efficacy of the 'quick-freeze' procedure as a means of establishing the facts and circumstances is comparable to that of data retention, since retention is ordered on a case-by-case basis only and not until there are objective grounds for doing so based on specific suspicions of a crime. Thus, data originating from the period before the retention order was issued can be collected only if and insofar as they remain available to the operators, e.g. for billing purposes; this is becoming increasingly rare in practice, however, given the growing number of flat-rate schemes and the absence of a corresponding retention obligation. Yet when it comes to solving crimes whose commission cannot be foreseen in advance, establishing the facts and circumstances of the events preceding the offence plays the salient role in the investigation of criminal networks or structures, respectively.

- Generalised retention of IP addresses assigned to the source of an internet connection for serious crime and serious threats to public security – Approach 3d

  - Do Member States see the benefits of this approach? Do they see any drawbacks in this approach e.g. that the IP address of the destination of a communication is not retained? Is there a lawful way to overcome this limitation?
  - Are there other technical identifiers that could, in line with the jurisprudence, be captured in such legislation for example time stamps and source-port numbers to allow for identification of individuals where IP addresses are shared across multiple users, as may be the case e.g. in mobile communications?
  - What cybercrimes are not currently covered by the notion of 'serious crime' in Member States' legislation?

In its decision on the joined cases C-511/18, C-512/18 and C-520/18 '*Quadrature du Net* a.o.,' the ECJ for the first time also addressed the general retention of IP addresses without any specific grounds calling for such retention; in this regard, the Court emphasised that IP addresses are less sensitive than other traffic data given that, in the context of emails and internet telephony, only the IP addresses of the source of the communication are retained, but not those of the communication's addressees. The ECJ supported its conclusion by reasoning that such addresses *per se* do not reveal any information about the third parties with whom the person initiating the communication was in contact.

The ECJ thereby acknowledges the fact that IP addresses – which telecommunications services often do not retain for their own purposes or which they retain for only very short periods – frequently constitute the sole investigative lead when crimes are committed online and thus are the only trail that can be followed to identify a perpetrator. This applies particularly to crimes involving child pornography. According to the jurisprudence of the ECJ, the only grounds besides national security that would justify such an intervention are combating serious crime and preventing serious threats to public security.

Under German law, a distinction is drawn between serious and especially serious criminal offenses. Based on the current legal situation, data retention pursuant to section 100g (2) of the Code of Criminal Procedure (*Strafprozessordnung* – StPO) is premised on the commission of an especially serious crime; the provision includes a list of offence categories that does not, however, cover all instances of cybercrime. For example, the following offences are not included under especially serious crimes: data espionage, phishing of data, acts preparatory to data espionage and phishing, handling of stolen data (sections 202a to 202d of the Criminal Code (*Strafgesetzbuch* – StGB), as well as computer fraud (section 263a of the Criminal Code); this latter is, however, classified as a serious crime.

In order to enable identification of an internet user, it is necessary to store not only the IP address but also the time stamp and, where applicable, the port number assigned. We are of the opinion that the retention of this data is covered by the case law of the Court of Justice.

- <u>Generalised retention of data of civil identity data to fight crime and threats to public security in general, Approach 3e</u>

  - Is retention of 'civil identity data' effective to fight crimes?
  - What specific elements should be included in this data category?

The term 'data relating to the civil identity of users of electronic means of communication,' which was used by the ECJ in its decision of 6 October 2020 (joined cases C-511/18, C-512/18 and C-520/18 '*Quadrature du Net, a.o.*') as well as in its decision of 2 March 2021 (Case C-746/18, '*Prokuratuur*'), in our perception is not yet an established terminological concept of EU (telecommunications) law, , so that it appears unclear which data categories the ECJ intended to cover by this term. Fundamentally, the degree of interference involved is not deemed grave by the ECJ, since these data – aside from contact data such as addresses – do not provide

any information concerning the actual communications of the person affected and thus concerning their private life.

In our understanding, the term ‘data relating to the civil identity of users of electronic means of communication’ most probably is intended to mean ‘subscriber data.’ Retaining and accessing such data is a key element of the initial investigations to discover the identity of an as yet unknown perpetrator. This said, the retrieval of said data always will serve as only the first step in establishing the facts and circumstances, and will not be sufficient in and of itself.

According to German law as it currently stands, the retrieval of subscriber information also can be effected by way of a dynamic IP address, even though the dynamic IP address itself qualifies as an item of traffic data. This means that the public prosecution authorities can use an IP address that becomes known to them (e.g. an address identified on a confiscated device) in order to contact the relevant telecommunications services providers and to ask them to disclose subscriber information concerning the user to whom the IP address was assigned at a given point in time. In order to be able to properly allocate the address – and thus to disclose the requested information – the telecommunications services providers are permitted to access all the traffic data available to them, including data that have been retained pursuant to section 113b of the Telecommunications Act (*Telekommunikationsgesetz* – TKG). The traffic data are used exclusively for purposes of performing the allocation, however, and are not disclosed to the public prosecution authorities. Only the relevant subscriber information is transmitted to the authorities, in other words. This plays a particularly important role in connection with cybercrime, namely when it comes to discovering the identity of a suspected perpetrator. Whether this is covered by the case law of the Court of Justice of the European Union, however, requires further clarification.

In this regards German law is aligned with the requirements established by the Constitutional Court (*Bundesverfassungsgericht*), which in its order of 27 May 2020 highlighted the fact that allocating a dynamic IP address entails a heightened degree of interference; in this same context, the Court also provided clarification on the fact that although general powers to transmit and retrieve subscriber information entail only moderate interference, they are still subject to certain preconditions: A concrete threat to a particularly weighty legal interest must exist in the individual case in order to justify measures serving the prevention of threats and the involvement of the intelligence services, and an initial suspicion must exist to justify criminal proceedings.