Additional comments:

Public consultation on improving cross-border access to electronic evidence in criminal matters

27.10.2017, Dutch National Public Prosectur's Office

Question 30:

- Loss of location is a big challenge for law enforcement: cloud based services, anonymity online, standard encryption are game changers;
- No support for limiting or weakening encryption, but there is a clear need to rapidly balance the wide digital instrumentarium available for cybercriminals, in a globally connected world, with law enforcement access to evidence and information;
- Current instruments like (Mutual Legal Assistance) MLA, mutual recognition and the EIO (European Investigation Order) are either slow, inflexible or cumbersome. There is a need for streamlined, well-defined ways for quick access to data and electronic evidence, with safeguards for due process and fundamental rights protection;
- Different regimes for different types of data can be considered: subscriber data and/or a (new) category of "access to account or device" data, vs. content data.

Question 60:

- EU-wide power to compel production of electronic evidence is necessary to encourage a similar level of cooperation amongst ISPs with law enforcement. Additionally, an effective and swift practice of production orders requires streamlining of formats of the orders and corresponding exchange systems or platforms to ensure maximum predictability and ease for all parties involved;
- Double criminality is a relevant condition. It is important to consider the existing differences in norms and traditions, also within the EU, especially regarding the protection of the fundamental right to free expression, freedom of association, the freedom of the media and the press; in these sensitive cases the condition of double criminality allows for sufficient national discretion. Alternatively, a negative list of crimes covered by the instrument could be drafted;
- The main added value of the instrument would be 1) power to compel to provide data, and 2) speed, which is absolutely key in a digitized society and with high tech crime; which leaves limited room for Member States to object to each specific production order (especially if a negative list is already established).

Question 66:

- Double criminality can't be assessed if the location of the data or suspect is unknown;
- Notification is not possible if the location is unknown, but could be done ex post, also to retain maximum efficiency and added value of the new instrument;
- Direct access to e-evidence is either possible through the ISPS or directly via the user (device, log-in), different regimes could be applied for these routes;
- Objections to direct access by the notified MS can in practice only be done after the location is determined and the data has been accessed, nevertheless the ability to object can (ex post) differentiate between types of offences and data, and what can be done with the electronic evidence directly accessed (consult, copy, destroy); can provide a desired level of control;
- Notification of the targeted person could jeopardize an investigation and should therefore not be mandatory ex ante, it should be done after direct access has taken place and if the investigation allows for it.

Question 70:

- Existing agreements with third countries (outside of the EU) on direct (voluntary) inquiries to ISPs do contribute to successful criminal investigations; any new instrument should be inspired by best practices.
- Cooperation with third countries and law enforcement is very relevant, but again also requires a certain level of standardization of processes and technical formats, this is taking shape between different sets of countries, but could also be considered at a broader scale (also within the EU), provided that national laws and constitutions allow for such cooperation;
- Bilateral treaties shouldn't be ruled out if no EU wide agreement can't be negotiated.

END