EUROPEAN JUDICIAL CYBERCRIME NETWORK
7TH PLENARY MEETING

EUROJUST, 14 - 15 NOVEMBER 2019

OUTCOME SUMMARY

1. Introduction

The European Judicial Cybercrime Network (EJCN) held its 7th plenary meeting on 14/15 November 2019 at the premises of Eurojust in The Hague. The meeting was attended by members of the EJCN from 24 Member States, Representatives of Switzerland, Norway and Serbia as Observer States as well as by Representatives from Eurojust, Europol/EC3, the European Commission (DG Home) and the Secretariat of the European Judicial Network (EJN).

This report reflects

- the key outcome points of the three topical discussions conducted during the meeting (below Nr. 2),
- state of play and next steps regarding activities conducted in the EJCN sub-groups on data retention, e-evidence, case-building, training and virtual currencies as discussed within separate subgroup meetings (below Nr. 3) and agreed upon by the plenary

2. Topical Discussions

2.1. Joint Investigation Teams (JITs) in cybercrime investigations

Further to the Conclusions of the 15th Annual Meeting of the JITs Network (Council doc. 13752/19) the following remarks on the use of JITs in cybercrime investigations can be highlighted:

- **Additional advantages** of the use of JITs in cybercrime investigations:
    - Depending on the movement of targets the interception of communication via mobile devices can fluently change between domestic and cross-border scenarios. In these situations the party of a JIT can extend interception measures to targets on the territory of another JIT party. The required consent of the other JIT party

can be provided in advance, e.g. within the JIT agreement. This allows JIT parties to efficiently deal with cross-border interceptions without having to apply the mechanism of Article 31 of Directive 2014/41/EU on the European Investigation Order.

- JITs provide a legal framework for the presence of JIT members of one JIT party on the territory of another JIT party. This can also include the possibility to conduct investigative measures on the territory of the other JIT party. On this basis it can be ensured that investigative measures taken by one JIT party can be seamlessly followed up upon through investigative measures on the territory of another JIT party.

- **Other remarks:**

  - The development of new processes within Eurojust, such as the use of model JIT agreements for specific situations (e.g. between specific countries regarding specific cooperation requirements) has helped to significantly accelerate the set-up procedure for JITs, which has proven to be particularly valuable in cybercrime investigations.

  - Spontaneous exchange of information (incl. based on Article 26 Budapest Convention, see 2.3. below) has been a useful basis for cooperation during the period preceding the set-up of a JIT especially for the initiation of investigations in other states which potentially could join a JIT.

  - Other characteristics of the cooperation within a JIT which are particularly valuable in cybercrime investigations include the JIT funding provided by Eurojust especially for JITs with third states and the close involvement of Europol with a special view to the handling of large amounts of data.

2.2. Legal challenges in relation to the use of facial recognition technologies in criminal investigations

- So far there is very limited experience with the application of facial recognition technologies in the context of criminal procedures. However, this can be expected to change in the near future in view of the increasing availability of relevant material resulting from e.g. video surveillance recordings or cooperation of social media providers.

- Legal issues encountered so far have been less related to the technology itself than to its indiscriminate application to large numbers of individuals which are not necessarily linked to any criminal conduct. This includes the processing of personal data of large numbers of individuals which requires a concrete legal basis according to the new EU data protection legislation (Directive (EU) 2016/680).

- In view of the above any kind of guidance on limits and specific legal or practical requirements of the application of facial recognition technologies for the purpose of criminal procedures would be beneficial for practitioners.

2.3. Spontaneous exchange of information acc. to Article 26 Budapest Convention ("Art. 26")

- The extent to which information can be exchanged under **Article 26 depends on the legal framework provided by the national law in both the providing and the receiving state**. The national law of the providing state can limit the application of Article 26 to cases, where the information relates to an ongoing investigation in the providing state and where the exchange of the information is approved through a dedicated decision by the competent judicial authority. It can also require the providing state to exchange the information only under specific conditions especially for its use as evidence in court proceedings. Similarly the national law of the receiving state can limit the use of the provided information, e.g. by allowing its use as evidence in court trials only on the basis of an additional Mutual Legal Assistance procedure.

- Furthermore there are **other legal frameworks enabling judicial authorities to spontaneously exchange information** from criminal proceedings. Such alternatives can include other instruments based on international law (such as e.g. Article 7 EU MLA Convention 2000, UNTOC, CoE 1959 MLA Convention, etc) as well as provisions under national law.

- **Subject to their national law** some states can apply a **broad interpretation of Article 26** in the following sense:

    - It serves as legal basis to provide the competent authority of another state with evidence to be used at a court trial without the receiving party having to send a prior request.

    - It does not only apply where the receiving party is unaware of the availability of the information but also where the parties are already cooperating and informed about each other´s investigations including the availability of the information/evidence.

- This broad interpretation of Article 26 can – where this is in compliance with the national law of the states involved – be used as an alternative for Mutual Legal Assistance Requests/European Investigation Orders to **simplify the process of exchanging evidence** between two or more states, which has proven to be particularly useful in the investigation of cybercrime or cyber-enabled crime where parallel investigations with a frequent requirement to share evidence are a common feature.

- Based on the above **the EJCN recommends a more frequent use of Article 26** in the broadest possible sense within the limits of the national law of the states involved.

3. Meetings of Subgroups

Meetings of the following sub-groups took place as detailed below. The other sub-groups remain active but did not meet on this occasion.

3.1. Subgroup on data retention

- The subgroup organized its discussion based on two background documents prepared by the EJCN support team: one is a compilation of replies received to the questionnaire sent out to all EJCN contact points in July and September 2019 and the other one is a qualitative analysis of case law and of judicial cooperation difficulties in Member States.

- The discussion touched upon the various legislative frameworks in Member States, the differences in content and non-content data, the potential future problem of 5G and the upcoming developments in EU law to trigger a more harmonized approach in data retention. The subgroup agreed that an EU Regulation rather than a Directive would be very much welcome from the Commission in order to give less room for differences in Member States' implemented national legal measures. The importance of retained data for billing purposes which the LEAs can have access to was extensively discussed and underlined as one of the most important sources of information at the moment for national judicial authorities.

- The subgroup expects a positive impact of the future judgements of CJEU concerning the preliminary request from Belgium, France and Estonia.

- As to future actions, the subgroup agreed to keep an eye on developments in the field and to circulate the Questionnaire amongst Member States who has not replied to date. The subgroup will ensure, that the results are shared with the European Commission, which currently is also working on a study of the topic.

3.2. Subgroup on e-evidence

- The subgroup discussed the topic of direct cross-border access to e-evidence and the overview of countries' possibilities in this respect. The legal possibilities for cross-border access to data differ significantly per country as well as type of cross-border measure, depending whether the location of the data is known or not. Especially when the location of the data is unknown, several countries assume in practice that the data is located domestically. It would be good to have a common understanding and agreement on the measures that would be allowed as a minimum in each country to perform effective cross-border searches. This would facilitate cooperation. For this purpose, already existing practices of countries who can have access to e-evidence abroad in a legal way, as well as different court rulings (CH, NO, DK) can serve as inspiration. Such effective measures of course need to be balanced in accordance with the (safeguards of each) national legal

system. The subgroup assessed that, for extended search and access based on lawfully obtained credentials, it should be possible to start looking at an 'international'/European solution that would create minimum common standards. Such an international agreement would enable to have a framework in which every state can act, and give legitimacy to such kind of measures that are already being applied by several countries (this would help to avoid conflicts of laws). For online searches, it is needed to look further into the practical and legal issues and problems arising currently. The legislative approach in Member States differs significantly. Therefore the subgroup concluded that it will continue this exercise.

- On the basis of this discussion and the results of a survey among the members of the EJCN the subgroup will prepare an overview of existing practices/rulings related to direct cross-border access to e-evidence based on extended searches and lawfully obtained credentials for publication on the EJCN public website.

- The subgroup discussed the possibility to have a warning system among the EJCN members, in case they become aware of service providers changing their place of establishment or policies. This will safe a time (taking into account the data retention situation in Europe), prevent the possible risk of loss of e-evidence if for instance an EIO is sent to the wrong country.

- Similarly, the suggestion was accepted to create a list of the most relevant European service providers and supplement it with the relevant information to be put on the restricted EJCN website and subsequently to share it within the SIRIUS project, where appropriate.

3.3. Subgroup on training

- The subgroup will explore further the possibilities regarding the training needs of the Network. The Network will be consulted on who can give training as well as who has specific expertise and experience in certain topics with the aim to fulfil the training needs from and to the Network.

- In line with the work program (3.2.2) the Network will continue contributing to training activities organised by other agencies and Institutions. Therefore, the subgroup proposes to create a training pool to support the requests to the Network based on the gained expertise of the Network members.

3.4. Subgroup on virtual currencies

- The focus of the subgroup activities will be on developing expertise and knowledge with the aim of creating comprehensive and practical guidelines customized to the needs of prosecutors/magistrates and building on already existing material on virtual currencies produced on national and European levels.

- The following topics will be covered when dealing with virtual currencies:

- **Concepts and definitions**
  - Comprehensive and understandable oversight of the different concepts and used terminology

- **(EU) definition(s) of Virtual Currencies**
  - DIRECTIVE (EU) 2018/843 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 30 May 2018, Article 1, 2), d: virtual currencies mean a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and **does not possess a legal status of currency or money,** but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically.
  - Nature of the „currency "and the difference between cryptocurrency and virtual currency.

- **Investigative environment**
  - Legal bases for each country to take investigative measures; principles of territoriality and jurisdiction.

- **Investigative opportunities**
  - What can be done with a wallet? What to think about and to look for during a house search? Which investigative orders/measures can be considered with regard to the transactions? Which are the investigative possibilities with regard to the exit points?