Council of the European Union

Brussels, 23 November 2015
(OR. en)

14369/15

JAI 895
COPEN 319
DROIPEN 150
CYBER 110

NOTE

From:	Presidency
To:	Permanent Representatives Committee/Council
No. prev. doc.:	13689/15
Subject:	Effective criminal justice in the digital age - what are the needs - State of Play

1. The 2015 Internet Organised Crime Threat Assessment (iOCTA)[1] concludes that cybercrime is becoming more aggressive and confrontational, encompassing an extremely diverse range of criminal activities, including traditional crimes that leave digital traces. This approach of putting pressure on individuals and businesses is indicative for the changes in the profile of cybercriminals, suggesting also organised crime involvement, as well as pointing to an increased psychological impact of cybercrime on victims.

2. New technological developments and innovations present specific challenges to conduct effective investigations and increase the pressure on criminal justice systems to adapt their tools and approaches accordingly. This is of particular relevance in the context of counter-terrorism policies and anti-radicalisation measures: Internet communication channels and multiple social media, including encryption based technologies are widely used modus operandi for terrorist purposes.

[1] doc. 12728/15

3. In such rapidly evolving technological environment, electronic data are increasingly relevant in the course of the criminal proceedings. Such data constitute electronic evidence (e-evidence). However, the challenges to collect and bring to court admissible e-evidence and get a final conviction for the offenders are persisting. This state of affairs calls for an assessment of the existing legal and practical tools available to the competent authorities against the needs of effective criminal justice in the digital age.

4. Further to the discussion at CATS on 10 November 2015, the present document sets out in the Annex a certain number of possible strands of work to be examined by the Ministers of Justice with a view to providing guidance on the way forward in addressing the challenges related to collection and use of e-evidence in criminal proceedings.

Ministers are invited to indicate which of the issues set out in this document should be addressed as a matter of priority.

These can be summarised as follows:

- The challenges posed by the processes of loss of data in digital environment that can prejudice the effectiveness of criminal investigations, including the impact that an effective data retention regime can have in this respect.

- The problems which competent authorities face in applying the traditional rules for mutual legal assistance, in particular in terms of the formal requirements needed to process an MLA request or the expediency of the proceedings, as well as the effect that an optimal use of the European Investigation Order might have in EU based cases.

- The need to optimise the cooperation framework with foreign service providers where the existing practice of the competent authorities to address them with direct requests needs to be reviewed against rising fundamental rights and procedural guarantees concerns.

- The legal consequences related to the location and ownership of major digital infrastructure, and in particular stepping up the dialogue with the US authorities in this respect.

- The specific challenges raised by cloud-computing, often referred as "loss of location", and the ensuing implications for the applicable jurisdiction rules , as well as the possible consideration of trans-border access to data to address situations where the location of data is unknown.

- The complexity arising from the varying rules and standards for the admissibility of e-evidence before the competent national courts

- The need to assess any measure or initiative enhancing the effective conduct of criminal proceedings in the digital age against the requirements of the Charter of Fundamental Rights of the EU and the standards of ECHR as interpreted by the European Court of Human Rights.

ANNEX

Challenges related to collection and use of e-evidence in criminal proceedings

1. The effective collection, transmission and admissibility of e-evidence[2] in criminal proceedings present important challenges from a criminal justice perspective. This has been confirmed by the first country reports delivered in the framework of the *Seventh round of mutual evaluations on the practical implementation and operation of European policies on preventing and combating cybercrime* and in various discussions held on e-evidence related issues, including the informal COSI -CATS meeting of 22-23 July 2015 and a Workshop on Mutual Legal Assistance (MLA) in the Digital Age, organised on 15 October 2015 by the Presidency together with the University of Luxembourg.
2. On 19 October and 11 November 2015 the Friends of the Presidency Group on Cyber Issues discussed, as envisaged in the list of priority actions for the implementation of the Renewed EU Internal Security Strategy, the (legal) gaps in the fight against cybercrime in order to seek global approaches aiming at overcoming existing obstacles to cybercrime investigations as well as providing practical input to the Commission on potential new legislative instruments, raise awareness and share good practices[3].
3. In a follow-up to these discussions, the present document builds upon input from Eurojust provided on the basis of Eurojust's case work, the final reports of their Cybercrime seminar of 19-20 November 2014 and their dedicated tactical meeting on Cybercrime of 1 July 2015. Other sources used to prepare this document are a number of topical reports of the Council of Europe Cybercrime Convention Committee (T-CY)[4], the 2015 iOCTA prepared by Europol/EC3, the outcomes of the Presidency Workshop on MLA in the Digital Age referred above, as well as the recent Study commissioned by the EP LIBE Committee on the law enforcement challenges of cybercrime[5]. It also takes into account the comments made by Member States at the CATS meeting on 10 November 2015.

---

2 For the purpose of this document, e-evidence refers to all electronic data related to a criminal offence, which can be relevant in the course of criminal proceedings. Collection, sharing and use of data solely for disruption or prevention purposes, therefore falls outside of the scope of this document.

3 doc. 12612/15

4 http://www.coe.int/en/web/cybercrime/t-cy-reports

5 EP LIBE Committee(2015), Study "The law enforcement challenges of cybercrime: are we really playing catch-up?", PE 536.471

1. Data retention and loss of data

4. Directive 2002/58/EC (the e-Privacy Directive) sets out specific rules on the processing of personal data in the electronic communication sector, while providing for the right of confidentiality of communications (Article 5) and the obligation for the service providers to erase traffic data after it is no longer needed for the purpose of the transmission of a communication, unless it is processed under certain conditions for the purposes of subscriber billing and interconnection payments. Article 15 (1)[6], thereof, allows under certain conditions the restriction of the rights and obligations under this Directive for a range of specific purposes, including *"to safeguard the prevention, investigation, detection and prosecution of criminal offences"*. In this respect, the establishment under certain conditions of national data retention measures is enabled. Directive 2006/24/EC (the Data Retention Directive) aimed to harmonise those rules, in order to ensure that the data is available in particular for the purpose of investigation, detection and prosecution of serious crime.

5. By nature, e-evidence is short-lived. Furthermore, the increased private use of live streaming, encryption, the rise of the Darknet and anonymisation enable criminals to completely hide critical evidence from law enforcement. Thus, critical e-evidence can be lost if there are no adequate means available to the competent authorities to react effectively. The availability of an effective data retention regime might prove instrumental in this respect.

---

[6] Article 15 (1) of Directive 2002/58/EC reads:
"Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, *inter alia*, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union."

6. Eurojust explains in its analysis of EU Member States' legal framework and current challenges on data retention of 26 October 2015[7] that the present fragmentation of the legal framework on data retention across the EU following the invalidation of the Directive 2006/24/ EC (Data Retention Directive) by the Judgment of the Court of Justice of the European Union (CJEU) of 8 April 2014 has an impact on the effectiveness of criminal investigations and prosecutions at national level, in particular in terms of reliability and admissibility of evidence to the courts, as well as on cross-border judicial cooperation between Member States and globally.

7. A specific discussion of Ministers on the current state of affairs and the effects of the Data Retention Judgment of the CJEU of 8 April 2014 will take place under a separate item of the Council agenda.

2. Mutual Legal Assistance (MLA) process

8. The collection of e-evidence is in principle a time-sensitive issue. The availability of expedient procedures for preservation and collection of e-evidence is crucial for the effective conduct of criminal proceedings. Since the electronic data are very often located in a foreign jurisdiction, the competent national authorities need to make use of the available tools for international cooperation, i.e. requesting mutual legal assistance (MLA) or if the proceedings concern EU Member States making recourse, as appropriate, to the available mutual recognition instruments for judicial cooperation in criminal matters.

9. Directive 2014/41/EU on the European Investigation Order (EIO)[8] is of particular relevance in this respect. As from 22 May 2017 it will replace the existing fragmented EU legislation relating to collection and transfer of evidence between EU Member Sates with the aim to make cross-border investigations faster and more efficient. Full use of this regime, within the scope of application of the EIO, should be made also in relation to e-evidence.

---

7 doc. 13085/15

8 OJ L 130 of 1.5.2014, p.1-36

10. Often electronic data is found in foreign third States jurisdictions. In such cases MLA should be requested. The existing MLA regimes, however, are increasingly perceived as being too slow and cumbersome to meet the time constraints. Thus, the question arises what could be done to speed up the MLA process, in the first place by optimising the available procedures. In this respect, the possibility to develop a standardised, simplified and possibly electronically transmittable and acceptable request form might be considered, including in the context of EIO. It could also be explored whether the formal requirements in the MLA procedures may be further differentiated depending what data is requested - is it a subscriber, traffic or content data. In many jurisdictions, requirements for access to subscriber data tend to be lower than for traffic data, while the most stringent regime applies to content data[9].

11. A common standard to treat a cooperation request as "urgent" could be set up. In addition, expedited procedures for transferring the evidence under certain conditions, as it exists for the preservation of evidence pursuant to the relevant provisions of the CoE Convention on Cybercrime might be envisaged. In general, as is the current state of affairs, even though evidence is preserved, it might take a long time before it is available for the criminal proceedings in the requesting country.

12. To operationalise the cooperation process an early coordination and involvement of the judicial authorities in the criminal proceedings should be considered. In this respect, further strengthening of the cooperation 24/7 networks, including those of judicial authorities, such as establishing a network of prosecutors dealing with cyber-related cases, might be envisaged. This will be instrumental in promoting and enhancing the direct contacts between judicial authorities, including in relation to MLA requests across the EU and globally. In this respect the role of Eurojust and Europol/EC3 should be also considered.

---

[9] See T-CY Discussion paper "Criminal justice access to data in the cloud: challenges", May 2015
(T-CY(2015)10), p. 7
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304b59

3. Direct requests and cooperation with foreign service providers

13. Cooperation with the private sector is vital in combating cybercrime. However, no common legal framework for such cooperation exists. The issue is of particular importance when it comes to obtaining access to data held by foreign service providers.

14. To overcome shortcomings of the existing MLA process in collecting e-evidence, competent authorities make recourse to alternative methods of obtaining digital evidence, by addressing for example a request directly to the foreign service providers. In such cases, service providers may be allowed under domestic legislation to disclose non-content data on a voluntary basis to (foreign) law enforcement authorities. However, this is not the case in all states. On the other hand, the service providers are not always willing to cooperate, even when permitted by national law. Also, not all Member States allow for a domestic production order to be sent to a private entity abroad. It is equally possible that even if the e-evidence is obtained through a voluntary disclosure, it would not be admissible before the court of the requesting state, since it has been obtained outside the MLA framework. In general, as pointed out at the Presidency workshop on MLA in Digital Age of 15 October, such a process might result in a phenomenon which could be defined as MLA "without assistance", which might raise fundamental rights and procedural safeguards concerns.

15. Addressing foreign service providers directly could make them on the other hand subject to conflicting requests from different states, but also of conflicting requirements for protection of privacy and procedural safeguards if they operate in multiple jurisdictions. For example, service providers may violate data protection rules of one State if they disclose data to the authorities of another State.

16. In view of all this, there is a need to set out clear conditions for a sustainable cooperation framework between private actors and public authorities concerning the collection of e-evidence, based on full respect of procedural guarantees for the suspected and accused persons in criminal proceedings and protection of personal data.

4. Legal consequences related to the location and ownership of digital infrastructure

17. In view of the impact that the national legislation of the executing State might have on the international cooperation process, intensifying the dialogue with countries that are key players in terms of operation and ownership of major digital infrastructure is crucial.

18. This aspect is of particular relevance as regards the cooperation with the US. As stated in the 2015 Study for the LIBE Committee on law enforcement challenges of Cybercrime, "US and US-based corporations play leading roles in the functioning of the Internet. Thus US legal framework have a significant impact on cybercrime law enforcement…"[10] . Beyond the issue of varying standards of data protection, from a strictly criminal justice perspective this situation has an impact on the standard of legal justification that should be observed in the MLA requests sent to US, especially when it comes to requests concerning content data.

19. In general all MLA requests have to include an explanation why the competent authority has a legitimate interest in the requested data. The US legislation requires an assessment of the requests against the so-called "probable cause" standard, which is a higher justification standard compared to the "reasonable suspicion" or its equivalent. The "probable cause" justification limits the interventions of the competent authorities only to those strictly necessary for the specific investigation. Therefore, it is very likely that an MLA request is refused by the US authorities because it does not fulfil the "probable cause" justification requirement. A proper balance of the possibilities of the US and foreign authorities to receive access to "local" US data on the one hand to any other type of data, on the other, needs to be also ensured. These issues should be addressed in the context of a continuous EU-US dialogue, including in the framework of the Review process of the EU-MLA Agreement.

[10] EP LIBE Committee(2015), Study "The law enforcement challenges of cybercrime: are we really playing catch-up?", PE 536.471, p. 46

5. Loss of location

20. While access to e-evidence in foreign jurisdictions is mainly carried out in the MLA framework, the increasing use of cloud computing and web-based services is presenting an additional challenge for the competent authorities described as "loss of location"[11]. In this case, the electronic evidence is stored "somewhere in the cloud", either on one server or distributed over several servers or being moved between servers in varying locations. Thus, the data concerned are physically located in foreign, unknown or multiple jurisdictions at the same time or are moving between jurisdictions.

21. In principle, location determines the competent authorities and the applicable law to the investigation, including the extent of coercive powers that could be applied, as well as the procedural guarantees available for the suspected or accused persons. In the context of the above-mentioned new technological developments, where the location of data is not stable, the underlying principle of territoriality, which determines the establishment of jurisdiction in criminal proceedings, seems to lose relevance and raises challenges for the effective conduct of the criminal proceedings.

22. In some cases, the lawful search within the original system based in the territory of the criminal investigation could be extended to a connected information system abroad without being aware of it or in cases where it is unclear in which territory the information system is located. Such situation may result in practice in trans-border access to data located in a foreign jurisdiction "without consent", which is beyond the existing legal possibilities (e.g. Article 32b of the Council of Europe "Budapest Convention on Cybercrime"). The handling and use of the data retrieved this way is governed in accordance with national legislation and consequently made subject to varying standards of procedural guarantees.

---

[11] See Report of the CoE Transborder Group of 6 December 2012 on Transborder access and jurisdiction: What are the options? http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/TCY2013/TCYreports/TCY_2012_3_transborder_rep_V31public_7Dec12.pdf

23. The "loss of location" may result in competing claims for prosecution or parallel investigations, which once again underlines the need for early involvement of the judicial authorities, but also for revisiting the rules governing the establishment of jurisdiction, as well as examining alternatives to the MLA process, to address situations where the location of the data is unknown, such as trans-border access to data for criminal justice purposes.

6. Admissibility of e-evidence

24. Eurojust points out that under domestic legislation, judicial authorities may need to fully assess on the basis of the criteria established by law the legality of the collection of evidence, as a condition it to be admissible to the court, contrary to legal models based on the principle of trust, where all evidence is submitted and assessed freely by the judge. These requirements need to be taken into account when collecting and sharing e-evidence. This might result, for instance, in a necessity for the competent authorities to secure and gather evidence according to the requirements of foreign judicial systems.

25. A correct interpretation of e-evidence in criminal proceedings may require expertise that may not be sufficiently present within the prosecution service or the courts. Furthermore, a correct presentation of e-evidence in judicial proceedings may require a forensic awareness within the judiciary that might not be always available.

26. In view of the above awareness raising, information sharing, exchange of good practice and targeted training might be considered.

7. Fundamental rights and rule of law assessment

27. Effective procedural safeguards, data protection guarantees, full respect for rule of law is the common platform on the basis of which any policy initiatives and practical solutions to enhance the effective conduct of criminal proceedings should be built.

28. Thus, a careful balancing of the needs of the criminal justice systems in cyber-related proceedings should be consistently carried out against the established fundamental rights principles. This is a challenging task. These difficulties have been encountered in the context of the Council of Europe' s work on an Additional Protocol on Transborder access to data. It has been also demonstrated in a range of recent European Court of Justice rulings where the Court has given a clear direction to the legislator that his work should be driven and consistently tested against fundamental rights and rule of law considerations.