Council of the European Union

Brussels, 4 November 2015
(OR. en)

13689/15

LIMITE

JAI 817
COPEN 297
DROIPEN 135
CYBER 103

NOTE

From:	Presidency
To:	CATS
Subject:	Collecting E-evidence in the digital age - the way forward - Preparation of the Council meeting (Justice Ministers)

I. Introduction

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 aggressive, confrontational 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. At the same time, new technological developments and innovations present growing challenges to conduct effective investigations and increase the pressure on criminal justice systems to adapt their tools and approaches accordingly.

2. While the number of successful law enforcement operations resulting in disruption and taking down of criminal networks and preventing of cyberattacks is growing, the difficulties to bring admissible evidence to court 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.

[1] doc. 12728/15

II. Criminal justice outlook

3. The effective collection, sharing and admissibility of e-evidence[2] in criminal proceedings present one of the main 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.

4. On 19 October 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]. A further discussion on these issues will be held on 11 November 2015.

5. 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].

---

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

6. The document outlines certain areas related to the collection, sharing and admissibility of e-evidence that might be considered in order to identify possible deficiencies and to determine whether further action is needed, possible or feasible. The objective of the Presidency is to submit these issues for discussion to the Ministers of Justice at the Council meeting of 3-4 December 2015 with a view to obtaining a political guidance on the way forward.

Data retention and loss of data

7. 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. The 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.

[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."

8. 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.

9. A scattered picture of data retention rules is currently materialising across the EU following the Judgment of the European Court of Justice of 8 April 2014 invalidating the Data Retention Directive *ab initio*, i.e. from the date it took effect in 2006 on the grounds that the Directive disproportionately restricted the right to privacy and to the protection of personal data as guaranteed by Articles 7 (respect for private and family life) and 8 (protection of personal data) of the Charter of Fundamental Rights.

10. Nonetheless, Article 15(1) of the e-Privacy Directive, as referred to above, applies including as regards national measures on data retention in the electronic communication sector. However, during the dedicated discussions on this issues at the meetings of GENVAL Working Party on 15 September and 29 October 2015 the absence of a common legal framework on data retention at Union's level has been outlined as a matter of concern that created a situation of legal uncertainty for a number of Member States.

11. At the last GENVAL meeting Eurojust presented an analysis of the legal framework and current challenges on data retention[7]. Eurojust pointed out that following the Data Retention Judgment, the current state of play is as follows: the transposition law of the Data Retention Directive has been invalidated in at least 11 Member States (AT, BE, BG, DE, LT, NL, PL[8], RO, SI, SK, UK[9]). Amongst these, 9 countries have had the law invalidated by the Constitutional Court (AT, BE, BG, DE, SI, NL, PL, RO, SK). In 14 Member States (CZ, DK, EE, ES, FI, FR, HR, HU, IE, LU, LV, MT, PT, SE) the domestic law on data retention remains in force, while they are still processing communication data.

---

7 See doc. 13085/15

8 On 30 July 2014, The Polish Constitutional Court ruled unconstitutional certain provisions of the data retention law, which shall become inoperative on 7 February 2016.

9 In the UK, the High Court struck down the data retention law but the judgment has been stayed until 31 March 2016.

12. Following the invalidation of the Data Retention Directive some Member States have already adopted or are in a process of preparing new legislation on data retention, that, according to the information received by delegations, aims at ensuring strengthened procedural guarantees and safeguards in compliance with the Charter and in line with the ruling of the Court (EE, ES, IE, LT, LU, LV, MT, PL), including some Member States where the national law has been invalidated by the constitutional Court (DE, BG, NL).

13. Eurojust explains in its analysis of the current state of affairs that the present fragmentation of the legal framework on data retention across the EU 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.

Mutual Legal Assistance (MLA) process

Processing

14. 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).

15. The existing MLA regimes, however, are increasingly perceived as being too slow and cumbersome to meet these 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 MLA request form might be considered. It could be also 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[10].

[10] 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

16. 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. 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.

17. 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 networks, including those of judicial authorities, such as 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.

Direct requests and cooperation with foreign service providers

18. 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.

19. To overcome shortcomings of the existing MLA process in collecting e-evidence, competent authorities may use 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".

20. At the same time, addressing foreign service providers directly could make them 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.

21. 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.

US ownership of digital infrastructures and impact of US legal requirements in MLA process

22. 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…"[11] . 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, especially when it comes to requests concerning content data.

23. 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 any equivalent known in many Member States. 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. To that end, strengthening of the EU-US dialogue with a view to enhancing the common understanding on requirements that should be fulfilled in the MLA process seems to be another area deserving further attention.

---

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

Loss of location

24. 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"[12]. 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.

25. 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.

26. 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.

[12] 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

27. 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.

Admissibility of e-evidence

28. 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.

29. 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.

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

Fundamental rights and rule of law assessment

31. 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.

32. 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.

III. Conclusion

33. The present paper sets out a 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. Since those issues are of a multifaceted nature, touching on a number of aspects of the criminal justice systems, it seems appropriate that a follow-up on the further developments is provided by CATS. This would also ensure an effective involvement and consideration of the judicial dimension in the implementation of the Renewed EU Internal Security Strategy.

Delegations are invited to express their views on the issues set out in this document with a view to preparing the debate of the Ministers of Justice, as well as to confirm the role of CATS in providing a follow-up to this debate, where appropriate.