Council of the European Union

Brussels, 25 May 2018
(OR. en)

9117/18

Interinstitutional Files:
2018/0107 (COD)
2018/0108 (COD)

LIMITE

JAI 442
COPEN 151
CYBER 109
DROIPEN 71
JAIEX 53
ENFOPOL 256
DAPIX 150
EJUSTICE 58
MI 368
CODEC 804

NOTE

From:	Presidency
To:	Permanent Representatives Committee
Subject:	E-evidence a) Regulation on European Production and Preservation Orders for e-evidence b) Directive on legal representatives for gathering evidence = Policy debate

I. Introduction

1. On 17 April 2018 the Commission adopted two legislative proposals: a *proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters*[1] and a *proposal for a Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*[2]. They aim to improve cross-border access to e-evidence by creating a legal framework for judicial orders addressed directly to legal representatives of service providers without the intervention of an authority of the Member State where their legal representative is located.

1 8110/18.
2 8115/18.

2. The first expert discussions and a debate at CATS showed a number of politically important issues that the Presidency wishes to bring to the Council (JHA) on 4 June to seek political guidance not only on the direction to be followed in the future negotiations on the proposals, but also with regard to the EU's external relations on this matter with key partners such as the US.

3. Coreper is therefore invited to agree that the explanations and questions set out in parts II and III below be submitted to the Council. As regards point 12 in particular, Coreper is invited to confirm that a public debate on this subject, at which Ministers could confirm their support for a common EU approach, would provide a clear signal of the willingness of the Member States and the EU to proceed swiftly with this matter.

II. Scope of the Commission legislative proposals

4. While welcoming the proposals, a number of delegations regretted the limited scope of the proposed Regulation as it does not address *direct access to e-evidence* (direct access to data without the assistance of a third party (service provider) as an intermediary), or *real-time interception of data*. Many delegations felt that these two elements needed to be addressed as they respond to an operational need and thus need to be studied further and in much greater detail. However, opinions are divided as to whether this should be done with a view to including them in the current proposals or rather in parallel to the current proposals so as not to delay or prolong the current negotiations.

5. As regards *real-time interception of data*, the following considerations have been made so far:

   – this is a sensitive and intrusive measure,

– this possibility is provided for in most national laws for domestic circumstances, in the Directive on the European Investigation Order and in the US CLOUD Act; any EU basis for real-time interception of data should be considered in this broader framework and take account of the need to equip Member States' authorities with the full range of tools to fight crime in the digital era [that are at the disposal of their US colleagues]. Moreover, Member States raised that the possibility to cover real-time interception in an Executive Agreement under the US CLOUD Act, on a reciprocal basis, should also be considered as part of the reflection on this measure.

6. As regards *direct access to e-evidence*, the following considerations have been made so far:

– it is a powerful tool in case of loss of location or non-cooperative service providers, empowering Member States' authorities to remotely access the data available following the search and seizure of a device or the use of lawfully obtained credentials for access to an account;

– there is a wide variation in national laws currently regulating such direct access in the Member States, in particular the safeguards and powers they provide;

– the possible creation of a common EU framework would be beneficial, but such an EU approach should be carefully considered in the light of those divergent national legal frameworks and a number of legal questions, including the appropriate legal basis, should be carefully examined.

7. Ministers are invited to exchange views on the urgency of the issue and the modalities for continuing the discussions on the creation of an EU framework for 'direct access to e-evidence' and 'real-time interception of data' [in the near future].

III. Recent international developments and the impact of the US CLOUD Act

8. The US CLOUD Act[3] adopted by the US Congress on 23 March 2018 clarifies through an amendment of the Stored Communications Act of 1986 that US service providers are obliged to comply with US orders to disclose content data regardless of where such data is stored[4]. In addition, the US Cloud Act allows the conclusion, under certain conditions, of executive agreements with foreign governments, on the basis of which US service providers would be able to deliver content data directly to these foreign governments (as well as to intercept wire communications), subject to conditions to be determined in the executive agreements.

9. When discussing this issue at the March (JHA) Council, Ministers spoke in favour of a common EU approach towards the US, underlining that this would not only contribute greatly towards the establishment of legal clarity for service providers and Member States' competent authorities, but also that it would prevent the proliferation of diverging regimes, fragmentation within the EU and the unequal treatment of Member States.

10. At the CATS meeting of 18 May, the Commission and the Council Legal Service clarified that the EU is competent to engage in such negotiations with the US and Member State should not enter into bilateral negotiations. The Commission also underlined some of the above-mentioned benefits. The Commission and the Presidency also clarified the EU's competence on the matter in the EU-US Ministerial meeting held in Sofia on 22 and 23 May 2018.

11. The conclusion of an executive agreement between the EU and the US should also be seen in light of the provisions of Article 48 GDPR, which just entered into application. That article envisages that '*any judgement […] requiring a controller or processor to transfer or disclose personal data may be only recognized or enforceable in any manner if based on an international agreement [….] between the requesting third state and the Union […] without prejudice to other grounds for transfer pursuant to Chapter [V]'.*

---

3 Clarifying Lawful Overseas Use of Data

4 Thus rendering moot the US vs. Microsoft Corporation case on the same subject, i.e. whether, under the Stored Communications Act of 1986, US law enforcement authorities can require a US-based service provider, on the basis of a judicial warrant, to produce the content of an email account stored on a server located overseas.

12. Finally, in defining the future relationship, particular attention should be paid to the rules contained in the respective legislative texts regarding cases where service providers are caught between conflicting national legislations. The US CLOUD Act contains a 'comity clause'[5], whilst the draft EU Regulation sets out in its Article 15[6] a review procedure in case of conflicting obligations. A careful and detailed examination of those provisions will be required to ensure reciprocity and operational effectiveness.

13. Ministers are invited to confirm their wish to swiftly engage in negotiations with the US on the conclusion of an executive agreement between the EU and the US and are further invited to request the Commission to urgently submit a recommendation for a negotiating mandate to this end to the Council. Ministers are invited to request the Commission to take similar steps with respect to the Second Additional Protocol to the Budapest Convention currently being drafted under the auspices of the Council of Europe.

---

[5] The comity clause enables service providers to ask a US court to quash or modify an order issued for preservation or disclosure of data if the data relate to a non-US person and if complying with the order would cause them to violate the laws of a country with which the US has an executive agreement that provides similar possibilities for service providers under their laws.

[6] Article 15 foresees a dialogue with the central authority of the third State concerned. Only in case this authority does not object, the European production order would be upheld and data would be provided.