17 January 2017

Cybercrime Convention - cross-border access to electronic evidence

European Digital Rights (EDRi)[1] is actively involved[2] in current European Union and Council of Europe discussions around cross-border access to electronic evidence. This issue is of importance for a wide variety of reasons – from defence of the rule of law to fighting crime.

The growth of electronic communications has put considerable strain on pre-existing mutual legal assistance frameworks. New solutions are needed, but these new solutions need to respect human rights principles. We argue that, for legal and practical reasons, predictable, accountable legal structures must be the default option for access to personal data.

We welcome the European Commission's approach of clearly defining the problems that need to be addressed, as well as assessing the pros and cons of the options available.[3] However, we are very concerned about the EU Council's explicit preference for less accountable and predictable arrangements with private actors. As these will almost always be "easier" than more accountable approaches this risks, de facto, eliminating existing frameworks, even after these have been streamlined and modernised.

The EU's approach is likely to involve close cooperation with the Council of Europe and efforts to find solutions to existing problems through the Cybercrime Convention,[4] In order to fulfil some of the unquestionably legitimate functions that are now being expected from the Convention, it is important to recognise and mitigate some concerns inherent with the use of that instrument.

1. The Cybercrime Convention is a Council of Europe Convention, not a "European Convention", and thus open to non-European states. All Council of Europe Member states (and therefore all EU Member States) are required, by virtue of their membership, to be full parties to the European Convention on Human Rights (ECHR), and all are also party to the Council of Europe's Data Protection Convention (Convention No. 108).[5] However, **accession to the Cybercrime Convention by non-European states does not require such states to be party to ECHR-comparable international human rights treaties, such as the International Covenant on Civil and Political Rights (ICCPR), or to Convention No. 108.**

This means that relevant activities are not automatically subject to international human standards in relation to highly human rights-sensitive activities by non-European state parties' law enforcement authorities in the digital environment. This is true in particular in relation to cross-border or extraterritorial activities of such authorities. This problem does not arise for Council of Europe Member states' authorities, because they must accept the application of the ECHR to their agencies' activities in the digital environment, also extraterritorially, in accordance with the case-law of the European Court of Human Rights (EctHR).[6]

1 EDRi is a coalition of 31 civil rights organisations. EDRi is thankful to the input received by Emeritus Professor of International Law Douwe Korff.

2 See our latest contributions: https://edri.org/files/surveillance/letter_coe_t-cy_accesstoe-evidence_cloud_20161110.pdf https://edri.org/files/surveillance/korff_note_coereport_leaaccesstocloud%20data_final.pdf

3 https://www.parlament.gv.at/PAKT/EU/XXV/EU/12/52/EU_125221/imfname_10677095.pdf

4 https://www.coe.int/en/web/cybercrime/the-budapest-convention

5 https://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/108/signatures?p_auth=qwpC6cQM

6 See section 3.4, "*Within [a contracting state's][territory and] jurisdiction*" in the Council of Europe Commissioner for Human Rights' *Issue Paper* on The Rule of Law on the Internet and in the wider digital

By contrast, the USA, for instance, although it is a party to the ICCPR, refuses to accept that it is subject to the requirements of the ICCPR in respect of activities of its agents or agencies outside U.S. territory that affect the rights of "non-U.S. persons".[7] The USA is also not a Party to the Data Protection Convention. Such a position should be incompatible with being a party to the Cybercrime Convention.

=> EDRi's recommendation: The structural problem of the Convention that underlies this anomaly must be fully taken into account and mitigated in the context of current plans to use the instrument to address the issue of cross-border access to evidence. In the same way that the T-CY decided to encourage "all States that are Parties to the Budapest Convention to sign, ratify or accede to the Additional Protocol (ETS 189) on Xenophobia and Racism" on its 16th Plenary,[8] EDRi encourages to add an agenda item point in the next T-CY plenary for the T-CY to strongly encourage Non-Council of Europe Members to sign, ratify or accede the ICCPR and Convention No. 108.

2. The T-CY Cloud Evidence Group's report on Criminal justice access to data in the cloud[9] states that "[i]t is presumed that the Parties to the Convention form a community of trust and that rule of law and human rights principles are respected in line with **Article 15 Budapest Convention**."[10] The T-CY unfortunately agreed with this assumption in its 16th plenary report.[11] However, that article **only requires compliance with human rights requirements in relation to** "the establishment, implementation and application of the powers and procedures provided for in [section 2 of the Convention]", which only relates to **procedural law. It neither ensures nor requires that Parties comply with international human rights standards in relation to any substantive criminal law** – which would include laws limiting freedom of speech in relation to blasphemy, defamation of the state, sexual matters, or even hate crimes (which can be very differently defined under the additional protocol to the Convention). Moreover, the Convention does not clarify **how Article 15**, even in this limited application, **is to be enforced.** If, as is proposed both in EU and CoE contexts, law enforcement agencies will be increasingly allowed to obtain personal data from non-state actors in other countries, without involvement of the state bodies in the target state or even unseen, by directly accessing devices, this opens significant scope for abuse of individuals' rights.

=> EDRi's recommendation: Article 15's human rights compliance application should be expanded to substantive criminal law and its enforcement should be clarified and improved in light of the policy and technological developments. This is in line with the 2014 Conclusions of the Conference on Article 15 safeguards and criminal justice access to data."[12]

world, 2014, pp. 50-55, available at: https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2933488&SecMode=1&DocId=2262340&Usage=2

7 See the sub-section "*The U.S. Government and the ICCPR*" in the above-mentioned *Issue Paper*, pp. 54-55.

8 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806cd270

9 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e

10 *Ibid*, p. 54

11 See p. 14: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806cd270

12 "Such solutions need to provide for safeguards, conditions and respect rule of law and human rights, including data protection, principles." cf.https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680303ebe

3. The danger outlined above is reinforced by the equally **legally unenforceable** provision in **Article 15.3 of the Convention** that each party "shall consider" the impact of the power and procedures in this section upon the rights, responsibilities and legitimate interests of third parties".

=> EDRi's recommendation: Compliance with international human rights - and data protection standards, specifically also in relation to the digital environment (which, by its very nature, is not defined by geography), must be guaranteed. There must be effective procedures and processes on the part of both the targeted states and the affected individuals to challenge any non-compliance. In practice, this means that States must continue to be able to regulate access to data in their jurisdiction and on their citizens and residents, in particular by foreign law enforcement - and national security – agencies. In addition, individuals must be able to seek protection and redress in their own country in this regard.

Conclusion

Staying true to the ideals and duties of the Council of Europe and, indeed, the EU's legal framework, any reform of the Cybercrime Convention via a new Additional Protocol should work towards mitigating the *lacunae* outlined above. EDRi is looking forward to keep working with the Council of Europe in ensuring human rights are effectively respected in this workstream. In this sense, EDRi encourages the T-CY to invite civil society organisations to the annual meetings it will be holding with providers.[13]

[13] Cf. 16th plenary report of the T-CY, p.3 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806cd270