Cross-border data in the fight against crime: What future for e-evidence?

Navigating the current legal framework and exploring ways forward within the EU and across the Atlantic

Proposal for a CEPS Task Force

Content

CONTEXT & MOTIVATION

Within the EU and across the Atlantic, investigation and prosecution of criminal offences increasingly rely on the possibility for law enforcement authorities to seek and obtain different types of electronic information held by private companies abroad, or in the cloud. While data are ever-often seen as precious evidentiary sources for the purpose of fighting crime, the processing of cross-border electronic information requests raises several legal and practical dilemmas that still requires careful consideration.

Access to electronic information held by companies and sought by law enforcement authorities for the purpose of preventing, detecting, investigating, and prosecuting crime is currently governed by a multilayered web of national, supranational, and international rules. As recent CEPS research has shown, correctly navigating the regulatory frameworks applying to cross-border data access by state actors is no easy task.

EU and third countries' authorities still struggle in mutually understanding the substantial and procedural conditions to be met in order to lawfully request, disclose and exchange electronic information held by private companies across-borders, or in the cloud. The transnational and cross-jurisdictional nature of the internet is often a source of challenges for legal practitioners. On the other hand, unilateral assertions of criminal jurisdiction in the field of data gathering can seriously harm trust in intra-EU and international relations. They can also lead to violations of the fundamental rights of persons accused or suspected of a crime, as well as of other data subjects including both citizens and third country nationals, and expose private companies to potential liabilities.

At the EU and international level, a number of instruments are available to investigating and prosecuting authorities' seeking to cooperate among them in order to demand and obtain data across borders. The European Investigation Order (EIO) allows EU Member State to issue and execute cross-border evidence gathering measures based on the principle of mutual recognition. Mutual legal Assistance Treaties (MLATs) provide the possibility to channel requests through formal judicial cooperation venues. Other fora of international cooperation such as the one provided by Council of Europe's Convention on Cybercrime (the Budapest Convention) also allow State parties' authorities to issue cross-border demands for data.

And yet, several implementation issues currently affect the functioning of existing EU and international cooperation instruments. The wide range of data-gathering instruments available to law enforcement actors reduce legal certainties and generate risks of forum shopping and fishing expeditions. International cooperation tools are also sometimes used in ways which lower down rule of law or fundamental rights protection standards otherwise applicable in domestic cases.

While substantial and procedural safeguards are formally in place to protect individuals affected by cross-border data-gathering measures, it appears that their effectiveness is not always guaranteed against unlawful, unnecessary or disproportionate electronic information requests.

A number of legislative initiatives are currently being discussed at the EU level, and adopted internationally with the intention of creating a 'level playing field' for cross-border cooperation in the access to data for crime-fighting purposes. The US CLOUD ACT and the EU 'E-Evidence package' represent the most significant developments in this respect. The latter comprises an internal component, and an external component. The internal component is inclusive of: the proposed Regulation on European Production and Preservation Orders, and; the proposed Directive on the appointment of legal representatives of providers marketing their services in the EU. The external component mainly consists of the envisaged EU-US Agreement of cross-border access to data.

Both the proposed E-Evidence Regulation and the envisaged EU-US Agreement rely on the idea that fundamental rights and rule of law safeguards can be ensured exclusively through the involvement of oversight authorities in the country of issuing of cross-border data-gathering measures. At the same time, this a priori 'presumption of trust' does not bode well in a context where several EU countries witness a process of rule of law deterioration.

Judicial cooperation under existing mutual recognition instruments have already been halted upon the findings by some Member States' courts that the lack of judicial independence in the other EU country involved in a criminal proceeding risk to expose the suspect or accused person to serious violation of his/her fair trial rights. Infringement procedures have even been launched by the Commission in response of some Member State's legislative and institutional reforms that allegedly undermined the independence of national judiciaries.

At the transatlantic level, the agreement on cross-border data access recently concluded between the US and the UK - which is set to provide 'a blueprint' for the future EU-Us agreement - raises questions related to reciprocity, effective judicial oversight and legal protection, and non-discrimination based on nationality.

The next months will see the EU co-legislators engaging in the negotiations of the e-evidence package. Further expert discussions on the exact ways in which electronic information can be requested, disclosed and exchanged across borders without breaching criminal justice, privacy and human rights rules becomes even more timely in a context where new tools for cross-border data access are being discussed at the European Union level, and introduced internationally.

A new CEPS Task Force will be set up to address outstanding issues related to the correct use and implementation of both existing and new proposed instruments of law enforcement or judicial cooperation for cross-border data-gathering.

OBJECTIVES & GOALS

The Task Force will provide a forum for exchange of knowledge among key communities of stakeholders including investigating and prosecuting authorities, specialised lawyers, but also private companies and non-governmental organisatons (NGOs), as well as academics and policy makers at the EU and national level.

It will help them to better understand how to formulate, transmit, process and execute requests for data that, while responding to the objective of investigating and prosecuting crime, also preserve fundamental rights and trust in the EU Area of Freedom Security and Justice, as well as in transatlantic police and criminal justice cooperation.

By fostering interdisciplinary expert dialogue, the Task Force will also inform the negotiations of the internal and external components of the e-evidence package, and contribute to assess the implications that initiatives such as the recently signed UK-US Bilateral Agreement on Data Access might have from an EU and international law perspective. Attention will moreover be paid to ongoing Council of Europe's discussions on new cybercrime instruments.

The new CEPS Task Force will address a set of distinct but closely interlinked challenges that, beside affecting cross-border law enforcement and criminal justice cooperation under the existing legal framework, are also likely to constitute crucial issues to be taken into account for the development of new EU and international rules on data gathering for criminal investigations purposes.

Results of the Task Force discussion will not only enhance the practical use of existing instruments of international cooperation for data gathering in police and criminal matters, but also contribute to inform the current legislative and policy debate on e-evidence at the EU and international level.

METHODOLOGY & SCHEDULE

The Task Force will ensure a venue for a structured closed-doors dialogue between a selected group of participants (Task Force Members) and leading experts in the field of EU and international law, criminal law, privacy and data protection. The dialogue will be informed by the findings of independent background research conducted by CEPS Justice and Home Affairs Section and other institutions which cooperated in the framework of the recently concluded JUD-IT Project.

The Task Force will be implemented in the form of **four meetings**:

- ✓ A **first meeting** will be organized in **January 2020**;
- ✓ A **second meeting** will be organized in **March 2020**;
- ✓ A **third meeting** will take place in **April 2020;**
- ✓ A **fourth meeting** will be organized in **May 2020**.

The **first Task Force meeting** will serve the purpose of presenting and defining the exact scope of the following Task Force discussions. It will be the occasion for the CEPS research team members acting as rapporteurs to gather views and discuss the Task Force's implementation plan with Task Force members. The **following meetings** will be devoted to different topics, the exploration of which is particular salience for the attainment of the Task Force objectives. A preliminary outline of the main questions to be addressed by the different Task Force meetings is provided below:

- *How to ensure trust, fundamental rights, and the rule of law under the proposed e-evidence regulation?*

The Task Force will focus on tackling key open questions surrounding the internal component of the e-evidence package (i.e. the proposed regulation and directive), including: legal basis; involvement of judicial authorities in the country of issuing and execution; notification duties; rights and responsibilities of private companies; access to remedies.

- *What future for transatlantic cooperation on access to data?*

Discussions will address the main challenges to be taken into account in the design of a new EU/US agreement on cross-border data access, including: structure and architecture; EU criminal justice and data protection safeguards; rule of law protections in different EU countries and their eligibility for a future EU-Us agreement on direct request; personal scope and reciprocity; oversight mechanisms; prevention and redress of conflicts of laws and jurisdictions.

- ***Task Force meeting 4:*** *Towards the second protocol of the Council of Europe Convention on Cybercrime – risk for coherence and forum shopping?*

Attention will be paid to legal issues related to the content and functioning of the envisaged second protocol of the Budapest Convention, including: coherence and compatibility with EU constitutional framework underpinning judicial and police cooperation and data transfers; variable geometry and practical application within the EU and across the Atlantic.

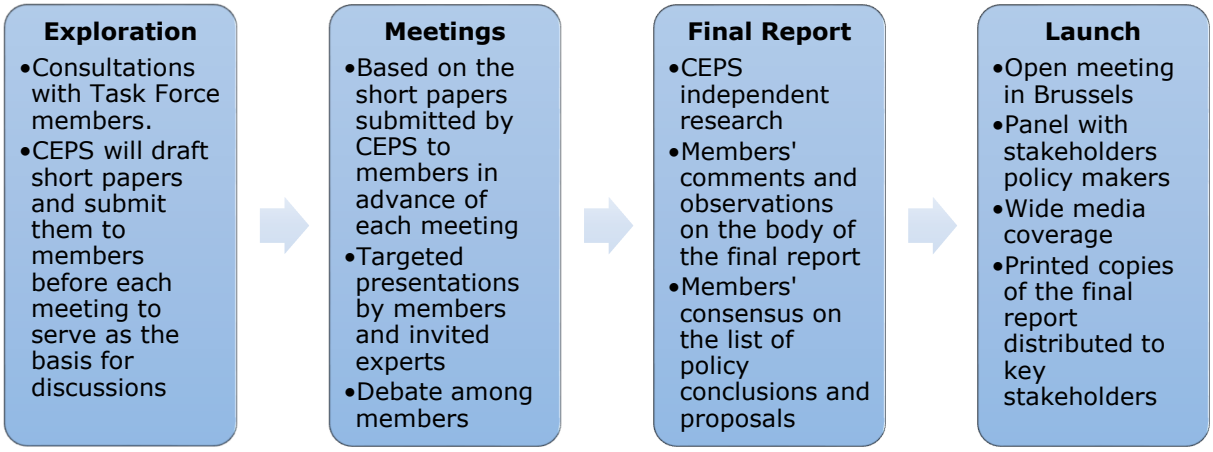
TARGET GROUPS & INTENDED STAKEHOLDERS

The Task Force will benefit from the participation of different communities of experts and practitioners. This Task Force is in particular intended for the following stakeholders:

- ✓ **Private sector** (e.g. Cloud and IT Service providers, Telecoms)
- ✓ **Legal practitioners** (Judges, Prosecutors, criminal and data protection lawyers)
- ✓ **Civil society organisations** (e.g. NGOs, professional associations)
- ✓ **EU bodies and national agencies** (e.g. data protection authorities, fundamental rights agencies, etc.)
- ✓ **International organisations** (e.g. UN representatives and CoE officials);
- ✓ **Experts from academia** (experts in criminal law, international law, privacy and data protection, international human rights)

Each meeting will count on the participation of the Task Force Members (core group), as well as on punctual interventions by key experts identified by the co-rapporteurs to address the different topics covered. The key experts will act as speakers during each meeting. Key experts/speakers might be asked to develop short notes to be presented during the Task Force meetings.

CEPS Task Forces usually benefit from the participation of representatives of national and international policymaking bodies as «observers». Few selected invitees will be also invited as keynotes.



PRINCIPLES & GUIDELINES

Task Forces are processes of structured dialogue among industry representatives, policymakers, consumers and NGOs, who are brought together over several meetings. Task Force reports are the final output of the research carried out independently by CEPS in the context of the Task Force.

Participants in a Task Force

- ✓ Rapporteurs are CEPS researchers who organise the Task Force, conduct the research independently and draft the final report.
- ✓ Chair is an expert appointed by CEPS to steer the dialogue during the meetings and advise as to the general conduct of the activities of the Task Force.
- ✓ Members are for-profit entities, membership organisations or NGOs which participate in a Task Force and contribute to its expenses by paying a fee.
- ✓ Observers are any policymakers or stakeholders who are invited to attend the Task Force meetings and provide oral and written input.

Objectives of a Task Force report

- ✓ Task Force reports are meant to contribute to policy debates by presenting a balanced set of arguments, based on the members' views, available data and literature.
- ✓ Reports seek to provide readers with a constructive basis for discussion. Conversely, they do not seek to advance a single position or misrepresent the complexity of any subject matter.
- ✓ Task Force reports also fulfil an educational purpose, and are therefore drafted in a manner that is easy to understand, without jargon, and with any technical terminology fully defined.

The role of the Task Force members

- ✓ Member contributions may take the form of participation in informal debate or a formal presentation in the course of the meetings, or a written submission.
- ✓ Input from members is encouraged and will be made available to all members, if it is to be used for the final report.
- ✓ Members represent their institutions but are asked to provide input as experts.
- ✓ Members are given ample opportunity to review the Task Force report before it is published, as detailed below.

Drafting of conclusions and recommendations

- ✓ Task Force reports feature a set of conclusions. To draft these conclusions, rapporteurs will summarise members' views.
- ✓ Wherever members' views do not lead to clear conclusions, general phrasing will be employed.
- ✓ Task Force reports feature a set of policy recommendations. These recommendations are meant to reflect members' views. - For a recommendation to be featured in the report, there needs to be 'consensus' or 'broad agreement' among Task Force members.

- ✓ Consensus does not however mean unanimity or full agreement as to every aspect of a given recommendation. - Where ‘consensus’ co-exists with a significant minority view, the report will feature this minority view next to the relevant recommendation.
- ✓ Where there is no ‘consensus’ but several contradictory views, the report will feature all these views and either refrain from making any recommendation or simply advise policymakers to clarify the given subject matter. - In all cases, the report will seek to identify the points where there is some form of agreement, for instance a common understanding of facts or opinions.
- ✓ Both conclusions and policy recommendations will be summarised at the beginning of the report in the form of an ‘executive summary’.
- ✓ Members will be given ample opportunity to review the text of both conclusions and recommendations.