

# **EVIDENCE2e-CODEX**

## **Newsletter #2**

### **May 2018 – August 2018**

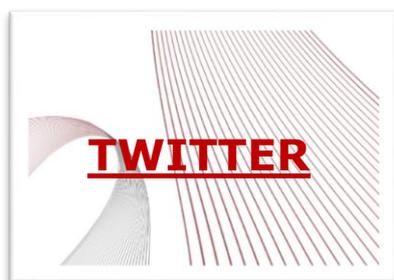
*The second project quarter brought us hard work and new ideas on several fronts: legal issues, technical developments and stakeholder engagement...*

*Meanwhile we are active online! If you are reading this, you already have accessed our website - [www.evidence2e-codex.eu](http://www.evidence2e-codex.eu); but do you know we are also on [Twitter](#) and [LinkedIn](#)? Follow us, join us, and contribute to our work!*

*Have a great summer!*

*Dr. Maria Angela Biasiotti, CNR-ITTIG, Italy*

*EVIDENCE2e-CODEX Project Coordinator*



## In this issue

## Updates

Stakeholder Mapping

Project technical developments

Project legal issues

Most recent project developments

Upcoming events

**Get in contact**

[office@evidence2e-codex.eu](mailto:office@evidence2e-codex.eu)



## EVIDENCE2e-CODEX legal issues

**Electronic evidence** as such is no longer only relating to cybercrime but to almost all areas of criminal activities; terrorists organize their attack by talking on social networks and by chatting online or via instant messaging systems. Taking these developments into account the European Union needs to develop better means to exchange information and evidence relating to crimes in a swift and secure manner – from one country to another, to a law enforcement agency (LEA), to a public prosecutor, etc.; in order to combat crimes in cross-border dimensions. The exchange becomes crucial in counterterrorism operations and in the fight against global crimes.

At the same time, **a secure and trusted exchange of information and electronic evidence** in criminal cases is the “key element” towards promoting judicial cooperation in criminal matters and contributing to an effective and coherent application of EU **European Investigation Order (EIO)** and **Mutual Legal Assistance (MLA)** procedures. This is the only way to achieve a common European area of justice and to ensure **cross-border cooperation** between Member States and/or with third countries in the field of **criminal investigations**.

Tackling new crimes, such as terrorism and organized crimes, including cybercrime, can be greatly improved by enabling efficient, secure and trusted exchange of qualified information and electronic evidence among public prosecutors and LEAs of different Member States, by adopting a **standardized language** and **standardized procedures** in a cross-border dimension fostering the **cooperation in criminal matters**.

Two EU **legal frameworks** need to be considered when thinking about actions enhancing judicial cooperation in criminal fields: the already existing MLA procedures and the new frontier of the EIO.

Mutual legal assistance consists of “cooperation between different countries for the purpose of gathering and exchanging information, and requesting and providing assistance in obtaining evidence located in one country to assist in criminal investigations or proceedings in another”. In other words, mutual legal assistance procedures have been designed specifically for gathering and exchanging of evidence; however, in criminal matters there are no universal instruments governing this cooperation. Moreover, MLA procedures have not been adapted to the realities of today’s crimes which are increasingly global and complex and heavily impact the potential for rapid and efficient transfers of potential electronic evidence. In June 2016, ministers of the JHA Council recommended that mutual



legal assistance procedures be streamlined, in particular with a view to exchanging electronic evidence.

Similar issues are to be considered also with respect to the European Investigation Order. Based on the flexibility of the traditional system of mutual legal assistance, the EIO is a judicial decision which has been issued or validated by a judicial authority of a Member State ("the issuing State") to have one or several specific investigative measure(-s) carried out in another Member State ("the executing State") to obtain evidence. The EIO may also be issued for obtaining evidence that is already in the possession of the competent authorities of the executing State. The transmission of the EIO, from the issuing authority to the executing authority, is carried out "by any means capable of producing a written record under conditions allowing the executing State to establish authenticity". As for the transfer of evidence, "the executing authority shall, without undue delay, transfer the evidence obtained or already in the possession of the competent authorities of the executing State as a result of the execution of the EIO to the issuing State". No reference to particular procedures or specific means is pointed out.

With respect to the above, EVIDENCE2e-CODEX seeks to:

- investigate how the European Investigation Order Directive is transposed and implemented in national legislation in selected EU Member States;
- analyse which (legal and/or operational) measures are required to establish successful execution of European Investigation Order between Member States;
- analyse how EIO and mutual legal assistance procedures (especially in the context of requests for evidence from third countries) interact;
- identify which legal and/or operational measures need to be put in place to further improve requests for electronic evidence using MLA procedures;
- examine how data protection implications in EIO and MLA procedures are being handled and to identify legal and/or operation measures that need to be put in place to ensure respect to data protection rights; and
- identify best practices that are in place in the Member States participating in the project.

In June 2018 EVIDENCE2e-CODEX, together with EXEC Project, [launched](#) a survey to collect and analyse information on the current practices related to electronic evidence and the use of the European Investigation Order. The survey results will be published by the end of 2018.



## Matching EVIDENCE into e-CODEX

The effectiveness of EIO and MLA procedures greatly rely on the implementation of a secure and trusted way of exchanging electronic evidences among the authorities involved. Therefore, the fundamental need addressed by this EVIDENCE2e-CODEX project is to increase, facilitate and support the cooperation in criminal matters in the EU context by fostering the exchange of information and electronic evidence in the specific contexts of EIO and MLA.

[e-CODEX](#) has already established a proven digital infrastructure that supports the exchange of data between legal authorities for many cross border legal procedures in civil and criminal law. However, for the purposes of EVIDENCE2e-CODEX further support in MLA/EIO procedures is especially relevant.

In response to the outlined needs the EVIDENCE2e-CODEX Project aims at initiating the implementation of a common European framework for the correct and harmonized handling of electronic evidence during its entire lifecycle: collection, preservation, use and – in particular – exchange of electronic evidence. Therefore, the EVIDENCE2e-CODEX team will pilot the achievements of the [EVIDENCE](#) in a real life criminal justice use case to verify the developed exchange scenario and pave the way for the electronic evidence exchange in EU Member States.

A '**true to life**' example is considered a substantial step in the modernization of **cross-border cooperation** in criminal law. It will allow the EVIDENCE2e-CODEX team to assess which are the **conditions, criteria** and **necessary impact measures** to be implemented from a **legal, technological** and **sociological** perspective towards connecting judges, prosecutors, LEA officers and other stakeholders to the e-CODEX infrastructure in a **user-friendly manner**. The foreseen actions will foster the harmonization of the framework and improve stakeholder awareness about the treatment and exchange of electronic evidence in EIO and MLA. Specific emphasis will be laid on the relationship and approach to be adopted when dealing with Internet service providers.

Special attention is also envisaged on handling large size files. Digital evidence can be of all sorts with shared characteristic of larger size than 'normal' text files. Established judicial practice refer to mainly text-based situations while expectations are that video, audio and multimedia will become more and more important in near future. As size does matter in the context of digital evidence and the IT infrastructure of e-CODEX and the Member States the outcomes of the



research meet the needs of the judiciary in establishing new practices in handling evidence.

The EVIDENCE2e-CODEX Project will pave the way towards an interconnected system without multiplying the systems and e-forms that are already in use. The project's objectives match the requirements identified during the November 2016 Expert Meeting, i.e. that e-CODEX should be a system for secure transmission of requests allowing also, to the extent possible, the transmission of e-evidence. The 'learning by doing' approach will be an added value for both EU institutions and Member States as the project's results will be developed and validated together with stakeholders and will contribute to establishing a reciprocal trust among them. The EVIDENCE2e-CODEX application will be designed bottom-up, starting from the specific context of electronic evidence exchange.

The implementation of the Evidence Exchange Standard Package Application has already began and several meetings have been organized to further explore specifics and technical issues:

- < 06 March 2018, [EVIDENCE2e-CODEX 'Synergies with INTLI International Exchange of Evidence' Seminar](#)
- < 08-09 March 2018, [EVIDENCE2e-CODEX @ EXEC Kick-off Meeting](#)
- < 10 April 2018, [WP3 First Technical Meeting in The Hague](#)
- < 31 May 2018, [WP3 Second Technical Meeting in Florence](#)
- < 29 June 2018, [EVIDENCE2e-CODEX @ EXEC Second Consortium Meeting, Vienna](#)

## EVIDENCE2e-CODEX stakeholder mapping

EVIDENCE2e-CODEX [Work Package 4 'Stakeholder Engagement, Mutual learning and Capacity Building for Professionals, Policy Makers and Technicians'](#) is dedicated to providing stakeholders with 'ready for use' information on EIO, electronic evidence and EVIDENCE2e-CODEX most recent developments and innovations.

EVIDENCE2-eCODEX will increase awareness towards solutions aimed at furthering the exchange of electronic evidence in EIO and MLA context and extending this implementation to a Member State level. All stakeholders involved will be thoroughly informed and trained to **understand, accept and further promote** electronic evidence exchange. To achieve that, the project activities also cover



**legal, political, technical, ethical and social aspects, LEA-related actions and professionalization** in the field of digital forensic.

The **awareness campaign** alongside an **open dialogue** with stakeholders and the realization of a concrete 'true to life' example will allow the EVIDENCE2e-CODEX team to assess and develop a '**tailor-made methodology**' for extending the secure electronic evidence exchange to all Member States.

The first step towards achieving these goals includes the **identification and mapping of stakeholders** involved in the electronic evidence field. The task leader developed the initial typology of stakeholders and now rely on the kind contribution of all project partners to further enrich the list of specific organizations or individuals considered particularly relevant to be involved in EVIDENCE2e-CODEX workshops and/or in other project initiatives. The review results will be published in the autumn of 2018. Stay tuned!

## Most recent project developments

Hard work within all project streams during second project quarter resulted in:

- < [WP3 Second Technical Meeting in Florence](#)
- < [Mapping the Stakeholders Engaged with Electronic Evidence](#)
- < [Joint EVIDENCE2e-CODEX and EXEC Projects' Survey](#)
- < [EVIDENCE2e-CODEX in Social Media](#)

The second consortium meeting of EVIDENCE2e-CODEX was held in Vienna, Austria, on 28 June 2018. Project partners discussed the current state of project implementation and the challenges to be overcome within the next couple of months under each work package. Special sessions were dedicated to project public events and liaising with other projects working in the field.



Guests to the meetings were members of the Electronic Xchange of e-Evidences with e-CODEX (EXEC) and representatives of EC, DG Justice and Consumers.

Key partners of the EVIDENCE2e-CODEX Consortium took part in the [second consortium meeting](#) of the „Electronic Xchange of e-Evidences with e-CODEX“ Project (EXEC) to ensure the synchronization of communication and organizational activities and the quality of the common activities between EXEC and EVIDENCE2e-CODEX. A special session was dedicated to the projects' joint questionnaire on the implementation of Directive 2014/41/EU.

---

In July 2018, [„Handling and Exchanging Electronic Evidence Across Europe“](#) (Biasiotti, M.A., Mifsud Bonnici, J.P., Cannataci, J., Turchi, F. (eds.)) was published by Springer. The volume offers a general overview on the handling and regulating electronic evidence in Europe, presenting a standard for the exchange process. Chapters explore the nature of electronic evidence and readers will learn of the challenges involved in upholding the necessary standards and maintaining the integrity of information. Challenges particularly occur when European Union member states collaborate and evidence is exchanged, as may be the case when solving a cybercrime. One such challenge is that the variety of possible evidences is so wide that potentially anything may become the evidence of a crime. Moreover, the introduction and the extensive use of information and communications technology has generated new forms of crimes or new ways of perpetrating them, as well as a new type of evidence.



Contributing authors examine the legal framework in place in various EU member states when dealing with electronic evidence, with prominence given to data protection and privacy issues. Readers may learn about the state of the art tools and standards utilized for treating and exchanging evidence, and existing platforms and environments run by different Law Enforcement Agencies (LEAs) at local and central level. Readers will also discover the operational point of view of LEAs when dealing with electronic evidence, and their requirements and expectations for the future.

Finally, readers may consider a proposal for realizing a unique legal framework for governing in a uniform and aligned way the treatment and cross border exchange of electronic evidence in Europe. The use, collection and exchange of electronic evidence in the European Union context and the rules, practices, operational



guidelines, standards and tools utilized by LEAs, judges, public prosecutors and other relevant stakeholders are all covered in this comprehensive work. It will appeal to researchers in both law and computer science, as well as those with an interest in privacy, digital forensics, electronic evidence, legal frameworks and law enforcement.

The book represent the story behind EVIDENCE2e-CODEX and current developments of implementation of a common European framework for the correct and harmonized handling of electronic evidence during its entire life-cycle within the project.

---

The 2018 edition of the Octopus Conference - 'Octopus 2018: Cooperation against Cybercrime' also took place in July 2018 The conference focused on evidence in cyberspace covering the following topics: (a) evidence in cyberspace - multi-stakeholder consultation on the Protocol to the Budapest Convention; (b) global state of cybercrime legislation and the progress during 2013–2018; (c) jurisdiction in cyberspace; (d) capacity building on cybercrime and e-evidence; (e) WHOIS; and (f) the current challenges and responses in cyberviolence.

The Octopus Conference is part of the Cybercrime@Octopus project which is currently funded by voluntary contributions from Estonia, Hungary, Japan, Monaco, Romania, Slovakia, United Kingdom, USA and Microsoft as well as the budget of the Council of Europe.

The Octopus Conference is preceded by the plenary of the Cybercrime Convention Committee (T-CY) on 9-11 July 2018.

More information about the event can be found [here](#).

## Upcoming events

The next six months of the project will bring us:

- < [Workshop on the Formal Language for Evidence Exchange Representation](#)
- < [Interim Workshop on Evidence Exchange Standard Package Application](#)
- < [EVIDENCE2e-CODEX: Meeting the Legal Community](#)

Stay tuned!

