e-Evidence: Collection, Analysis, and Sharing

An evidence-based policy perspective by the EU funded research projects LOCARD, ROXANNE & FORMOBILE

Meet the authors

Denitsa Kozhuharova,
Head of Human Rights Department,
Law and Internet Foundation

Denitsa has more than 5-year professional experience in the area of fundamental rights and electronic governance as a researcher and consultant. On behalf of Law and Internet Foundation, Denitsa has participated in research projects in her capacity of ethics and legal researcher focusing predominantly on data protection and privacy issues. Her work there also includes the analysis of fundamental rights and their appropriate consideration in data-driven technological solutions. Denitsa is also involved in the implementation of action grants in the field of personal data protection (manner of interpretation and application by different state actors) and criminal procedure rights (perpetrators, and victims' rights during the pre-trial stage of the criminal procedure).

Joshua Hughes, Senior Research Analyst, TRILATERAL RESEARCH

Josh has a research background in security, conflict, policing, forensic science, technology, international relations, and international law. At Trilateral, he has worked on integrated ethical, societal, and legal impact assessments, implementing Ethics-by-Design and Privacy-by-Design approaches to technologies and organisations, and leads the development of Trilateral's human rights impact assessment and Human-Rights-by-Design approach. Josh leads Trilateral's contributions to the ROXANNE and INSPECTr projects, oversees Trilateral's work on the HEROES project, and has also contributed to the PREVISION project.

Ashwinee Kumar, Researcher, "Law, Science, Technology and Society" research group of Vrije University Brussels

His research focuses on the interplay between Blockchain Technology and the data protection law, particularly privacy impact assessments. He has been associated with the EU-Funded projects like ALADIN (Advance hoListic Adverse Drone Detection, Identification, and Neutralization) and ARC (Awareness Raising Campaign for SMEs about GDPR). His contribution with Prof. Paul De Hert is now a book chapter "Blockchain, Privacy, and Data Protection" in Edward Elgar's publication "Blockchain and Public Law: Global Challenges in the Era of Decentralisation". His research interest includes data protection and privacy, ICT laws, Legal Informatics, Comparative Constitutionalism, Human Rights, EU Law, and Legal Philosophy.

LOCARD

ROXANNE

FORMOBILE

• FROM MOBILE PHONES TO COURT •

Meet the projects

This presentation notes policy observations and recommendations on the basis of the research findings of legal and ethical nature performed by the teams of three EU-funded projects, namely LOCARD, ROXANNE, and FORMOBILE

Lawful evidence cOllecting & Continuity plAtfoRm Development (LOCARD Project)

- LOCARD aims to provide a holistic platform for chain of custody assurance along with the forensic workflow, a trusted distributed platform allowing the storage of digital evidence metadata on a blockchain. Each node of LOCARD will be able to independently set its own permission policies and to selectively share access to digital evidence with other nodes when deemed necessary and upon proper authorization through fine-grained policies. LOCARD's modularity will also allow diverse actors to tailor the platform to their specific needs and role in the digital forensic workflow, from preparation and readiness, to collection, analysis, and reporting.
- LOCARD will have a crowdsource module to collect citizen reports of selected violations, a crawler to detect and correlate online deviant behaviour, and a toolkit for investigators that will assist them in collecting online and offline evidence. This will be powered by an immutable storage and an identity management system that will protect privacy and handle access to evidence data using a Trusted Execution Environment. Blockchain technology will not only guarantee that information about the evidence cannot be tampered with but allow interoperability without the need for a trusted third party.

Real time network, text, and speaker analytics for combating organized crime (ROXANNE Project)

- ROXANNE aims to unmask criminal networks and their members as well as to reveal the true identity of perpetrators by combining the capabilities of speech/language technologies and visual analysis with network analysis.
- ROXANNE collaborates with Law Enforcement Agencies (LEAs), industry and researchers to develop new tools to speed up investigative processes and support LEA decision-making. The end-product will be an advanced technical platform that uses new tools to uncover and track organized criminal networks, underpinned by a strong legal framework.
- The project consortium comprises 25 European organisations from 16 countries while 11 of them are LEAs from 10 different countries.

ROXANNE

From Mobile Phones to Court (FORMOBILE Project)

- FORMOBILE aims at developing a complete forensic investigation chain, targeting mobile devices. A result of the project should be a holistic view of all areas of mobile forensics, including fundamental rights, allowing continued research on the complete investigation chain.
- The project has been divided into 10 Work Packages that reflect the analysis chain used by security practitioners that examine mobile evidence.
- The forensic investigation chain is broken into three steps: acquisition, decoding and analysis of data.

FORMOBILE
· FROM MOBILE PHONES TO COURT ·

e-Evidence and Data Collection: The role of the right to privacy and data protection

Current legal framework regulating collection of e-Evidence data (Law Enforcement Directive, rights to privacy and data protection)

- The current legal framework for processing of personal data by Law Enforcement Agencies (LEAs) in the EU during their work investigating and preventing crime is primarily developed through the domestic implementation of the legal regime created in the Law Enforcement Directive 680/2016 (LED) and rights to privacy and data protection, which are informed by Convention 108+.
- The LED applies to 'Competent Authorities' that can be the data controllers under this regime. In the context of e-Evidence collection, this would be LEAs who gather data during investigations, or are otherwise provided with data about (suspected) criminality.
- A key part of data protection, for data collection in LEAs' investigations is the requirement for a controller to have a legal basis for the processing of personal data. Under the LED, this can be for the 'purposes of the prevention, investigation, detection … of criminal offences.'
- The processing of personal data by LEAs can be considered sensitive, especially when biometric data is processed.
- LEAs should differentiate offences, depending on the nature & seriousness of a crime; for example, sensitive personal data collected during the investigation of petty offences should not be held for long as it is done for the investigation of serious criminal offences. The controllers (LEAs in this case) need to take great care to ensure the protection of personal data while collecting e-Evidence during operations.

How will the proposed e-Evidence regulation change the status quo?

- The main premise of the e-Evidence proposal allows one authority to request another authority to either preserve or produce data. When a production order is issued, the authority receiving the request 'shall ensure that the requested data is transmitted directly' to the requesting authority. Where a preservation order is issued, the authority receiving the request shall 'preserve the data requested' for up to 60 days. This specific requirement for receiving authorities to act in a particular way is different from other forms of international police cooperation and data sharing, where requesting and receiving authorities are often asked to 'co-operate'.
- It would therefore seem that a requesting authority would be deciding the **purpose of the processing** as the receiving authority would only be processing the data to provide or preserve it for the requesting authority. Where an entity decides on the purpose, they are seen as the de facto data controller as decisions on means of processing can often be left to a data processor. As such, requesting authorities would seem to be a data controller over the data that they request to be produced or preserved. However, the receiving authority must consider if they can respond to the request, and whom they can share the data with. It is arguable that a receiving authority could be seen as a data processor, but a controllership role seems more appropriate. Thus, both authorities should be considered as joint controllers, meaning that a joint controller agreement should be made under Article 21 of the LED.
- The drafters of the e-Evidence proposal should consider whether a more practical solution needs to be developed, and whether it could be incorporated into the proposal itself. The most obvious solution would be to develop a standard joint controller agreement for competent authorities to apply automatically when a production/preservation order is being fulfilled.

What lessons from ROXANNE could inform the development of the proposed e-Evidence regulation?

- In ROXANNE, the project developed a decision-support tool that asks specific questions of end-users to ensure that they critically engage with the outputs/results of the analytic technologies. A similar approach could be used with responding to production/preservation orders. For example, an LEA officer dealing with incoming orders could ask themselves, amongst other things, whether the order would infringe upon the privacy of the data-subject and whether that is necessary and proportionate in the circumstances of the case being investigated. Developing a series of questions for such persons to answer would seem to facilitate critical engagement with the nature and purpose of the production/preservation orders and what response would be most appropriate.
- Considering the amount of detail provided on production certificates, it would seem logical that details of an investigation could be included on the certificates so that a receiving authority could carry out an assessment of what data is '**adequate, relevant and not excessive**' for the purpose of meeting a production order, especially if the data has been incidentally collected. Due to the potentially large amounts of data that might need to be considered, it is important that a receiving authority has sufficient opportunity to consider whether it would be proportionate to share the requested data as it is, or if it could be minimised.
- The **ROXANNE technologies** can assist in scoping what data might be relevant to an investigation, and a response to a production/preservation order. Where data-analysis tools show that some data is not relevant, then that file might not need to be examined. Having knowledge about what data is relevant to an investigation or to a production/preservation order will allow a receiving authority to quickly assess what data could be provided to the requesting authority.

e-Evidence in Data Analysis and Processing: The role of the right to privacy and data protection

Status Quo: How the pertinent legal regime outlined by the LED is shaping the way e-Evidence is analysed? (1)

- The ECtHR has reiterated consistently in its case law practice that the right to privacy is not absolute, yet going beyond the reasonable intrusion presents a violation of Art. 8 of the European Convention of Human Rights (ECHR). The EU has gone a step further to harmonise existing practices and set minimum standards across the members states when it comes to personal data processing in criminal matter.
- Analysis of e-Evidence is an investigative step which takes places after collection, usually under the scope of the pre-trial criminal proceedings. From data protection point of view, several considerations should be acknowledged:
  - ➢ Analysis of e-evidence might be carried out by different types of actors: experts stationed within the police or the prosecution, by dedicated public bodies charged with forensics' performance or by a private body specifically entrusted to exercise public authority for the investigation of criminal offences. The LED applies to all of them.
  - ➢ It is important to reflect who is the originator of the data which is being analysed. The LED clearly calls competent authorities to differentiate the approach depending on the category of the data subject. In the case of e-Evidence analysis, the main categories of data subjects which would entail differentiation of the approach are the suspect/ accused, the witness, and the victim. In case of the analysis of personal data belonging to the suspect/ accused, an assessment to which degree the intrusion of privacy is justified must always be made. The same is also valid for witnesses – when analysing e-Evidence a fair balance should be sought between the interest of the investigation and the private sphere of the individual. When information pertaining to victims is being analysed it should always be considered that preserving the confidentiality of their identity might be vital, and in general they enjoy a higher degree of privacy.

Status Quo: How the pertinent legal regime outlined by the LED is shaping the way e-Evidence is analysed? (2)

- ➢ Attention should be paid also in case the data, subject to analysis, is generated by one and more users, and whether they effectively belong to different categories of data subjects e.g., it might be the case that the data, subject to analysis, is jointly produced by the suspect and the victim. Therefore, it should be born in mind that the mere analysis of e-evidence might infringe the rights of third parties (not related in any way with the investigation). Thus, the fair balance between finding hidden data concerning a suspect/ accused and respecting data privacy is equally as important as difficult to strike.
- ➢ Another major consideration pertains to the nature of the content of the data that is undergoing analysis. On the one hand, the provision of Art. 7 (1) LED needs to be observed, namely that the competent authority, in this case the e-evidence analyst, it is required that a distinction is made between data based on facts and data based on opinions. On the other hand, it should be examined whether the analysis of data might infringe fundamental rights such as the right to remain silent or it is protected by legal privileged e.g., the analysed data constitutes communication between the suspect/ accused and their lawyer.
- ➢ Last but not least the principles of necessity and proportionality should be observed in the course of e-evidence analysis. In the case of e-evidence analysis, the principle of necessity should be understood in the meaning of demonstrating a necessity to interfere with the private life of the individual concerned. This entails the performance of the test, whether the processing satisfies the following criteria pursuant Art. 8 of the European Convention of Human Rights (ECHR):
  - ✓ accordance with the law,
  - ✓ in pursuit of one of the legitimate aims, namely national security, public safety or the economic well-being of the country, for the prevention or detection of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others, and
  - ✓ it is necessary in a democratic society.

As for the proportionality criteria, in this context, it is to be interpreted in the spirit of the ECtHR as that the processing "should go no further than needed to fulfil the legitimate aim being pursued".

Ethical concerns pertinent to e-Evidence Analysis

- In addition to the challenges related to the practical implementation of the LED by the EU member states met by legal experts in the context of e-evidence analysis, existing ethical concerns further exacerbate the complexities of the issue. The central ethics conundrum is related to the probative value of e-evidence.
- Reiterating the findings from other research, the FORMOBILE Study showed that mobile evidence is almost never scrutinised neither by the court nor the defence. Its objectiveness and authenticity are always presumed, relying entirely on the conclusion of the forensic examiner.
- However, a recent case from Denmark (the so-called Danish cases) rings the alarm that even the most sophisticated methods for evidence analysis should be questioned and respectively duly justified in front of a court of law. The Danish cases refer to an identified error in the police IT system in 2019 by the Danish Director of Public Prosecutions. As a result, more than 10,000 criminal cases from the period 2010-2019 are undergoing review to determine the consequences resulting from admitting evidence which may have been impacted by errors and uncertainties. This case illustrates a potential weakness of evidence produced by mobile forensics, namely that it might be inaccurate or event faulty.

Sharing of digital evidence within member states: Up to what extent can Blockchain driven platform afford flexibility to it

Data protection in LOCARD

- It is believed that Blockchain technology, because of its inherent characteristics of immutability and design, can be detrimental to certain rights of the data subject like the right to rectification and erasure or transfer of personal data from the existing platform to another where there is uncertainty about the availability of the blockchain-like platform. However, data stored on the LOCARD blockchain are only hashes coming from combinations of data, namely evidence files, metadata strings, and so on, thus, the issue of immutability is minimised. Moreover, the LOCARD platform uses hashes over a combination of data and never over a single datum, which ultimately leads to complexity and prevents the use of hashes as a pseudonymization tool. As far as rectification and deletion of personal data are concerned, the data is stored on the LOCARD database, which allows flexibility to the users to modify the incorrect information or to delete it completely.
- Furthermore, towards compliance with the ‘data minimisation’ and ‘purpose limitation’ principles, the LOCARD system provides better transparency to the LEAs by uniquely identifying every single piece of digital evidence that can be regularly checked and audited.
- This motivates LEAs to store only the information that is strictly required for investigation purposes. The LOCARD system enables the flow of transferring evidence. The evidence will appear as transferred in the system if required for the investigation purposes, despite the other endpoint does not have a LOCARD-like system. Further materials can be manually uploaded to complement the investigation and guarantee the full chain of custody, e.g., a signed file related to the proper transfer of the case or evidence to another end user.

Threat to data protection in sharing digital evidence

- Even though cybercrimes are extraterritorial in nature, the principle of accountability and proportionality are common within the member states. However, legal requirements behind digital evidence collection and its admissibility in a court may vary from state to state.
- The Commission holds cybercrime as a borderless issue and classifies it as crimes specific to the Internet, online fraud and forgery, and illegal online content.

The Challenges in sharing of digital evidence

- Admissibility of a piece of digital evidence in the court of another member state could be a challenge, especially when the trial court works in a language different than that of the evidence itself. The evidence can also be opposed on the ground of its collection if the way used to gather the evidence does not fulfill all the standards of the laws of the trial court. Additionally, different member states can have different levels of ethical and administrative standards for collecting evidence. It may be a further cause to dispute the admissibility of a particular piece of digital evidence that fulfills the domestic requirement in its gathering.
- Although many cooperative steps are being taken at the Union level, due to the highly jurisdictional-centric nature of the courts, admissibility of a piece of digital evidence can easily be opposed on those grounds. Once discarded of being accepted as valid evidence, the inadmissibility would bring many legal dilemmas in the future for that piece of digital evidence e.g., regarding the persuasive value of both the judgement and the inadmissible evidence itself.
- However, the LOCARD system cannot add fuel to the fire as it does not provide simultaneous translation of the digital evidence while sharing it to a different jurisdiction. It would be upon the LEAs to upload the verified translation copy of the evidence on the blockchain.

Thank you

Ashwinee Kumar

ashwinee.kumar@vub.be

https://lsts.research.vub.be/en