D6.9 Mobile technologies for LEAs

Lead Beneficiary:	COSMOTE
Dissemination Level:	PU - Public
Date:	30/11/2023
GA Number:	101102641

The TRACY project has received funding from the DIGITAL 2022 programme under grant agreement No 101102641.

Project Information

Grant Agreement Number	101102641
Acronym	TRACY
Name	a big-data analyTics from base-stations Registrations And Cdrs e-evidence sYstem
Topic	DIGITAL-2022-DEPLOY-02-LAW-SECURITY-AI
Free keywords	Digital SME Support Actions
Start Date	01/06/2023
Duration	24 Months
Coordinator	Performance Technologies SA

Document Information

Work Package	WP6: Dissemination, Exploitation and EU Impact
Deliverable	D6.9 Mobile technologies for LEAs
Date	30/11/2023
Type	Report
Dissemination Level	PU - Public
Lead Beneficiary	COSMOTE
Main Author(s)	Konstantinos Filis
Contributors	Eleni Theodoropoulou (COSM), George Lyberopoulos (COSM), Kasia Kostka (Timelex), Manolis Tsangaris, Michaela Antonopoulou, Panagiotis Mertis, Nikos Desipris (PT), Vasiliki Sergianni (HPOL), Petr Motlicek (IDIAP)
Document Reviewers	Nikos Desipris (PT), Manolis Tsangaris (PT), Panagiotis Mertis (PT), Vasiliki Sergianni (HPOL)
Security Reviewer	PT
Ethics Reviewer	(TMX)

Revision History

Version	Date	Author	Comments
0.1	15/11/2023	Konstantinos Filis	Table of Contents and initial structure
0.2	20/11/2023	Konstantinos Filis	First draft
0.3	22/11/2023	Konstantinos Filis	Initial version including material from COSMOTE's presentation
0.4	23/11/2023	Kasia Kostka	Additional input from Timelex
0.5	24/11/2023	Michaela Antonopoulou	Additional input from PT
0.6	27/11/2023	Konstantinos Filis	Additional input from COSM
0.7	29/11/2023	Petr Motlicek	Additional input from IDIAP
1.0	29/11/2023	Konstantinos Filis	Final version

Disclaimer

The contents of this deliverable are the sole responsibility of the author(s) and do not necessarily reflect the opinion of the European Union.

Copyright

Abbreviations

Acronyms and Abbreviations	Meaning
AI	Artificial Intelligence
CDR	Call Detail Records
CSPs	Communications Service Providers
DRD	Data Retention Directive
DSL	Digital Subscriber Line
EC	European Commission
EU	European Union
GCPI	Inspectoratul de Politie Judeatan Galati
HPOL	Hellenic Police
IGP	Inspectoratul General al Politiei
IMEI	International mobile equipment identity
IMSI	International mobile subscriber identity
IoT	Internet of Things
IP	Internet Protocol
ISP	Internet Service Provider
LEA	Law enforcement authority
MNO	Mobile Network Operators
MNT	Mobile Network Topology
MSE	Mobile Signalling Events
MS	Member State
NCD	Non-Content Data
RRC	Radio Resource Control
SMS	Short Message Service
SPOC	Single Point of Contact
TRACY	a big-data analyTics from base-stations Registrations And Cdrs e-evidence sYstem
UE	User Equipment
VoIP	Voice over IP
WP	Work Package

List of Figures

Table of Contents

Executive Summary

Deliverable D6.9 “Mobile technologies for LEAs” comprises the outcome of the first workshop which was organized for and presented to LEAs in the context of the internal dissemination activities of the project. This workshop was the first among the three workshops that are planned to be organized in the context of task T6.1 “Preparation and implementation of the Dissemination, communication and exploitation Plan”. The purpose of the workshop was to offer Law Enforcement Authorities (LEAs) the chance to better understand the basic technologies and procedures of mobile telecommunication networks, as well as the current legal framework in Europe and at national level that defines the data that the Mobile Network Operators (MNOs) are obliged to retain and provide to LEAs.

1 Introduction

TRACY project aims to develop new technological solutions that allow the fast and accurate search for new evidence during criminal investigations, considering new methods of extraction and processing of information from lawfully accessed communications data. TRACY considers specifically non-content data (NCD), as those data are often reported by Law Enforcement Agencies (LEAs) and obtained through electronic Communications Service Providers (CSPs). Such data can offer valuable information in an investigation or for the prosecution of cases of organized crime and terrorism.

One of the main goals of the Project is to prepare and implement dissemination activities. From the beginning of the project, a detailed plan containing the dissemination, communication and exploitation strategy has been prepared and will be updated throughout the duration of the project and will be implemented by all partners. According to this plan, 3 workshops will take place during the Project:

1. Mobile technologies for LEAs
2. Data analytics for LEAs
3. Legal - ethical issues and AI for LEAs and a final conference for LEAs regarding the project results/outcomes by the end of the project.

Deliverable D6.9 presents the outcome of the first workshop which was organized for and presented to LEAs in the context of the dissemination activities of the project. The purpose of the workshop was to offer Law Enforcement Authorities (LEAs) the chance to better understand the basic technologies and procedures of mobile telecommunication networks, as well as the current legal framework in Europe and at national level that defines the data that the Mobile Network Operators (MNOs) are obliged to retain and provide to LEAs. Due to the sensitive nature of its content, this workshop addressed only the project partners.

The Deliverable is divided into four chapters and an Annex. Chapter 1 is the present short introduction to this Deliverable and its contents. Chapter 2 presents the scope of the workshop including its main objectives and expected outcomes, as well as the overall structure of the Workshop. Chapter 4 includes a summary of each partner's presentation, and chapter 5 presents the conclusions and the key takeaway points of the Workshop. Finally, a list of the presentations of the Workshop and links to the relevant folders in the project repository are included in the Annex.

2 Scope and Structure of the Workshop

The 1st Workshop on Mobile Technologies for LEAs took place on 13 November 2023 and it was attended by 25 members of the consortium and an external expert. It was organized in a way that it would include basic albeit useful technical and legal information for LEAs including not only presentations, but also Q&A sessions. The objectives of this Workshop were the following:

- The first one was that partners obtained a common understanding on how the mobile network operates and what are the interactions of the user equipment (UE) with the network and which of them are identifiable by the network.

- Another aim of the Workshop was to describe the current legal framework in Europe and at national level that defines the data that the Mobile Network Operators (MNOs) are obliged to retain or not – to preserve the users' privacy - as well as the information exchanged between LEAs and MNOs.

The Workshop was structured as shown in the agenda of Figure 1, and it started with a short introduction of the TRACY project, which described the objectives and the expected outcomes of the Project.

Next, the basic principles of the operation of mobile communication networks were presented, including information about several mobile network technologies (2G, 3G, 4G, 5G, 6G), as well as procedures that take place when a UE is turned on, connects to a network, and changes its position.

After that, the current legal framework in Europe and in Greece was described that defines the data that the MNOs are obliged to retain and provide to LEAs.

The Workshop also presented the use cases that the TRACY project envisions along with the difficulties the LEAs are facing and the tools that are currently utilized by the LEAs to investigate various crimes and malicious events.

In addition, it was discussed how Artificial Intelligence (AI) can assist LEAs in crime investigation by pinpointing the datasets required, whether there are technical concerns from the MNO's perspective and/or potential legal issues, as well as the framework updates needed for exchanging info between MNOs and LEAs in a new ecosystem based on AI requirements and processes.

On top of the above, during the workshop, other tools and further information that could potentially be exploited by the LEAs were presented and discussed.

The Workshop ended up with a Q&A session aiming at leading in specific conclusions to be utilized in the next steps of the project decisions, developments, and actions.

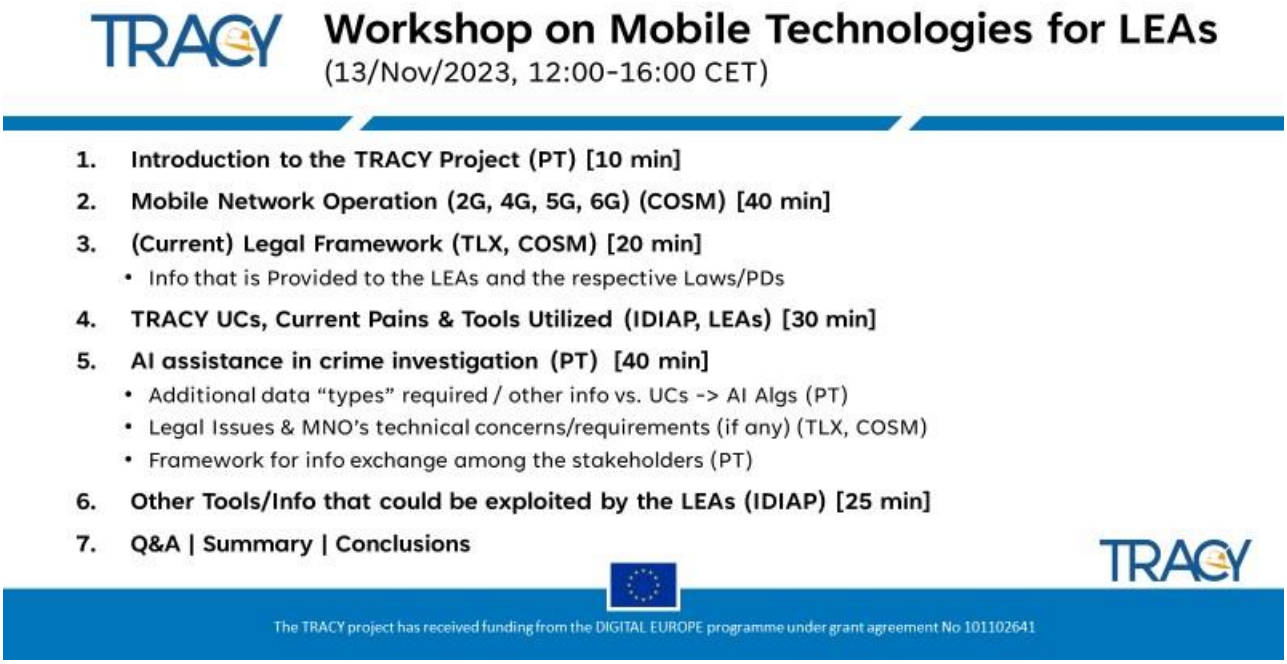

Figure 1: Agenda of the Workshop

Figure 2: Workshop participants

3 Summary of Partner Presentations

3.1 PT - Introduction to the TRACY Project

The Workshop started with an introduction to the TRACY Project providing a comprehensive overview of the HPOL User Story 1 outlined in the latest TRACY's deliverable, D2.1. In this user story, distinct datasets were provided to HPOL by the MNOs, based on hard evidence and after the prosecutor's approval. These datasets were aligned with key locations suspects were seen, like the crime scene, the last known sighting according to eyewitnesses, the discovery site of the stolen motorcycle, and the safehouse. The challenges of this User Story were also mentioned at this point.

Subsequently, the above user story was contextualized within the framework of the TRACY's methodology, showing how the application of TRACY's methodology could reform the LEAs approach. The presentation also referred to the complexity of the Mobile Network by showcasing a video depicting cells serving pedestrians within an area in Athens.

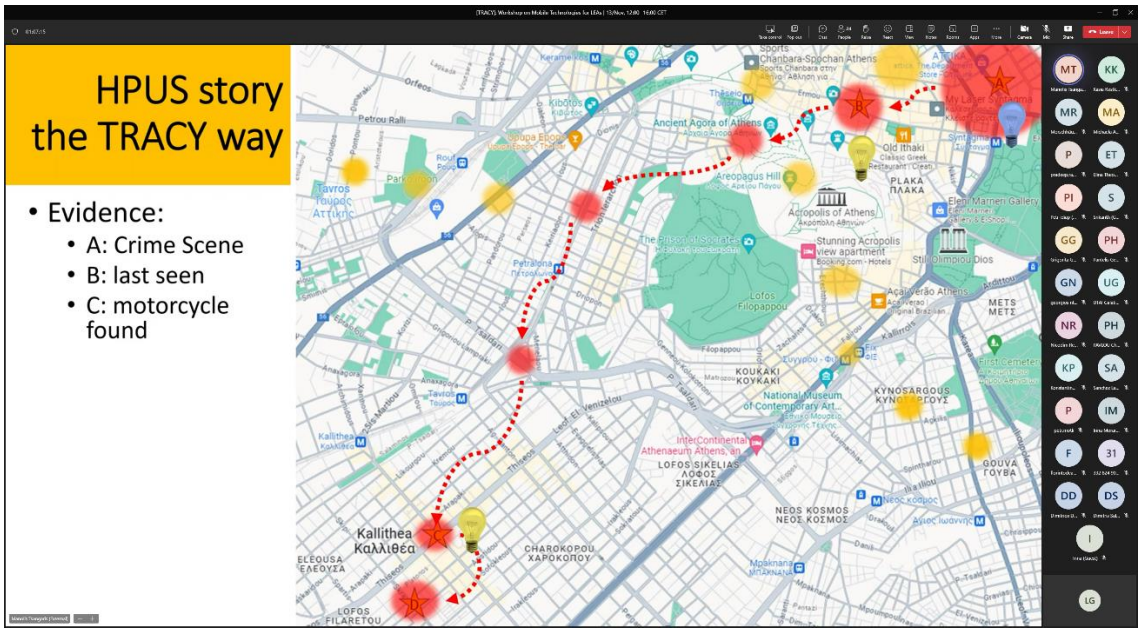

Figure 3: Snapshot from the presentation Introduction to the TRACY Project

Afterwards, the TRACY's appliances were mentioned, with reference to the creation of four platforms: a development platform, a pre-production and a production platform located at the HPOL premises and a Validation/Training platform for the other LEA partners.

The presentation concluded with an overall Status Report on the project. This included an account of deliverables accomplished during the first semester and a roadmap outlining upcoming milestones in the subsequent months. An overview of project progression was

provided, organized by work packages (WPs), semesters, and thematic sections, ensuring a thorough reference to all project steps and deliverables until its culmination.

3.2 COSM – Mobile Network Operation

The purpose of this presentation was to explain to LEAs how mobile communications networks operate, in particular during their interaction with the UEs. The presentation covered the following topics:

- Overview of the Mobile Communications Systems (1G – 6G) evolution
- Basic Principles on UE Interaction with the Network
- Idle Mode - Cell Search/Selection/Reselection, Location Update, Paging
- Connected Mode - Handovers

During the overview of the mobile communications systems a brief description of the major characteristics of each technology (1G, 2G, 3G, 4G, 5G, 6G) was presented highlighting the major advantages and drawbacks of each technology.

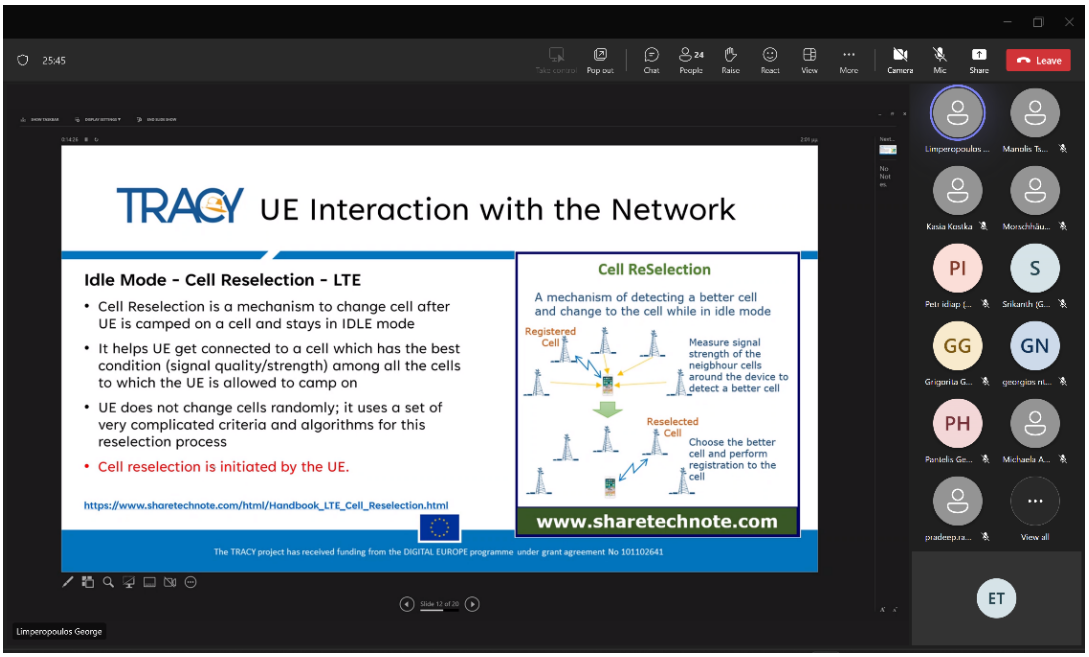

Figure 4: Snapshot from the presentation Mobile Network Operation

Next, the basic principles on the UE interaction with the network were presented, for the case of 4G, which is the dominant technology at the present time, starting with the IDLE mode where the UE has no RRC (Radio Resource Control) connection attached to it. It was explained that in this state the UE can perform a number of UE-initiated activities such as: Cell Measurement (Measure the signal quality of neighboring cells and determine which cell it would camp on to), Cell Selection (Determine a cell and perform registration), Cell Reselection (Change cell if the signal/quality of the current one deteriorates), Tracking Area (TA) Update and Paging

monitoring to detect incoming calls. It was emphasized that in the IDLE mode the UE is not known by the radio network or the base station, therefore we are not able to know its location on a cell level.

Then, the CONNECTED Mode was explained, which enters when the user performs any activity using the UE (web surfing, messaging, calls, etc.). it was emphasized that in the CONNECTED mode the UE is known to the radio network and the location of UE is known at the cell level. It was mentioned that in this mode mobility is UE assisted and network controlled with the UE monitoring control channels associated with shared data channel to determine if there are data scheduled for it or not.

Finally, the handover procedure was explained which takes place when a user moves out of coverage of one cell forcing the UE to change cells to ensure smooth operation and to avoid call drop. It was emphasized that handovers happen only in the case of a connected UE, while the main difference between cell reselection and handover is that cell reselection is a proactive process, while handover is a reactive one. It was also mentioned that during cell reselection, the UE initiates the process itself, while in handover, the network initiates the process in response to a change in the device's location.

3.3 Timelex – Current Legal Framework (EU)

This presentation provided the participants with an introduction to the legal regime surrounding the use of non-content data by LEAs. The agenda included the fundamental rights concerned, the overview of the law in the European Union as well National examples of Romania and Moldova as members of the consortium.

The presentation started with the fundamental rights found in the Charter of Fundamental Rights of the European Union involved in the ongoing discussion on data retention which are:

- The right to the integrity of the person (article 3)
- The right to liberty and security (article 6)
- Respect for private and family life (article 7)
- Protection of personal data (article 8)
- Freedom of expression and information (article 11)

When it comes to the legislative overview, the main pieces of legislation on the European level are:

- Data Retention Directive (DRD) [Directive 2006/22/EC]; although invalidated in 2014, most Member States 'data retention regimes continue to be based on this Regulation,
- General Data Protection Regulation (GDPR) [Regulation (EU) 2018/1725],
- Law Enforcement Directive (LED) [Directive (EU) 2016/680],
- Privacy and Electronic Communications Directive (e-Privacy Directive) [Directive (EU) 2002/658]

The ongoing development and proposed amendments to the European data regime were discussed including the planned update of the e-Privacy Directive and the CJEU decisions.

The use of non-content data in Romania and Moldova were then presented. It has been concluded that both countries have similar regimes, based on the aforementioned Data Retention Directive.

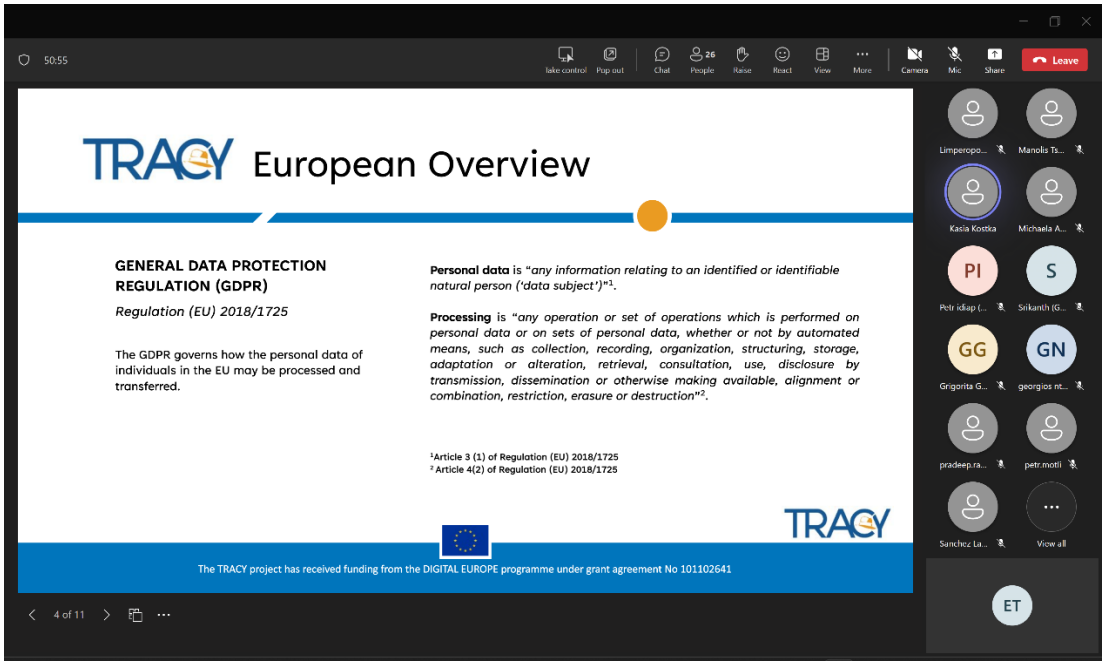

Figure 5: Snapshot from the presentation Current Legal Framework (EU)

In Romania, the collection and the use of non-content data are regulated by Chapter IV of the Criminal Procedure Code. The criminal investigation bodies, with prior authorization, can request traffic and location data if: there is a reasonable suspicion of crimes cases for which the law provides a prison sentence of 5 years or more, there are justified grounds to believe that the requested data constitute evidence, the evidence could not be obtained in any other way or obtaining it would involve special difficulties that would prejudice the investigation or there is a danger for the safety of people or valuable goods, the measure is proportional to the restriction of fundamental rights and freedoms, given the particularities of the case, the importance of the information or evidence to be obtained or the seriousness of the crime.

Similarly in Moldova, as stated in the Electronic Communications Law (Law No. 241), data from electronic communications may be requested by the bodies authorized by law only based on the authorization of the investigating judge to ensure national security and defense, public security, as well as in cases of prevention, investigation, detection and prosecution of serious, particularly serious and exceptionally serious crimes.

3.4 COSM - Current Legal Framework (Greece)

The purpose of this presentation was to describe Non-Content Data (NCD), Call Detail Records (CDRs), the information currently provided to LEAs by MNOs, and the current legal framework in Greece for the information exchange between LEAs and MNOs.

Non-content data (NCD) can be classified into three groups: a) Subscriber data, that include the information enabling identification of the sender of a communication (e.g., name, address, username, phone number), b) traffic data, that include the information necessary to identify the type, date, time and duration of a communication, and c) location data, that include the information necessary to identify the location of the subscriber's communication device (e.g., cell tower / antenna coordinates serving the subscriber).

Next, the meaning of CDR was explained. A CDR is a formatted collection of information about a chargeable telecommunication event (e.g., time of call set-up, duration of the call, amount of data transferred, etc.). CDRs are obtainable from telecom operators only, that are the data owners, and are routinely recorded as part of the normal business operations. For each party to be charged for parts of or all charges of a chargeable event a separate CDR is generated. It was emphasized that CDRs do not contain telephone conversations or messages exchanged.

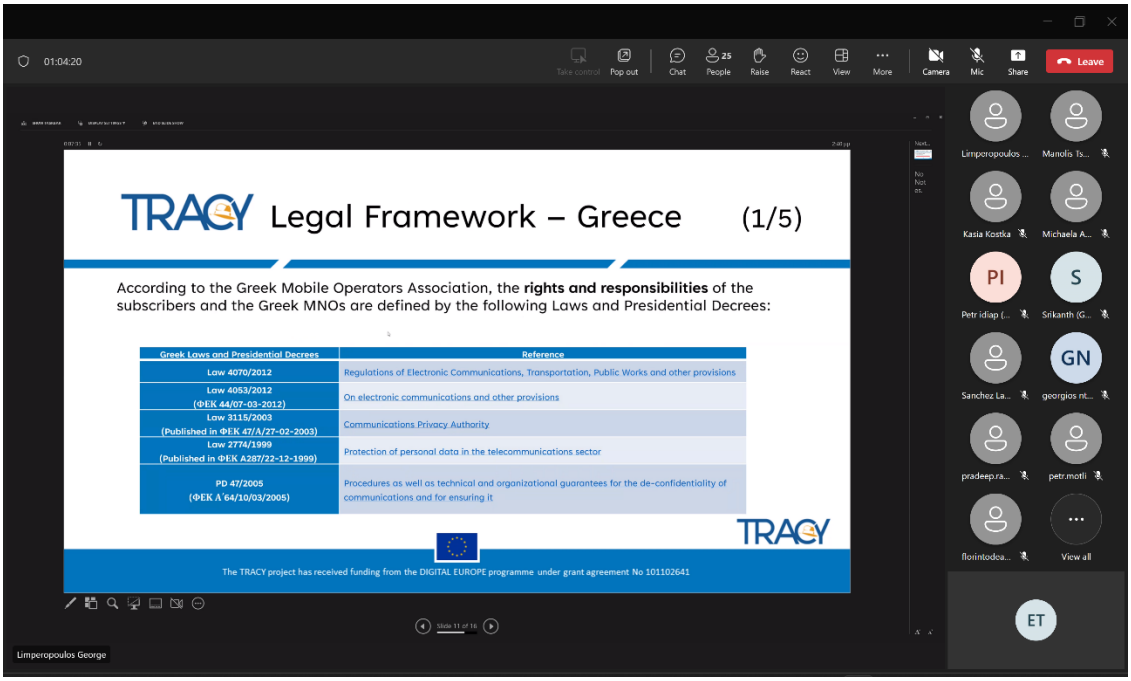

Figure 6: Current Legal Framework (Greece)

The next part of the presentation described the Current Legal Framework in Greece. The obligations of the MNOs are defined in the Greek Presidential Decree 47/2005 but also in Law N.3917/2011 which state that the providers are required to execute the order sent by the competent Authority as soon as possible and within a reasonable time and in the execution process the minimum necessary number of authorized persons is involved.

It was emphasized that for location data, according to law N.3471/2006, "exceptionally, the processing of location data by the providers of a public network or a publicly available electronic communications service is permitted, without the prior consent of the subscriber or the user, in order to provide the Authorities responsible for dealing with emergency situations, such as law enforcement authorities, first aid and fire services, the information necessary to locate the caller and only for this specific purpose".

Finally, regarding the data retention period (Law N.3917/2011) according to law N.3917/2011 (paragraph 3 of article 3), "the retention of data that reveals the content of the communication is prohibited". Also, by virtue of Law N.3917/2011 (article 6) "the data, which are produced or processed in accordance with the applicable legislation, are stored without culpable delay for the purposes of this Chapter in physical media, which are exclusively within the limits of the Greek Territory, within which they are kept for the purposes of this Chapter for twelve (12) months from the date of communication."

3.5 IDIAP, LEAs - TRACY UCs, Current Pains & Tools Utilized

This presentation focused on three areas closely relevant to LEAs. Below a summary of these areas are presented:

Use-case scenarios:

As a result of deliverable D2.1, which was drafted and submitted in collaboration with all project partners, by end of October 2023, a recap on typical use-case scenarios was presented. Obviously, the investigative scenarios were closely related to the use of traffic data, which are often requested as part of lawfully intercepted data.

In addition to use-cases collected by Romania, Greece, and Moldova internal LEAs, we also presented feedback from other (external) LEAs, which were analyzed in the near past and resulted from other discussions on extracting complementary information from traffic data, in addition to other type of (content) data typically used for criminal investigations.

Pains:

Although criminal use-cases across different countries and across different types of crimes are often very specific, thus for non-experts it might not be straightforward to find any correlation between them, the type of data to be processed to extract meaningful evidence can be similar. Obviously, this is especially due to the communication technologies used which are identical (i.e., their objective is to offer fast exchange of information between individuals and groups, which can of course be abused for criminal activities).

The session on LEA's pains therefore focused on what type of communication data is typically lawfully intercepted by LEAs to uncover criminal activities, and how this data is further processed to extracted meaningful evidence. This also touch the open issues on type of tools being used (as mentioned below).

Tools:

LEAs are required to uncover more and more complex criminal activities, involving more and more individuals, or larger groups. In order to minimize any impact on innocents, protect victims of serious crimes, etc., complex, large, and often heterogenous data need to be processed and analyzed by LEAs. Having access to efficient data analysis tools, which can well support investigators in their decision-making, and/or can reduce their workload especially in repetitive tasks, is a necessity.

The last part of the presentation therefore focused on collected information from project internal and external LEAs on tools being used by them to process the quantity of input data. We specifically explored tools and technologies available from 3rd commercial parties, as well as open-source (very advanced but less tested) solutions.

Across the whole session, the word was also given to LEA partners to comment on the discussed material. A long discussion was held at the end of this session.

3.6 PT - AI Assistance in Crime Investigation

In this presentation, AI assistance in crime investigation was discussed together with additional data types that can be used.

Firstly, a description of the current situation involved an overview of the methodology followed by LEAs today, along with potential issues associated with it. Subsequently, there was an explanation on how artificial intelligence (AI) and TRACY can assist LEAs in enhancing and optimizing this process. These procedures can be automated and multicriteria selection can be applied when necessary. A common model will be applied for data coming from different MNOs to enhance data analysis and rule-based methodology will be set to assist with filtering and prioritization of the suspects. Route prediction algorithms can also be an important tool provided for LEAs.

The value of the data provided by the MNOs was then showcased using some indicative experiments, before proceeding to a short description of two direction/route prediction algorithms: angle-direction estimator and Map Matching. These algorithms can improve the prioritization of suspects whose post-crime trajectory aligns with established evidence (ex. safehouse). Also, people that were together on the crime scene location and then met again in a different area even through separate routes, can be handled as possible co-suspects. Emphasis was put on the Map-Matching algorithm that can give added value by assisting in hard evidence

collection. It is an algorithm used in navigation systems to associate observed GPS points with a digital map of a road network which can be adjusted to match the project's needs. Instead of GPS points, the locations of the cells that served a terminal can be used. Based on the cellular coverage information for each serving cell and the road network activity, this algorithm identifies the path most likely taken by a suspect based on the highest probability. This technique contains distinct steps including data collection, digital map creation, noise reduction, state space search, transition probability assignment, application of the Viterbi algorithm and post-processing. With the necessary adjustments, map matching algorithm can be a key tool in crime investigation.

At the second part of the presentation, TRACY datasets were described. TRACY does not require any CDR-related attribute, or any indication of the service used by a terminal at any point of time. In case TRACY detects a suspicious terminal, the actual IMEI will be requested by the LEAs for them to link it to a particular subscriber. Specifically, we are referring to a special case of non-content data of signaling nature. Even when on idle mode, there will still be some information about the greater area a terminal is in. The TRACY algorithms want to take advantage of the network footprint, to detect the most likely position of a terminal, given additional evidence. There are two datasets that we would like to use. The first is the Mobile Signaling Events, that will contain the timestamp of the interaction with the network, the cellid with which the terminal was associated with at the given timestamp, the terminal id which would be an encrypted version of the IMEI, and the duration of the above interaction. The second dataset will include the Mobile Network Topology, which is a description of each cell included in the first dataset. For these cells, cellid, latitude and longitude, direction, span, height, coverage, and frequency band are the attributes that TRACY would like to obtain.

Ultimately, there was a brief reference to the potential future of crime investigation, including the analysis of behavioral patterns, integration with social network tools such as Roxanne, cellular prediction, and the establishment of an advanced analytics framework.

3.7 COSM - Additional Data Types for TRACY: Availability, Issues/Concerns, Info Exchange Framework

This presentation described the availability, the issues and concerns, as well as the info exchange framework for additional data types that may be provided by COSMOTE.

It was stated that Mobile Network Topology (MNT) data could be made available, while Mobile Signaling Events (MSE) data (IDLE mode) are available, but they are anonymized. COSMOTE also collects "interactions"- related data (CONNECTED mode) for network optimization, capacity planning, service assurance, traffic predictions, fraud, etc. these data refer to all user interactions (i.e., info exchange) between the mobile device and the network (voice, SMS and data sessions,

incl. handover info) and they are anonymized (masked IMEIs, IMSIs, etc.), so that real IDs are encrypted. "Original-Info" can be made available only for a maximum period of 24 hours. Encryption keys are stored in-memory and altered daily. These data are available about 1,5 hours after the "event" due to processing. All (anonymized) data is stored in a database which is searchable based on masked IMEI, IMSI, cell-id. However, this is not a standard process followed by ALL MNOs!

The indicative info that could be provided include all "interactions" of all subscribers residing in a specific geographical area within a specified time period, by querying a database for a time that includes the last 24 hours!

These data are useful for the Project. Even though, based on this data, one cannot tell, due to the masked IMEIs, who the subscriber may be, an AI-based processing may identify "patterns" and at the end, come up with a shortlist of IMEIs (i.e., candidate suspects) for further investigation.

These data are not normally provided to LEAs, but for the purposes of the TRACY Project, the following process could be investigated internally both technically and legally (in any case approval is needed): The input could be an area of interest for a certain time period. After a query in the Database, the encrypted data are saved in a USB stick, which is delivered at the Hellenic Police, where the content is decrypted, and the anonymized data are processed in order to reveal specific patterns and come up with a candidate IMEIs' list.

Currently, COSMOTE maintains "transaction" - related info for all subscribers, nationwide! In COSMOTE's network there are approximately 14 billion records/day. Currently, we utilize a cluster of 40 servers to process the info coming from the network and 11 servers (DB) for data storage. Additional infrastructure for firewalling, info exposure to other systems, etc. has been deployed as well.

Taking into consideration the existing (internal) solution, no major technical concerns are envisaged. However, a huge investment is required in terms of both hardware and software. Legal issues, however, regarding the potential accessibility/transfer of such data to external entities (LEAs) needs to be investigated and resolved.

3.8 PT - The Single Point of Contact (SPOC)

Next, a brief presentation was given regarding the Single Point of Contact (SPOC), as well as its architecture and benefits.

Currently, LEAs require access to mobile data to facilitate their crime investigations. However, the challenge lies in the fact that multiple MNOs, varying in number from one country to another, provide these data with different schemas and attributes. The inconsistency in data collection and presentation necessitates LEAs to manage these datasets differently, leading to delays in the overall investigative process. A potential solution to this issue could be the implementation of a

SPOC. SPOC will be designed to act as an intermediary, information hub for LEAs. The primary purpose of the SPOC will be simplifying and speeding up MNO-related procedures for LEAs, offering a unified centralized point for managing procedural interactions and information requests in the investigation context. Such solutions are already applied in some EU countries such as France and Germany.

Specifically, the SPOC protocol will consist of the following steps:

- LEA request scans (ex.) (approval by the prosecutor is necessary)
- SPOC requests scan from the multiple MNOs
- Once collected, SPOC notifies LEA
- LEA gets the request response

The SPOC protocol will comply with strict security measures, including SSL web services, strongly encrypted payloads, and encrypted sensitive information.

To summarize, the SPOC offers several advantages, such as providing a solitary contact point for data requests from various MNOs, standardizing response formats, ensuring responses with low latency, a necessity that underlines the significance of the SPOC.

4 Conclusions – Key Takeaway Points

This deliverable presented the outcome of the first workshop that was organized for and presented to LEAs in the context of the dissemination activities of the project. The purpose of the Workshop was to offer LEAs the chance to better understand the basic technologies and procedures of mobile telecommunication networks, as well as the current legal framework, in Europe and at national level, that defines the data that MNOs are obliged to retain and provide to LEAs.

LEAs face several challenges when processing data they receive from the MNOs. These challenges are complicated and multifold (large volume of datasets, time of dataset generation, location referring to, etc.). This is the point where TRACY aims to contribute by defining a methodology and an interaction framework between LEAs and MNOs for info exchange. In this Workshop it became clear that the project has additional challenges to address (such as the capability to use the appropriate real datasets without violating the current legal framework).

A series of basic mobile network processes were presented during which the UE interacts with the network, the idle vs. connected mode of the UE were explained with regards to the activities of the mobile subscriber, as well as the reselection and handover procedures. The info provided by MNOs to LEAs upon request was also explained. Such info could potentially provide valuable information for the developments of TRACY.

In addition, the current framework for info exchange between LEAs and MNOs in Greece, Romania and Moldova was briefly presented.

The various tools utilized by LEAs are of interest to TRACY to serve as the baseline that the platform to be developed will build upon, as well as for understanding how these tools could potentially support the AI-based TRACY system.

Also, a user story was utilized as the basis for explaining the TRACY methodology (e.g., traces on map) and the info needed to progress was discussed.

COSM presented information regarding the data types (indicating interaction of UE with the network) that are retained at the COSM network (in accordance with the Greek laws), the process of anonymization and encryption, and the availability of geolocation info. All this data may help identify subscriber activity patterns in the context of the project and contribute to shorten the list of suspects by the LEAs in crime investigation.

Finally, the SPOC concept was presented by PT, which can be used to simplify and speed up MNO-related procedures for LEAs, offering a unified centralized point for managing procedural interactions and information requests in the investigation context. SPOC addresses the problem that multiple MNOs, serving different countries, provide data with different configurations and

attributes. This inconsistency in data collection and presentation necessitates LEAs to manage these datasets differently, leading to delays in the overall investigative process.

Annex – List of Partner Presentations

We include here a) a screenshot of the relevant sharepoint folder showing the presentations we used in the workshop and b) a list of the presentations with a link associated to each. These links can be accessed by internal users only.

Since this is a public document, we avoid including the actual presentations in this deliverable, due to the sensitive nature of the content of these ppts.

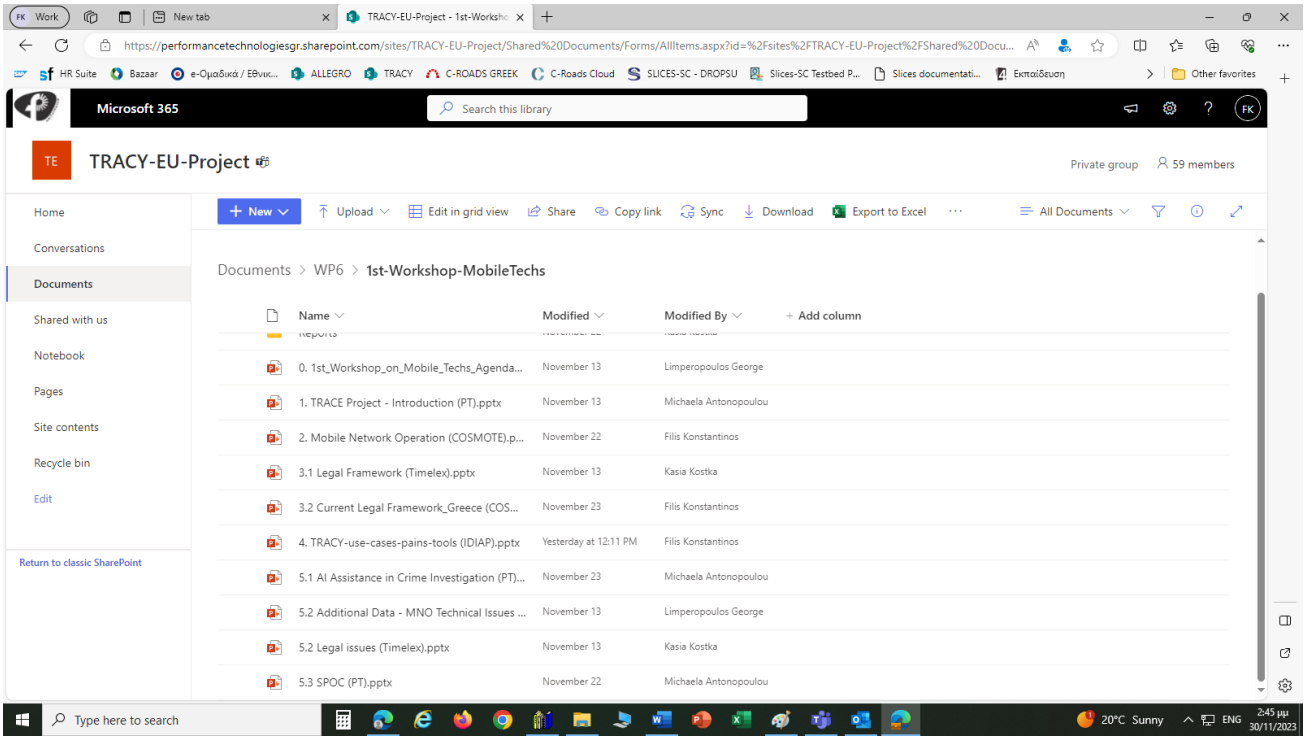

Figure 7: Screenshot of the sharepoint folder showing the presentations used in the workshop

List of presentations with associated link to the sharepoint ppt

1. TRACE Project - Introduction (PT)

2. Mobile Network Operation (COSMOTE)

3.1 Legal Framework (Timelex)

3.2 Current Legal Framework_Greece (COSMOTE)

4. TRACY-use-cases-pains-tools (IDIAP)

5.1 AI Assistance in Crime Investigation (PT)

5.2 Additional Data - MNO Technical Issues (COSMOTE)

The TRACY project has received funding from the DIGITAL 2022 programme under grant agreement No 101102641.