Brussels, 13 April 2018

COST 035/18

DECISION

Subject: **Memorandum of Understanding for the implementation of the COST Action "Digital forensics: evidence analysis via intelligent systems and practices" (DigForASP) CA17124**

The COST Member Countries and/or the COST Cooperating State will find attached the Memorandum of Understanding for the COST Action Digital forensics: evidence analysis via intelligent systems and practices approved by the Committee of Senior Officials through written procedure on 13 April 2018.

Funded by the Horizon 2020 Framework Programme
of the European Union

MEMORANDUM OF UNDERSTANDING

For the implementation of a COST Action designated as

COST Action CA17124
DIGITAL FORENSICS: EVIDENCE ANALYSIS VIA INTELLIGENT SYSTEMS AND PRACTICES (DigForASP)

The COST Member Countries and/or the COST Cooperating State, accepting the present Memorandum of Understanding (MoU) wish to undertake joint activities of mutual interest and declare their common intention to participate in the COST Action (the Action), referred to above and described in the Technical Annex of this MoU.

The Action will be carried out in accordance with the set of COST Implementation Rules approved by the Committee of Senior Officials (CSO), or any new document amending or replacing them:

a. “Rules for Participation in and Implementation of COST Activities” (COST 132/14 REV2);
b. “COST Action Proposal Submission, Evaluation, Selection and Approval” (COST 133/14 REV);
c. “COST Action Management, Monitoring and Final Assessment” (COST 134/14 REV2);
d. “COST International Cooperation and Specific Organisations Participation” (COST 135/14 REV).

The main aim and objective of the Action is to create a network to explore the potential of the application of Mathematics, Artificial Intelligence and Automated Reasoning to Digital Forensics, and to establish synergies between these fields through the development of new theoretical frameworks, methodologies and tools to support Law Enforcement by evidence analysis and problem solving during digital investigations. This will be achieved through the specific objectives detailed in the Technical Annex.

The economic dimension of the activities carried out under the Action has been estimated, on the basis of information available during the planning of the Action, at EUR 76 million in 2017.

The MoU will enter into force once at least seven (7) COST Member Countries and/or COST Cooperating State have accepted it, and the corresponding Management Committee Members have been appointed, as described in the CSO Decision COST 134/14 REV2.

The COST Action will start from the date of the first Management Committee meeting and shall be implemented for a period of four (4) years, unless an extension is approved by the CSO following the procedure described in the CSO Decision COST 134/14 REV2.

OVERVIEW

Summary

Digital Forensics is a part of the Criminalistics Sciences which deals with digital evidence recovery and exploitation in the solution of criminal cases through the application of scientific principles. There are several and increasingly sophisticated methods for collecting digital evidence. As a matter of fact, the evolution of technology continuously pushes such kind of methods. Rough evidence must however be used to elicit hypotheses concerning events, actions and facts (or sequences of them) with the goal to obtain evidence to present in court. Evidence analysis involves examining fragmented incomplete knowledge, and reconstructing and aggregating complex scenarios involving time, uncertainty, causality, and alternative possibilities. No established methodology exists today for digital evidence analysis. The Scientific Investigation experts usually proceed by means of their experience and intuition.

The Challenge of the proposed COST Action consists in creating a Network for exploring the potential of the application of Artificial Intelligence and Automated Reasoning in the Digital Forensics field, and creating synergies between these fields. Specifically, the challenge is to address the Evidence Analysis phase, where evidence about possible crimes and crimes perpetrators collected from various electronic devices (by means of specialized software, and according to specific regulations) must be exploited so as to reconstruct possible events, event sequences and scenarios related to a crime. Evidence Analysis results are then made available to law enforcement, investigators, public prosecutors, lawyers and judges: it is therefore crucial that the adopted techniques guarantee reliability and verifiability, and that their result can be explained to the human actors.

Areas of Expertise Relevant for the Action	**Keywords**
● Computer and Information Sciences: Theoretical computer science and formal methods	● Digital Forensics ● Automated Reasoning ● Artificial Intelligence ● Computational Logic

Specific Objectives

To achieve the main objective described in this MoU, the following specific objectives shall be accomplished:

Research Coordination

- Raise awareness among researchers in AI and Automated Reasoning of the main issues and problems in the daily work of digital forensics scientists and the technical, legal and criminological aspects they involve.
- Identify a list of realistically applicable AI and Automated Reasoning techniques, focusing on Computational Logic for verifiability and justifiability reasons (essential in a legal environment).
- Promote R&amp;D activities for integrating such techniques and defining new methods and tools.
- Foster and coordinate related R&amp;D activities of the partners.
- Collect and organise anonymised data extracted from real cases provided by the Digital Forensics Action partners, and devising suitable benchmarks concerning the solution of such cases.
- Put into practice the new methods developed in the Action on the collected data thus providing a foundation for future practical tools.

Capacity Building

- Increase awareness among Digital Forensics experts of new methods and techniques and their applicability.
- Assist Digital Forensics experts in the practical experimentation of the new methods.
- Disseminate the Action results to stakeholders, not only Government Agencies and Institutions but also

private companies working in the Digital Forensics field.

- Implement training schemes for the parties that are potentially involved.

TECHNICAL ANNEX

1. S&T EXCELLENCE

1.1. CHALLENGE

1.1.1. DESCRIPTION OF THE CHALLENGE (MAIN AIM)

Digital Forensics is a branch of criminalistics which deals with the identification, acquisition, preservation, analysis and presentation of the information content of computer systems, or in general of digital devices. The Challenge of the proposed Action is to create a research infrastructure for the application of Artificial Intelligence (AI) and Automated Reasoning, together with other complementary areas, in the field of Digital Forensics in order to reduce the gap between both disciplines. In particular, the main focus of the challenge is to address the phase of Evidence Analysis, where evidence about possible crimes and crime perpetrators collected from various electronic devices (by means of specialized software, and according to specific regulations) is examined and aggregated so as to reconstruct possible events, event sequences and scenarios related to a crime. Evidence Analysis results are then made available to law enforcement, investigators, intelligence agencies, public prosecutors, lawyers and judges; in the case of cybercrime for example, in line with the recommendation of the Commission to the European Parliament in document 22.11.2010 COM (2010) 673 final (Communication from the Commission to the European Parliament and the Council, The EU Internal Security Strategy in Action: Five steps towards a secure Europe) - on page 10, "At national level, Member States should ensure common standards among police, judges, prosecutors and forensic investigators in investigating and prosecuting cybercrime offenses". Concerning the policies used by Police institutions for sharing technologies and information, the European institutions adopt procedures established within the ENFSI (European Network of Forensic Science Institutes).

This proposal constitutes a timely challenge for both areas: Digital Forensics and AI & Automated Reasoning. From the AI perspective, the proposed research infrastructure will foster the development of new theoretical results, methods and techniques that will contribute in the long term to the development of new software tools that will rely on a complex combination of concepts and results from different areas of Knowledge Representation (KR) and Automated Reasoning such as diagnosis, causal explanation, temporal reasoning about actions, epistemic reasoning, the treatment of incomplete knowledge, deontic and legal reasoning, inductive learning and formal concept analysis, which will be complemented by other ones needed for the purpose of the Action. At the same time, the application of (intelligent) automated tools in Digital Forensics, capable of reliable and exhaustive exploration of evidence and with a level of analysis that goes beyond the scope of human observation and in time will constitute a breakthrough that will have a direct impact on the practical investigation of crime scenarios. Notice that the time is very important and the results must be given very quickly. This necessity is increasing nowadays, in which a quick answer to ensure the responsible at the justice or for a rapidly prosecution of the investigations.

To meet the challenge, the Action has built a Network composed of researchers and engineers from Artificial Intelligence and Automated Reasoning together with experts in Digital Forensics and Digital Investigations belonging to Government Institutions and NGOs alongside scholars from the field of Information and Communication Technologies (ICT) and Law as well as social scientists, criminologists and philosophers (ethics). The Network is carrying out a set of activities and building resources to promote interaction, exchange and cooperation between these different areas. It is enabling computer

Funded by the Horizon 2020 Framework Programme
of the European Union

scientists to understand the main issues and open problems of Digital Forensics, especially Evidence Analysis, and it is helping to promote the exploitation of AI for addressing in an innovative, effective and adaptive way the key problems in this domain. Network partners is thus being able to identify Automated Reasoning techniques which can be applied to Evidence Analysis, and to suggest guidelines for creating and developing suitable new techniques and methods aimed at advancing the state of the art in both Digital Forensics and Artificial Intelligence and Automated Reasoning, strengthening European research and innovation capability in these areas. The long-term objective of the Network is the increasing of know-how and study, devise and implement concrete projects and tools to be applied by Police Scientific Investigation Departments in solving real cases in COST Member Countries, COST Near Neighbour Countries (NNCs) and COST International Partner Countries (IPCs), promoting coherent and effective cooperation with third countries.

1.1.2. RELEVANCE AND TIMELINESS

Digital Forensics is a rapidly expanding field. It has became a very important research area due to the worldwide diffusion of ICT, its rapid evolution, the increasing number of cyber crimes and world wide terrorism acts. So far, Evidence Analysis has not been automated and there is a clear indication that Digital Forensics experts feel the need of such an automatisation: this is testified by the requests that Action partners have received from Digital Investigation Departments, and by the fact that some of these Departments choose to be among the founding Action partners. An important feature of Digital Forensics is its technical dependence on a highly volatile area such as ICT, where frequent innovations are continuously introducing new forms of cybercrime but, at the same time, potentially allow new methods for evidence analysis that could not be exploited before. For this reason, the automation of Digital Forensics tasks does not make sense without a high degree of *flexibility* for adapting these tasks to new technological environments. This flexibility is where Knowledge Representation (KR) and Automated Reasoning techniques provide a key feature for the project resolution. To sum up, the Action challenge is at the moment both relevant and well-situated with respect to existing demands and needs that might otherwise be fulfilled by non-European research and development. Furthermore, this Action follows the suggestion of the Commission of the European Parliament detailed in the previous section.

In the latest years in fact, the Commission sustained other projects devoted to design, implement and commercialize digital forensic tools. A first example is the LASIE project (http://www.lasie-project.eu) (FP7) focused on extracting evidence from multiple and heterogeneous sources (e.g., CCTV content surveillance, data from confiscated hard disks and mobile devices, handwritten documents and so on) and analysing collected evidence; experimentally, this project also applies some techniques from Answer Set Programming (ASP), but for preliminary inferential tasks. A second example is the IDENTITY project (Horizon 2020, http://www2.warwick.ac.uk/fac/sci/dcs/research/df/identity), which addresses Multimedia forensics, intended as the extraction, analysis and classification of digital evidence generated by multimedia sources, such as imaging devices. Finally, there exists a related COST action, MIFE, which focuses on the integration of a broad spectrum of imaging techniques (e.g., optical, spectroscopic, chemical, physical) with computational modelling tools to increase the usability of collected evidence. All these examples have a clear orientation towards evidence collection and classification, which is a previous phase to Evidence Analysis, the main concern of our current proposal. Our initiative is thus complementary, as it will apply Automated Reasoning and AI techniques for the analysis of the collected evidence and the integration of information obtained from different (possibly distributed and virtualized) data sources.

The Action involves a wide group of recognised experts in KR and automated reasoning covering different areas and techniques. Although different orientations have being tried, the main technical approach that will constitute the cornerstone of the Action is the paradigm of Answer Set Programming (ASP). Due to its solid theoretical foundations and the availability of efficient tools, ASP has become nowadays a de facto standard or lingua franca for practical KR and problem solving, with a growing list of heterogeneous application areas including relevant topics such as diagnosis, information integration, scheduling, planning, timetabling and configuration. Besides, there exist preliminary applications of ASP to specific Digital Forensics cases developed by Action's members that have provided evidence for a trial (in 2015 in Italy), probably constituting the first case of a KR and Automated Reasoning application for that purpose. On the theoretical side, different extensions of ASP have been proposed and developed for dealing with temporal reasoning, epistemic operators (modelling agent's beliefs), argumentation, causal explanations, abduction, uncertainty or fuzzy and approximate reasoning, all of which are of crucial importance for the network proposal and its application to Evidence Analysis.

1.2. OBJECTIVES

1.2.1. RESEARCH COORDINATION OBJECTIVES

The main Research Coordination Objectives are:
O1. Raising awareness among researchers in AI and Automated Reasoning of the main issues and problems in the daily work of digital forensics scientists and the technical, legal and criminological aspects they involve.
O2. Identifying a list of realistically applicable AI and Automated Reasoning techniques, focusing on Computational Logic for verifiability and justifiability reasons (essential in a legal environment).
O3. Promoting R&D activities for integrating such techniques and defining new methods and tools.
O4. Fostering and coordinating related R&D activities of the partners.
O5. Collecting and organising anonymised data extracted from real cases provided by the Digital Forensics Action partners, and devising suitable benchmarks concerning the solution of such cases.
O6. Put into practice the new methods developed in the Action on the collected data thus providing a foundation for future practical tools.

1.2.2. CAPACITY-BUILDING OBJECTIVES

OC1. Increase awareness among Digital Forensics experts of new methods and techniques and their applicability.
OC2. Assist Digital Forensics experts in the practical experimentation of the new methods.
OC3. Disseminate the Action results to stakeholders, not only Government Agencies and Institutions but also private companies working in the Digital Forensics field.
OC4. Implement training schemes for the parties that are potentially involved.

1.3. PROGRESS BEYOND THE STATE-OF-THE-ART AND INNOVATION POTENTIAL

1.3.1. DESCRIPTION OF THE STATE-OF-THE-ART

Digital Forensics (DF) is a complex and rapidly evolving field, where methods for collecting evidence are varied, rapidly evolving and becoming increasingly sophisticated. In fact, such methods must continuously adapt to the evolution of technology. The aim is to identify digital sources of evidence, and to organize such evidence in order to make it robust in view of its discussion in court, either in civil or penal trials. DF is concerned with the analysis of possible sources of evidence after a crime has been committed. Digital Forensics involves the following phases:
Phase 1: Identification, i.e. retrieving, via forms of Digital Investigation, devices that may possibly contain digital data useful to the identification of a potential crime perpetrator, or anyway useful to help the investigators in their activities.
Phase 2: Acquisition, i.e., retrieving evidence in the form of data collected either from storage devices or from network interception.
Phase 3: Preservation, where collected evidence must be stored and preserved (according to specific precise regulations) so as to guarantee integrity and authenticity.
Phase 4: Evidence Analysis, where the evidence collected is examined and aggregated to determine the existence of possible sources of proof that can be useful to law enforcement, investigators, public prosecutor, lawyers and judges in various phases of trial. It involves examining fragmented, incomplete knowledge, and aggregating evidence items into complex scenarios possibly involving time, uncertainty, causality and alternative possibilities. Currently, no single established procedure exists for Evidence Analysis, which is usually performed by Scientific Investigation experts on the basis of their experience and intuition.
Phase 5: Presentation, where sources of evidence identified by means of Evidence Analysis are formalized in official documents.

Clearly, the development of DF is highly related to the development of Information and Communication Technologies in the last decades, and to the widespread diffusion of electronic devices and infrastructures. It involves various disciplines such as computer science, electronic engineering, various branches of law, investigation techniques and criminological sciences. Organizational aspects are also relevant and DF investigation involves, in general, several experts working with sophisticated instruments and software, with limited resources and tight timing.

Digital Forensics is usually seen as divided into:

- **Computer Forensics**: concerns the extraction of data from various storage devices, such as Hard Disk, SSD, CD, DVD, Flash Memories etc. Adopted techniques include Data Recovery, Data mining, Password Cracking & Discovery, Events correlation.
- **Live Forensics**: concerns the analysis of working systems that cannot be stopped. Live Forensics activities include: run-time analysis of critical infrastructures; Password Cracking & Discovery; Data interception; Virus, Trojan and Malware Analysis.
- **Mobile Forensics**: concerns the analysis of storage devices and activities related to mobile devices such as cellular phones, smartphones, tablets, satellite navigation systems, etc. Mobile Forensics activities include: data retrieval from mobile phones and tablets, fixed and removable storage (address book, text messages, multimedia messages); app analysis; Forensic Localization; Events correlation. Data Mining techniques are often used for this.
- **Database Forensics**: concerns database analysis for the retrieval of data or of transaction activities and logs.
- **Network & Internet Forensics**: concerns the analysis of network infrastructures, and involves the interception, storage and examination of network events. Network & Internet Forensics activities include: identification of security violations and attacks; e-mail tracking and sender identification; web providers, sites and services tracking; chat and file sharing tracking; social networking analysis; device localization.
- **Embedded Forensics**: concerns the analysis of embedded systems.
- **Cloud Forensics**: concerns the analysis of infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS).
- **Multimedia Forensics**: concerns the analysis of multimedia (audio/video) files with the purpose of discovering possible alterations or hidden content.

Phases 1-3 are supported by a number of hardware and software tools, the latter being both proprietary and open source. These tools are continuously evolving to follow the evolution of the involved technologies and devices, and recently related procedures have been standardized in all communities. However they do not require advanced reasoning capabilities.

Phase 4, Evidence Analysis, is where the main thrust of the Action will lie. This phase requires advanced reasoning capabilities that are not currently supported by available devices and software. In fact, these are limited to data recovery (and data recognition) and to providing metadata (size, dates of creation/modification/elimination, etc.). Therefore, such retrieved data must be analysed by human experts. Some of the most used proprietary tools are “Encase” (developed by “Guidance Software”), “Forensic Toolkit” (developed by “AccessData”), “UFED” (developed by “Celebrate”), “XRY” (developed by “MSAB”) and “AXIOM” (developed by Magnet Forensics). Concerning open source alternatives there are “The Sleuth Kit (+Autopsy)” and other minor tools included in forensics Linux distributions (such as “CAINE” and “DEFT”) and suggested by NIST (National Institute of Standards and Technology - U.S. Department) that merely cover aspects of data recovery and data recognition.

Although some of these latter applications are equipped with modules able to give a graphical representation of some content on the style of i2 Analyst Notebook (i.e. represent the conversations between applications and/or devices), none of them is capable of eliciting significant evidence from the retrieved data. In some cases, specifically in proprietary tools, apart from text analysis, header files analysis and mining software packages, the tools operate as a “black box” (i.e., they provide results without motivation or explanation), and for verification of the results one needs a secondary analysis with open source tools.

1.3.2. PROGRESS BEYOND THE STATE-OF-THE-ART

Evidence Analysis involves examining fragmented incomplete knowledge, and aggregation of evidence items into complex scenarios possibly involving time, uncertainty, causality and alternative possibilities. Currently, no single established procedure exists for Evidence Analysis, which is usually performed by Scientific Investigation experts on the basis of their experience and intuition. **The network is therefore focused on promoting formal and verifiable AI and Automated Reasoning methods and techniques for Evidence Analysis that aim at the elicitation of sources of evidence.** Relevant aspects to consider include:

- Timing of events and actions;

- Possible causal correlations;
- Contexts in which suspicious actions occurred;
- Skills of the involved suspects;
- Awareness of the involved suspects of committing a violation or a crime and of the degree of severity of the violation/crime.

Moreover, given available evidence, several possible underlying scenarios may exist that should be identified, examined and evaluated.

The aim of the Action is that all the above should be performed via techniques that are verifiable with respect to the results they provide, how such results are generated, and how the results can be explained. **Therefore, such software tools can be reliable and provide a high level of assurance**, in the sense of confidence in the system's correct behaviour. Otherwise there remains an undesirable uncertainty about the outcome of these stages, and different technicians analysing the same case can reach different conclusions which may lead to different judgements in court. Some initial promising applications of Computational Logic and in particular of ASP exist, that exploit provably correct encodings of known mathematical problems to elicit scenarios from Digital Forensics data. This is achieved by means of a correlation of the elements of the given cases to the elements of the considered mathematical problems.

In AI and Automated Reasoning, several methods and techniques have been developed over the years for uncertain, causal and temporal reasoning, and for devising and examining alternative consistent scenarios that might be compatible with a set of known facts. To the best of our knowledge, (apart from the above-mentioned experiments with ASP) these techniques have never been applied to Digital Forensics evidence analysis. Therefore, **studying their applicability for development of suitable prototypes is *per se* a significant advance over the state of the art**. Moreover, **the application to such a challenging field will foster refinements and improvements of the known methods and techniques, and development of novel ones**.

Unlike the phase of crime identification or detection, where the exploration of big data and the application of machine learning techniques can be useful, the phase of Evidence Analysis has particular requirements that make our proposal based upon KR and Automated Reasoning a much more promising approach, potentially becoming a breakthrough in the state-of-the-art. The final goal of Evidence Analysis is the formulation of verifiable evidence that can be rationally presented in a trial. Under this perspective, the results provided by machine learning classifiers or other types of "black box" recommender systems do not have more value than human witness' suspicions and cannot be used as legal evidence. Logical methods provide a broad range of proof-based reasoning functionalities that can be implemented in a declarative framework where the problem specification and the computational program are closely aligned. This has the benefit that the correctness of such declarative systems based on computational logic can be formally verified. Moreover, recent research has led to new methods for visualising and explaining the results of computed answers (e.g., based on argumentation schemes). So one can not only represent and solve relevant problems, but also provide tools to explain the conclusions (and their proofs) in a transparent, comprehensible and justified way.

In summary, the rationale for the choice of Computational Logic relies on the fact that, by its very nature, it is based on precise formalizations, and thus allows for the affordable verification of desired properties of the systems that will be devised in the future as a follow-up of the Action. Verifiability, reliability and justifiability are keys features for software tools to be applied in a field such as Digital Forensics, where the evidence produced is aimed at the reconstruction of crimes and assist/facilitate the court in the decision process to establish if an accused is innocent or guilty.

1.3.3. INNOVATION IN TACKLING THE CHALLENGE

Although AI techniques have been applied to Digital Forensics for different purposes, they have mainly been exploited for data retrieval and categorization. For instance, the analysis of image and video multimedia files by pattern recognition algorithms or the detection of anomalies in large databases such as email exchanges, network transactions, etc. are examples of such applications. These tasks benefit from intelligent techniques and in particular from machine-learning and classification techniques. **The Action takes a step beyond as it involves the main stakeholders in order to apply Automated Reasoning methods to retrieved data in order to elicit evidence that can be used in a trial.** For instance, from data items retrieved from different sources (like, e.g., mobile devices, social network activities, cloud computing tracks, etc.), we may obtain the set of all possible patterns of activity of a suspect during the execution of a crime. Automated Reasoning techniques can constitute a crucial advantage since the amount of data to examine and interpret is large and keeps growing with the increasing adoption of digital devices in everyday life. Thus, **the Action proposes innovations** in the following two directions:

1) a substantial evolution of the current paradigm of evaluation and interpretation of data in DF analysis, which might be exportable, in the future, also to other Forensic Sciences;
2) a "breakthrough innovation" for the judicial system, based on the possibility of adopting intelligent, reliable and dependable decision-support systems for the reconstruction of facts, able to take into account the wide number of elements and variables involved in complex cases, so as to aid judges in their assessments and decisions.

1.4. ADDED VALUE OF NETWORKING

1.4.1. IN RELATION TO THE CHALLENGE

Tackling issues related to Digital Forensics in an effective way requires the synergic cooperation of experts from the Digital Forensics field, crime investigators, lawyer and experts from several areas of AI and Automated Reasoning. On the one hand, DF experts alone are not even aware of the potential that European research offers for designing and building novel advanced tools for aiding them in their activities; on the other hand, researchers alone are not familiar with the complexity and the subtleties of such a challenging interdisciplinary field that involves issues related not only to technology, but also to the legal and criminological aspects of the application of technology. Moreover, there is no single technique, which suffices to provide DF experts with innovative and effective working tools. Therefore, bringing together researchers from several areas of AI and Automated Reasoning, Criminal Law and criminology experts can foster a productive exchange that can lead to scientific and technological breakthroughs. Performing this interaction between researchers and experts in a network, instead of separately between single institutions, result in an optimal use of human and time resources. The initial network partners includes researchers from areas of AI that can be particularly useful in Evidence Analysis, including: ASP, for plausible scenario reconstruction; Causal Reasoning, for eliciting causally-linked possible event/action sequences; Temporal Reasoning, for taking time and temporal constraints into account; Fuzzy Logic, for dealing with uncertainty in information and information aggregation; Neural Networks, for complementing logical techniques with a powerful classification methodology.

The partners in the Action comprehend experts in DF and AI, scholars from Philosophy, Social Sciences Criminalistics and Law, and industrial researchers; this in order to cope with the technical and practical aspects and also with foundational and societal issues and with the ethical aspects involved in the development and use of AI techniques in this field. With a network structure, individual efforts in the different national groups can be properly exploited and integrated, rather than lost in some ad hoc applications. Additionally, the Action becomes a catalyst for future specific research projects with an international and multidisciplinary composition. The existence of companies in the Action provides their direct involvement in exploiting Action results at the commercial level, thus obtaining revenues that should be at least partly reinvested in Action-related research activities. New companies will be attracted by the effective diffusion activities and the interesting advanced given by the Action. The involved DF experts have indeed a direct professional interest in the application of Action’s results.

1.4.2. IN RELATION TO EXISTING EFFORTS AT EUROPEAN AND/OR INTERNATIONAL LEVEL

Digital Forensics at the European Union faces a globalised environment where large criminal organisations operate at a transnational level and, at the same time, individual perpetrators may easily access technological knowledge quickly spread in the internet. This context undoubtedly requires a *coordinated* response. ENFSI (European Network of Forensic Science Institutes, http://www.enfsi.eu/) is the best established and most widely recognized international organization at European level in forensic science, whose mission is to share knowledge, exchange experiences and come to mutual agreements in the field. Indeed, the European Commission recognised ENFSI as the sole voice of the forensic science community in Europe. Since its mission includes developing and promoting a discipline of forensic technology and to cultivate relations and cooperation with major technical organisations, this Action will use its expertise in order to: ensure the quality and appropriateness of its activities in relation to existing standards; exchange information about technical aspects, state of the art and new

developments, also in relation to the possible legal obstacles when sharing data from one partner to another, as well as on privacy and confidentiality matters.
The Action's results on addressing DF Evidence Analysis by means of intelligent systems, and the planned activities and deliverables (detailed in Section 3.1) can be usefully exploited in the ENFSI context and can foster further profitable interactions with the ENFSI Working Group on Forensic Information Technologies and its members. The role of ENFSI for knowledge and methods exchange is crucial for its participants and for the European Community as a whole, and the Action will develop its activities in close cooperation with ENFSI and with some of its members. The inclusion of ENFSI is ensured since one important member is involved in the Action and we have already initiated the procedure in order to sign a collaboration formal document.

Another important added value from the networking is that, when deployed in practice, the developed tools will need to comply with all the applicable laws and regulations of each country participating in the network. This has the side effect of a cross-country communication that may potentially improve the existing policies and regulations for mutual benefit.

2. IMPACT

2.1. EXPECTED IMPACT

2.1.1. SHORT-TERM AND LONG-TERM SCIENTIFIC, TECHNOLOGICAL, AND/OR SOCIOECONOMIC IMPACTS

The innovative use of methods and techniques from a well-established research area (AI and Automated Reasoning) to a critical field (Evidence Analysis) where no significant previous efforts and results on computer-based intelligent decision support exist so far, is already a potential breeding ground for new and significant scientific and technological results. In the long-term, a challenging interdisciplinary area such as Digital Forensics will, with the help of this Action, provide a strong impetus for new developments that may result in scientific breakthroughs, publications, software prototypes and tools. From the scientific perspective, Evidence Analysis constitutes an ***ideal application domain*** for logical reasoning in AI, as it *combines* different classical aspects of knowledge representation such as hypothetical reasoning, causality, argumentation, spatio-temporal problems, case-based reasoning or uncertainty, all of them classical topics in any KR forum. Even the underlying orientation and goal, the ***search for a proof***, is aligned in both areas (a formal proof vs a valid argumentation in a trial). In the short term, Digital Forensics can provide the AI & KR community with non-trivial benchmarks of automated reasoning that constitute a breakthrough with respect to available synthetic or *ad hoc* examples used in the scientific literature. It will act as a proof of concept to check whether different available KR techniques and tools are directly applicable or, most probably, require adjustments to take into account the domain features.

From the **socio-economical perspective**, the use of automated reasoning tools will become, in the long-term, **a positive benefit for all the involved stakeholders. Law enforcement, investigators, intelligence agencies, criminologists, public prosecutors, lawyers and judges will be provided with decision-support-systems that can effectively support them in their activities by providing motivated suggestions**. In the short-term, the most relevant impact will be a twofold improvement both on **efficiency** and **quality**. On the one hand, investigators will work more efficiently thanks to new tools that guide them, helping with hypotheses formulation, the exhaustive application of case-based reasoning on large collections of data, and the development of proofs that can be formally checked with correct logic-based inference systems. This will save enormous effort on tasks that are currently done by hand and in most cases require tedious repetitions to ensure that human errors will not spoil the validity of the final evidence. On the other hand, once the evidence is obtained, KR-based computational logic tools allow the formal proof obtained to be presented in a form that can be understood and followed *step by step* by non-expert humans so it can be transparently used as a trial evidence. But, what is more important, this evidence will come with the additional guarantee that it can be also checked and verified using automated inference tools (theorem provers and model checkers), improving its quality and reliability. In the long-term, this method could yield an ***evidence certificate*** that will guarantee that the argument presented in a trial has been checked to be logically sound using a standardized formal verifier (in an analogous way to current applications of Formal Verification to Software Certifications) and according to tests performed on a relevant number of real cases. This kind of certificate could potentially allow ruling out cases of unintended (or intended) fallacies that are frequent in a purely rhetorical argumentation.

2.2. MEASURES TO MAXIMISE IMPACT

2.2.1. PLAN FOR INVOLVING THE MOST RELEVANT STAKEHOLDERS

The proposed Action already involves the start partners from Departments of Scientific Investigation of the Police of different countries. Thus, key relevant stakeholders will be directly participating to the Action efforts. Their presence will help to identify and involve other relevant stakeholders, not only Police Institutions but also companies involved in specific software and hardware development for its application in Digital Forensics. Moreover, the leading institution of the Action has an extensive experience working with their national police force as well as the Justice Administration and its national intelligence service.

Furthermore, in order to involve institutions from COST Near Neighbour Countries (NNCs) and COST International Partner Countries (IPCs), we will carry out a specific dissemination with **conferences in these countries, press releases, promotional materials, etc.**

2.2.2. DISSEMINATION AND/OR EXPLOITATION PLAN

To achieve a successful impact, the proposal will use effective dissemination measures besides press releases and promotional materials. On the AI side, the Action members are active in several scientific sub-communities and enjoy a high level of international cooperation and visibility. The members are also active and participate in science policy, and management through conference organisation, programme and steering committees, publishing, consultancy, networking and other activities. This will ensure good visibility for the Action and its results.

In addition, we will disseminate results via a webpage providing internal communication links between partners, as well as making available technical reports, articles, software prototypes and a synopses of the COST Action to a wider audience. Results will also be disseminated regularly at international conferences on AI, logical reasoning or logic programming as well as via guest lectures at other institutions. Articles will be published in scientific journals, with special attention to those specialised journals having a high impact factor in the ISI Journal Citation Report. Frequent contact and interchange of researchers between the main external collaboration partners will be a further dissemination path. At least one international seminar or workshop will be organised per year at which both partners and other external collaborators and key scientists from the involved fields will be invited to participate.

On the Digital Forensics professional side, we will focus our dissemination efforts on specialised journals such as Digital Investigation or the IEEE Transactions on Information Forensics and Security, plus other journals on Forensic Science that regularly include contributions on Digital Forensics, such as the FBI's Forensic Science Communications or the Journal of Forensic Sciences. Regarding conferences, the dissemination of results is potentially more restricted due to legal constraints and to security issues. An exception is perhaps the International Workshop on Digital Forensics and Incident Analysis (www.wfdia.org), though it has a limited scope. At present, the dissemination of new results and techniques is mostly made inside the Police corps or at a national or European level through cooperation networks. In the case of Forensic Science, the most relevant of these networks in our context is, as mentioned, ENFSI, organized by working groups on different disciplines, including Forensic Information Technology
(http://www.enfsi.eu/about-enfsi/structure/working-groups/information-technology).

In the US, it is also worth mentioning the research activities developed at the National Institute of Standards and Technology (NIST) which has a section devoted to research on Digital and Multimedia Evidence (http://www.nist.gov/forensics/research/digital.cfm) that includes information on ongoing research projects as well as a list of regular publications on this topic such as the ITL Bulletin maintained by the Computer Security Resource Center or the National Institute of Justice, that includes publications on Digital Forensics. Finally, although not specifically focused on Digital Forensics, there are several events that include in their scope the topic of computer security, where Action results can be presented (e.g. the ACM Conference on Computer and Communications Security (CCS)).

On education and training, the Action will establish periodical “Collaboration Exercises” in order to check the developed methodologies on sample realistic (anonymised) cases. ENFSI will also be present in different of these exercises. The Action will produce material of potentially use in the training of experts but also in university courses on either AI (where DF may provide useful and interesting case studies) or Digital Forensics or even Law. The Action will organize annual Training Schools accessible to technicians, law enforcement agents and students, also at the Ph.D. level; representatives of companies working in the field of Digital Forensics will be also invited to these Schools, so as to foster future cooperation for the development and exploitation of real tools stemming from the Action results; action partners have already established contacts with more companies. An objective of the Training Schools will be that of involving in the Action more Law Enforcement Agencies, which would be encouraged to join by testing “first hand” the usefulness and effectiveness of the developed tools.

2.3. POTENTIAL FOR INNOVATION VERSUS RISK LEVEL

2.3.1. POTENTIAL FOR SCIENTIFIC, TECHNOLOGICAL AND/OR SOCIOECONOMIC INNOVATION BREAKTHROUGHS

Equipping judges, public prosecutors, law enforcement, lawyers, investigators, intelligence agencies, criminologists, and other parties with intelligent decision support systems capable to effectively support their activities in a reliable way constitutes both a technological and sociological breakthrough. This long-term objective will be pursued and supported by the Action, and the already inclusion of criminologists and criminal law experts in the network helps to ensure the uptake of the new technologies in the future. The new methods will also allow optimizing the use of available resources by relieving human experts from time-consuming and highly error-prone tasks that can instead be reliably performed by the future AI applications fostered by the Action results. A potential risk concerning the proposed Action and its outcomes is that it may be difficult to convince the involved parties and the general public of the real applicability of such systems. While for some forensic techniques, such as DNA analysis, there is nowadays a high and widespread level of trust, an Artificial-Intelligence-based decision support system may initially appear unconvincing or even threatening. However, the general acceptance of DNA analysis paved the way for the introduction of other scientific methodologies. The non-technical Action partners will be helpful in identifying and enacting strategies for transforming scientific concept such as verifiability, completeness and correctness into humanistic and social concepts such as psychological reliability and trust, taking also into account specific cultural, legal and ethical aspects.

3. IMPLEMENTATION

3.1. DESCRIPTION OF THE WORK PLAN

3.1.1. DESCRIPTION OF WORKING GROUPS

The Working Groups (WGs) and their contribution to the Action objectives are listed below.

WG N.	Work Group Name	Aims & Objectives
WG1	Digital Forensics requirement analysis	O1
WG2	Research on applications of AI/Automated Reasoning to DF	OC1, O2, O3
WG3	Prototypes and Platforms	O3, O5, O6
WG4	Benchmarks based on real cases	O3, O5, OC1
WG5	Platforms integration and multi-dimensional environment	O5, O6
WG6	Meetings, workshops and conferences	O4, OC1,OC2, OC3
WG7	Training, education and dissemination activities	O4, O7,OC1,OC3,OC4
WG8	Short-Term Scientific Missions and internal organization	O4, OC1, OC2

We have divided the different activities into these nine WGs in order to optimize the procedures and the personal resources. The **composition** of each WG is as follows:

WGs from 1 to 5 are formed by members of the Action. All members must be in at least one WG. From these WGs one WG leader and two WG Co-leader (at least, one of them will be Early Career Investigator (ECI)) will be chosen to be part of each WG6-8. The WG leader will be the responsible for the good functioning of the WG.
WGs from 6 to 8 are formed by six experts, one for each WG from 1 to 5 and the Action Chair or another researcher of the MC designated by him. The members will choose a WG leader, a WG ECI co-leader and a WG co-leader. In WG 8 one of these leaders will be the STSM coordinator.
The leaders and co-leaders will be chosen mainly from ITCs and NNCs members and will be gender-balanced. Hence, these countries and ECIs will have an active role in the Action.

The **tasks** of each WG are listed below:

Tasks WG 1 - 5
T1.Organise specific meetings for the members of the WG.
T2.Set dates and milestones for intermediate deliverables.
T3.Propose Training Schools, Dissemination Activities and Publications.
T4.Decide on topics and strategies for the Short-Term Scientific Missions Training Schools, Dissemination Activities and Publications for each specific WG.
T5.Suggest specific tasks to the different members of the WG.

Tasks WG 6
T6.Collect and study the different proposals to hold specific meetings, workshops and conferences.
T7.Propose generic meetings, workshops and conferences in which information on the progress of each WG will be disseminated.
T8.Suggest meetings, workshops and conferences to the Management Committee.

Tasks WG 7
T9. Produce and maintain the Action Website; oversee Social Media presence.
T10. Collect and study the different proposals to organize Training Schools and dissemination activities and publications.
T11.Propose Training Schools and dissemination activities and publications to the MC.
T12. Study the negative impact of the given results and advances before the publication.
T13. Guarantee that the Action preserves the societal, ethical and legal aspects, and RRI.

Tasks WG 8
T14.Collect and study the different proposals for Short-Term Scientific Missions.
T15.Study the proposals of *ad hoc* participants and provide recommendations to the MC.
T16.Suggest the WG in which each new participant should be incorporated.
T17.Prepare general reports.

The **activities** are listed below:
A1.**Management Committee meetings**. In these meetings the MC evaluates the proposal of the WGs and the rest of activities detailed in Task T0. Planned number: 2 by year.
A2.**General Meetings, Workshops and Conferences**. These activities are general and every researcher, engineer or scholar in fields related to the topic of the Action can participate. Specific conferences for young researchers will be scheduled. Planned number: 2 events by year. At the start the Action will stage two key events (possibly co-located): a general planning and organizational event, and a familiarization event that includes tutorials and lectures designed to give AI researchers and other scholars some basic training in DF, and to present some basic techniques of KR and AI to non-computer scientists. By the end of the last year of the Action, a *wrap up workshop* will be organised to present the achieved results and discuss the lessons learned with other stakeholders including, at least, an ENFSI representative. At the end of the workshop, a general meeting will take place and outline the transition from the network results to real products under the umbrella of one or more specific research projects. The participants will also study potentially relevant European and National funding programmes. Additionally, the workshop will be preceded by a pair of days of tutorials specifically directed towards young researchers.
A3.**Specific Meetings of each Working Group**. These meetings are specific for each WG in order to communicate and update the advances in each WG, every member of the Action will be invited to participate. Planned number: 2 by year for each WG.
A4.**Short-Term Scientific Missions**. These activities are very important and will be promoted by the members of the Action. Planned number: 10 by year.
A5.**Training Schools**: these fundamental activities will be held in summer. Planned number: 1 per year.

A6.**Dissemination Activities and Publications**. Dissemination is a priority. A key goal of the Action is the public disclosure its scientific results and concrete progress. Planned number: 2 by year.

The **deliverables** are listed below (with related task/WG):

D1. **Web and Societal Media (T9)**. A webpage, Facebook account, etc., will be created in order to publicly disclose the activities and advances of the Action.

D2. **Documents summarizing the advances of each WG**. Every year (at the end of every Grant Period) the WGs will publish a report providing the relevant information of the different studies carried out. One intermediate report will also be generated every year. (Task for each technical WG)

D3. **Proceedings of workshops and conferences**. After each conference or workshop organized by the Action, related proceedings will be edited. (Task for each organiser).

D4. **Material for Training Schools and Education (T11)**. For each training school and for University Courses, specific material will be created by the Action and by other invited companies. All this (non-confidential) material will be shared on the web page. Note that the Action is taking attention on the dual usage for offensive cyber tools.

D5. **Press releases (T10)**. This will be another tool for the dissemination of the advancements and results of the Action, also to make the general public aware of the Action's success cases.

D6. **Promotional material (T10)**. This material will be sent to every researcher, engineer or scholar related to the topic of the Action, also for distribution to conferences, workshops, etc.

D7. **Intermediate Report (T15)**. After 2 years an intermediate progress report will be prepared.

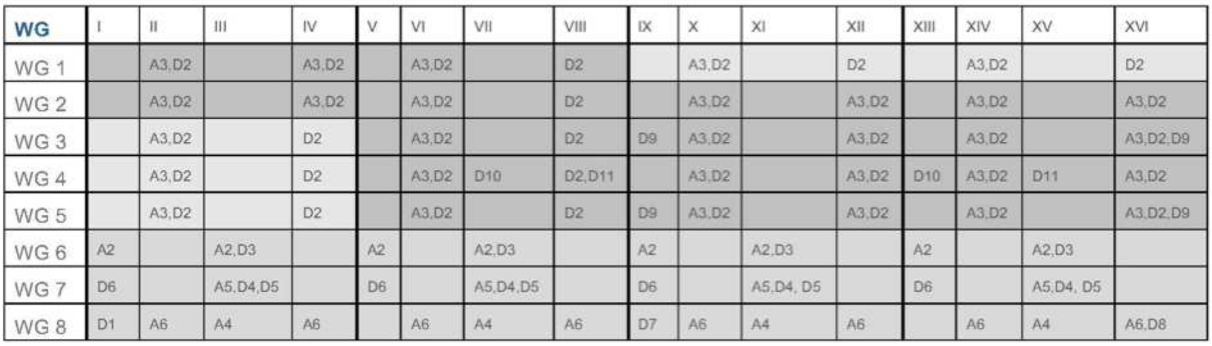
D8. **Final report (T15)**. A final report of the Action will be prepared.

D9. **Software prototypes** package (WG3, WG5). The network (mostly by WG3) will generate preliminary prototypes to automate aspects of the Evidence Analysis and thus provide evaluation elements to the human experts; such tools will be developed as proof of concepts by following suggestions of Action's DF experts; full-fledged implementation and, possibly, the deployment in real environments (under each country regulation) are left as goals for future specific research projects. Prototypes will be inserted in a software package published under Open Source software licence. Their deployment will be done preceded by a test process (see D10-D11).

D10. **Benchmarks suite**: the network groups (mostly WG4) will collect anonymised practical cases (acquired legally from the judiciary authority) that show representative and relevant features of real crimes, producing a first suite of benchmarks for testing the developed prototypes and extended later for future software tools implemented in research projects born from the network.

D11. **Tests reports:** experts (WG4 with help from WG3, WG5) will be also in charge of validation and verification as prototype testing, using benchmarks and past (solved) cases as a testbed. Performance measures will be defined based on the percentage of practical cases that the developed tools are able to successfully and coherently process.

3.1.2. GANTT DIAGRAM



WG	I	II	III	IV	V	VI	VII	VIII	IX	X	XI	XII	XIII	XIV	XV	XVI
WG 1		A3,D2		A3,D2		A3,D2		D2		A3,D2		D2		A3,D2		D2
WG 2		A3,D2		A3,D2		A3,D2		D2		A3,D2		A3,D2		A3,D2		A3,D2
WG 3		A3,D2		D2		A3,D2		D2	D9	A3,D2		A3,D2		A3,D2		A3,D2,D9
WG 4		A3,D2		D2		A3,D2	D10	D2,D11		A3,D2		A3,D2	D10	A3,D2	D11	A3,D2
WG 5		A3,D2		D2		A3,D2		D2	D9	A3,D2		A3,D2		A3,D2		A3,D2,D9
WG 6	A2		A2,D3		A2		A2,D3		A2		A2,D3		A2		A2,D3	
WG 7	D6		A5,D4,D5		D6		A5,D4,D5		D6		A5,D4, D5		D6		A5,D4, D5	
WG 8	D1	A6	A4	A6		A6	A4	A6	D7	A6	A4	A6		A6	A4	A6,D8

3.1.4. RISK AND CONTINGENCY PLANS

Potential risk 1: the most relevant risk in this Action is a lack of understanding and/or agreement between the two components, namely, researchers in AI and Automated Reasoning and experts in Digital Forensics (possibly belonging to Scientific Investigation Departments of Law Enforcement Agencies). In fact, the latter are very well acquainted with many practical and technological aspects of computer science and engineering, but have (often) little perception of the scientific aspects involved;

however, they are highly motivated to employ the Action's results in their everyday work. The former instead lack experience in the legal and normative aspects and are perhaps less familiar with technological aspects related to DF. To limit the risk, a significant effort will be devoted to mutual understanding via meetings, seminars, and joint activities, including the specific familiarization conference planned for the start of the Action. Also, and importantly, the Action's basic partners include Scientific Investigation Departments that have already cooperated with some of the research partners, via joint projects and by sending some of their employees to attend Ph.D. Programmes in Artificial Intelligence. The cooperation among institutions will be organized at a high level so as to be independent of the specific personnel involved.

Potential risk 2: what if there is a lack of consensus among partners among the modalities for performing the different activities and the lines of enterprise? The existing collaborations and mutual respect between participants will be invaluable in ensuring constructive dynamics within the Action. However, as the Action tackles some research issues that are open-ended, there is always the risk for disagreement. This risk will be managed by an agreed mechanism for decision-making, that will be explicitly devised as a first management step after the network's actual definition, applied where consensus proves difficult, to be specified in a suitable Collaboration Plan. If consensus is not reached, the partners agree to seek arbitration of external experts.

Potential risk 3: what about accounting? Operational decisions will be the responsibility of work group leaders, as defined in the Detailed Work Plan. Administrative issues will be dealt with through the Action Coordinator. Agreed-upon procedures defined in the Collaboration Plan will be used to resolve any difficulties, and will also establish modalities of communication among partners concerning advances, but also problems and risks that might arise, so as to dynamically devise plans for coping with them. The Action will not employ an external financial project advisor as the Academic Partners already have dedicated branches to perform this task.

Potential risk 4: what if the Action will lead, via its cooperation activities, to foster the future development of technologies with limited general applicability? The Action already involves also industrial participants with commercial interests and will try to attract more of them. These participants help steer the Action towards applicable technologies, thus mitigating this potential risk. Also, the basic partners are representative of different fields of AI and Automated Reasoning, thus encouraging an exchange of ideas which should lead to a wider perspective.

Potential risk 5: what if the Action will lead with the development of capabilities with follow-ups on research with only long-term applicability? This risk should be mitigated due to the participation of DF experts who are aware of the immediate realistic needs. Moreover, the detailed work plan includes a number of checkpoints on the relevance of the working group activities towards the practical development of useful tools also in the short-medium term.

Potential risk 6: what if the capabilities developed within the Action will foster the future development of technologies that external parties involved, namely judges, lawyers and the general public will not accept and/or rely upon? This risk is mitigated by the focus on verifiable technologies, but most importantly, thanks to the involvement of experts in law, social sciences and philosophy from the beginning of the Action: they will in fact help to formulate competences and results in a socially and legally acceptable and convincing way. For the general public, the results of collaborative exercises organized by the Action can be presented as success cases via the Action website, and on television and social media. This should increase the public awareness about effectivity, usefulness and reliability of AI techniques.

Societal, Ethical and Legal Implications and Risks: the use of personal data in order to tackle the investigation and prosecution of criminal activities is not new and it is at the core of the work that law enforcement agencies and other practitioners working in the field need to develop. The use of technologies that can enhance the capability of collecting and processing such data is currently a very discussed and controversial issue. The need to find a balance between freedom, justice and security has never been as significant as it is now, also due to the dual offensive use of the developed technologies. The Partners are aware that this is a highly sensitive topic for society and therefore are committed to develop the proposed Action in line with the principles of RRI (Responsible Research and Innovation) currently promoted by the European Commission. In this sense, the project will ensure the participation of stakeholders, academic experts and society in general in the discussion on:
i) how the application of AI to Digital Forensics may impact on society; and
ii) how can we maximize the positive impact and minimize the negative impact.

Furthermore, an ethical development of the project will be ensured by taking into account the European values and principles set up in the Charter of the Fundamental Rights of the EU and the European Convention for the Protection of Human Rights and Fundamental Freedoms. Moreover, the Action will take into account the EU's General Data Protection Regulation (GDPR).

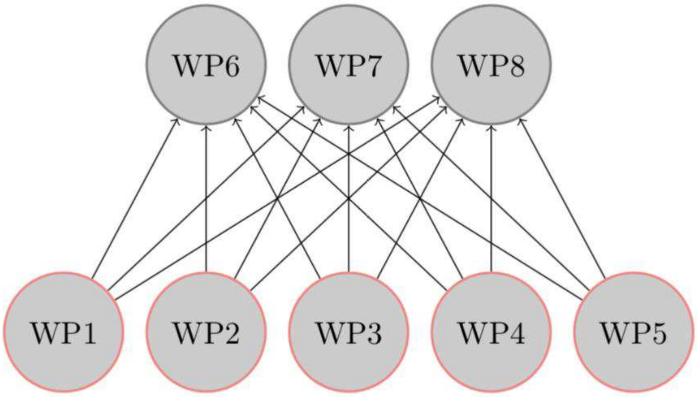
From a legal perspective the main risks that the proposed research entails are related to the protection of personal data. As Article 29 Working Party has stated "personal data processing which, in the general/common context, might not be perceived as a threat to fundamental rights may require particular attention when carried out in a law enforcement/judicial context, as the risks to fundamental rights become greater." (Article 29WP Opinion 03/2015, WP 233). The Action will take into account applicable EU legislation, international conventions and declarations pertaining. Mainly the new Regulation on the protection of personal data (General Data Protection Regulation (GDPR)) and the new Directive on the protection of personal data for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

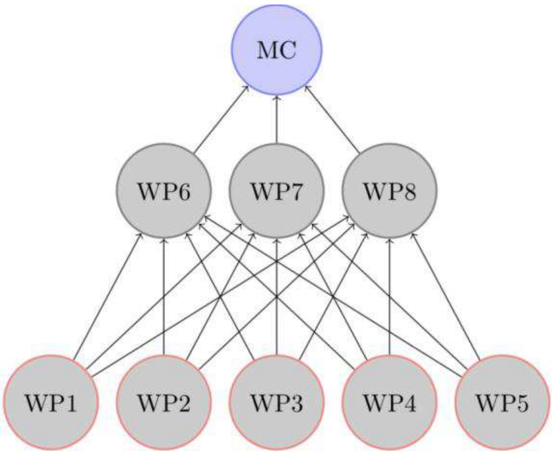
In order to ensure that the proposed activities are compliant with the requirements set up by these legal instruments, a specific strategy will be defined. This will involve an *ad hoc* and ongoing process of monitoring. The methodological approach to be used combines qualitative and quantitative methodologies according with the type of issues that need to be solved. First, an extensive empirical study will be carried out for the specific research context of DigforASP. The aim is to elicit and describe the needs of all the involved stakeholders in the field of digital forensics, and the possibilities offered by AI technologies. An active participation of all the stakeholders involved in DigForASP will be sought by the Action's experts on data protection from the beginning of the project. Second, to introduce an external perspective, the Action already includes European experts in the field of Data Protection and will involve other ones as external experts in order to supervise the measures adopted by the Action.

The proposal has been developed taking into account the data-protection-by-design requirement and therefore some risks have already been identified and measures adopted to minimize them:
i) all samples will be anonymised at the original source. This anonymity will be preserved during all the phases of data processing;
ii) the experts on data protection will ensure that the data are obtained in a lawful and fair way;
iii) adequate security and protection measures will be applied to assure the required level of protection: data transmitted will be encrypted, access to data will be registered in a strict log file, and backups will be encrypted;
iv) the data protection procedures will be validated with European and national experts and authorities.

3.2. MANAGEMENT STRUCTURES AND PROCEDURES

The proposed Action organisation and management structure will respect COST rules. In Section 3.1.1 the composition and responsibilities of the Management Committee and other WGs have been described. The workflow is summarized in the figure below.





- Decisions in each WG are taken by simple majority, with one vote per WG member. Note that WG6-8 are formed by 7 members one for each WG1-5 and the Action Chair or another person in the MC. Regular video conference conversations will be scheduled, besides the specific meetings (Activities A3).
- Decisions in WG6-8 on external requests (from other WGs, ad-hoc participants, etc.) will be issued within one month from their submission. Approval of short-term scientific missions is given by the WG leader in consultation with the co-leaders. Decisions on workshops, conferences and training schools are made by the MC upon recommendations from the relevant WGs.
- Each WG will have its own mailing list. This will be handled by the WG leader and will be used to communicate the decisions to the corresponding WGs or to external requesters, to distribute documents of the Action, etc.
- In the selection of leaders and co-leaders of the WGs a gender balance will be sought. Note that maintaining a gender balance overall is an objective of the Action.
- All Privacy, Data protection prevention, ethical issues, etc., will be accomplished according to COST Association rules.

3.3. NETWORK AS A WHOLE

The initial network includes highly qualified experts from relevant areas, many of whom have a strong track record of international collaborations. The composition of ENFSI shows a strong presence of Inclusiveness Target Countries (ITCs) of COST and many of these countries are represented in the Action (ITCs currently form over half of the countries represented). In addition, two COST Near Neighbour Countries (NNCs) are initially involved, which will increase. As we commented in Section 2.2.1, ITCs and NNCs will carry out a specific dissemination with conferences in these countries, press releases, promotional materials, etc. Moreover, the leaders and co-leaders of the WGs will be chosen mainly from the ITCs and NNCs partners.

Therefore, the participation from ITCs and NNCs will be increased through dissemination activities and events specifically targeting these countries. Such efforts will involve not only their Forensic Departments but also researchers, scholars and other relevant stakeholders. The proposal already includes Digital Forensic Departments and Organizations of Law Enforcement Agencies as members, and more of them will be contacted and involved in the future, also as a by-product of dissemination of the Action’s results. However, the needs and specificities of these third countries are different from the ones of COST Member Countries: hence, involving them is fundamental and will be a priority. Overall, there is already the critical mass of expertise and a geographical distribution needed for addressing the challenge and the objectives of this Action. This will be used to attract new valid collaborators and stakeholders.