



Spoke 1

DISE

Digital Sovereignty

PI: Fabio Martinelli (fabio.martinelli@iit.cnr.it)

Partners

CNR (Institutes IAC, ICAR, IIT, IRCRES, ISTI)

Abstract

Digital sovereignty entails capability of citizens, organizations and states to control their data, usage of such **data** and their **computations** and ensure those are compliant with business rules, laws, social norms, usability, privacy and/or other **human, social, and legal (HSL)** aspects.

We study **methods** to extract knowledge and rules and then translate those into data and computation usage policies and verify these policies and assess their **compliance**; we build mechanisms **for data usage control** enforcement for scenarios as iot, big data, cloud...

- **Economic** aspects as understanding costs and incentives for data sharing, and the value of data sovereignty and interactions and conflict management between laws and market
- We study **data sovereignty and trust models** for **trustworthy AI**, providing proper data collection, aggregation, fusion and corresponding policies on derived data/algorithms.
- Data are also instrumental to full situation awareness for **threats to on line services**. We need specific technologies for ensuring data sovereignty of cyber threat intelligence (CTI), providing data credibility and integrity, mandatory data routing and compliant data flow control

A main focus is on **confidentiality and compliance of computations** that should be done in agreement with laws, norms and standards, in particular for secure analytics, as application of **AI for social security**:

- We research in privacy preserving computation, social behavior analysis, and analytics for malware/ransomware



- Once we have full spectrum awareness of cyber and physical threats through proper data sharing and analysis
- Advanced testing approaches for access and usage control policies will be defined and developed.

We plan Lab validation of methodologies/tools in at least ones of the possible scenarios as **smart grids, social communities, transport or e-health.**

WP Breakdown Structure

WP1 - Analysis of laws and regulations for DiSe

Task 1.1 - Analysis of the safety requirements deriving from the study of laws and regulations on digital sovereignty.

Partners involved in the execution of the task: OC

Task Description: This task will analyze the requirements driving the laws and regulations for digital sovereignty, considering security and privacy issues. The investigation will consider, e.g., GDPR implications to potential problems of mass surveillance. It will also consider aspects for data usage and sharing, and risk management, as it follows from relevant directives, e.g. the NIS ones.

Task 1.2 - Technologies to support digital sovereignty, in particular for the semi-automatic definition and understanding of regulations

Task 1.3: Analysis of some socio-economic aspects of digital sovereignty



WP2 - Digital sovereignty and regulatory compliance

Task 2.1 - Models for digital sovereignty, management of trust and identity in on-line services, and control of the use of data in accordance with regulations

Task 2.2 - Collection of reliable data for trustworthy AI - data sovereignty for AI and secure management of information on cyber and non-cyber threats, in accordance with regulations.

Task 2.3 - Techniques for monitoring network traffic compliance with the rules imposed by digital sovereignty and detection of possible violations

Partners involved in the execution of the task: OC

Task Description: This task will model and study the security aspects of virtualized network scenarios both on remote and local Networks. The objectives are a better understanding and awareness of the security implications and requirements imposed by the implementation of the regulations regarding network traffic.

WP3 - Development of secure, privacy preserving and reliable methodologies for Digital sovereignty and laboratory validation in specific domains such as energy and transport

Task 3.1 - Methods and techniques to guarantee the privacy and confidentiality of computations in distributed environments in accordance with current regulations and with associated dynamic risk management also in cloud infrastructures

Task 3.2 - Methodologies for the secure development of technologies for digital sovereignty, including usability aspects and awareness

Task 3.3 - Development and validation of technologies in laboratory of the previous methodologies applied in particular to the energy and transport sector

Partners involved in the execution of the task: OC

Task Description: This task is devoted to the application of the previously descriptive approaches in several scenarios, we envisage at least the energy and the transport ones. The validation and experimentation are planned in laboratory.

