

TECHNICAL ANNEX

1. EXCELLENCE IN S&T AND NETWORKING

A. MAIN CHALLENGE

The widespread reliance on software and digital systems has prompted both local and international efforts to regulate its operation through legislation. Paradigmatic examples are European laws such as the General Data Protection Regulation (GDPR) or the AI Act, the UK Data Protection Act, the French Loi pour une République Numérique. Also, regulatory aspects of digital systems and software are present in different sectors such as e-finance, health systems, education, etc. A very cogent issue is the ethical imperative on AI, the human rights perspective, its ecological impact, its geo-political implications, etc.

In the following, we will refer to digital systems and software, as well as, hardware and physical devices as **digital solutions**.

Legal texts and regulations are technical and strive for being formal and precise, yet they can be subject to multiple interpretations as they are framed in natural language. For instance, this is the case with several regulations designed to prevent the manipulation of consumers of digital services: [1]

the EU regulation 2022/2065 on a Single Market For Digital Services prescribes that “the maximum amount of the fine that may be imposed for the supply of incorrect, incomplete or misleading information, failure to reply or rectify incorrect, incomplete or misleading information and failure to submit to an inspection shall be 1% of the annual income or worldwide turnover of the provider of intermediary services or person concerned in the preceding financial year”;

the GDPR forbids *unfair* data processing techniques;

the AI Act forbids practices aimed to “the placing on the market, the putting into service or the use of an AI system that deploys subliminal techniques beyond a person’s consciousness or purposefully manipulative or deceptive techniques”.

Besides introducing coordination and interpretation in conjunction with other legislation (such as the competition law), this proliferation of regulations shows that there is an extremely high level of complexity in the precise legal boundaries of (properties and requirements of) digital systems [1]. Moreover, the form of these documents can be more *descriptive/permissive* (defining rights, statuses, or situations without imposing action) than *normative* (defining duties, obligations and how to ensure them), also depending on their position in the hierarchy.

In contrast, digital solutions must be defined in formal languages in order to meet their requirements when used in the field. This fundamental mismatch hinders effective enforcement of legal aspects and can result in the misapplication of the law.

The aim of this Action is twofold in order to fill the significant gap that remains between *legal frameworks* and the *digital solutions*: on one hand to validate digital solutions against the legislation governing them and, on the other hand, to develop approaches to support legal processes through sound digital solutions.

A number of specific problems are being addressed by different communities:

P1. What are the models amenable to automation and suitable to support formal and precise human-based analysis

P2. How to extract algorithmic models for normative aspects of legal texts.

P3. How to determine inconsistencies and inadequacies in the models extracted.

P4. How to assess efficiency and efficacy of the verification methods use in terms of decidability, complexity, resource requirements, modularity

P5. How to determine if algorithmic solutions should be applied or not?

P6. How to establish the adequacy of state-of-the-art digital solutions for supporting the realisation of legal requirements?

Addressing these problems requires a coordinated effort. We need a community building initiative to create the critical mass to understand these problems both from the regulators and from the digital developers point-of-view. As observed in [2] “debating some issues intelligently required not just a knowledge of law or of technology, but of both. That is, some problems cannot be discussed purely on technical grounds or purely on legal grounds; the crux of the matter lies in the intersection.”

Despite the fact that Computer Science (CS) has important legal applications (and it is offered to students in some departments of humanities subjects as an optional module), it is far apart from Law or Socio-Political and Human Sciences. The construction of common grounds starts from the reconciliation of the different interpretations of seemingly similar concepts adopted in these disciplines. A paradigmatic example is the notion of ‘formality’ which in CS refers to mathematical and logical rigour amenable to the development of computational systems while in e.g., Law ‘formality’ may primarily refer, especially when legal practitioners and academics use it in argumentation either of legal concepts constituting the structure of law or of authoritative sources [3]. Ultimately, our aim is to propose approaches and tools to make sure the adoption of digital solutions leads to practices following the laws regulating them.

B. OBJECTIVES

The Action aims to bridge the gap between digital solutions and the legal frameworks that govern them. To achieve this goals, we focus on two key intermediate components:

Models that suitably represent regulations, such as logical rules in the case of laws, or workflows in the case of judicial and administrative procedures;

Verification/Audit methods that ensure these formalised regulations are upheld by digital solutions, such as consistency checks or *on-field* monitoring.

Specifically, our scientific objectives are:

SO1. *Extract normative key elements from regulations.* Laws for digital solutions comprise *neustic* components (i.e., normative parts) that need to be told apart from *phrastic* ones (i.e., descriptive parts) and be turned into prescriptive requirements in order to give tangible mandatory obligations that can be automatically converted in checking tools. Like Taxation Law is algorithmic, and thus automatically calculatable, law in this domain should clearly identify what needs to be enforced. We aim to identify approaches to automatically tackle such mandatory obligations (cf. P1).

SO2. *Support the analysis of descriptive regulations.* As noted, not all legal requirements can be faithfully captured within digital solutions – many laws set out general principles or rights that usually can hardly be given a computational interpretation. We will define mechanisms (tools, procedures, best practices) to bridge this gap, enabling digital solution designers to work with legal experts and social scientists in assessing compliance with such principles. For example, while a law might broadly require “fairness” or “transparency” in an AI system, our Action will produce guidelines and adaptive software components that help auditors and domain experts judge whether those qualitative standards are met in practice. This interdisciplinary approach (cf. P1, P2) ensures that even high-level legal expectations can be monitored and verified in digital solutions with appropriate human judgement involved.

SO3. *Realise law-compliant digital solutions.* The introduction of legislation like the EU Data Act or GDPR imposes that new digital solutions guarantee their norms. Current practices to assess compliance include . However, these usually concern aspects of software that are weakly related with its behaviour, often falling short of guaranteeing that the code follows the law. This advocates either for - effective tools to build and automatically assess the compliance of digital solutions to such obligations (cf. P1 and P3), whenever these can be formalised; or - approaches based on, e.g., check-lists, experts’ analysis, users’ feedback, etc., when formalisation of some criteria is not possible/desirable (cf. P5 and P6).

SO4. *Assessing how digital solutions respect regulations.* It is commonplace for stakeholders to claim compliance with various sort of regulations without clear evidence. Existing tools are still experimental and there is no consensus on which elements and requirements need to be included. This calls for identifying and enhancing auditing processes, developing tools and (semi-)automatic techniques to assess such claims, to identify pitfalls, and to verify that legal requirements are respected. Moreover, interoperability issues of digital solutions have to be taken into account. Besides, this objective requires the development of common vocabularies (cf. P4).

The Action will create an inclusive network of European researchers and foster lasting collaboration beyond its lifetime that will shape future interdisciplinary research, promote excellence, and support Early Career Investigators and increase their visibility. This will be achieved pursuing the following organisational objectives:

OO1. *Knowledge advancement.* Build reference methods for the specification, analysis, and implementation of legal aspects of digital solutions as well as news about publications, and tools (such as guidelines, good practices, software tools, tutorials, illustrative use cases, etc.)

OO2. *Community building.* Bring together members of the different European communities working on legal aspects of digital solutions, specifically the communities around symbolic and data-driven AI, natural language processing, formal methods, law (including financial regulations and taxation), political sciences, and social sciences.

OO3. *Training.* Ease access to the topics of the Action in education and other areas of science, by organising training courses, summer schools, workshops, and publishing technical papers, position papers, and tutorials.

OO4. *Networking.* Foster interdisciplinary collaborations among participants of the Action through intensive use of Short Term Scientific Missions (STSM) and educational programs. Support young researchers in developing their research network for a fruitful career in an international environment.

OO5. *Transfer knowledge.* Create the opportunities to transfer expertise, scientific tools, and human resources across the different disciplines, between academia and industry, and between academia/industry and public administration.

OO6. *Inclusiveness.* Support young researchers, under-represented groups, and teams from regions with less capacity, allowing them to establish scientific collaborations with leading groups across Europe, participations to scientific events, involving them in the initiatives of the Action.

OO7. *Communication and Dissemination.* Foster the impact of the Action by disseminating its results to the scientific community and communicating it to other stakeholders in industry, certification bodies, European institutions, and the general public.

C. STATE-OF-THE-ART

Nowaday, digital solutions are often ensembles of components, each developed for a specific purpose, and interacting with people or even the physical environment. This yields a high degree of complexity that sets digital solutions among the most elusive critical infrastructures of modern societies. In fact, guaranteeing the correctness of digital solutions is notoriously very challenging. In particular, legal and regulatory requirements add further challenges to this endeavour because, on the one hand, such requirements are described in technical jargon that developers can understand only with intense liasons with domain experts and, on the other hand, the adoption of digital solutions is sometimes decided without properly pondering the feasibility or the impact on other technical and societal facets. The following quotes are representative of this state of affaire:

- “Today, all privacy regulations around the world are based on the 50-year-old paradigm of notice and consent. It no longer works. The systems we deal with—web pages with their multiple levels of advertising, the Internet of Things, and more—are too complex; consumers have no idea what sites they are contacting nor what their privacy policies are.” [5]
- “A legal rule may have multiple semantic annotations, where each annotation can represent a different legal interpretation.” [4]

[SC&FM2](#)

[GDPR ComplianceX](#)

[Bits of FreedomX](#)

D. RATIONALE FOR CHOOSING NETWORKING TO ADDRESS THE MAIN CHALLENGE

The complexity of the problems discussed above is high due to two main factors: (i) the ample gap between CS and (ii) the fragmentation of regulatory and legal practices among different sectors and countries. This separation has a negative impact on the realisation of digital solutions that actually realise the intentions of regulators as well as the development of practices that do not effectively verify the adequacy of digital solutions. Besides the impact on economic costs, not tackling this problems can cause distortion in democratic processes, in the application of human rights, in correct relations between citizens and institutions.

A networked approach is essential to tackle the main challenge because of its interdisciplinary and pan-European nature. The gap between legal frameworks and digital solutions is too broad and complex for any single research group or field to handle. Only a concerted network can assemble the necessary critical mass of expertise –from legal theorists and CS communities and developers to sociologists and domain experts– to address all facets of the problem.

A COST Action is the ideal instrument: it enables collaboration across countries and disciplines, ensuring that solutions are not one-dimensional or siloed. By networking, we avoid duplicate efforts and instead coordinate research and create the opportunities to identify and study research themes that could have hardly been discovered by separated communities. For example, one working group can develop formal models of laws while another tests those models on real software systems, providing immediate feedback on the one hand while, on the other hand, spotting the limits of traditional techniques and practices that can be overcome only by developing new approaches.

The Action will facilitate this via frequent workshops, cross-disciplinary working groups, and Short-Term Scientific Missions (STSMs) that allow researchers to visit each other's institutions to transfer knowledge and tools. The Action will also develop a new generation of researchers with interdisciplinary skills through the planned training activities, the mentoring activities, and the schools. All these activities are crucial to build a community involving experts, Non-Governmental Organisations (NGOs), human rights activists, etc. that will systematically investigate the borders between regulatory frameworks and theoretical and applied CS.

These instruments will knit together a community that speaks a common language across law and tech. Furthermore, the challenges and their solutions have a strong European dimension. Regulations like the GDPR or AI Act must be implemented uniformly across Member States; sharing methods through a European network ensures that a tool or guideline developed in one country can benefit all. The network will include participants from across Europe (with particular encouragement to those from less research-intensive countries) to maximize diversity of perspectives and to build capacity where it's needed – reflecting COST's mission of spreading excellence.

E. CRITICAL MASS OF THE NETWORK

The Action's network of proposers consists of 13 COST countries, 7 of which are ITC (Cyprus, Czech Republic, Greece, Malta, Portugal, Serbia, and Ukraine) and include scholars with a proven track-record of high-impact publications in several fields ranging from (non-)symbolic AI, NLP, theoretical CS, formal methods, Law, Anthropology, Philosophy of Law, Logics and Metamathematics, and medical physics distributed over 24 institutions. Many secondary proposers have established relations with institutions hosting relevant stakeholders such as NGOs, human rights activists, medical sectors, economy. Also, many proposers have collaborated in the context of past other COST Actions and MSCA networks (in some of which they had leadership roles). In particular, the Action involves proposers specializing in technology law (data protection, AI regulation, cybersecurity law, etc.) and public policy experts. This will ensure that the Action's outputs will be grounded in legal reality and aligned with European and national legislative contexts. For instance, team members with backgrounds in European studies and public administration will connect the Action's work with EU digital strategy and governance frameworks.

This varied consortium will actively seek out for new participants to grow the critical mass with particular attention to gender and geographical balance and, quite crucially, striving to engage young researchers. The Action's main aim is to create a long-lasting community and a new generation of researchers with interdisciplinary competences that can tackle the challenges described above. All the proposers are well-known and renowned academics in their field. The initial network therefore ensures a good balance of emerging and innovative talent and established expertise.

2. IMPACT

A. IMPACT RELATED TO OBJECTIVES

Impact on Governance, Trust and Society (O2 & O4).

The Action's work on handling descriptive regulations and auditing (O2 and O4) will directly impact how AI and digital systems are governed and perceived in society. We will propose practical processes for human-in-the-loop auditing of algorithms – empowering regulators, certification bodies, or independent auditors with better techniques to inspect and certify AI systems. For example, outcome of O4 could be a guideline or even a prototype “AI Compliance Certificate” that stakeholders can use as evidence of adherence to laws (aligning with mechanisms like GDPR's voluntary certification and the AI Act's conformity assessments). This boosts transparency and accountability of digital solutions, helping to increase public trust. Citizens and end-users ultimately benefit because they can be more confident that certified systems respect their rights (no unlawful bias, proper data protection, etc.). Moreover, by involving social scientists and ethicists, the Action will ensure that notions of fairness, transparency, and accountability are translated into technical criteria – this can inform policymakers' ongoing efforts to operationalize ethics in AI. The broader societal impact is a contribution to “Trustworthy AI” in Europe: technology that is not only innovative but also aligned with legal and ethical norms, thereby fostering social acceptance.

original version

The ultimate impact result we aim at, in the timeframe of the action, is a set of formal guarantees developers should provide to show they abide to EU regulations, namely to the GDPR or the Data Act.

These guarantees will be proposed to constitute a certificate of conformance

and should be simple to automatically extract from critical parts of the code dealing with the sensible data. The required tools should be developed and validated according to recommendations resulting from the work of this action.

Regarding objective O1,

TO BE DEVELOPED

B. INVOLVEMENT OF STAKEHOLDERS

The Action intends to foster the involvement of stakeholders from different communities by establishing a Stakeholder Advisory Board (SAB) to ensure that the Action's methodologies align with regulatory expectations.

NGOs

Standardisation Organisation The Action will liaise with European standardisation organisations to realise the standards advocated in regulations. For instance, according to the Data Act the European Commission may demand European standardisation bodies to harmonise standards to enable vendors of smart contracts to establish data-sharing agreements for the correct data manipulation from third

parties. The Action's results can attract such standardisation bodies also through existing collaborations with some of the Action proposers.

Regulators and Policymakers The Action will include liaisons with European and national regulatory bodies. We intend to involve representatives from the European Commission (for instance, officials working on the AI Act and Data Strategy) and national Data Protection Authorities or AI oversight agencies. The Action will invite members of the European Data Protection Board (EDPB) or EU's High-Level Expert Group on AI (or its successor bodies) to provide feedback on our "formal guarantees" approach. Engaging regulators early means our proposed certification or audit frameworks could be considered in future policy refinements.

Industry and Public Sector Among the Action's proposers there are researchers that collaborate with companies, public administrations, and no-profit organisations that will be involved on the SAB.

Academia

C. COMMUNICATION, DISSEMINATION AND VALORISATION

The dissemination strategy will hinge on OA publications and a public website collecting the Action's results, advertising events related to the Action's topics, and linked to popular social media.

3. IMPLEMENTATION

A. ACTION STRUCTURE

Building on the experience obtained in the participation and leadership of previous COST actions and MSCA networking projects, the coordination of the Action and of its activities will be in accordance with the COST principles in order to foster inter-disciplinary and trans-disciplinary research. Particular attention will be given to inclusiveness and diversity which the action will value by implementing policies to avoid any kind of discrimination.

The **Management Committee** (MC) will coordinate the Action promoting professionalism and establishing a cooperative and inclusive attitude in the governance, management, and execution of the Action's activities. The MC will foster participation in the decision making process of the Action and appreciate constructive comments from the members of the Action and promptly manage risks or react to unexpected circumstances. The MC will strive for objectiveness and impartiality.

The MC, presided by the Action Chair, will elect a Vice-Chair who will assist the Action Chair. The MC will meet every year during the annual Action Workshop which will be organised as a satellite event of major flagship international conferences. The workshop will be open to all Action participants, advertised on through main social media (e.g., LinkedIn, thematic mailing lists, etc.) to attract the participation of interested people, and will feature invited speakers from scientific, governmental, and industrial institutions.

The **scientific activities** of the Action will be carried out in the following Working Groups

WG 1: Legal requirements of computing infrastructures <ADD A PARAGRAPH DESCRIBING HOW THE WG RELATES TO THE OBJECTIVES IN SECTION I.B>

Tasks: <GIVE A LIST OF TASKS BY COMPLETING/MODIFYING THE ONES BELOW - Approaches and standards - Categorisation of legal requirements (general principles, code of conduct, regulations, etc.) - Capabilities and limitations >

Activities: <GIVE A LIST OF ACTIVITIES THAT THE WG WILL CARRY OUT AS THE ONES SKETCHED BELOW e.g., The WG will coordinate the definition of a taxonomy of legal requirements, meetings with external experts, consultations with members of official and standardisation bodies... >

Deliverables: <GIVE A DESCRIPTION OF 1/2 DELIVERABLES e.g., - Glossary of common terms adopted in different domains - Survey of common practices/tools - Comparison of certification procedures - ... >

WG 2 ((Graca + Raphael)): Analysing legal requirements

Assessing positive/negative effects

Framing ambiguous/ambitious regulations

Assessing how key requirements are realised in computing infrastructures

Identifying techniques and practices for validation via automatic analysis (via e.g., static or dynamic techniques) or manual analysis (via e.g., experts' judgement, auditing)

This Working Group directly contributes to SO1, SO3, and SO4 of the Action. With respect to SO1, it develops methodologies to identify and extract prescriptive obligations from legal texts and translate them into operational requirements. In line with SO3, it supports the design of digital solutions that are compliant with such obligations by clarifying how legal requirements can be embedded into development and auditing practices. Finally, in accordance with SO4, it enhances verification and auditing by assessing how digital solutions effectively respect regulatory demands, providing tools and practices to validate compliance claims and detect shortcomings. In order to perform these tasks, this working group will gather experts from academia, administrations and NGOs to ensure a diversity of viewpoints and backgrounds.

Tasks: - Creating a community of experts from various backgrounds interested in legal requirements and their analysis. - Mapping key legal requirements (e.g. transparency, fairness, accountability) to concrete features of computing infrastructures. - Identifying and classifying techniques for validation and compliance checking, including automatic methods (e.g., monitoring) and manual methods (e.g., expert judgment) - Defining methods to test, or certify, how digital solutions respect legal frameworks.

Activities: - Create a glossary of terms related to legal frameworks and digital solutions, in order to ensure experts with various backgrounds (computer science, law, ...) can understand each other. - Produce reference case studies demonstrating how legal requirements can be operationalised and validated in real-world systems. - Study previously operationalised legal requirements and their impact on real-world systems.

WG 3 ((Joost + Jelena)): From regulations to digital solutions and back

Narrowing gaps (requirement elicitation, Natural Language Processing, generative or symbolic AI, machine learning, formal methods, etc.)

Explainability and transparency

Validation of digital solutions (via techniques such as reachability and satisfiability analyses, type checking, model checking, runtime verification)

Evaluation of mechanisability of legal requirements of digital solutions and of their applicability (degree of biases of classification algorithms, procedures' fairness, ecological impact of AI-based systems, etc.)

WG 4 ((Mohammed + Federico)): Socio-Political implications between legal requirements and digital solutions

Enforcing Sovereignty, Fundamental Rights, Ethical Principles

Impact of digital solutions in the large (e.g., ecological impact of GenAI, digital warfare, biases in algorithmic recommendation systems, etc.)

...

WG 5 ((Giovanni + Dragisa)): Application areas

Identifying interesting case studies in different domains (health systems, finance, public administration, taxation, etc.)

Analysing concerns specific to some application domain (e.g., ethical requirements are more relevant to the health domain than to online trading)

Exploring generality, applicability, limitations of tools/techniques/approaches (both current and new ones)

Refining/adapting approaches/tools to specific contexts and across domains

WG 6: ???

The MC will appoint a chair and a co-chair for each WG. All WG chairs and co-chairs will report on the progress of their WG at MC meetings. Interactions among WGs will normally take place on-line (via email or common video conferencing platforms) as well as with in-person meetings; in particular, there will be a yearly WG meetings.

A main device to tackle fragmentation of research will be Short-Term Scientific Missions (STSMs). The Action will strive to establish a smooth application procedure to run STSMs. The MC will appoint a small committee responsible to set regular deadlines for applications and advertise those properly across the various scientific communities. The committee will also evaluate STSM applications.

The Action will actively promote participation and training of young researchers both through STSMs and organising training events intended for PhD students and early-career researchers. Specifically, the Action will organise two main training schools, one in Year 2 and another one in year 4.

The Action will set up and maintain a website to host a discussion forum, to ease the communication among MC and WGs as well as among the Action Participants, and to support dissemination of the results of the Action. The Website manager, appointed by the MC, will be responsible for the website.

B. WORK PLAN (TASKS, ACTIVITIES AND TIMEFRAME)

Text

C. DELIVERABLES

D1.1 Survey on State of the art and standards

D1.2 White paper to identify opportunities/obstacles

D1.3 Online collection of tools, practices, regulations

D3.1 Guidelines

D3.2 Code of practices

D3.3 Tool support ### D. Gantt chart

References

[1] Sabine Bernheim-Desvaux, Juliette Sénéchal. Vers un droit neuro-éthique ?. Bibliothèque de l'Institut de Recherche Juridique de la Sorbonne – André Tunc, Tome 136, June 20255.

[2] S. M. Bellovin. Computer Science and the Law. CACM Vol. 68 No. 6

[3] M. I. Niemi. Form and Substance in Legal Reasoning: Two Conceptions. Ratio Juris. Vol. 23 No. 4, 2010

[4] M. Palmirani, G. Governatori. LegalRuleML Core Specification Version 1.0. OASIS Standard, 2021

[5] S. M. Bellovin. Rethinking Privacy Regulation, GWJOLT, vol. 1, 2025