L'impatto della regolamentazione della cybersicurezza nella dimensione esterna dell'azione dell'Unione europea

Descrizione del Progetto di ricerca

La ricerca, che si svolge nell'ambito del partenariato esteso PE7 SERICS (*SEcurity and RIghts In the CyberSpace*) Spoke 8, affronta i profili giuridici e informatico giuridici della gestione dei rischi in ecosistemi cyber-fisici del futuro. Proporre metodi e soluzioni originali per contribuire alla resilienza informatica dei futuri sistemi e servizi caratterizzati da componenti digitali sempre più interconnessi e intrinsecamente vulnerabili, come richiesto dall'Unione europea attraverso le direttive NIS e NIS2, nonché dall'Agenzia Nazionale per la Cybersicurezza (ACN) rappresenta l'obiettivo prevalente del progetto EcoCyber (*Risk management for future cyber-physical ecosystems*), in cui la ricerca si colloca. Il progetto, seguendo un approccio multidisciplinare, pone le basi per una visione olistica della cybersicurezza, che includa anche la resilienza, la privacy, e la sicurezza delle organizzazioni, delle industrie, delle infrastrutture critiche e delle relative filiere - prerogativa essenziale non solo per la fiducia e l'utilizzo dell'innovazione e della connettività, ma anche per sostenere i diritti e le libertà fondamentali degli individui.

Tale impostazione è al centro della *Strategia dell'UE per la cibersicurezza per il decennio digitale* del 2020 (JOIN/2020/18 final), che prevede non solo il rafforzamento degli strumenti normativi già esistenti, ma anche l'adozione di nuovi per costruire un'Unione resiliente e digitale. Nello specifico, tre sono le esigenze illustrate nella Strategia: 1) resilienza, sovranità tecnologica e leadership; 2) sviluppo delle capacità operative volte alla prevenzione, alla dissuasione e alla risposta; e 3) promozione di un ciberspazio globale e aperto. Al fine di aumentare il livello di cyberresilienza e cybersicurezza è stata promossa una serie di interventi normativi: un regolamento (il *Cyber Resilience Act*) volto a introdurre requisiti di sicurezza essenziali per i dispositivi interconnessi via Internet per inviare e ricevere dati; una revisione mirata del *Cybersecurity Act* per rafforzare il ruolo dell'ENISA e il sistema di certificazione obbligatoria sui prodotti informatici; e, infine, un regolamento volto ad introdurre un meccanismo di prevenzione, preparazione e risposta a minacce cibernetiche su larga scala (*Cyber Solidarity Act*).

In questo contesto, la ricerca in ambito di diritto dell'Unione europea si concentra sul quadro normativo sovranazionale in materia di cybersicurezza per tracciare i principali elementi in tema di *governance* e problematizzare i più recenti sviluppi normativi rispetto all'impianto costituzionale dell'UE.

Piano delle attività

Tenuto conto del necessario coordinamento con i risultati già prodotti dal gruppo di ricerca dello Spoke 8, l'assegnista dovrà concentrarsi sugli sviluppi normativi più recenti in materia di cybersicurezza, con particolare riferimento alla dimensione esterna e, nello specifico, alla politica commerciale comune anche alla luce del necessario coordinamento con la dimensione della sostenibilità connessa a tale politica. Ciò consentirà, peraltro, di rafforzare il rapporto sinergico con altre componenti universitarie partecipanti al medesimo Spoke 8.

Questa valutazione relativa alla proiezione esterna della strategia di cybersicurezza dovrà poi necessariamente tenere conto della dimensione valoriale e costituzionale dell'UE. A tal fine, l'assegnista dovrà svolgere un'analisi critica sull'utilizzo degli strumenti giuridici di cybersicurezza nella costruzione di una sovranità digitale/tecnologica europea nell'ambito della più ampia nozione di autonomia strategica dell'UE.

All'assegnista sarà richiesto di contribuire all'organizzazione delle attività divulgative e scientifiche e di pubblicare almeno 2 contributi sui temi oggetto dell'assegno nonché su altri filoni di indagine che vengano individuati di concerto col personale strutturato impegnato sul Progetto.

The impact of cybersecurity regulation on the European Union's external dimension

Description of the research project

The research, carried out under the PE7 SERICS (*SEcurity and RIghts In the CyberSpace*) Spoke 8 Extended Partnership, addresses the legal and cyber-legal profiles of risk management in future cyber-physical ecosystems. The overarching objective of the EcoCyber project (*Risk management for future cyber-physical ecosystems*) is to propose original methods and solutions to contribute to the cyber resilience of future systems and services characterised by increasingly interconnected and inherently vulnerable digital components, as requested by NIS and NIS2 as well as by the National Cybersecurity Agency.

Following a multidisciplinary approach, the project lays the foundation for a holistic view of cybersecurity, including resilience, privacy, and the security of organizations, industries, critical infrastructures, and related supply chains-essential prerogative not only for the trust and use of innovation and connectivity, but also for sustaining the fundamental rights and freedoms of individuals.

This approach is at the heart of the 2020 EU's *Cybersecurity Strategy for the Digital Decade* (JOIN/2020/18 final), which envisages not only strengthening existing regulatory tools but also adopting new ones to build a digitally resilient Union. Specifically, there are three requirements outlined in the Strategy: 1) resilience, technological sovereignty and leadership; 2) development of operational capabilities aimed at prevention, deterrence and response; and 3) promotion of a global and open cyberspace. In order to raise the level of cyber resilience and cybersecurity, a series of regulatory interventions have been promoted: a regulation (the *Cyber Resilience Act*) aimed at introducing essential security requirements for devices interconnected via the Internet to send and receive data; a targeted revision of the *Cybersecurity Act* to strengthen the role of ENISA and the mandatory certification system on cyber products; and, finally, a regulation aimed at introducing a mechanism for prevention, preparedness and response to largescale cyber threats (the *Cyber Solidarity Act*).

In this context, the research in the field of European Union law focuses on the supranational regulatory framework on cybersecurity to trace the main elements in terms of governance and critically investigate the most recent regulatory developments with respect to the EU constitutional framework.

Description of the activities

Taking into account the results already produced by the Spoke 8 research group, the research fellow will have to focus on the most recent regulatory developments in cybersecurity, with particular reference to the EU external dimension and, specifically, to the common commercial policy, also in the light of the necessary coordination with the sustainability dimension related to this policy. This will, moreover, allow strengthening the synergistic relationship with other academic members of the same Spoke 8.

The assessment regarding the external projection of the cybersecurity strategy will then necessarily have to consider the EU's values and constitutional dimension. To this end, the research fellow will

conduct a critical analysis of the use of cybersecurity legal instruments in the construction of European digital/technological sovereignty within the broader notion of EU strategic autonomy.

The research fellow will be required to help organize dissemination and scientific activities and to publish at least 2 articles on the topics covered by the research project as well as on other lines of inquiry that are identified in consultation with the structured staff engaged on the Project.