Finanziato dall'Unione europea NextGenerationEU | Ministero dell'Università e della Ricerca | Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA | ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA

ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA | DIPARTIMENTO DI SCIENZE GIURIDICHE

Policing with Big Data: Cybersecurity and the Other Risks of Data-Driven Control in Digital Societies

One-day Workshop, 27 October 2025

Department of Legal Sciences, University of Bologna

Via Zamboni 27/29, Bologna (BO)

The increasing use of data-driven technologies in policing raises serious concerns about the risks involved in using big data for prevention, investigation, and surveillance. These risks include not only the protection of personal data—of both citizens and non-citizens—held by police forces from external attacks and privacy breaches, but also the potential harms resulting from the improper collection, storage, or interpretation of such information.

Big data are often celebrated for strengthening investigative capabilities and enabling more effective information sharing—especially in intelligence work. However, their effectiveness depends on the quality, reliability, and security of large datasets containing sensitive information. These datasets may consist of data collected and held by police forces, or of data generated by devices and stored in centralized systems that law enforcement can later access. When police collect and store such information, poor cybersecurity can expose it to breaches, unauthorized access, and cyberattacks. This not only threatens investigations but also erodes public trust in policing and control agencies.

At the same time, the risks associated with the use of big data by police forces in a digital society go far beyond the protection of personal information. They involve a broader dimension of security—one that affects both citizens and non-citizens. Key concerns include how data are collected, managed, stored, and used by law enforcement, as well as the implications of these processes. There are also risks linked to how such data are interpreted and applied, the purposes they serve, and the kind of knowledge they help to produce.

Both areas are crucial for researchers studying police control and its transformation in response to technological innovation. The data collected are constantly exposed to the risk of attacks, theft, or tampering. At the same time, they can produce a distorted representation of the population and pose risks to specific groups, selectively and discriminatorily influencing criminalization processes directed at those groups.

Research on big data and data-driven control has repeatedly highlighted the biases present in the datasets and in the algorithms used to analyze them. Addressing these challenges requires examining cybersecurity while also focusing on the operational practices of law enforcement and their interaction with technology.

The workshop is designed as a critical forum for discussing the (cyber)security risks embedded in data-driven forms of control, with a specific focus on the use of big data by police forces. It seeks to bring together scholars from across Europe working on these issues through sociological, criminological, and socio-legal lenses, with the aim of fostering interdisciplinary dialogue and critical reflection on the transformations of policing in the digital society.

We particularly welcome contributions that engage critically—either theoretically or empirically—with one or more of the following topics (or closely related areas):

- the technosocial nature of interaction in the digital society and its implications for police control;
- the opacity of algorithmic decision-making (the "black box" of automated control);
- the role of human actors in the development and use of policing technologies, versus the agency and accountability of machines;
- police perceptions of the promises and pitfalls of technology in everyday practice;
- predictive policing and its operational, social, and ethical implications;
- the interoperability of police databases and its potential effects on surveillance and control;
- algorithmic bias in data-driven policing systems;
- cybersecurity challenges related to the use of big data in police operations;
- the protection of personal data—of both citizens and non-citizens—collected by control agencies, and associated risks;
- the design and deployment of algorithms and software for big data analysis aimed at prevention, control, or surveillance;
- continuities and discontinuities in policing practices in response to technological innovation;
- the role of technology in shaping processes of criminalization;
- the contribution of digital tools to the selective nature of policing and surveillance;
- public-private interactions in the production and governance of big data and analytical technologies.

Abstract Submission

Abstracts (in English, up to 250 words) must be submitted by filling out the designated form no later than **1 September 2025 (deadline postponed to 15 September)**.
Notification of acceptance will be sent by **10 September 2025 (postponed to 20 September)**.
Selected participants will be required to complete the registration process by **20 September 2025**. Instructions for registration will be provided upon acceptance. The workshop will be held in English.
Participation in the workshop is free of charge. However, travel and accommodation expenses will be the responsibility of the participants.

Organisation: Giulia Fabini, Alvise Sbraccia, Raffaella Brighi, Department of Legal Sciences, University of Bologna. @info: giulia.fabini@unibo.it

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

Finanziato dall'Unione Europea - NextGenerationEU attraverso il Ministero dell'Università e della Ricerca italiano nell'ambito del PNRR – Missione 4 Componente 2, Investimento 1.3 "Partenariati estesi a Università, centri di ricerca, imprese e finanziamento progetti di ricerca", Avviso MUR n. 341 del 15/03/2022, Progetto SERICS - SEcurity and RIghts in the CyberSpace, Codice proposta: PE00000014, CUP: J33C22002810001, finanziato con Decreto MUR n. 1556 del 11/10/2022