Editorial eucrim 4-2025

Ralf Poscher

eucrim
European Law Forum: Prevention • Investigation • Prosecution

Editorial

EDITORIAL

AUTHOR

Ralf Poscher

Director
Max Planck Institute for the Study of Crime, Security and Law

CITATION SUGGESTION

R. Poscher, "Editorial eucrim 4-2025", 2025, Vol. 20(4), eucrim, p249. DOI: https://doi.org/10.30709/eu-crim-2025-022

Published in
2025, Vol. 20(4) eucrim p 249
ISSN: 1862-6947
https://eucrim.eu

Dear Readers,

This *eucrim* issue provides insights into various aspects of state surveillance, a subject that has long engaged both the public and the legal community. Rapid technological advances, political initiatives, and landmark rulings by the highest national and European courts have fueled this interest. Digitalisation and the (seemingly) boundless potential of artificial intelligence provide new opportunities for data mining and analysis that can be (mis-)used for the surveillance of citizens, with potentially unprecedented consequences for those targeted. Prominent examples of the potential impact of contemporary surveillance practices, based on the retrieval, transfer, and processing of personal data through forensic analyses, are the recent landmark police operations targeting encrypted phone providers like EncroChat, SkyECC, and ANOM, which are also highlighted in this issue. For some, these cases serve to underline the promise of new technologies, while for others they exemplify the risks of pervasive surveillance.

In the past, discourse on surveillance has mostly centered on the powers of law enforcement and intelligence agencies. Less attention has been paid to surveillance carried out by police and other security agencies in the course of their preventive agendas, even though the boundary between preventive and repressive police activities has become increasingly fluid. In principle, any untargeted police observation and activity on the streets may find its way into a prosecutorial or court file. Moreover, the transnational dimension of data sharing is of growing significance.

Apart from the spectacular and sometimes pioneering cases that attract the most attention, little is known about the day-to-day routines of security agencies. These practices can affect communications, online activities and interpersonal interactions on social media, daily commuting by car and occasional air travel, ordinary and extraordinary financial activities, and anything stored on a local computer or in the cloud. In short, people's entire digital lives can easily be traced and retrieved by public agencies.

New opportunities give rise to new fundamental-rights questions. The sheer volume of digitalized data available to state agencies, whether for preventative or repressive purposes, requires a re-calibration of traditional proportionality models and new methods to determine the impact of digital, data-based surveillance activities. This impact must be assessed according to the severity of the related human-rights infringements. From this perspective, proportionality calibrated to severity has both qualitative and quantitative dimensions. One such assessment model is the Surveillance Barometer developed in my department at the Max Planck Institute for the Study of Crime, Security and Law. Designed as a theoretically and empirically grounded instrument, it measures and assesses the current state of surveillance and the associated burdens from a citizen's perspective in Germany.

A crucial issue we identified is the need for state agencies to be transparent about their activities. Reliable statistical data on the types and numbers of surveillance measures actually carried out is often lacking. This lacuna on the part of state actors can intensify public concern based on misguided assumptions. As Kilchling and Ellebrecht rightly point out in their article outlining the Surveillance Barometer project, the popular discursive picture of excessive surveillance of citizens may be considered a symptom of deficiencies in transparency.

I hope that transparency will improve in more areas in the future, including surveillance powers and their application from national and supranational perspectives. A good starting point is Union legislation requiring Member States to provide meaningful statistical data on the implementation of Union-law-based activities on a regular basis.

https://doi.org/10.30709/eucrim-2025-022

About eucrim

eucrim is the leading journal serving as a European forum for insight and debate on criminal and “criministrative” law. For over 20 years, it has brought together practitioners, academics, and policymakers to exchange ideas and shape the future of European justice. From its inception, eucrim has placed focus on the protection of the EU’s financial interests – a key driver of European integration in “criministrative” justice policy.
Editorially reviewed articles published in English, French, or German, are complemented by timely news and analysis of legal and policy developments across Europe.
All content is freely accessible at https://eucrim.eu, with four online and print issues published annually.

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union