# Abstracts LIPIT Panel IRIS2026

## Andreas Wiebe

## From data protection to data sovereignty

The concept of digital sovereignty is multi-facetted. In its individual approach it relates to the issue of how an individual can keep autonomy in increasing digital webs and constraints. The European data legislation will be analysed as to how it relates to this concept. The fundamental thesis is that the individual autonomy needs a new form of safeguards in the legal framework that could be found in considering data autonomy as a legal principle. This does not mean to be the end of data protection but its update in a comprehensively digitized economy and society. Interrelations to fundamental rights and the principle of private autonomy will be elaborated. Next to being a defensive right the aspects of positive participation and power to share data will be included. In addition, practical implementation of enabling structures within data governance is part of the securing data sovereignty.

## Andrii Prylutskyi

## Data Protection in the Reintegration of Veterans and Weapon Management in Ukraine: Lessons from Post-Yugoslav Countries and the Role of European Law

**Abstract:**
This paper examines how Ukraine can integrate EU IT-law standards into its post-war digital reconstruction, specifically addressing two interconnected challenges: the reintegration of over four million returning veterans and the prevention of illicit weapons proliferation.

Through a comparative analysis, the paper evaluates how post-Yugoslav states attempted to digitalise veteran registries and arms-control systems. It highlights how insufficient legal regulation in Bosnia and Herzegovina, Serbia, Croatia, and North Macedonia resulted in data leaks, the politicisation of records, discrimination, and a loss of public trust.

Against this historical backdrop, the core objective of the manuscript is to demonstrate how strong European legal frameworks, including the GDPR, the Law Enforcement Directive, NIS2, the EU Cybersecurity Act, the EHDS, and the EU Firearms Directive, can support Ukraine in designing secure, transparent, and rights-respecting digital systems. The project explores technical and legal safeguards for protecting sensitive data, such as military service history, trauma records, and firearm-holder status, within a high-risk post-conflict environment.

The paper fills a significant gap in existing research by connecting EU data protection law with post-conflict governance and cybersecurity standards. It ultimately argues that aligning Ukrainian digital infrastructure with EU acquis is not only a requirement for accession but a prerequisite for internal security and social stability.

## Murat Kegaduev

## Digital Sovereignty and Cross-Border Training Data: How EU Law Shapes the Architecture of AI Datasets

Artificial intelligence depends on access to large and diverse training datasets, many of which require cross-border data flows. In the European Union, however, the growing emphasis on digital sovereignty is reshaping the legal and technical conditions under which such datasets may be collected, transferred, and used. This paper examines how EU regulatory instruments — including the GDPR and its restrictions on international transfers, the Schrems jurisprudence, the Data Act, the Data Governance Act, and the emerging 2025 Digital Omnibus proposal — collectively function as sovereignty-driven mechanisms that structure the availability, movement, and permissible use of data for AI training. The topic advances the hypothesis that digital sovereignty in the EU has evolved into a structural force that directly shapes the architecture of AI training pipelines. Legal constraints on cross border data flows — such as third-country prohibitions, localisation effects, lifecycle obligations, and restrictions on foreign governmental access — do not merely regulate processing, but operate as de facto technical design parameters. They determine which data can be included in training datasets, how these data must be engineered, and where they may lawfully be stored or transmitted. Under this hypothesis, AI dataset governance in the EU is shifting from a privacy-centric compliance model toward a sovereignty-aware framework characterised by regional segmentation and jurisdiction-dependent data infrastructures. The topic concludes by outlining the implications of this shift for the feasibility of globally trained AI systems, arguing that digital sovereignty is becoming a defining factor in how AI datasets are formed, maintained, and governed within the EU.

## Ligia Cristina de Carvalho Ferraz

## Algorithmic Decision-Making and Human Rights: The Impact of AI in Immigration and Law Enforcement

The scope of this paper is to analyze the intersection and growing integration of Artificial Intelligence (AI) systems into immigration and policing, which has introduced new possibilities for efficiency but also significant risks for the violation of human rights, including privacy and equality. Automated decision-making tools, often trained on biased datasets, have been shown to perpetuate discrimination, specially against marginalized communities, such as immigrants and racial minorities.

Within immigration control, algorithmic systems used for visa screening or risk assessment, such as biometric recognition and language analysis, can reinforce stereotypes and reduce complex human narratives and backgrounds to data outputs. In policing, predictive algorithms

may intensify the state surveillance in historically over-policed areas, amplifying social inequalities and the circle of violence instead of preventing crime.

This paper further explores the role of European Data Protection framework and IT Law in safeguarding individuals 'fundamental rights in increasingly automated-decision environments, and how to mitigate the risks of violations of subject's rights. It also seeks to investigate the implications of AI decision-making on fundamental rights**,** including privacy, non-discrimination, and due process, while analyzing regulatory mechanisms such as the GDPR and emerging AI governance models**.** To do so, the research will focus in highlighting existing gaps in accountability, transparency, and proposes strategies to align technological innovation with ethical and human rights–based standards**.**

## Jyoti Goyal

## Is the Omnibus Proposal Quietly Rewriting EU Data Protection Laws?

This paper critically examines the European Commission's **Omnibus Proposal**--the sweeping legislative package intended to streamline the EU's digital regulatory landscape and argues that several proposed amendments to the **GDPR** risk producing *deregulation by stealth* rather than genuine simplification.

The paper highlights several proposed key amendments and their criticism:

1. **Relative Definition of Personal Data.**
2. **Expansion of legitimate interest to include AI Model development.**
3. **Narrowing Controllers' Accountability Burdens by DPIA Standardization and changes in cookie banner requirements.**
4. **Clarifications to Data Subject Rights by making DSARs chargeable and open to rejection.**

The paper draws on doctrinal analysis, regulatory-design theory, and critical scholarship on algorithmic governance to assess whether these proposals subtly shift the constitutional balance of EU data protection law. Taken together, the paper argues that the amendments go further than administrative streamlining. They gradually move the GDPR in a direction that may favour operational ease for major digital and AI actors while making the system less accessible and more opaque for individuals.

The paper concludes by questioning whether the Omnibus Proposal, in its current form, remains true to the underlying aims of EU data protection, or whether it marks the beginning of a quieter move toward a lighter regulatory environment.

## Durva Chaturverdi

## Trade Secret Protection in the Data Act: Is it Enough for Software Vendors?

This paper will contain a summary of a chapter of my thesis – The EU Data Act and its impact on International Software Agreements.

The EU Data Act has brought about strict disclosure regulations for software vendors in the IoT arena, and has provided limited exceptions for prevention of such disclosures. It is debatable how software vendors will now look to protect the confidentiality and preserve their trade secrets without disturbing the main agenda of the EU Data Act – to increase competition in the European IoT market. Recently, the Digital Omnibus Proposal in connection with the Data Act has also relaxed some of the disclosure requirements, however, in the paper we will examine if this proposal will effectively achieve anything to protect trade secrets of the IoT vendors.

We will also examine what additions can be done to traditional confidentiality, data security and IP clauses to better protect trade secrets in view of the EU Data Act. We will assess whether it is possible for software vendors, or data holders to take additional measures, besides contractual provisions to protect their trade secrets from disclosure under the Data Act, most importantly, how to effectively use the 'commercial disadvantage' option to protect themselves from mandated disclosures of information constituting or containing trade secrets under the EU Data Act.