Data and International Law: Where Do They Meet?

Lodz Cyber Hub Masterclass - May 9, 2025

---

1. Introduction (Dr. Joanna Kulesza):

- Welcomed participants to the session, part of the ongoing cyber law masterclass series.
- Highlighted the importance of gender balance and warmly introduced Dr. Eneken Tikk.
- Mentioned their past collaborations on international law and cyberspace governance.

---

2. Presentation by Dr. Eneken Tikk:

Main goals:

- Go beyond just the question of data flows and look at broader intersections of data and international law.
- Examine not just agreements but also tensions, gaps, and emerging issues.

Key areas covered:

- **Clear intersections of international law and data:**
  - Human rights: privacy, freedom of expression, access to information, personal data protection.
  - Global communications: radio regulations, undersea cables, space infrastructure, crisis communication systems.
  - Regulation of data as a resource: electromagnetic spectrum, formal international data exchanges.
  - International organizations' data handling (e.g., UN systems).
  - Bilateral data agreements: cross-border data facilities, data localization, security, and residency arrangements.
  - Cyber operations: whether data can be a target under the law of armed conflict.
- **Emerging legal and policy challenges:**
  - Blurred lines between domestic and international law, rising importance of soft law.
  - Conceptual challenges: Is data an "object"? A commodity? A sovereign asset?
  - Growing need to address metadata, proprietary data, trade secrets, and data integrity in international law.
- **Regional approaches and examples:**
  - EU: ambitious regulatory framework (GDPR, data governance, AI Act, Digital Markets Act), extraterritorial reach, and global regulatory influence.
  - US: limited direct regulation but rapid development through litigation, especially in AI and data-driven cases.
  - Bilateral examples: Estonia–Luxembourg "data embassy" arrangement, WTO e-commerce agreements (with notable non-participation by major powers like China and the US).
- **Security, sovereignty, and conflict:**
  - Cyber operations, espionage, influence campaigns, and the lack of clear international standards.
  - Unresolved debates over sovereignty, non-intervention, and coercion in the data context.
  - The Tallinn Manual and Oxford Process offering scholarly insights but no binding law.
- **Role of private actors and soft law:**
  - Companies like Microsoft proposing initiatives like a Digital Geneva Convention.
  - Elon Musk's stance on platform neutrality and the limits of corporate responsibility.

- o OECD initiatives on data sharing and information integrity.
- **Development agenda and global inequalities:**
  - o UN focus on data for sustainable development, reducing the global "data divide."
  - o The need to build resilient, inclusive frameworks to allow developing countries to benefit from digital transformation.

---

3. Discussion and Q&A:

- **Personal vs. non-personal data (prompted by Kulesza):**
  Tikk explained that GDPR was deliberately not emphasized because it's well-known, and she wanted to highlight the less-discussed but equally important area of non-personal data.
- **Data embassies:**
  Explained as physical or virtual arrangements to safeguard critical national data in other countries, motivated by cybersecurity, political stability, and continuity concerns.
  Estonia's agreement with Luxembourg was discussed as a leading example.
- **State sovereignty and security concerns (Prof. Erich Schweighofer, University of Vienna):**
  Explored the tension between sovereignty, free data flows, and national security limits (e.g., child exploitation, hacking, censorship in China).
- **Global digital inequality (Allan Chongwe, University of Malawi):**
  Raised concerns about regions excluded from services and infrastructure, and the need for public interest rules in data center development.
- **AI and international law:**
  Tikk stressed the need to move away from vague terms like "AI" and focus on specific technologies (machine learning, LLMs, etc.).
  The EU is pushing its regulatory vision, but significant divergences exist with countries like China.
  Domestic legal experimentation is seen as a necessary step before international consensus.

---

4. Closing remarks (Dr. Joanna Kulesza):

- Thanked Dr. Tikk for a rich and thought-provoking session.
- Highlighted the importance of discussing underexplored areas of data governance.

- Mentioned follow-up materials (recording, slides) and invited participants to continue engaging with the topic.

Main Takeaways:

- The data-international law relationship is complex, fast-evolving, and covers much more than personal data privacy.
- There's no one-size-fits-all international solution; states, companies, and international bodies all have roles to play.
- Scholars, regulators, and practitioners must look beyond security concerns and personal data to fully grasp the transformative role of data in law, economy, and society.