[LAoCS] Legal Aspects of Computer Science

Instructor: Dr Joanna Kulesza

Faculty: Faculty of Law and Administration
Course ID: 1100-AP0ADLI-A
Level: Bachelor of Arts (BA)
ECTS Credits: 0 or 3 (depending on study program)
Language of Instruction: English
Form of Completion: Credit (zaliczenie)
Study Mode: Full-time (stacjonarne)
Date Published: 06 October 2025

Course Overview

How does the law evolve in the digital age?
The *Legal Aspects of Computer Science* course introduces students to the interaction between technology and law in the contemporary digital environment. It examines how legal systems respond to the challenges posed by cyberspace, digital data, cybersecurity, and emerging technologies.

The course combines **lectures**, **seminar discussions**, and **interactive case studies** to explore national and international legal responses to digital transformation. Students will gain foundational knowledge of key legal instruments governing information security, privacy, data protection, and cybercrime. The program further encourages students to reflect on the ethical, political, and societal implications of technological development.

Aims of the Course

The primary aim of the course is to familiarise students with the principal legal frameworks regulating digital trade, data protection, and cybersecurity.
Upon completion, participants will possess the fundamental knowledge necessary to understand and apply relevant legal norms within their professional and academic activities.

Learning Outcomes

Upon successful completion of the course, students will be able to:

Knowledge

- **E1.** Recognise the key challenges and risks in applying law to cyberspace.
- **E2.** Identify fundamental legal acts related to online data processing, including personal data.
- **E3.** Describe national and international legal instruments addressing secure information systems and cybercrime.

Skills

- **E4.** Indicate areas requiring improvement in legal data protection and information system security.
- **E5.** Locate specialist legal and technical resources relevant to professional practice.
- **E6.** Explain the principal legal regulations governing the circulation of digital data.
- **E7.** Identify security threats associated with electronic communication and transactions.

Social Competence

- **E8.** Appreciate the importance of effective and comprehensive digital data protection, including personal data, and the necessity of continuously updating one’s knowledge in this area.

- **E9.** Demonstrate awareness of legislative, ethical, and social developments influencing the regulation of cyberspace.

LODZ CYBER HUB
University of Lodz

Course Content

Section 1: Fundamental Principles of Law (Modules 1-4)

1.1 Introduction to Law and Technology

Law and technology are profoundly interconnected. As digital innovation advances, legal systems must continually adapt to regulate new realities and safeguard fundamental rights. Technology affects how societies communicate, trade, and govern; consequently, the law provides the framework that ensures these transformations remain consistent with principles of justice, privacy, and accountability.

In the digital context, legal regulation addresses issues such as **data protection**, **cybersecurity**, **intellectual property**, and **online crime**. These concerns extend across national borders, requiring cooperation between multiple legal domains:

- **Private international law (conflict of laws)** determines which national legal system and court have jurisdiction in cross-border digital disputes.
- **Public international law** governs relations among states, shaping rules on state behaviour in cyberspace.
- **Supranational law**, found in entities such as the European Union, establishes shared obligations that override conflicting national laws.

Understanding these layers is essential to appreciate how the law supports technological progress while protecting individual and collective interests.

1.2 Sources of Cyber Law

Cyber law draws authority from multiple levels—**international**, **regional**, and **national**—each contributing to the regulation of cyberspace.

International Sources

Article 38 of the **Statute of the International Court of Justice** defines the primary sources of international law:

1. **International conventions and treaties** – written agreements among states establishing explicit legal rules (e.g., the *Budapest Convention on Cybercrime*).
2. **Customary international law** – general state practice accepted as law (*usus* + *opinio juris*).
3. **General principles of law** – foundational doctrines common to most legal systems, such as good faith, equity, and estoppel.
4. **Judicial decisions and scholarly writings** – subsidiary means for interpreting legal norms.

Additional contemporary sources include **binding decisions of international organisations**, **state practice**, and **soft-law instruments**, such as resolutions and policy guidelines, which influence behaviour without formal enforceability.

Regional Sources

Regional integration frameworks, notably the **European Union**, produce supranational norms directly applicable to member states. Instruments like the **General Data Protection Regulation (GDPR)** and the **NIS Directive** (Network and Information Security) harmonise data-protection and cybersecurity obligations across Europe, reflecting the principle that digital governance benefits from coordinated regional regulation.

National Sources

At the domestic level, each country establishes its own hierarchy of legal norms. In **Poland**, the Constitution stands as the supreme law (Article 8), followed by statutes (*ustawy*), ratified international agreements, and governmental regulations (*rozporządzenia*).
Key constitutional provisions include:

- **Article 2** – the Republic of Poland is a democratic state ruled by law and guided by social justice.
- **Article 30** – human dignity is the source of personal freedoms and rights.
- **Article 31** – individual freedoms are protected, and any limitations must be lawful, necessary, and proportionate.
- **Article 64** – property rights are protected and can be limited only by statute.
- **Article 73** – guarantees freedom of research, teaching, and culture.
- **Articles 87–92** – define the sources of law and conditions for promulgation.
- **Articles 89 and 91** – outline procedures for treaty ratification and the precedence of ratified international agreements over domestic statutes.
- **Article 9** – obliges Poland to respect international law binding upon it.

Together, these provisions ensure that international and regional norms are integrated into the national legal order, demonstrating the constitutional openness of Polish law to global digital governance.

Private and Public International Law

- **Private international law** (2011 Act on Private International Law) determines applicable law and jurisdiction in cross-border private matters. For instance, Article 4 permits parties to select the governing law, while Article 2 defines nationality criteria for legal conflicts.
- **Public international law** governs the conduct of states and international organisations. It includes fields such as treaty law, maritime law, international criminal and humanitarian law, environmental law, and emerging **international Internet law**.

Supranational Law

Supranational law arises when states delegate part of their sovereignty to a regional organisation empowered to enact binding norms superior to national legislation. The European Union exemplifies this system, where directly applicable regulations take precedence over conflicting domestic laws. This structure ensures consistency in addressing transnational issues such as data protection, digital trade, and cross-border cybersecurity.

1.3 International Law and Digital Sovereignty

Digital sovereignty refers to a state's capacity to exercise control over its digital infrastructure, data flows, and cyberspace governance while cooperating internationally. As digital interactions transcend borders, questions of **jurisdiction** become increasingly complex.

Jurisdiction in Cyberspace

Jurisdiction denotes a state's legal authority to legislate, adjudicate, and enforce laws. In cyberspace, five traditional bases for jurisdiction are applied flexibly:

1. **Territoriality** – jurisdiction arises from conduct occurring within a state's borders.
2. **Effects principle** – jurisdiction extends to foreign acts producing substantial effects within the state.
3. **Personality principle** – jurisdiction applies to nationals, even for actions abroad.
4. **Protective principle** – jurisdiction protects national security and essential interests.
5. **Universality principle** – certain crimes (e.g., cyber-terrorism or crimes against humanity) are prosecutable by any state, regardless of location.

The digital environment often involves overlapping claims of jurisdiction. For instance, a single cyberattack can originate in one state, target users in another, and involve infrastructure located in a third. To mitigate such conflicts, international cooperation is vital. Instruments like the **Budapest Convention on Cybercrime** encourage consultation and mutual legal assistance when multiple jurisdictions are implicated.

Conflicts and Cooperation

Because cyber activities disregard physical borders, states increasingly rely on **bilateral and multilateral cooperation**, **extraterritorial legislation**, and **mutual recognition agreements** to enforce digital laws. Regional frameworks, such as the EU's cooperation mechanisms or the Council of Europe's conventions, illustrate efforts to balance sovereignty with global interdependence. Ultimately, effective governance of cyberspace depends on shared principles of due process, proportionality, and human-rights protection.

1.4 National Legal Frameworks

The regulation of cyberspace varies significantly across jurisdictions, reflecting different legal traditions, governance philosophies, and levels of technological development. A comparative perspective highlights the diversity of approaches among the **European Union**, the **United States**, and selected **Asian** systems.

European Union

The EU exemplifies a **supranational legal order**, where digital policy and data protection are harmonised through binding legislation.

- The **GDPR** (2018) establishes comprehensive rules for personal-data processing, consent, and cross-border transfers.
- The **NIS Directive** strengthens cybersecurity resilience for operators of essential services.
- The principle of **direct effect** allows individuals to invoke certain EU provisions before national courts when the rule is clear, unconditional, and grants rights.
  EU law thus ensures uniform standards across member states, reinforcing trust in the digital single market while promoting fundamental-rights protection.

United States

The U.S. follows a **common-law** tradition, relying heavily on judicial precedent and sector-specific legislation.
Key instruments include:

- The **USA PATRIOT Act** and **Foreign Intelligence Surveillance Amendments Act (FISAA)**, which extend surveillance powers for national-security purposes.
- The **CLOUD Act** (2018), enabling U.S. authorities to access data held overseas by companies under U.S. jurisdiction.
  While the U.S. legal framework prioritises innovation and free enterprise, it faces criticism for fragmented privacy protection and expansive state surveillance.

Asia

Asian jurisdictions demonstrate wide legal diversity:

- **Japan** combines civil-law foundations with modern privacy and cybersecurity statutes, aligning with global standards through active participation in international fora.
- **China** exercises strong state control over cyberspace through the **Cybersecurity Law** (2017) and **Data Security Law** (2021), asserting data localisation and content-control measures grounded in national-security concerns.

- **India** maintains a hybrid system influenced by common law. Its **Information Technology Act** and forthcoming **Digital Personal Data Protection Act** aim to balance economic development with individual rights.

These regional variations illustrate that cyber governance reflects broader political and cultural values. Whereas the EU emphasises **fundamental-rights protection**, the U.S. favours **market freedom**, and China prioritises **state sovereignty**. Nonetheless, all recognise the necessity of international cooperation to confront cyber threats and ensure global interoperability.

Conclusion

Law serves as the backbone of digital transformation. From the global norms of international law to the detailed provisions of national constitutions, legal frameworks provide both **predictability** and **protection** in an era of technological disruption. Understanding the **sources of cyber law**, the **principles of jurisdiction**, and the **comparative models of governance** equips students and practitioners to navigate the complex, borderless environment of cyberspace responsibly and effectively.

Through this first module, students should appreciate how the rule of law underpins digital innovation, ensuring that technological progress remains consistent with human rights, security, and social justice.