

LEGAL ASPECTS OF COMPUTER SCIENCE

Law • Technology • Data • Cybersecurity • Digital Governance



Sources of
cyber law



International law
and digital sovereignty



Jurisdiction
and responsibility



Comparative national
frameworks



ISP and intermediary
liability



Privacy, GDPR and
international data transfers



Surveillance and
encryption



DNS architecture
and governance



ICANN policies,
UDRP and DNS abuse



Phishing and malware
mitigation



Legal Aspects of Computer Science

Joanna Kulesza, Ph.D.

Lodz Cyber Hub, University of Lodz

Contents

Course information.....	3
Instructor.....	3
Course data.....	4
General course content.....	4
Short description.....	4
Learning outcomes.....	4
Teaching method.....	5
Form of assessment.....	5
Lecture scope: 14 meetings.....	6
Resources.....	7
Section 1: Law, ethics and sources of law.....	8
Law and ethics in computer science.....	8
Sources of law.....	8
National sources of law.....	9
Sources of law in Poland.....	10
The Constitution as supreme law.....	11
Statutes, regulations and ratified agreements.....	13
National, international and European law.....	16
Private international law.....	17
Public international law.....	18
Supranational law and European Union law.....	18
Sources of international law.....	20
Case studies.....	25
Case study 1: A statute and a treaty in conflict.....	25
Case study 2: A cross-border software licence.....	25
Case study 3: An attack launched through servers in a third state.....	26
Case study 4: An artificial intelligence service offered from outside the Union.....	26
Case study 5: A foreign order for data stored in Europe.....	27
Quiz.....	28
Summary.....	32

A note for students

These materials respond to students' request for a concise summary of the lectures. They are not a stand-alone teaching resource. They complement the face-to-face classes, where you will learn most. We look forward to working with you in class.

These are study materials for students, prepared with AI assistance on the basis of course notes by Joanna Kulesza. Relevant copyright applies.

Course information

Instructor

Joanna Kulesza, PhD, Assistant Professor of International Law, Department of Public International Law and International Relations, Faculty of Law and Administration, University of Lodz. Executive Director of the Lodz Cyber Hub.

Joanna Kulesza is a scholar of public international law whose research concentrates on state responsibility, due diligence, jurisdiction and internet governance. She is the author of *International Internet Law* (Routledge, 2012) and *Due Diligence in International Law* (Brill, 2016), co-editor, with Roy Balleste, of *Cybersecurity and Human Rights in the Age of Cyberveillance* (Rowman & Littlefield, 2015) and of *Global Governance of Low Earth Orbit Satellites* (Lodz University Press, 2025, with Berna Akcali Gur).

She takes part in the Oxford Process on International Law Protections in Cyberspace and in the Sino-European Working Group on the Application of International Law in Cyberspace. She is a former member of the Scientific Committee of the European Union Agency for Fundamental Rights, and a founding member of the academic advisory board of EU Cyber Direct. She directs the Summer School on Internet Governance and International Law (SSIGIL) and the Executive Training Course on International Law and Cybersecurity of the European Security and Defence College (ESDC), and she has long been active in the community of the Internet Corporation for Assigned Names and Numbers (ICANN).

- Speaking hours: MS Teams, by prior e-mail appointment
- E-mail: available in USOSweb
- Web: <https://www.uni.lodz.pl/pracownicy/joanna-kulesza>

Lodz Cyber Hub

The Lodz Cyber Hub (in Polish: Centrum Badań nad Stosowaniem Prawa Międzynarodowego w Cyberprzestrzeni "Lodz Cyber Hub") is a research centre at the Department of Public International Law and International Relations, Faculty of Law and Administration, University of Lodz. It conducts research on the application of international law in cyberspace and brings together researchers, students and practitioners. Its activities include research projects, seminars and teaching, among them the international Summer School on Internet Governance and International Law (SSIGIL). Further projects of the centre include the LCH Masterclasses, which bring invited experts to the University.

CyberAmbassadors. The CyberAmbassadors programme engages students of the University in the work of the centre. Ambassadors are selected from three faculties: the Faculty of Law and Administration, the Faculty of Mathematics and Computer Science, and the Faculty of Economics and Sociology. They serve for one year. Ambassadors initiate and promote educational events in their own environments, help to organise workshops and masterclasses, and represent the centre in public debate and in the media. The programme connects students with the international institutions that shape policy, internet governance and technical standards, such as the United Nations, the International Telecommunication Union, the European Union, the Organization for Security and Co-operation in Europe (OSCE), the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Engineering Task Force (IETF) and the Réseaux IP Européens Network Coordination Centre (RIPE NCC). Active participants receive mentoring, opportunities to develop their skills, certificates and recommendations, and the possibility to join international projects.

Course data

Item	Value
Course ID	1100-AP0ADLI-A
ISCED	(0610) Information and Communication Technologies (ICTs), not further defined
Course title	Legal Aspects of Computer Science
Organizational unit	Faculty of Mathematics and Computer Science
ECTS credit allocation (and other scores)	0 or 3.00 (depends on study program)
Language	English
Form of credit (in Polish)	zaliczenie
Level	BA
Form of study (in Polish)	stacjonarne
Prerequisites	No formal prerequisites are required.
Type of class	Lecture, 28 hours
Course information	https://www.uni.lodz.pl/en/news/details/laocs

General course content

The course covers legal issues related to the functioning of information systems and the circulation of information in the digital environment. It addresses the fundamental concepts and principles of technology law, with particular emphasis on cyberspace regulation, personal data protection, cybersecurity, and legal liability in networked environments. The course analyses national, European Union, and international regulatory frameworks governing data processing, information system security, cybercrime prevention, and legal risk management in the ICT sector. Special attention is given to the practical relevance of legal regulations for the professional activities of computer scientists, data analysts, and IT specialists.

Short description

The subject of the lecture is a framework presentation of issues related to the legal aspects of computing, cyber security and the protection of digital data, including personal data.

The aim of the course is to familiarise participants with the basic legal regulations applicable to digital trading, with a particular focus on cyber security and the protection of personal data. Upon completion of the course, participants will have a basic knowledge of the topics used in their daily work.

The issues discussed and the teaching methods used are among the most up-to-date and innovative on the market, both in terms of electronic data security regulation and data protection and the use of methods and interactive activities.

Learning outcomes

- E1.** The student knows the basic challenges and threats to the application of law in cyberspace.
- E2.** The student is able to indicate basic legal acts concerning data processing on the Internet, including personal data.

- E3.** The student is able to identify basic legal acts concerning national and international secure information systems and cybercrime.
- E4.** The student is able to identify those areas of activity that require improvement in legal protection of data and information systems.
- E5.** The student is able to find specialist information to strengthen his/her position in the job market.
- E6.** The student is able to describe the most important legal regulations concerning the circulation of digital data and information systems.
- E7.** The student is able to identify security threats related to electronic circulation.
- E8.** The student is familiar with the meaning of effective and comprehensive digital data protection, including personal data, and is aware of the necessity of constantly updating his/her knowledge within this scope.
- E9.** The student is aware of legislative and social changes concerning the discussed issues.

Learning outcome codes: W09, K01, K03, K04, K05

Teaching method

The teaching method for this course is an interactive lecture format enriched by the incorporation of pertinent case studies. Interactive lectures, comprising multimedia elements, open-ended inquiries, and active discussions, serve to stimulate student engagement and participation while fostering a dynamic exchange of ideas. Case studies, carefully selected to reflect real-world scenarios within these domains, complement theoretical concepts, nurturing critical thinking and problem-solving skills among students. Moreover, hosting guest lecturers on a regular basis presents an opportunity for the students to confront the obtained theoretical knowledge with valuable practical insights from speakers from external organizations.

Form of assessment

- Single-choice test.
- The date of the test is agreed with the students.
- Attendance at lectures is not compulsory.

Lecture scope: 14 meetings

Section 1: Law, ethics and sources of law

Meeting 1. Introduction to the course and the contents discussed; introduction to law; law and ethics in computer science

Meeting 2. Sources of law: national law and the hierarchy of sources

Meeting 3. National, international and European law

Section 2: Jurisdiction, cybercrime and cybersecurity

Meeting 4. Trias politica and principles of jurisdiction

Meeting 5. Jurisdiction in practice: exercises

Meeting 6. Cybercrime: the Budapest Convention and its offences

Meeting 7. Cybercrime: the Hanoi Convention and international cooperation

Meeting 8. Cybersecurity: the NIS 2 Directive

Meeting 9. Cybersecurity: the Polish act on the national cybersecurity system

Section 3: Data and artificial intelligence

Meeting 10. Personal data protection: the GDPR, principles and actors

Meeting 11. The GDPR: rights of data subjects, transfers and enforcement

Meeting 12. The Artificial Intelligence Act

Meeting 13. The Digital Services Act and the Digital Markets Act; case workshop and revision

Final meeting

Meeting 14. Assessment test

The schedule will be adjusted to the needs of the group. We will focus on the topics in which the students show particular interest.

Resources

Author	Year	Title
Legal instruments		
Republic of Poland	1997	Constitution of the Republic of Poland
Council of Europe	2001	Convention on Cybercrime (Budapest Convention)
United Nations	2024	United Nations Convention against Cybercrime (Hanoi Convention)
European Union	2016	Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, GDPR)
European Union	2022	Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive)
European Union	2024	Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act)
European Union	2024	Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)
United States	2018	Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Division V of the Consolidated Appropriations Act, 2018, Pub. L. 115-141
Selected publications		
Roy Balleste, Joanna Kulesza	2013	Signs and Portents in Cyberspace: The Rise of Jus Internet as New Order in International Law. <i>Fordham Intellectual Property, Media and Entertainment Law Journal</i> 23(4): 1311
Joanna Kulesza, Roy Balleste (eds)	2015	Cybersecurity and Human Rights in the Age of Cyberveillance. Rowman & Littlefield
Roy Balleste	2022	The Law of Space Cyber Operations: Gripping Mysteries, Entangled Frontiers, and Security Challenges. <i>Journal of Law, Technology & the Internet</i> 13(1): 146
Lee A. Bygrave	2025	The emergence of EU cybersecurity law: A tale of lemons, angst, turf, surf and grey boxes. <i>Computer Law & Security Review</i> 56: 106071
Supplementary reading		
Joanna Kulesza, François Delerue, Patryk Pawlak	2019	The application of international law in cyberspace: is there a European way? Research paper, EU Cyber Direct
Joanna Kulesza	2025	Cyber Diplomacy in Action: EU and Partners Deliver a UN Permanent Mechanism for Responsible State Behaviour and International Law in Cyberspace. Casimir Pulaski Foundation

Section 1: Law, ethics and sources of law

Law and ethics in computer science

Law is a set of binding rules created or recognised by a state or by the international community. Breach of a legal rule may lead to enforcement and sanctions. Ethics concerns moral principles about what is right and wrong. It is not enforced by public authorities, although a breach may lead to professional or social consequences.

Several other types of norms should be distinguished from binding law:

- professional codes of conduct, adopted by professional associations;
- technical standards, for example ISO standards, which bind only if a legal act or a contract makes them binding;
- soft law, such as guidelines of international organisations, which is not binding but may influence the interpretation of binding rules.

A lawful act is not always ethical, and an ethical act may still be unlawful. In computer science, questions often appear first as ethical problems, for example the fairness of algorithms, and later become legal obligations, as the Artificial Intelligence Act of the European Union shows.

Sources of law

Where does the law come from? Who makes the law?



Figure 1. Origins of law: religious origins, contract as the basis of societal norms, and judge-made law in common law systems.
Author's own compilation.

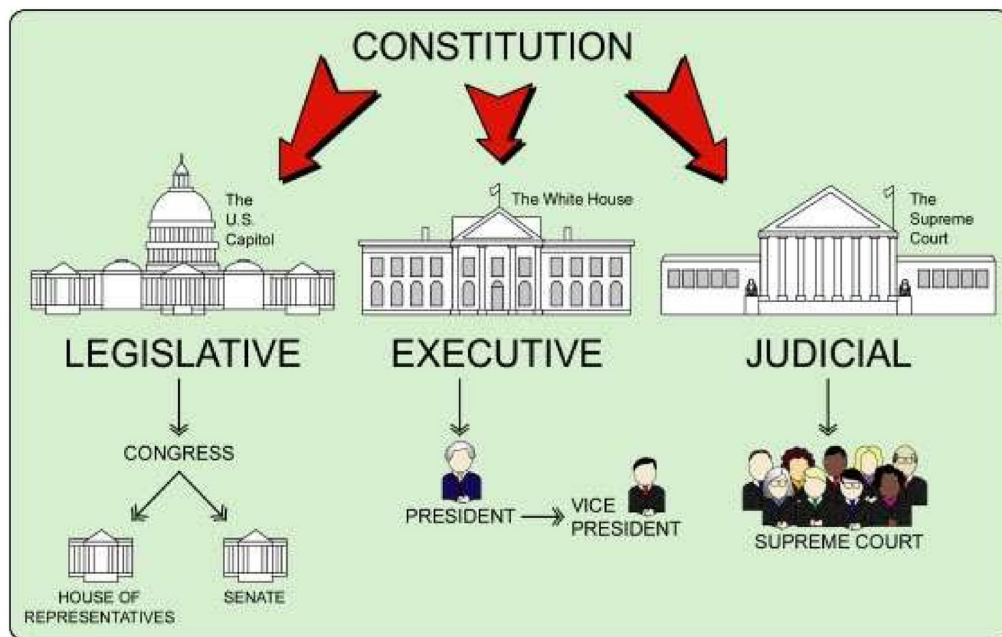


Figure 2. Separation of powers: the example of the United States. Source: <https://sites.google.com/site/perkinsconvention/home/c>



Figure 3. Montesquieu (1689-1755), author of *The Spirit of the Laws* (1748), who developed the doctrine of the separation of powers.

National sources of law

Legislative power in Poland

Article 95

1. Legislative power in the Republic of Poland shall be exercised by the Sejm and the Senate.
2. The Sejm shall exercise control over the activities of the Council of Ministers within the scope specified by the provisions of the Constitution and statutes.

Supreme power in Poland



Figure 4. The Constitution of the Republic of Poland (Konstytucja RP).

Article 4

1. Supreme power in the Republic of Poland shall be vested in the Nation.
2. The Nation shall exercise such power directly or through their representatives.

Sources of law in Poland

Article 87

1. The sources of universally binding law of the Republic of Poland shall be: the Constitution, statutes, ratified international agreements, and regulations.
2. Enactments of local law issued by the operation of organs shall be a source of universally binding law of the Republic of Poland in the territory of the organ issuing such enactments.

Article 88

1. The condition precedent for the coming into force of statutes, regulations and enactments of local law shall be the promulgation thereof.
2. The principles of and procedures for promulgation of normative acts shall be specified by statute.
3. International agreements ratified with prior consent granted by statute shall be promulgated in accordance with the procedures required for statutes. The principles of promulgation of other international agreements shall be specified by statute.

Official publication of statutes: Journal of Laws of the Republic of Poland (Dziennik Ustaw).

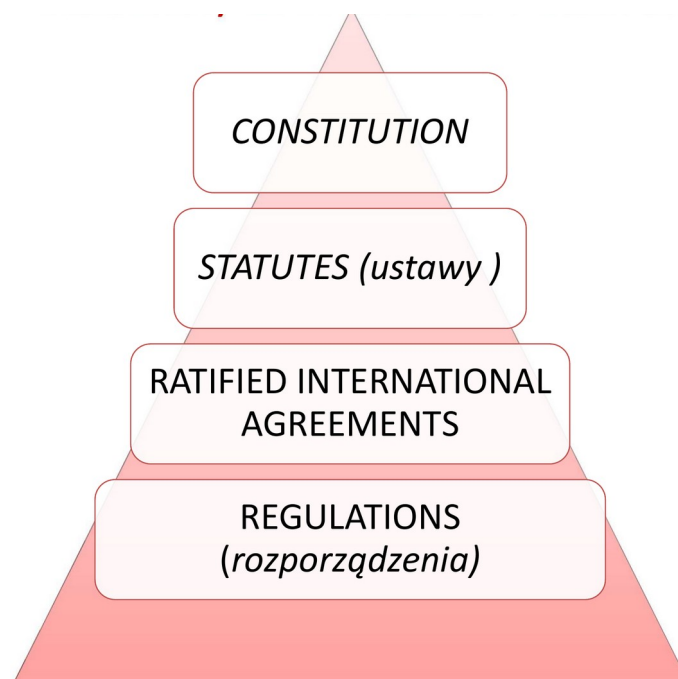


Figure 5. Hierarchy of sources of universally binding law in Poland.

The Constitution as supreme law

Article 8

1. The Constitution shall be the supreme law of the Republic of Poland.
2. The provisions of the Constitution shall apply directly, unless the Constitution provides otherwise.

Constitutional principles

Article 2

The Republic of Poland shall be a democratic state ruled by law and implementing the principles of social justice.

Freedoms, rights and obligations of persons and citizens

Article 30

The inherent and inalienable dignity of the person shall constitute a source of freedoms and rights of persons and citizens. It shall be inviolable. The respect and protection thereof shall be the obligation of public authorities.

Article 31

1. Freedom of the person shall receive legal protection.
2. Everyone shall respect the freedoms and rights of others. No one shall be compelled to do that which is not required by law.
3. Any limitation upon the exercise of constitutional freedoms and rights may be imposed only by statute, and only when necessary, in a democratic state for the protection of its security or public order, or to protect the natural environment, health or public morals, or the freedoms and rights of other persons. Such limitations shall not violate the essence of freedoms and rights.

Right to ownership

Article 64

1. Everyone shall have the right to ownership, other property rights and the right of succession.
2. Everyone, on an equal basis, shall receive legal protection regarding ownership, other property rights and the right of succession.
3. The right of ownership may only be limited by means of a statute and only to the extent that it does not violate the substance of such right.

Freedom of artistic creation

Article 73

The freedom of artistic creation and scientific research as well as dissemination of the fruits thereof, the freedom to teach and to enjoy the products of culture, shall be ensured to everyone.

Rights relevant to the digital environment

The following provisions are frequently invoked in disputes about privacy, personal data, communications and online speech.

Article 47

Everyone shall have the right to legal protection of his private and family life, of his honour and good reputation and to make decisions about his personal life.

Article 49

The freedom and privacy of communication shall be ensured. Any limitations thereon may be imposed only in cases and in a manner specified by statute.

Article 50

The inviolability of the home shall be ensured. Any search of a home, premises or vehicles may be made only in cases and in a manner specified by statute.

Article 51

1. No one may be obliged, except on the basis of statute, to disclose information concerning his person.
2. Public authorities shall not acquire, collect nor make accessible information on citizens other than that which is necessary in a democratic state ruled by law.
3. Everyone shall have a right of access to official documents and data collections concerning himself. Limitations upon such rights may be established by statute.
4. Everyone shall have the right to demand the correction or deletion of untrue or incomplete information, or information acquired by means contrary to statute.
5. Principles and procedures for collection of and access to information shall be specified by statute.

Article 54

1. The freedom to express opinions, to acquire and to disseminate information shall be ensured to everyone.

2. Preventive censorship of the means of social communication and the licensing of the press shall be forbidden. Statutes may require the receipt of a permit for the operation of a radio or television station.

Article 77

1. Everyone shall have the right to compensation for any harm done to him by any action of an organ of public authority contrary to law.

2. Statutes shall not bar the recourse by any person to the courts in pursuit of claims alleging infringement of freedoms or rights.

Statutes, regulations and ratified agreements

Statutes

A statute (ustawa) is a general legal act adopted by the Sejm, with the participation of the Senat, signed by the President and promulgated in the Journal of Laws. It ranks directly below the Constitution. Matters that affect the rights and obligations of individuals, and the powers of public authorities, must be regulated by statute. Regulations (see below) may be issued only on the basis of a statute.

The following are examples of areas of national law that are regulated by statutes:

- **Intellectual property**, including copyright and industrial property (for example patents and trade marks);
- **Civil law**, for example contracts, ownership and liability for damage;
- **Administrative law**, the organisation and powers of public administration;
- **Law of administrative procedure**, the rules by which public authorities decide individual cases;
- **Criminal law**, the definition of offences and penalties, including offences committed with the use of computers.

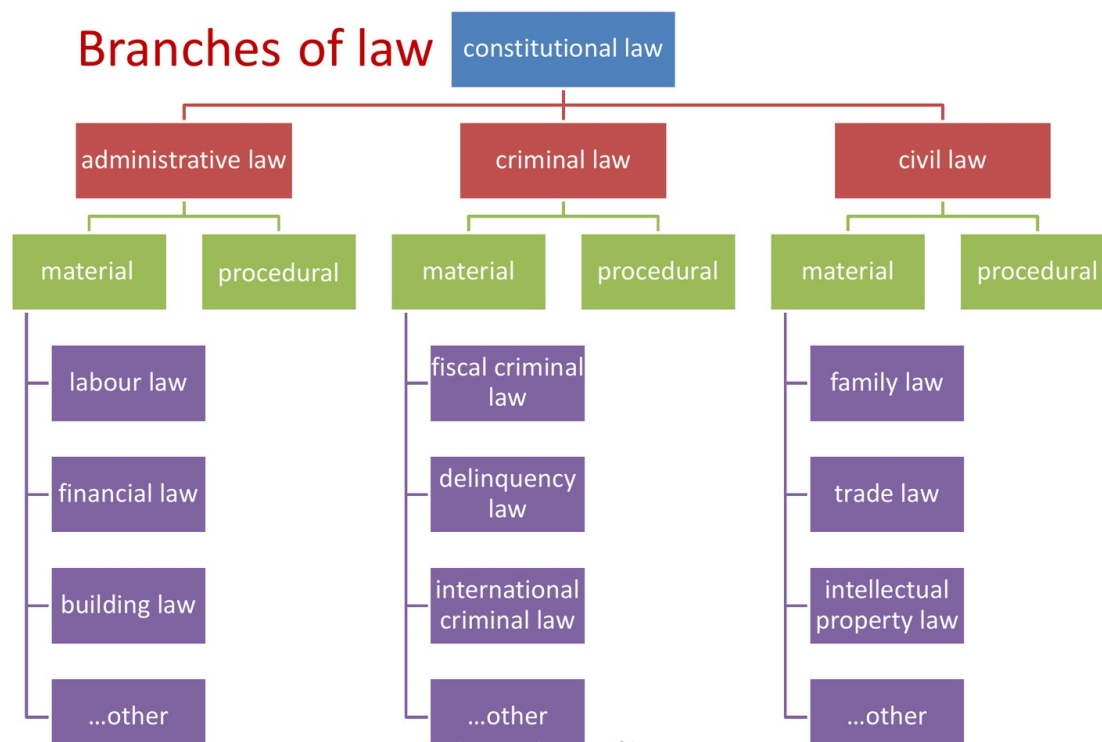


Figure 6. Branches of law.

Criminal law and international cooperation

Criminal law defines offences and penalties, and in Poland it does so by statute, above all in the Criminal Code. It includes offences committed with the use of computers, such as unlawful access to information systems and the interception of data. These provisions can be enforced only if evidence is obtained. In cybercrime cases, the offender, the victim, the servers and the service provider are often in different states, and the authorities of one state may not investigate on the territory of another. International cooperation is therefore needed: mutual legal assistance, requests to preserve data, joint investigation teams and contact points that work around the clock, many of them based on treaties.

Regulations

Article 92

1. Regulations shall be issued on the basis of specific authorization contained in, and for the purpose of implementation of, statutes by the organs specified in the Constitution. The authorization shall specify the organ appropriate to issue a regulation and the scope of matters to be regulated as well as guidelines concerning the provisions of such act.
2. An organ authorized to issue a regulation shall not delegate its competence, referred to in para. 1 above, to another organ.

Ratified international agreements

Ratification: approval (signature) of an international treaty by the President.

- **Great ratification:** the President is presented the treaty for signature after its acceptance by the Parliament expressed in a statute.
- **Small ratification:** the President is presented the treaty for signature after its acceptance by the government (Prime Minister).

The Polish Act on International Agreements

The procedure for concluding international agreements is specified in the Act of 14 April 2000 on International Agreements (Ustawa z dnia 14 kwietnia 2000 r. o umowach międzynarodowych), Journal of Laws 2000 No. 39, item 443, as amended. The Act implements the constitutional rules and regulates the whole life cycle of a treaty: preparation and negotiation, signature, ratification or approval, entry into force, publication and termination.

In summary, the procedure has the following features:

- The Minister of Foreign Affairs has a central coordinating role. Draft agreements, and the positions of the Polish delegation, are consulted with the ministries concerned, and the Minister gives an opinion on their legal and political aspects.
- The Act distinguishes agreements concluded in the name of the Republic of Poland, which are ratified by the President, from agreements concluded in the name of the Government, which are approved by the Council of Ministers.
- Where a treaty requires great ratification, the Council of Ministers submits to the Sejm a draft statute granting consent to ratification. After Parliament has given consent, the President decides on ratification. Before ratifying, the President may refer the agreement to the Constitutional Tribunal for review of its conformity with the Constitution.
- Where consent by statute is not required, the President ratifies the agreement on the basis of a decision of the Council of Ministers, and the Sejm and the Senat are only notified.

- A ratified agreement is then promulgated in the Journal of Laws. According to Article 91(1) of the Constitution, promulgation is the condition for its application in the domestic legal order.

The Act therefore translates the choice between great and small ratification into a clear administrative procedure and gives the government, Parliament and the President separate roles. The summary above is a simplified description for study purposes. Students who need exact details should read the consolidated text of the Act in the Internet System of Legal Acts (ISAP).

Small ratification. When the parties of the treaty decide so, then:

- the treaty is presented to the President by the Prime Minister;
- the Sejm is informed of the ratification taking place (does not vote on it).

Great ratification. The Constitution lists the matters that require prior consent granted by statute:

Article 89

1. Ratification of an international agreement by the Republic of Poland, as well as renunciation thereof, shall require prior consent granted by statute, if such agreement concerns:

- 1) peace, alliances, political or military treaties;
- 2) freedoms, rights or obligations of citizens, as specified in the Constitution;
- 3) the Republic of Poland's membership in an international organization;
- 4) considerable financial responsibilities imposed on the State;
- 5) matters regulated by statute or those in respect of which the Constitution requires the form of a statute.

2. The President of the Council of Ministers (the Prime Minister) shall inform the Sejm of any intention to submit, for ratification by the President of the Republic, any international agreements whose ratification does not require consent granted by statute.

Position of a ratified treaty in the Polish legal system

Article 91

1. After promulgation thereof in the Journal of Laws of the Republic of Poland (Dziennik Ustaw), a ratified international agreement shall constitute part of the domestic legal order and shall be applied directly, unless its application depends on the enactment of a statute.

2. An international agreement ratified upon prior consent granted by statute shall have precedence over statutes if such an agreement cannot be reconciled with the provisions of such statutes.

3. If an agreement, ratified by the Republic of Poland, establishing an international organization so provides, the laws established by it shall be applied directly and have precedence in the event of a conflict of laws.

Direct effect of European Union law

European Union law is applied not only by the institutions of the Union but also by national courts and authorities. For individuals, the key question is whether they can rely on a provision of Union law before a national court. This is the question of **direct effect**. It should be distinguished from **direct applicability**: a directly applicable act becomes part of the national legal order without any national

implementing measure, while direct effect concerns the possibility of invoking a provision to claim a right.

In *Van Gend en Loos v. Nederlandse Administratie der Belastingen* [ECJ case 26/62; [1963] ECR 1; [1970] CMLR 1] the European Court of Justice laid down the criteria ("Van Gend en Loos criteria") for establishing direct effect. The provision of an international treaty must:

- be sufficiently clear and precisely stated,
- be unconditional or non-dependent, and
- confer a specific right for the citizen to base his or her claim on.

The legal acts of the Union differ in this respect. Article 288 of the Treaty on the Functioning of the European Union (TFEU) provides:

Article 288 TFEU

To exercise the Union's competences, the institutions shall adopt regulations, directives, decisions, recommendations and opinions.

A regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States.

A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods.

A decision shall be binding in its entirety. A decision which specifies those to whom it is addressed shall be binding only on them.

Recommendations and opinions shall have no binding force.

- **Treaty provisions** and **regulations** may have vertical direct effect (against the state) and, if they meet the criteria, also horizontal direct effect (against other private parties).
- **Directives** may, after the deadline for implementation has passed, have vertical direct effect against the state (*Van Duyn*, case 41/74). They do not have horizontal direct effect between private parties (*Marshall*, case 152/84).
- Where a directive cannot be invoked directly, national courts must interpret national law in conformity with it as far as possible (*Marleasing*, case C-106/89), and a member state may be liable in damages for failure to implement it (*Francovich*, joined cases C-6/90 and C-9/90).

Direct effect works together with the **primacy** of Union law over conflicting national law, established in *Costa v ENEL* (case 6/64). Together, the two principles explain why Union rules such as the GDPR can be enforced by individuals before Polish courts.

National, international and European law

Article 9

The Republic of Poland shall respect international law binding upon it.

Does "international law" mean only ratified international agreements? The term "international law" can refer to three legal disciplines:

1. private international law
2. public international law
3. supranational law

International law and national law

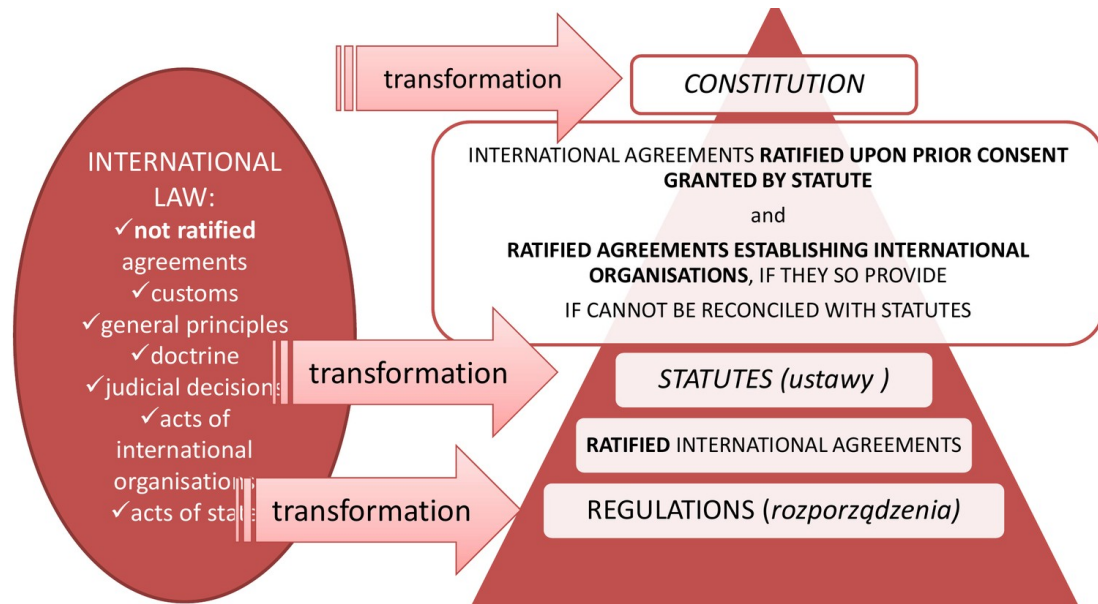


Figure 7. International law in the Polish legal system: the transformation of international law into the hierarchy of national sources.

Private international law

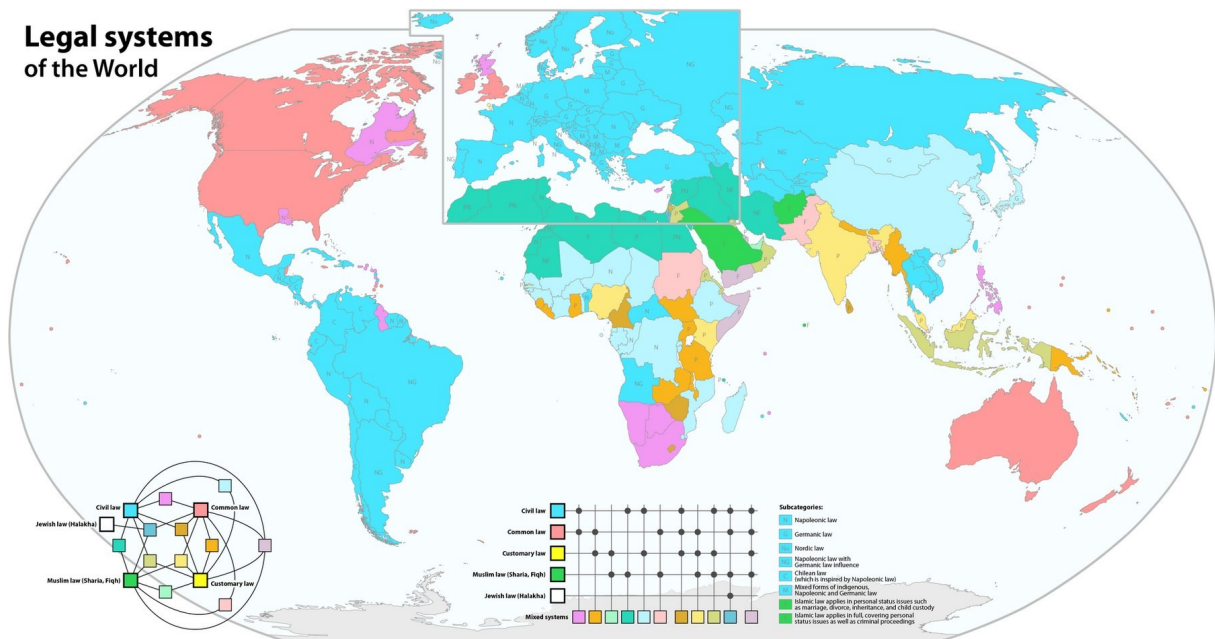


Figure 8. Legal systems of the world. Source: Wikimedia Commons, file "Map of the Legal systems of the world (en).png", licence CC BY. Author: see [https://pl.wikipedia.org/wiki/Plik:Map_of_the_Legal_systems_of_the_world_\(en\).png](https://pl.wikipedia.org/wiki/Plik:Map_of_the_Legal_systems_of_the_world_(en).png)

Private international law (conflict of laws) addresses the questions of:

1. national court jurisdiction over a particular case;
2. national law(s) applicable to the case matter.

Polish Act of 4 February 2011, Private International Law (Ustawa z dnia 4 lutego 2011 r. Prawo prywatne międzynarodowe), Journal of Laws (Dziennik Ustaw) 2011 No. 80, item 432.

The Act regulates the law applicable to private law relations with a foreign element. It identifies the applicable national law through connecting factors such as nationality, and it permits the parties to choose the applicable law where the statute allows. Public policy and overriding mandatory provisions

limit the effect of foreign law. The Act applies only where European Union law or an international agreement, such as the Rome I and Rome II Regulations, does not govern the matter.

Selected provisions

Article 2

1. If statutory law specifies the law of one's nationality as applicable, a Polish national shall be subject to Polish law, even if the law of another country recognizes him as its own national.
2. A foreigner who is a national of two or more States shall be subject, as to the law of his nationality, to the law of the country with which he is most closely connected.

Article 4

1. In cases provided by the statutory law, the applicable law may be chosen by the parties.
2. The choice of law shall be made expressly or shall clearly result from the circumstances of the case, unless the provision allowing a choice of law provides otherwise.

Translation of Articles 2 and 4 © Mateusz Pilich & Andrzej W. Wiśniewski

Public international law

Public international law is the body of rules governing relations among independent states and international organisations. It differs from other legal systems in that it primarily regulates the actions and omissions of states rather than individuals. There is no world legislature. States are both authors and subjects of the rules, and are normally bound only by rules they have accepted.

Public international law includes:

- law of treaties (agreements between states)
- law of the sea
- international criminal law (individual responsibility for the gravest crimes)
- international humanitarian law (the conduct of armed conflict)
- international environmental law
- international Internet law (these rules applied to cyberspace)

Supranational law and European Union law

Supranational law, or the law of supranational organizations, concerns regional agreements where the special distinguishing quality is that laws of nation states are held inapplicable when conflicting with a supranational legal system. European Union law is the main example: it is autonomous, it applies directly in the member states and it takes precedence over conflicting national law.

Sources of EU law:

- **Primary law:** the Treaties, the Charter of Fundamental Rights and general principles.
- **Secondary law:** regulations (directly applicable), directives (requiring national implementation) and decisions.
- **Case law** of the Court of Justice of the European Union.

Examples of EU law relevant for computer science:

- **Personal data:** General Data Protection Regulation (GDPR), Regulation (EU) 2016/679; Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive).

- **Cybersecurity:** NIS 2 Directive, Directive (EU) 2022/2555; Cyber Resilience Act, Regulation (EU) 2024/2847; Directive 2013/40/EU on attacks against information systems.
- **Data:** Data Act, Regulation (EU) 2023/2854, on access to and use of data generated by connected products and related services.
- **Online services and markets:** Digital Services Act, Regulation (EU) 2022/2065; Digital Markets Act, Regulation (EU) 2022/1925 (both described below).
- **Electronic identification and trust services:** Regulation (EU) No 910/2014 (eIDAS), as amended by Regulation (EU) 2024/1183.
- **Copyright:** Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market.
- **Artificial intelligence:** Artificial Intelligence Act, Regulation (EU) 2024/1689 (see the box below).

Artificial Intelligence Act, Regulation (EU) 2024/1689. It follows a risk-based approach: some practices are prohibited, high-risk systems face strict duties, and others face transparency duties. **Its transboundary effect is central.** It applies to providers placing AI systems on the EU market wherever they are established, and to providers and deployers in third countries whose system output is used in the Union. Like the GDPR, it exports EU standards beyond EU borders.

The CLOUD Act is not EU law. It is a United States statute allowing US authorities to require providers to disclose data stored abroad. It may conflict with EU data protection rules, notably Article 48 GDPR:

Article 48 GDPR, Transfers or disclosures not authorised by Union law

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

Digital Services Act

The Digital Services Act (DSA), Regulation (EU) 2022/2065 on a Single Market for Digital Services, sets common rules for providers of intermediary services in the Union: services that only transmit or store information provided by users, such as internet access providers, caching services, hosting services, online marketplaces and social networks. It keeps the principle that these providers are not liable for illegal content they do not know about, provided that they act expeditiously to remove or disable access to it once they obtain knowledge. It also confirms that they have no general obligation to monitor the information they transmit or store.

The DSA adds due diligence obligations that grow with the size and role of the provider. All providers must designate contact points and publish transparency reports. Hosting services must offer a notice and action mechanism for illegal content. Online platforms must provide complaint handling and explain their moderation decisions. Very large online platforms and search engines, with more than 45 million monthly active recipients in the Union, must assess and mitigate systemic risks, such as the spread of illegal content or effects on fundamental rights, and they are subject to independent audits. The Regulation applies to services offered to recipients in the Union, whatever the place of establishment of the provider. It is enforced by national Digital Services Coordinators and, for very large platforms, by the European Commission.

Digital Markets Act

The Digital Markets Act (DMA), Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector, is a competition-oriented instrument. It addresses the market power of very large digital

companies that act as important gateways between businesses and users. The European Commission designates such companies as gatekeepers when they provide a core platform service, for example an operating system, a search engine, an online intermediation service or a social network, and meet quantitative criteria on size, user numbers and market position.

Gatekeepers must comply with a list of obligations and prohibitions. For example, they may not unfairly favour their own services over those of competitors, they may not combine personal data from different services without consent, and they must allow business users and, in some cases, third-party services to interoperate with their systems. The Commission monitors compliance and may impose fines of up to 10 percent of the total worldwide annual turnover of the gatekeeper. For computer scientists, the DMA is relevant because it shapes the design of operating systems, application stores, browsers and interfaces.

Sources of international law

States create international law through treaties and practice. International organisations, such as the United Nations, adopt binding and non-binding acts. Courts apply the rules, and scholars help to identify them.

Article 38, Statute of the International Court of Justice

1. The Court, whose function is to decide in accordance with international law such disputes as are submitted to it, shall apply:
 - a. international conventions, whether general or particular, establishing rules expressly recognized by the contesting states;
 - b. international custom, as evidence of a general practice accepted as law;
 - c. the general principles of law recognized by civilized nations;
 - d. subject to the provisions of Article 59, judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law.
2. This provision shall not prejudice the power of the Court to decide a case *ex aequo et bono*, if the parties agree thereto.

Article 38 is the standard list of formal sources. Conventions, custom and general principles are primary sources. Judicial decisions and scholarly writing are only subsidiary means.

International conventions

International conventions, whether general or particular, establish rules expressly recognized by the contesting states:

- treaties, conventions, agreements and charters differ in name, not in legal effect;
- agreements are usually written, although oral agreements may also bind states;
- they may be bilateral or multilateral, and they bind only the states that have accepted them.

Treaties are the most precise and the most widely used source of obligations between states. A treaty binds the states that have consented to be bound by it (the rule *pacta sunt servanda*), and as a rule it does not create obligations for third states. Treaties are interpreted in good faith, in accordance with the ordinary meaning of their terms, in their context and in the light of their object and purpose.

Examples relevant for this course are the Budapest Convention of the Council of Europe, which is open to non-member states, and the United Nations Convention against Cybercrime.

International custom

International custom is evidence of a **general practice accepted as law**. It is the original source of international law, known as *ius gentium*. It has two elements: *usus* (consistent state practice) and *opinio juris* (the belief that the practice is legally required). State practice is shown by the conduct of state organs, such as heads of state.

- **When is a practice "accepted as law"?** When states act from a sense of legal obligation, and not only from courtesy or convenience.
- **How many customary rules are there?** The number is not fixed, because custom changes with practice.
- **How do you find them?** By examining state conduct, official statements, national legislation, treaty practice and court decisions.

Customary rules bind all states, including states that did not take part in their formation, with the exception of a state that has consistently objected to the rule while it was being formed. Custom is particularly important in cyberspace, where few binding treaties exist. Rules such as respect for the sovereignty of other states and the duty of due diligence are discussed in state positions and in scholarship as possible customary rules, although states do not agree on all their details. Outer space shows that custom can form quickly: the launch of the first satellite was accepted by other states without protest.

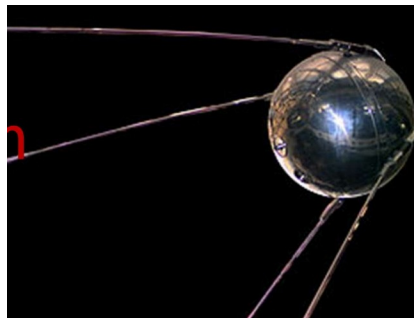


Figure 9. Sputnik 1 (1957): the practice of states in outer space as an example of rapidly formed custom.

General principles of law recognized by civilized nations

- The scope is unclear and controversial.
- They may include legal principles common to a large number of systems of national law:
 - principle of good faith
 - estoppel: a state that has, by its conduct, encouraged another state to believe in the existence of a certain legal or factual situation, and to rely upon that belief, may be estopped from asserting a contrary situation in its dealings
 - equity is said to "mitigate the rigor of common law", allowing courts to use their discretion and apply justice in accordance with natural law

General principles are used mainly to fill gaps when neither a treaty nor a customary rule gives an answer. They are identified by comparing national legal systems and by recognising principles that are common to them, for example good faith, the principle that no one may be a judge in his or her own case, and the duty to make reparation for harm caused. They also operate within international law itself, for example as principles of procedure applied by international courts and tribunals.

Judicial decisions

Judicial decisions are a subsidiary means for the determination of rules of law. The principal judicial organ of the United Nations is the International Court of Justice (ICJ) in The Hague.

Decisions of international courts and tribunals, and of national courts that apply international law, are not binding precedents in the sense known from common law systems. A judgment of the ICJ binds only the parties to the case. In practice, however, judgments and advisory opinions are cited as authoritative evidence of what the law is, and later courts rarely depart from them without explanation.



Figure 10. The courtroom of the International Court of Justice, The Hague. CC BY, Wikipedia.

Teachings of the most highly qualified publicists

Scholarly writing does not create law. It helps to identify and interpret the rules. Standard textbooks are an example.

The teachings of publicists include textbooks and monographs, the work of expert bodies such as the International Law Commission and the Institut de droit international, and expert studies prepared outside governments. A relevant example in cyberspace is the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, prepared by an independent group of experts. It is an influential scholarly interpretation of existing law, but it is not binding and does not represent the agreed position of states.

Other sources of international law

- binding decisions of international organisations, for example of the United Nations Security Council;

Some international organisations are empowered by their founding treaties to adopt decisions that bind their members. The best known example is the Security Council of the United Nations, whose decisions on threats to international peace are binding on all members of the organisation. Such acts derive their binding force from the founding treaty and not from the will of the organisation alone.

- acts of state;

A state may create legal obligations for itself through a unilateral act, for example a declaration made publicly with the intention to be bound. Acts of state, such as legislation, official statements and diplomatic notes, are also important as evidence of state practice and of *opinio juris*, the elements of custom.

- soft law, for example resolutions of the United Nations General Assembly, which are generally recommendations.

Soft law is explained in more detail in the next subsection.



Figure 11. The United Nations General Assembly Hall. CC BY, Wikipedia.

Soft law

Soft law is a collective name for international instruments and standards that are not legally binding but are intended to guide the behaviour of states and other actors. Typical forms are resolutions and declarations of international organisations, codes of conduct, guidelines, recommendations and reports of expert groups. Soft law is created more quickly and more flexibly than a treaty. It does not require ratification, and states may agree on a text that they would not accept as a binding obligation. For this reason it is used where states disagree on binding rules, or where the subject changes fast, as is the case with technology.

Soft law should not be confused with binding law. A breach of a soft law instrument is not a breach of international law and does not engage state responsibility. Soft law nevertheless has legal significance. It can guide the interpretation of treaties, it can be evidence of the expectations of states, and it can contribute to the formation of customary law when it is followed by consistent practice accompanied by *opinio juris*. It can also be a first step towards a treaty. Comparable patterns are known from other fields of international law: the declarations adopted at the Stockholm and Rio conferences in environmental law, and the standards of the Basel Committee on Banking Supervision in international economic law.

In cyberspace, soft law plays a particularly important role. The norms of responsible state behaviour, which were developed by groups of governmental experts and endorsed by the United Nations General Assembly, are voluntary and non-binding. They are a political commitment of states, and at the same time they are used to discuss how binding rules apply to cyber operations. For students of computer science, the same distinction applies to professional codes of conduct and technical standards: they are important in practice, but they are binding only if a legal act or a contract makes them so.

Sustainable development and the Sustainable Development Goals

Sustainable development is the idea that economic and social development should meet the needs of the present generation without endangering the ability of future generations to meet their own needs. It developed in international environmental law, in reports of the United Nations and in instruments such as the Rio Declaration on Environment and Development. The International Court of Justice referred to it in the *Gabcikovo-Nagymaros Project* case, when it spoke of the need to reconcile economic development with the protection of the environment. Many lawyers describe sustainable development as a guiding principle that influences the interpretation of binding rules, and not as a rule with a precise content of its own.

The Sustainable Development Goals (SDGs) are 17 goals, with 169 targets, set out in the 2030 Agenda for Sustainable Development, which the United Nations General Assembly adopted in resolution 70/1.

The Agenda is an example of soft law: it is a political commitment of states and it is not legally binding. It nevertheless shapes national policies, development financing, European Union policies and the content of later treaties. Several goals concern the work of computer scientists, for example Goal 9 on industry, innovation and infrastructure, Goal 16 on peace, justice and strong institutions, which includes public access to information and the protection of fundamental freedoms, and the goals on energy and climate, which are relevant for the energy use of data centres. The sustainable development example also shows a pattern known from environmental law: principles first appear in non-binding declarations and are later reflected in binding instruments.

Case studies

The five fictional case studies below apply the material of this document. They are intended for discussion in class or for individual study.

Case study 1: A statute and a treaty in conflict

Poland ratified an international agreement on cooperation in the investigation of cybercrime, after Parliament had given prior consent by statute. The agreement allows authorities of other parties to obtain stored traffic data from service providers under defined safeguards, and it was promulgated in the Journal of Laws. Later, Parliament adopted an ordinary statute with a stricter procedure that excludes such access, and a ministry issued a regulation restricting the disclosure of traffic data.

A Polish telecommunications provider received a request from a foreign authority based on the agreement. The provider refused, relying on the later statute and the regulation. The foreign authority insisted on the agreement. The provider also argued that disclosure would unduly limit the privacy of its customers.

Questions for discussion

1. Which sources of universally binding law are involved, and how are they ranked in the hierarchy of sources in Polish law?
2. Why did the agreement require prior consent granted by statute (great ratification), and what is the legal effect of its promulgation?
3. Which act prevails in case of conflict: the agreement, the later statute or the regulation? Refer to the relevant provisions of Article 91 of the Constitution.
4. May the legislature limit privacy by statute, and under what conditions does Article 31 of the Constitution allow limitations of constitutional freedoms and rights?

Case study 2: A cross-border software licence

A Polish software company concluded an online licence agreement with a company established in a third country. The agreement contains a clause stating that it is governed by the law of a named state. A dispute arose about liability for a security flaw. The licensee argues that the clause is invalid and that Polish courts should decide the case under Polish law.

The signatory of the licensee, an individual developer, holds both Polish nationality and the nationality of the third country, and the Polish company questions his capacity to act. The chosen law contains a rule that excludes liability for intentional breaches of security obligations, which the Polish company considers contrary to the basic principles of the Polish legal order.

Questions for discussion

1. What two questions does private international law address, and how do they apply to this dispute?
2. May the parties choose the applicable law, and how must the choice be expressed (Article 4 of the Polish Act on Private International Law)?
3. Which law governs the capacity of the developer, and how does Article 2 of the Act treat a person who holds Polish and foreign nationality?

4. Could the Polish court refuse to apply the chosen law on grounds of public policy, and how would it establish the content of foreign law? What is the role of European Union instruments and international agreements?

Case study 3: An attack launched through servers in a third state

A ransomware attack disrupted the network of a hospital group in State A. Technical analysis showed that the attack was controlled from servers located in State B. The authorities of State A informed those of State B several times and asked them to stop the operation, but State B took no action. State A is considering countermeasures and invokes a duty of State B to act with due diligence.

State B replies that it is not a party to any treaty with State A on this matter and that no rule of customary international law obliges it to prevent harmful cyber activity from its territory. It adds that documents of international organisations on responsible state behaviour in cyberspace are political and not binding.

Questions for discussion

1. What are the sources of international law under Article 38 of the Statute of the International Court of Justice, and which of them could State A rely on?
2. What two elements are required to establish a customary rule? Which questions would a court ask about state practice and *opinio juris* in this case?
3. What is the legal value of documents that are not treaties, such as decisions of international organisations and soft law?
4. Public international law primarily regulates the actions and omissions of states. How does this feature apply to the attack, which was carried out by private actors?

Case study 4: An artificial intelligence service offered from outside the Union

A company established outside the European Union develops an artificial intelligence system for screening job applicants. The system is sold to employers in several states. One employer, also established outside the Union, uses the system to rank applicants who are residents of a member state. The same company also sells connected devices with digital elements to consumers in the Union, and it operates a cloud platform used by an operator of energy infrastructure in a member state.

The company states that, as it has no establishment in the Union, none of the Union rules apply to it. A national authority disagrees and refers to the Artificial Intelligence Act, the General Data Protection Regulation, the Cyber Resilience Act and the NIS 2 Directive.

Questions for discussion

1. What is the territorial reach of the Artificial Intelligence Act, and why is it described as having a transboundary effect?
2. Is the company right that the absence of an establishment in the Union excludes the application of Union law? Consider the role of the General Data Protection Regulation as a comparison.
3. Which of the instruments mentioned are regulations and which is a directive? What is the consequence of this difference for the obligations of the company?
4. How do direct effect and primacy explain the position of Union law in the legal systems of the member states?

Case study 5: A foreign order for data stored in Europe

A cloud provider established in the United States stores data of a Polish company in a data centre in the Union. A United States authority issues an order requiring the provider to disclose the data under the CLOUD Act. The provider fears that compliance would violate Article 48 of the General Data Protection Regulation, while refusal could lead to sanctions in the United States.

At the same time, Polish prosecutors investigating the same persons seek cooperation with foreign authorities under the Convention on Cybercrime. A third state, party to the United Nations Convention against Cybercrime, also requests assistance. The Polish company asks its lawyers which rules apply and who may lawfully obtain the data.

Questions for discussion

1. What is the legal nature of the CLOUD Act, and why does it raise a conflict with European Union data protection rules?
2. What is the role of international agreements such as the Budapest Convention and the Hanoi Convention, and which states are bound by them?
3. If Poland becomes bound by such a treaty, what is its position in the hierarchy of sources in Polish law?
4. Would a Polish court be able to refuse the effects of foreign law or foreign orders that conflict with the fundamental principles of the Polish legal order?

Quiz

Choose one correct answer for each question.

1. According to Article 87 of the Constitution of the Republic of Poland, which of the following lists correctly identifies the sources of universally binding law in the Polish legal system? Consider that the provision names a closed catalogue of sources.

- A. The Constitution, statutes, regulations and internal guidelines of ministries, which bind all persons once they have been issued by the competent administrative body.
- B. The Constitution, statutes, ratified international agreements and regulations, which together form the catalogue of universally binding sources of law in the Republic of Poland.
- C. The Constitution, statutes, regulations and unratified international agreements, which are all directly applicable as soon as they have been signed by the executive.
- D. Statutes, regulations and customary international law only, because the Constitution itself is not a source of universally binding law but merely a political declaration of the Nation.

2. A ratified international agreement was approved by Parliament through a statute granting prior consent. Later, an ordinary statute is adopted that cannot be reconciled with a provision of that agreement. Under Article 91 of the Constitution, which rule applies in the Polish legal order?

- A. The later statute prevails, because the more recent act always replaces earlier norms, regardless of the manner in which the international agreement was ratified.
- B. Both acts are suspended until the President decides which of them is to be applied, because the Constitution does not rank statutes and agreements and leaves the matter to the head of state.
- C. The statute prevails unless the agreement has been published in the Official Journal of the European Union, which is the only publication that gives treaties domestic effect in Poland.
- D. The agreement has precedence over the conflicting statute, because it was ratified upon prior consent granted by statute and forms part of the domestic legal order after promulgation.

3. Under Article 89 of the Constitution, ratification of an international agreement by Poland requires prior consent granted by statute when the agreement concerns certain matters. Which of the following agreements clearly falls within the matters listed in that article?

- A. An agreement that imposes considerable financial responsibilities on the State, which therefore may be ratified only after Parliament has consented by statute.
- B. An agreement of a purely technical nature on the exchange of publications between two ministries, without any financial or legal consequences for citizens or for the State.
- C. An agreement that sets an administrative timetable for meetings of officials of two states, without creating rights or obligations for citizens.
- D. A political declaration without binding force, which merely expresses the intention of two governments to cooperate in the future.

4. A Polish company and a foreign company conclude a contract containing a clause that names the national law governing their dispute. According to Article 4 of the Polish Act on Private International Law, as presented in the lecture, what is required for a valid choice of law where a provision allows it?

- A. The choice must always be approved by a Polish court before the contract takes effect, in order to protect the weaker party against unfair clauses.
- B. The choice is valid only if it designates Polish law, because Polish courts are not allowed to apply the law of another state to a private dispute.
- C. The choice may be made by the parties only in cases provided by statute, and it must be made expressly or clearly result from the circumstances of the case.
- D. The choice is valid only if it is made in notarial form and then entered in a public register, which is kept by the competent ministry.

5. Article 38 of the Statute of the International Court of Justice describes international custom as evidence of a general practice accepted as law. Which statement correctly describes the two elements that are normally required to establish a rule of customary international law?

- A. The written ratification of the rule by at least two states, together with its publication in a treaty series that is maintained by the United Nations.
- B. Judicial decisions and the teachings of the most highly qualified publicists, which together create binding custom without any need for the practice of states.
- C. The prior consent of every state in the world and the codification of the rule by an international organisation, which must adopt it by unanimous vote.
- D. State practice (usus) and the belief that the practice is required by law (opinio juris), which must both be shown to establish a rule of customary law.

6. A lecturer explains that public international law differs from private international law and from most national legal systems. Which statement best captures the distinguishing feature of public international law, as described in the course materials?

- A. It governs relations among independent states and international organisations, and it primarily regulates the actions and omissions of states rather than those of individuals.
- B. It determines which national court has jurisdiction over a private dispute and which national law applies to the case, using connecting factors such as nationality.
- C. It consists exclusively of treaties which a state has ratified, and it never includes custom, general principles of law or the decisions of international organisations of any kind.
- D. It regulates contracts between private parties across borders and is created by national parliaments, which adopt it as statutes for their own territories only.

7. In the case known as Van Gend en Loos, the Court of Justice set criteria for the direct effect of a provision of Union law. According to the lecture, which conditions must a provision meet so that individuals can rely on it before national courts?

- A. It must be adopted unanimously by all member states and be published in the national gazette of every member state before it can be invoked.
- B. It must be contained in a directive and not in a regulation, and it must be addressed to the individual by name in the text of the act.
- C. It must be sufficiently clear and precisely stated, unconditional or non-dependent, and confer a specific right on the citizen on which he or she can base a claim.
- D. It must have been transposed into national law by every member state, since only national legislation can give rights to private persons, and never the Treaties themselves.

8. A company wishes to understand the difference between the General Data Protection Regulation, which is a regulation, and the NIS 2 Directive, which is a directive. Which statement correctly distinguishes these two types of secondary Union law?

- A. Regulations bind only the institutions of the Union, whereas directives bind individuals directly in all situations and need no action by the member states at all.
- B. Regulations are binding and directly applicable in the member states, whereas directives are binding as to the result to be achieved and require implementation in national law.
- C. Regulations are mere recommendations without binding force, whereas directives are binding and prevail over the constitutions of all member states.
- D. Regulations and directives are identical in effect, and the choice between them depends only on the length of the text adopted by the legislature.

9. A company established outside the European Union places an artificial intelligence system on the Union market, and a company in a third country uses the output of a system in the Union. Which statement best describes the territorial reach of the Artificial Intelligence Act, Regulation (EU) 2024/1689?

- A. It applies only to providers established in the Union, because regulating companies outside the Union would always violate the sovereignty of third states.
- B. It applies only if the provider has a physical office in a member state, and it never reaches companies that offer services solely over the internet.
- C. It applies only to public authorities of the member states, while private companies are governed exclusively by their national law of establishment and by contract.
- D. It applies to providers placing systems on the Union market wherever they are established, and to providers and deployers in third countries whose output is used in the Union.

10. A cloud provider that stores data in a data centre in the European Union receives an order from United States authorities based on the CLOUD Act. Which statement is correct about the legal nature of the CLOUD Act and its relation to Union law?

- A. It is a United States statute that allows United States authorities to require providers to disclose data stored abroad, and it may conflict with Union data protection rules, notably Article 48 of the General Data Protection Regulation.
- B. It is a regulation of the Union that applies directly in all member states, so that no conflict with other Union rules can arise in practice, whatever the content of the order received.
- C. It is a treaty of the Council of Europe that Poland has ratified, and it therefore ranks above the Constitution in the Polish hierarchy of sources, so that no further analysis is needed.
- D. It is a convention of the United Nations that replaced the Budapest Convention and binds every state, including those that did not sign it, once it has been published.

Summary

This summary brings together the main points of the course materials.

1. **Law and ethics.** Law consists of binding rules that can be enforced. Ethics, professional codes, technical standards and soft law are different types of norms. Many questions of computer science appear first as ethical problems and later become legal obligations.
2. **Sources of law in Poland.** Article 87 of the Constitution lists the sources of universally binding law: the Constitution, statutes, ratified international agreements and regulations. The Constitution is the supreme law. Statutes regulate the matters that concern the rights and obligations of individuals, and regulations may be issued only on the basis of a statute.
3. **Constitutional rights.** The Constitution protects human dignity, private life, the privacy of communication, the inviolability of the home, information about a person, freedom of expression and the right to compensation. Limitations of rights are allowed only by statute and under the conditions of Article 31.
4. **Treaties in the Polish legal order.** A treaty is ratified by the President, after consent by statute (great ratification) in the cases listed in Article 89, or without it (small ratification). The procedure is specified in the Act on International Agreements. After promulgation, a ratified treaty is part of the domestic legal order and a treaty ratified with consent by statute prevails over conflicting statutes.
5. **Three meanings of international law.** Private international law decides which court has jurisdiction and which national law applies in cases with a foreign element. Public international law governs relations among states and international organisations. Supranational law, above all the law of the European Union, applies directly and prevails over national law.
6. **European Union law.** Regulations are directly applicable, directives require implementation, and provisions that are clear, unconditional and confer rights have direct effect. Instruments relevant for computer science include the GDPR, the NIS 2 Directive, the Cyber Resilience Act, the Data Act, the Digital Services Act, the Digital Markets Act and the Artificial Intelligence Act. The AI Act and the GDPR have a transboundary effect, because they also apply to providers established outside the Union. The CLOUD Act of the United States may conflict with Article 48 GDPR.
7. **Sources of international law.** Article 38 of the Statute of the International Court of Justice lists treaties, custom and general principles as primary sources, and judicial decisions and scholarly writing as subsidiary means. Custom requires state practice and *opinio juris*. Binding decisions of international organisations, acts of state and soft law complete the picture. Binding law should be distinguished clearly from soft law, such as the Sustainable Development Goals.
8. **Cybercrime and cybersecurity.** The Budapest Convention and the United Nations Convention against Cybercrime are treaties, while the NIS 2 Directive and the Cyber Resilience Act are Union law. These instruments will be studied in the following parts of the course, together with the principles of jurisdiction.

The common message is that technology law is not a separate field. It is built from the same sources, hierarchies and principles as the rest of national, European and international law, and the ability to identify the source of a rule and its place in the hierarchy is the first step in solving a legal problem.