LODZ CYBER HUB
University of Lodz

Legal Aspects of Computer Science — **Student Guide**

Section 2: ISP Liability (Modules 5–7)

Lodz Cyber Hub - www.cyber.uni.lodz.pl

University of Lodz Law School
Dr Joanna Kulesza
Academic Year 2025/26
For internal student use only

Preliminary Note

The term **Internet Service Provider (ISP)** is used in this module in a broad, technologically neutral manner. It includes traditional access, caching, and hosting entities, as well as contemporary online platforms and communication services—such as **TikTok, Instagram, WhatsApp, VKontakte, and WeChat**—which function as intermediaries under current European regulatory frameworks. Many such services fall within the categories of **online platforms** or **Very Large Online Platforms (VLOPs)** under the **Digital Services Act (DSA)**.

Recommended Reading

Kulesza, J. (2025). *Privacy and data protection*. In R. Balleste, G. Doucet & M. L. D. Hanlon (eds.), **A Research Agenda for Cybersecurity Law and Policy** (pp. 173–188). Cheltenham–Northampton: Edward Elgar Publishing.

Kulesza, J., & Burdiak, P. (2024). *Countering Disinformation on Social Media Platforms: Developments in the EU and Poland*. **Mediaforum: Analytics, Forecasts, Information Management**.

Van Benthem, T., Kulesza, J., Liu, Y., & Sun, N. (2024). *Jurisdiction in cyberspace*. Geneva: Geneva Centre for Security Policy (GCSP).

Overview of Section 2

This section examines the legal and institutional architecture governing intermediary services in the European Union and internationally. It addresses the evolution of safe-harbour regimes, the responsibilities of online platforms, procedural obligations for content governance, and the relationship between intermediaries and cybercrime enforcement. Discussion integrates the **E-Commerce Directive**, **Digital Services Act**, **DSM Copyright Directive**, **AVMS Directive**, **Terrorist Content Online Regulation**, the **Codes of Conduct** for online platforms, and related soft-law instruments.

2.1 Legal Status of Internet Service Providers

Definitions and Regulatory Sources

The foundational classification of intermediaries—**mere conduit**, **caching**, and **hosting**—derives from the **E-Commerce Directive 2000/31/EC**. The **Digital Services Act (Regulation (EU) 2022/2065)** supplements this framework with extensive procedural duties, particularly for online platforms and VLOPs.
Additional relevant instruments include the **Audiovisual Media Services Directive (AVMSD)**, the **Terrorist Content Online Regulation**, the **European Electronic Communications Code (EECC)**, and the **NIS2 Directive**.

The legal taxonomy of information-society intermediaries within the European Union rests primarily on the E-Commerce Directive 2000/31/EC (ECD). Articles 12–14 ECD establish three functional categories—mere conduit, caching, and hosting—each defined by the nature of the service and the degree of control exercised over transmitted or stored information. Article 12 regulates "mere conduit" services whose activities are limited to the technical transmission of data without modification. Article 13 defines caching as the automatic, intermediate, and temporary storage of information for the sole purpose of efficient onward transmission. Article 14 outlines hosting, characterised by the storage of information provided by a recipient of the service, subject to conditional liability exemptions where the provider lacks actual knowledge of unlawful activity and acts expeditiously upon obtaining such knowledge.

This foundational structure has been substantially modernised by the Digital Services Act (Regulation (EU) 2022/2065, DSA), which recalibrates intermediary duties while preserving the liability exemptions of Articles 4–6 DSA, which mirror and update the ECD safe harbours. The DSA introduces granular procedural obligations, including notice-and-action mechanisms (Art. 16), internal complaint-handling systems (Art. 20), transparency reporting (Art. 15), and specific due-diligence duties for online platforms (Arts. 19–24). Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) must additionally conduct systemic risk assessments (Art. 34), implement risk-mitigation measures (Art. 35), and submit to enhanced auditing and data-access obligations (Arts. 37–40).

Complementary legislation further shapes the regulatory landscape. The Audiovisual Media Services Directive (Directive 2010/13/EU, as amended) imposes obligations on video-sharing platforms, including measures to protect minors and address hate speech (Arts. 28a–28b). Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online mandates removal of such content within one hour of a removal order (Art. 3). The European Electronic Communications Code (Directive (EU) 2018/1972) governs providers of interpersonal communications services, supplementing the intermediary framework with sector-specific obligations. Cybersecurity duties arise under the NIS2 Directive (Directive (EU) 2022/2555), which imposes risk-management, incident-reporting, and supply-chain security obligations (Arts. 21–23).

Core Obligations

Intermediaries are subject to obligations relating to cybersecurity, cooperation with lawful data-access requests (**E-Evidence package**), consumer protection, copyright compliance (**DSM Directive**), and structured processes for addressing illegal content (**DSA**). These obligations intersect with data-protection requirements under the **GDPR** and fundamental-rights safeguards under the **EU Charter of Fundamental Rights**.

Intermediaries must comply with a dense network of substantive and procedural duties that transcend technical categorizations. Cybersecurity obligations under NIS2 require entities to implement "appropriate and proportionate" organisational and technical measures, including encryption, incident-handling protocols, and business continuity plans pursuant to Article 21. The proposed E-Evidence package introduces harmonised mechanisms for cross-border production and preservation orders, enabling competent authorities to seek direct cooperation from service providers.

Copyright obligations derive from the Directive on Copyright in the Digital Single Market (Directive (EU) 2019/790, DSM). Article 17 significantly reshapes the liability of online content-sharing service providers by imposing a regime of conditional liability linked to licensing efforts, best-efforts obligations to prevent future uploads of unauthorised works, and rapid removal duties following notice.

The DSA reinforces procedures for the removal of illegal content, requiring accessible notice mechanisms (Art. 16), effective redress structures (Arts. 20–21), and cooperation with trusted flaggers (Art. 22). These duties operate alongside GDPR constraints, particularly lawful-processing principles under Articles 5–6 GDPR and data-subject rights. All measures must respect fundamental rights enshrined in the EU Charter, notably freedom of expression (Art. 11) and the right to data protection (Art. 8).

Evolution of Roles and Governance

The regulatory environment combines binding legislation with co- and self-regulatory instruments, including the **Code of Conduct on Countering Illegal Hate Speech Online**, the **Strengthened Code of Practice on Disinformation**, and initiatives under the EU Internet Forum. These frameworks shape platform behaviour and supplement statutory obligations.

The regulatory framework is complemented by co-regulatory and voluntary governance instruments that shape intermediary practices beyond binding legislation. The Code of Conduct on Countering Illegal Hate Speech Online (2016, regularly updated) establishes commitments by major platforms to review hate-speech notifications within defined timeframes and adopt effective content-moderation procedures. The Strengthened Code of Practice on Disinformation (2022) introduces voluntary but monitored commitments for mitigating systemic risks, enhancing algorithmic transparency, and supporting independent research access. Additional initiatives, such as those emerging from the EU Internet Forum, facilitate cooperation between platforms and governmental authorities on issues including violent extremist content and crisis-response mechanisms.

Together, these instruments foster an evolving hybrid governance model in which statutory obligations, co-regulatory standards, and platform self-regulation interact. This layered structure recognises the increasingly complex societal functions of intermediaries—including social media platforms, communication services such as WhatsApp, WeChat, and VKontakte, and content-distribution services—and seeks to balance innovation, security, and the protection of fundamental rights within the European digital environment.

2.2 Intermediary Liability Regimes

Safe-Harbour Principles under EU Law

Intermediary liability within the European Union continues to be structured around the safe-harbour regime established by the **E-Commerce Directive 2000/31/EC (ECD)**. Articles **12–14 ECD** set out conditional liability exemptions for three categories of intermediary activity: *mere conduit* (Art. 12), *caching* (Art. 13), and *hosting* (Art. 14). Under Article 12, providers engaged solely in the technical transmission of information are exempt from liability where they neither initiate transmission nor select or modify transmitted data. Article 13 offers protection for automatic, temporary caching, provided the provider acts to remove or disable access to cached material when required. Article 14, central to contemporary platform governance, grants a conditional exemption to hosting providers who have no actual knowledge of illegal activity or information and act expeditiously upon obtaining such knowledge.

These safe harbours remain formally preserved under the **Digital Services Act (Regulation (EU) 2022/2065, DSA)**, specifically Articles **4–6 DSA**, which reaffirm the non-general-monitoring principle (Art. 8) while integrating new due-diligence obligations. At the intersection of liability and content governance, the **Copyright in the Digital Single Market Directive (Directive (EU) 2019/790, DSM)** introduces a distinct structure for platforms enabling the large-scale sharing of copyrighted material. Article **17 DSM** imposes "best efforts" obligations to obtain licences, prevent unauthorised uploads, and ensure swift removal of infringing works. This effectively narrows the applicability of the hosting safe harbour for online content-sharing service providers, reflecting the European legislature's sector-specific recalibration of intermediary liability.

Notice-and-Action Mechanisms under the DSA

The DSA introduces harmonised and structured notice-and-action procedures applicable to all hosting services. Article 16 DSA requires providers to maintain accessible, user-friendly notice mechanisms enabling individuals or entities to report potentially illegal content. Notices must be assessed diligently, and successful notifications generate actual knowledge, triggering the provider's duty to act expeditiously as required under Article 14 ECD and Article 6 DSA.

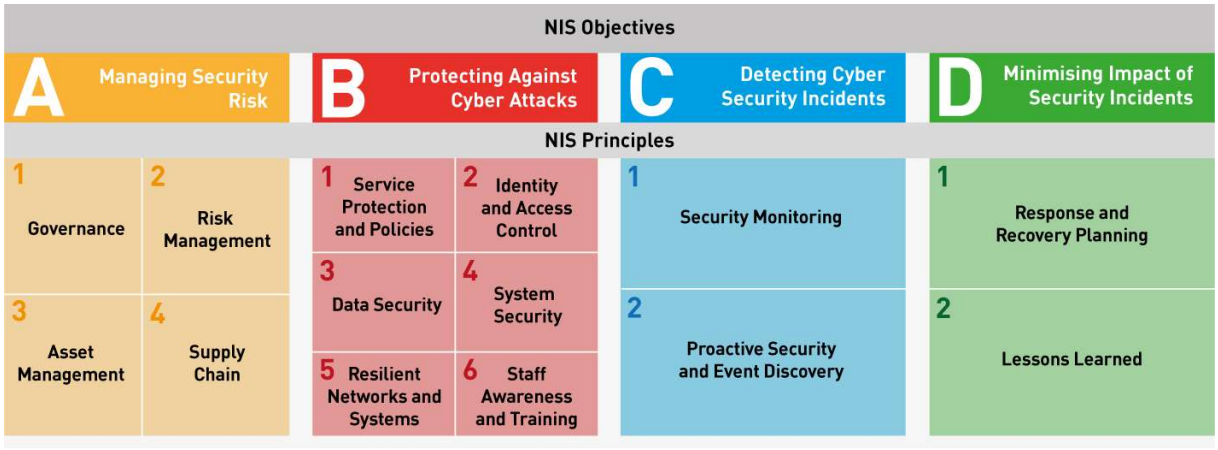
Articles 20–21 DSA require intermediaries to establish internal complaint-handling systems and provide access to certified out-of-court dispute settlement bodies, enhancing procedural fairness and user redress. Transparency obligations under Articles 15 and 23 DSA mandate periodic public reporting on content moderation, algorithmic recommendations, and enforcement actions. These mechanisms coexist with sector-specific regimes such as the Audiovisual Media Services Directive (Directive 2010/13/EU, AVMSD), particularly Articles 28a–

28b, and the Terrorist Content Online Regulation (Regulation (EU) 2021/784, TCO), which imposes one-hour takedown requirements (Art. 3 TCO).

Platform Governance and Systemic Risks

A major innovation of the DSA lies in its obligations relating to algorithmic governance and systemic risks. Articles **34–35 DSA** require Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) to conduct periodic systemic-risk assessments addressing illegal content, fundamental-rights impacts, disinformation, and intentional manipulation of services. Platforms must adopt proportionate mitigation measures, including adapting algorithmic systems or moderating amplification mechanics. Article **36 DSA** establishes special *crisis-response mechanisms*, while Articles **37–39** impose annual independent audits, reinforced transparency duties, and data-access obligations for researchers.

These duties interact closely with cybersecurity requirements under the **NIS2 Directive (Directive (EU) 2022/2555)**. Entities classified as "important" or "essential" under Articles **2–3 NIS2** must implement risk management measures (Art. 21), report significant incidents (Art. 23), and ensure supply-chain security. For major platforms, NIS2 reinforces the DSA framework by mandating robust technical safeguards—including encryption, incident handling, and operational resilience—thereby linking liability, content moderation, and cybersecurity governance into an integrated regulatory landscape.



Img 1. NIS Objectives and Principles. source Nexor; For more info see https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf

Co- and self-regulatory instruments, including the **Code of Conduct on Countering Illegal Hate Speech Online** and the **Strengthened Code of Practice on Disinformation**, complement legislative obligations by shaping platform standards, informing best practices, and supporting systemic-risk mitigation under the DSA.

Test Question 1

Which statement best describes the purpose of EU safe-harbour rules for online intermediaries?

A. To impose strict liability for all user-generated content.
B. ✔ **To exempt intermediaries from liability when acting as neutral technical conduits.**

C. To require platforms to monitor all content proactively.
D. To ensure intermediaries directly license all copyrighted works.

Test Question 2

What is the primary goal of EU notice-and-action procedures?

A. To replace judicial review with automated decision-making.
B. ✔ **To facilitate user reporting of illegal content and ensure timely platform response.**
C. To grant platforms complete discretion over whether to act on user complaints.
D. To harmonise copyright licences across all Member States.

Test Question 3

Which of the following best characterises the systemic-risk obligations imposed on major online platforms?

A. They require platforms to shut down user accounts without explanation.
B. ✔ **They oblige platforms to assess and mitigate broad societal risks such as disinformation and harmful design choices.**
C. They allow platforms to outsource all compliance responsibilities.
D. They apply only to small and medium-sized service providers.

2.3 Cybercrime and ISP Accountability

Budapest Convention and EU Cybercrime Instruments

The **Budapest Convention** remains the principal international treaty guiding state cooperation on cybercrime. EU developments—such as the **E-Evidence Regulation and Directive**, **NIS2**, and the **Europol Regulation**—further define procedural duties for intermediaries regarding data preservation, disclosure, and investigative cooperation.

Content Moderation and Security Regulation

Intermediaries play a crucial role in addressing harmful and illegal content, including obligations arising from the **Terrorist Content Online Regulation**, DSA systemic-risk mitigation requirements, and practices developed under the EU's disinformation and hate-speech frameworks.

Limits to Intermediary Responsibility

Under EU law, intermediaries cannot be subjected to general monitoring obligations (**Art. 8 DSA; Art. 15 ECD**). All regulatory measures must respect fundamental rights, particularly freedom of expression (Art. 11 CFR) and data-protection principles (GDPR).

Annex A: Budapest Convention on Cybercrime and Polish Implementation

The Budapest Convention on Cybercrime (Council of Europe Treaty No. 185), adopted on 23 November 2001, represents the foundational legal framework for addressing crimes committed via or against computer systems. It is the first binding international treaty to harmonise criminal law provisions, improve investigative techniques, and enhance international cooperation in combating cybercrime. Its transnational importance reflects the borderless nature of digital offences. The Convention seeks not only punitive but also protective aims: it preserves security and integrity in the digital environment while maintaining the rule of law and protecting fundamental human rights.

Poland ratified the Convention in 2015. It incorporated its norms into the **Penal Code (Kodeks Karny)** and the **Code of Criminal Procedure (Kodeks Postępowania Karnego)**, ensuring that domestic law mirrors the Convention's structure, which is divided into substantive offences (Articles 2–10), procedural powers and safeguards (Articles 15–21), and rules on jurisdiction and international cooperation (Articles 22–35). This annex provides the full text of key articles, the relevant Polish statutory provisions, interpretative commentary, and examination questions for students of computer science and cybersecurity law.

I. Introduction

Conventional Basis and Ratification
The Budapest Convention establishes a universal, binding, and transnational legal basis for combating cybercrime. Its innovative design covers:

1. **Substantive criminal offences** (Articles 2–10) – defining illegal acts such as unauthorised access, data interference, fraud, and child sexual and abusive materials (CSAM);
2. **Procedural powers and safeguards** (Articles 15–21) – enabling evidence preservation, interception, and search, subject to rights protections;
3. **Jurisdiction and cooperation** (Articles 22–35) – governing how States exercise jurisdiction and cooperate with each other in investigations and prosecutions.

Upon ratifying, Poland integrated these obligations into national law to ensure coherence between its criminal provisions and the Convention's mandates.

II. Substantive Criminal Law (Articles 2–10)

Article 2 – Illegal Access
Full text (Budapest Convention):
"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right.
A Party may require that the offence be committed by infringing security measures, with the

intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system."

Polish Implementation – Penal Code Article 267 (English translation):
§1. Whoever, without authorisation, obtains information not intended for them, by opening a sealed letter, connecting to a telecommunications network, or using another technical means, shall be subject to a fine, restriction of liberty, or imprisonment for up to two years.
§2. The same penalty shall apply to whoever, without authorisation, gains access to information contained in a computer system or network.
§3. Whoever, without authorisation, installs or uses equipment, software, or other means intended to obtain information, shall be subject to imprisonment for up to three years.

Explanation:
This article criminalises intentional unauthorised access, commonly referred to as "hacking." The offence requires a lack of right or permission — accidental or lawful administrative access is excluded. Under Polish law, the protection extends to any information medium, reflecting a technology-neutral standard.

Test Question:
Which of the following constitutes illegal access under Article 2 of the Budapest Convention?
A) Accessing public websites for research
B) Logging into another person's email account without permission ✅
C) Testing one's own company's network security
D) Sending encrypted data to a friend

Correct answer: B

Article 3 – Illegal Interception
Full text (Budapest Convention):
"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the interception by technical means of non-public transmissions of computer data to, from, or within a computer system, including electromagnetic emissions."

Polish Implementation – Penal Code Article 267 §3 (English translation):
"Whoever, without authorisation, intercepts information transmitted in a telecommunications network, including computer data or electronic communications, shall be subject to imprisonment for up to three years."

Explanation:
Illegal interception concerns the eavesdropping of non-public data transmissions. It protects confidentiality in motion—such as network packets, e-mails, or other data flows. Legitimate interception under judicial or prosecutor authorisation is not criminalised here.

Test Question:
Under Article 3, interception becomes illegal when:
A) It occurs through public Wi-Fi monitoring
B) It captures non-public data without authorisation ✅

C) It is performed under a judicial warrant
D) It involves encryption

Correct answer: B

Article 4 – Data Interference
Full text (Budapest Convention):
"Each Party shall adopt such measures as may be necessary to criminalise the damaging, deletion, deterioration, alteration, or suppression of computer data without right."

Polish Implementation – Penal Code Article 268 (English translation):
§1. Whoever, without authorisation, damages, deletes, alters, or prevents access to computer data shall be subject to imprisonment for up to three years.
§2. If the act causes significant harm or affects public interest, the perpetrator shall be subject to imprisonment for up to five years.

Explanation:
This crime protects the integrity of computer data. It covers acts such as malware deployment, deletion, or sabotage, but also unauthorised data alteration. Polish law further escalates the punishment where public interest or significant damage is involved.

Test Question:
Which act qualifies as data interference?
A) Viewing a file without permission
B) Deleting another person's files without right ✅
C) Copying public data
D) Encrypting one's own documents

Correct answer: B

Article 5 – System Interference
Full text (Budapest Convention):
"Each Party shall adopt such measures as may be necessary to criminalise the intentional serious hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data."

Polish Implementation – Penal Code Article 269 (English translation):
§1. Whoever, without authorisation, interferes with the functioning of an information system by introducing, deleting, or altering computer data, shall be subject to imprisonment for three months to five years.
§2. If the act results in significant disruption of system functioning, the penalty shall be imprisonment from one to eight years.

Explanation:
System interference targets disruption rather than mere access or data damage. It encompasses denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks, or other

malicious interventions that impair system functionality. Polish law includes aggravated penalties when disruption is grave.

Test Question:
A Distributed Denial-of-Service (DDoS) attack qualifies under:
A) Article 2 – Illegal Access
B) Article 5 – System Interference ✅
C) Article 6 – Misuse of Devices
D) Article 4 – Data Interference

Correct answer: B

Article 6 – Misuse of Devices
Full text (Budapest Convention):

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:
   (a) the production, sale, procurement for use, import, distribution or otherwise making available of:
      (i) a device, including a computer programme, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5 of this Convention;
      (ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed;
   (b) the possession of an item referred to in paragraph (a) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5.

2. This article shall not be interpreted as imposing criminal liability where the production, possession, or use of such devices is for the authorised testing or protection of computer systems.

3. Each Party may reserve the right not to apply paragraph 1(b) of this article.

Polish Implementation – Penal Code Article 269b (English translation):
§1. Whoever produces, acquires, sells, or provides to another person devices, computer programmes, passwords, or access data adapted for committing an offence specified in Articles 267–269, shall be subject to imprisonment for up to three years.
§2. The same penalty applies to anyone who possesses such items with the intent to commit such an offence.
§3. Acts committed in the course of authorised testing, research, or security assessment are not punishable.

Explanation:
This article penalises not only the direct misuse of systems but also the creation, distribution, or procurement of tools (software, passwords, devices) designed to facilitate cyberoffences. The

Convention explicitly excludes legitimate security research or testing from criminal liability. Polish law reflects this exclusion.

Test Question:
Under Article 6, which situation constitutes an offence?
A) A cybersecurity firm owning malware samples for training
B) A researcher testing his own system's defences
C) Selling access credentials to third parties without right ✅
D) Using open-source encryption software

Correct answer: C

Article 7 – Computer-Related Forgery
Full text (Budapest Convention):
"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic. A Party may require an intent to defraud or similar dishonest intent before criminal liability attaches."

Polish Implementation – Penal Code Article 270 (English translation):
§1. Whoever, with intent to use as authentic, forges or alters a document or uses such a document as authentic, shall be subject to imprisonment for three months to five years.
§2. Whoever fills in a signed blank form contrary to the will of the person who signed it, shall be subject to the same penalty.
§3. The same penalty applies to whoever commits these acts with respect to an electronic document.
§4. Attempt and aiding are punishable.

Explanation:
Computer-related forgery protects the authenticity of legal and transactional documents. It criminalises falsifying electronic documents or signatures so that they appear genuine, with the intent that others rely on them legally. Polish law applies traditional forgery principles to electronic documents, thereby aligning with the Convention's technology-neutral approach.

Test Question:
What is a key element of computer-related forgery?
A) Unauthorised reading of data
B) Creation of false electronic information intended to appear genuine ✅
C) Failure to secure a server
D) Lawful alteration of one's own data

Correct answer: B

Article 8 – Computer-Related Fraud
Full text (Budapest Convention):

"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:
(a) any input, alteration, deletion or suppression of computer data;
(b) any interference with the functioning of a computer system,
with fraudulent or dishonest intent of procuring an economic benefit for oneself or for another person."

Polish Implementation – Penal Code Article 286 (English translation):
§1. Whoever, with intent to gain a material benefit, induces another person to an unfavourable disposition of property by misleading them or by exploiting their mistake or inability to understand the action undertaken, shall be subject to imprisonment for six months to eight years.
§2. Preparation and attempt are punishable.
§3. The same applies when the act is committed by using a computer system or data transmission network.

Explanation:
This crime emphasises deception: fraudulent actions through electronic means to mislead someone into a disadvantageous transaction. Forms include phishing, falsified transactions, or using malware to manipulate financial data. The dishonest intention and economic loss requirement are essential. Polish law explicitly criminalises such acts when performed via computer systems.

Test Question:
Which condition must exist for computer-related fraud?
A) Loss of data integrity
B) Unauthorised access alone
C) Intent to gain material benefit through deception ✅
D) Use of encryption

Correct answer: C

Article 9 – Offences Related to Child Pornography
Full text (Budapest Convention):

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:
   (a) producing child pornography for the purpose of its distribution through a computer system;
   (b) offering or making available child pornography through a computer system;
   (c) distributing or transmitting child pornography through a computer system;
   (d) procuring child pornography through a computer system for oneself or for another person;
   (e) possessing child pornography in a computer system or on a data storage medium.

2. For the purpose of paragraph 1 above, "child pornography" shall include pornographic material that visually depicts:
   (a) a minor engaged in sexually explicit conduct;
   (b) a person appearing to be a minor engaged in sexually explicit conduct;
   (c) realistic images representing a minor engaged in such conduct.

3. For the purpose of paragraph 2 above, "minor" shall include all persons under 18 years of age. A Party may require a lower age limit not less than 16 years.

Explanation:
This article criminalises a broad array of child-pornography offences within the digital space: production, distribution, possession, and procurement. It also covers virtual or simulated imagery. Polish law aligns with these definitions and imposes severe penalties especially for distribution and production.

Test Question:
Under Article 9, which conduct is criminal?
A) Viewing public art depicting minors
B) Possession of illegal images of minors in digital form ✅
C) Educational research on child psychology
D) Transmission of anonymised data

Correct answer: B

Article 10 – Offences Related to Copyright and Related Rights
Full text (Budapest Convention):
"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright and related rights, when such acts are committed wilfully, on a commercial scale and by means of a computer system."

Polish Implementation – Copyright and Related Rights Act (English translation):

- Article 116: "Whoever, without authorisation or in violation of conditions, disseminates or reproduces another's work in the field of copyright shall be subject to imprisonment for up to two years; if committed for material benefit or on a large scale, imprisonment shall be from six months to five years."
- Article 118[1]: "Whoever possesses, imports, or uses devices or computer programmes adapted for illegal reproduction or dissemination of works shall be subject to imprisonment for up to three years."

Explanation:
This provision criminalises copyright infringement facilitated by computer systems, especially where done for commercial benefit or at scale. The Polish Copyright Act reflects this by penalising not just illegal sharing, but also possession of tools (e.g., pirate software) designed to facilitate such infringement.

III. Procedural and Jurisdictional Provisions

Article 15 – Conditions and Safeguards
Full text (Budapest Convention):
"Each Party shall ensure that the establishment, implementation and application of powers and procedures under this Chapter are subject to conditions and safeguards provided for under its domestic law. Such safeguards shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations undertaken under the 1950 European Convention on Human Rights, the 1966 International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and shall incorporate the principle of proportionality."

Polish Implementation:

- Constitution of the Republic of Poland (Article 47): "Everyone shall have the right to legal protection of his private and family life, honour and good name, and to decide about his personal life."
- Code of Criminal Procedure (Articles 109–111, English translation): "Any surveillance, interception, or search of communications shall require a judicial warrant or prosecutor's order specifying the scope, duration, and purpose of such measure."

Explanation:
The Convention embeds procedural guarantees. States must ensure any investigative power is compatible with human rights standards and proportionate to the aim pursued. In Poland, constitutional protection of private life is complemented by judicial oversight of surveillance and interception, reflecting these obligations.

Test Question:
The principle of proportionality ensures that:
A) All surveillance is forbidden
B) Powers used are necessary and not excessive ✅
C) Data must always be deleted
D) Investigations occur without warrants

Correct answer: B

Article 22 – Jurisdiction
Full text (Budapest Convention):

1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with this Convention, when the offence is committed:
   (a) in its territory; or
   (b) on board a ship flying the flag of that Party; or
   (c) on board an aircraft registered under the laws of that Party; or
   (d) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules established in paragraph 1(d).
3. Each Party shall adopt measures to establish jurisdiction when the alleged offender is present in its territory and it does not extradite them solely on the basis of nationality.
4. This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.
5. In cases where more than one Party claims jurisdiction over an alleged offence, the Parties involved shall, where appropriate, consult to determine the most appropriate jurisdiction for prosecution.

Polish Implementation – Penal Code Articles 109–111 (English translation):

- Article 109: "Polish criminal law shall apply to anyone who commits an offence within the territory of the Republic of Poland."
- Article 110: "§1. Polish criminal law shall also apply to a Polish citizen who commits an offence abroad. §2. It shall also apply to a foreigner who commits abroad an offence against the interests of the Republic of Poland, a Polish citizen, or a Polish legal entity."
- Article 111: "§1. If an act is punishable both under Polish law and the law of the place where it was committed, the penalty shall not exceed the maximum provided by Polish law. §2. A foreigner who committed an offence abroad may be prosecuted in Poland if he remains within Polish territory and is not extradited."

Explanation:
The Convention establishes multiple jurisdictions: territorial, flag, nationality, and presence-based jurisdiction. These rules prevent "safe havens" for cybercriminals. Poland's Penal Code integrates these principles, allowing for prosecution of nationals abroad and foreigners present in Poland, with limitations to avoid double jeopardy.

Test Question:
According to Article 22, a State may prosecute an offence committed abroad if:
A) The offender is a national of that State ✅
B) The offender is unknown
C) The offence occurred on an unregistered network
D) The act is not illegal elsewhere

Correct answer: A

IV. Additional Protocol I (2003) – Racist and Xenophobic Content via Computer Systems

Overview:
Adopted on 28 January 2003, the Protocol supplements the Convention by criminalising hate speech, threats, and the denial or justification of genocide when disseminated through computer systems.

Protocol Provisions:

- **Article 2:** Distribution of racist or xenophobic material via computer systems.
- **Article 3:** Threats against individuals or groups based on race, ethnicity, religion, etc., committed through computer systems.
- **Article 4:** Public insults via computer systems.
- **Article 5:** Denial, gross minimisation, approval, or justification of genocide or crimes against humanity.

Polish Implementation – Penal Code Articles 119–256 (English translation):

- Article 119: "Whoever uses violence or unlawful threats against a group or individual on account of national, ethnic, racial, political or religious affiliation shall be subject to imprisonment for three months to five years."
- Article 256: "§1. Whoever publicly propagates a fascist or other totalitarian state system or incites hatred on the grounds of national, ethnic, racial or religious differences, shall be subject to imprisonment for up to two years. §2. The same penalty applies to anyone producing or distributing material containing such content."

Explanation:
The Protocol requires States to criminalise online hate speech and extremist content. Poland's Penal Code addresses these acts—both the dissemination of extremist ideology and violent threats or insults motivated by protected characteristics—while balancing freedom of expression.

Test Question:
Which of the following is covered by the First Additional Protocol?
A) Copyright infringement
B) Dissemination of racist material online ✅
C) Phishing fraud
D) Data interference

Correct answer: B

V. Additional Protocol II (2022) – Enhanced Cooperation and e-Evidence

Overview:
Adopted on 12 May 2022, this Protocol modernises the Convention's cooperation mechanisms to reflect the realities of cloud computing, cross-border data flows, and the globalisation of service providers.

Key Provisions:

- **Article 7 – Direct Disclosure of Subscriber Information:** competent authorities can request subscriber data directly from foreign service providers.
- **Article 8 – Expedited Disclosure of Stored Computer Data:** stored electronic evidence may be preserved and shared rapidly.

- **Article 9 – Emergency Cooperation:** provides for urgent data preservation and transfer in situations of imminent risk.
- **Article 14 – Joint Investigation Teams:** enables multinational operational teams.
- **Article 15 – Data Protection and Oversight:** requires safeguards, judicial or independent review, and accountability for data requests.

Explanation:
The Second Protocol streamlines cross-border evidence collection, enabling direct communication with service providers. It introduces faster procedures—particularly for emergencies—and ensures data disclosure is accompanied by robust protections, oversight, and respect for privacy rights.

Test Question:
The Second Additional Protocol (2022) primarily addresses:
A) Data protection for minors
B) Cross-border disclosure of electronic evidence ✅
C) Prevention of hate speech
D) Copyright enforcement

Correct answer: B
