Visegrad Alliance
for Digital Rights
and Disinformation Defense

NATIONAL REPORT

POLAND

Legal framework as of November 30, 2025.

The project is co-financed by the governments of Czechia, Hungary, Poland, and Slovakia through Visegrad Grants from the International Visegrad Fund. The mission of the fund is to advance ideas for sustainable regional cooperation in Central Europe.

ABOUT THE AUTHORS

EWA MILCZAREK

Assistant Professor
University of Szczecin

Dr. Ewa Milczarek is a legal scholar and constitutional law expert with a focus on digital constitutionalism, digital sovereignty, and algorithmic governance, analyzing how technological and economic changes influence identity rights, state authority, and the protection of fundamental freedoms in the digital age. Her research seeks to develop a rights-based framework for democratic governance that ensures transparency, accountability, and the preservation of constitutional values in an increasingly data-driven society.

EWA MICHAŁKIEWICZ-KĄDZIELA

Assistant Professor
University of Szczecin

Dr. Ewa Michałkiewicz-Kądziela is a legal scholar and constitutional law expert with a focus on constitutional law, EU law, international law, and human rights protection within national, EU, and international frameworks. Her research delves into identity rights and contemporary human rights challenges arising from social, economic, and technological transformations.

1
LEGISLATION AND CASE-LAW CONCERNING DISINFORMATION AND HATE SPEECH

Attach the full range of public authority instruments, from criminal sanctions to administrative offences and other instruments, including noteworthy legislative proposals that did not pass.

1.1 Legal Framework and Definitions

Does your national legal framework define disinformation?

There is no general legal definition of "disinformation" in the national legal framework. However, the Act of 6 June 1997 – *Criminal Code*[1] (Journal of Laws of 2022, item 1138, as amended) was amended in 2023 to include Article 130 in the chapter *Offences against the Republic of Poland*. According to § 9 of this article, anyone who, by participating in the activities of a foreign intelligence service or acting on its behalf, spreads disinformation consisting in the dissemination of false or misleading information with the aim of causing serious disruption to the political system or economy of the Republic of Poland, an allied state, or an international organisation of which Poland is a member, or to induce a public authority to take or refrain from taking specific actions, shall be subject to imprisonment for a term of not less than eight years.

Does your national legal framework define hate speech?

There is no legal definition of "hate speech" in the national legal framework. However, the Act of 6 June 1997 – Criminal Code (Journal of Laws of 2022, item 1138, as amended) includes several provisions that criminalize conduct commonly understood as hate speech.

According to Article 119 § 1, anyone who uses violence or makes an unlawful threat against a group of persons or an individual because of their national, ethnic, racial,

[1] Ustawa z dnia 17 sierpnia 2023 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw, Dz.U. 2023 poz. 1834

political, or religious affiliation, or because of their lack of religious beliefs, is subject to imprisonment for a term of 3 months to 5 years.

Article 256 § 1 penalizes anyone who publicly promotes a Nazi, communist, fascist, or other totalitarian system of state, or incites hatred based on national, ethnic, racial, or religious differences, or because of lack of religious beliefs, with imprisonment for up to 3 years. § 1a extends this penalty to those who publicly promote Nazi, communist, or fascist ideology, or any ideology inciting violence to influence political or social life. § 2 further penalizes those who produce, distribute, or possess materials promoting such ideologies.Article 257 provides that anyone who publicly insults a group of people or an individual because of their national, ethnic, racial, or religious affiliation, or lack of religious beliefs, or who for such reasons violates another person's bodily integrity, is subject to imprisonment for up to 3 years.

Thus, while Polish law does not define "hate speech" as a legal term, it prohibits a range of acts motivated by hatred or intolerance under these provisions.

Are there any specific distinctions made between online and offline disinformation or hate speech in your legislation?

No, there are no specific distinctions made between online and offline disinformation or hate speech in the national legislation.

1.2 Criminal Sanctions

Which criminal offences address disinformation in your jurisdiction (e.g., spreading false news, incitement, etc.)?

Disinformation is addressed in Article 130 § 9 of the Criminal Code. This provision states that anyone who, by participating in the activities of a foreign intelligence service or acting on its behalf, conducts disinformation consisting in the dissemination of false or misleading information with the aim of causing serious disruption to the political system or economy of the Republic of Poland, an allied state, or an international organisation of which Poland is a member, or to induce a public authority of such entities to take or refrain from taking specific actions, is subject to imprisonment for a term of not less than eight years.

Which criminal offences address hate speech in your jurisdiction?

Hate speech is addressed in several provisions of the Criminal Code:

- Article 119 § 1 – Anyone who uses violence or makes an unlawful threat against a group of persons or an individual because of their national, ethnic, racial, political, or religious affiliation, or because of their lack of religious beliefs, is subject to imprisonment for a term of 3 months to 5 years.

- Article 256 § 1 – Anyone who publicly promotes a Nazi, communist, fascist, or other totalitarian system of state, or incites hatred based on national, ethnic, racial, or religious differences, or because of lack of religious beliefs, is subject to imprisonment for up to 3 years.

    - § 1a – The same penalty applies to anyone who publicly promotes Nazi, communist, or fascist ideology, or an ideology inciting the use of violence to influence political or social life.

    - § 2 – The same penalty also applies to anyone who, for the purpose of dissemination, produces, records, imports, acquires, sells, offers, stores, possesses, presents, transports, or transmits any print, recording, or other item containing such content or bearing Nazi, communist, fascist, or other totalitarian symbols, used to promote the content specified in § 1 or § 1a.

- Article 257 – Anyone who publicly insults a group of people or an individual because of their national, ethnic, racial, or religious affiliation, or because of their lack of religious beliefs, or for such reasons violates the bodily integrity of another person, is subject to imprisonment for up to 3 years.

What are the typical penalties (fines, imprisonment, etc.) associated with these offences? (if available)

Police data on initiated investigations[2]. Number of offences under Article 119(1), Article 256 and Article 257 of the Penal Code, including those committed using the Internet

Act	Article	Meaning	Confirmed offences	by the internet

[2] KR-DŚ - 4381/4227/2024, https://bip.brpo.gov.pl/sites/default/files/2024-12/Odpowiedz_KGP_nienawisc_przestepstwa_zwalczanie_21_12_2024.pdf

			2022	2023	I-XI 2024	2023	2024
Act of 6 June 1997 - Penal Code	Art. 119 § 1	violence or unlawful threats against a group of people or an individual because of their nationality, ethnicity, race, politics, or religion	122	157	113	0	1
	Art. 256 § 1	against the promotion of Nazi, communist, fascist or other totalitarian state systems or incites hatred on the basis of nationality, ethnicity, race, religion or lack of religion	282	253	213	0	0
	Art. 256 § la	against the promotion of Nazi, communist, fascist ideologies or ideologies advocating violence in order to influence political or social life	0	0	2	2	1
	Art. 256 § 2	against the distribution of any printed or recorded material or any other object containing the content specified in the above points, or against the distribution of such material produced, recorded or imported, or acquired, sold, offered, stored, possessed, presented, transported or forwarded	18	19	6	0	0
	Art. 257	against insulting a group of people or a person publicly because of their nationality, ethnicity, race, religion, lack of religion or because of their physical integrity violating the physical integrity of another person for such reasons	502	339	311	0	0
Total			924	768	645	2	1

The number of proceedings initiated and completed concerning the acts typified in Article 119 § 1 of the Penal Code, Article 256 of the Penal Code and Article 257 of the Penal Code.

			Initiated proceedings			Finished proceedings		
Act	Article	Meaning	2022	2023	2024	2022	2023	2024
Act of 6 June 1997 - Penal Code	Art. 119 § 1	violence or unlawful threats against a group of people or an individual because of their nationality, ethnicity, race, politics, or religion	171	129	103	128	168	120
	Art. 256 § 1	against the promotion of Nazi, communist, fascist or other totalitarian state systems or incites hatred on the basis of nationality, ethnicity, race, religion or lack of religion	302	236	284	293	288	263
	Art. 256 § la	against the promotion of Nazi, communist, fascist ideologies or ideologies advocating violence in order to influence political or social life	0	0	6	0	0	4

	Art. 256 § 2	against the distribution of any printed or recorded material or any other object containing the content specified in the above points, or against the distribution of such material produced, recorded or imported, or acquired, sold, offered, stored, possessed, presented, transported or forwarded	14	12	11	27	19	9
	Art. 257	against insulting a group of people or a person publicly because of their nationality, ethnicity, race, religion, lack of religion or because of their physical integrity violating the physical integrity of another person for such reasons	478	341	412	497	380	338
Total			965	718	816	945	855	734

Number of people detained:

Act	Article	Meaning	Detention notice	Initiated proceedings		
				2022	2023	I-XI 2024
Act of 6 June 1997 - Penal Code	Art. 119 § 1	violence or unlawful threats against a group of people or an individual because of their nationality, ethnicity, race, politics, or religion	Adults	40	39	31
			Minors	2	0	0
	Art. 256 § 1	against the promotion of Nazi, communist, fascist or other totalitarian state systems or incites hatred on the basis of nationality, ethnicity, race, religion or lack of religion	Adults	16	10	10
			Minors	0	1	5
	Art. 256 § 2	against the distribution of any printed or recorded material or any other object containing the content specified in the above points, or against the distribution of such material produced, recorded or imported, or acquired, sold, offered, stored, possessed, presented, transported or forwarded	Adults	2	0	0
	Art. 257	against insulting a group of people or a person publicly because of their nationality, ethnicity, race, religion, lack of religion or because of their physical integrity violating the physical integrity of another person for such reasons	Adults	61	51	49
			Minors	0	0	1
Total				121	101	96

The most common penalty: imprisonment (usually from 6 months to 1 year).

Adults legally convicted by public prosecution for selected crimes in the years 2015-2020[3]

Types of crimes	Convicted							
	Total	Fine	Restriction of libety	Deprovation of liberty	Hybrid sentence	25 years of imprisonment	life imprisonment	Independent penal measures
2015								
Total	260 034	61 461	31 096	167 028	370	64	6	9
Including								
Art.119 §1 kk	66	2	5	59	-	-	-	-
Art.256 §1 kk	21	9	6	6	-	-	-	-
Art.256 §2 kk	2	2	-	-	-	-	-	-
Art.257 kk	75	19	12	44	-	-	-	-
2016								
Total	289 512	98 776	61 720	125 368	3 544	68	20	16
Including								
Art.119 §1 kk	72	14	9	43	6	-	-	-
Art.256 §1 kk	54	37	16	1	-	-	-	-
Art.256 §2 kk	1	-	1	-	-	-	-	-
Art.257 kk	90	35	23	32	-	-	-	-
2017								
Total	241 436	84 721	53 854	99 346	3 424	50	12	29
Including								
Art.119 §1 kk	116	16	29	60	11	-	-	-
Art.256 §1 kk	39	18	17	4	-	-	-	-
Art.256 §2 kk	1	1	-	-	-	-	-	-
Art.257 kk	80	35	34	10	1	-	-	-
2018								
Total	275 768	90 491	78 172	103 814	3 212	41	24	14
Including								
Art.119 §1 kk	128	16	26	82	4	-	-	-
Art.256 §1 kk	40	20	17	3	-	-	-	-
Art.256 §2 kk	4	3	-	1	-	-		-
Art.257 kk	101	44	35	20	2	-	-	-
2019								

[3] Study based on data from the Polish Ministry of Justice: Final convictions by public prosecutor for hate crimes in the years 2008-2020 Final convictions by public prosecutor for hate crimes in the years 2008-2020, https://isws.ms.gov.pl/pl/baza-statystyczna/opracowania-wieloletnie/

Total	287 978	93 843	84 992	105 841	3 137	74	19	72
Including								
Art.119 §1 kk	153	33	15	104	1	-	-	-
Art.256 §1 kk	38	16	18	4	-	-	-	-
Art.256 §2 kk	8	6	1	1	-	-	-	-
Art.257 kk	141	64	33	44	-	-	-	-
2020								
Total	251 369	84 081	74 012	90 524	2 619	50	11	72
Including								
Art.119 §1 kk	110	7	18	81	4	-	-	-
Art.196kk	6	1	5	-	-	-	-	-
Art.256 kk	-	-	-	-	-	-	-	-
Art.256 §1 kk	29	14	12	3	-	-	-	-
Art.256 §2 kk	2	-	1	1	-	-	-	-
Art.257 kk	122	45	49	28	-	-	-	-

Are there any aggravating factors that increase penalties for disinformation or hate speech (e.g., content targeting vulnerable groups)?

No, there are no specific aggravating factors in the national legislation that increase penalties for disinformation or hate speech, such as when the content targets vulnerable groups.

However, in practice, hate speech in Poland most often targets the following groups[4]:

- Non-heteronormative minorities (LGBT+ persons)
- The Roma minority
- Black people
- The Jewish minority
- Muslims
- The Ukrainian minority

[4] Michał Bilewicz, Marta Marchlewska, Wiktor Soral,Mikołaj Winiewski, Mowa nienawiści Raport z badań sondażowych, Warszawa 2014; Mikołaj Winiewski Karolina Hansen, Michał Bilewicz, Wiktor Soral, Aleksandra Świderska, Dominika Bulska, Mowa nienawiści, mowa pogardy. Raport z badania przemocy werbalnej wobec grup mniejszościowych, https://bip.brpo.gov.pl/sites/default/files/Raport%20Mowa%20Nienawi%C5%9Bci,%20Mowa%20Pogardy,%2027.02.2017.pdf

1.3 Administrative Offences and Civil Measures

Beyond criminal law, are there any administrative offences covering disinformation or hate speech?

No, there are no administrative offences covering disinformation or hate speech beyond criminal law.

What types of administrative penalties are imposed (e.g., fines, warning notices, temporary bans)?

No, there are no administrative penalties imposed for disinformation or hate speech.

Are there civil law remedies (e.g., defamation suits, injunctions) available for victims or affected parties?

Yes, civil law remedies are available for victims or affected parties.

Under the Civil Code, the protection of personal rights (*dobra osobiste*) is provided by Articles 23 and 24.

- Article 23 lists personal rights such as health, freedom, dignity, conscience, name, image, privacy of correspondence, and inviolability of one's home, among others, and states that they are protected by civil law regardless of other legal protections.
- Article 24 § 1 provides that a person whose personal rights are threatened or violated may demand cessation of the unlawful act, removal of its effects (e.g., a public apology), or monetary compensation for non-material harm, or payment of an appropriate sum to a designated social cause.
- Article 24 § 2 allows the injured party to seek compensation for material damage resulting from the violation of personal rights.

In addition, under the Criminal Code, victims may pursue private prosecutions for:

- Defamation (Article 212) – publicly or privately making false statements that may damage someone's reputation or cause loss of trust necessary for their position or profession.

- Insult (Article 216) – offending another person publicly or through mass communication.

These provisions, although part of criminal law, may complement civil remedies such as defamation suits, injunctions, or claims for damages under civil proceedings.

1.4 Scope of Instruments and Enforcement

Which public authorities or institutions are responsible for enforcing laws on disinformation and hate speech?

In case of hate speech:

1. Polish National Police, which is responsible for detecting hate crimes, including the prosecution of hate speech;
2. Prosecutor`s Office, which are responsible for prosecutions of offences;
3. The courts, which decided on conviction.
4. Polish Ombudsman and his Office in the context of monitoring of hate speech cases.

In case of disinformation:

1. Ministry of Foreign Affairs of Poland – the Department for Strategic Communications and Countering Foreign Disinformation, works on external/manipulative information threats;
2. Internal Security Agency (ABW) – responsible for internal security, including countering disinformation and information manipulation especially from foreign states;
3. National Council of Radio Broadcasting and Television (KRRiT) — as regulator of media/broadcasting, it has powers over broadcasting content and can penalise for e.g. disinformation in broadcasts.
4. NASK – National Research Insitute, which Department for Counteracting Disinformation monitors online content, accounts, coordinates detection of harmful materials and flags them for public administration response.

How do these authorities identify and investigate potential cases?

1. Police could work on a base of complaints from individuals, NGO`s or their own discoverv.

2. Incidents classified as hate crimes are recorded both on the incident report form and in the police's electronic information system. Dedicated coordinators — operating at the national level (the National Hate Crime Coordinator within the Criminal Bureau of the General Police Headquarters) and at the regional level (in each Voivodeship Police Headquarters and the Metropolitan Police Headquarters) — are tasked with preventing and investigating hate crimes, as well as collecting data from their respective jurisdictions. They submit monthly reports to the Electronic Investigation Activities Register (Elektroniczny Rejestr Czynności Śledczych, ERCDŚ), which has been in use since January 2022. It is important to note that the notion of a hate crime encompasses a broader range of behaviour than hate speech.
3. Guidelines introduced by the Prosecutor General in 2014 standardize how hate crime cases are handled and reported across the prosecution service. Each case that reaches the prosecution stage must be submitted to a higher-level Prosecutor's Office for notification. In addition, the Department of Preparatory Proceedings within the National Public Prosecutor's Office oversees these cases, prepares comprehensive reports for the Prosecutor General, and offers guidance to lower-level prosecutor offices based on its findings.

Source: https://hatecrime.osce.org/national-frameworks-poland#dataCollection

In case of disinformation:

1. Monitoring: NASK's Department for Counteracting Disinformation monitors online content, accounts, coordinates detection of harmful materials and flags them for public administration response.
2. The Ministry of Foreign Affairs' Department monitors foreign media, diplomatic missions track disinformation campaigns abroad (via embassies/consulates) and cooperates with civil society.
3. Regulatory/broadcast sector: KRRiT (the National Council of Radio Broadcasting and Television) monitors broadcasting content; for example, it issued a sanction against a radio company for broadcasting disinformation.
4. Cross-agency cooperation: ABW, Ministry of Interior & Administration, Police and Border Guard are involved when disinformation intersects national security, elections, foreign interference, etc

Are there any specialized agencies or task forces focusing on online disinformation or hate speech?
Yes. NASK and KRRiT (the National Council of Radio Broadcasting and Televisio).

Could you provide any statistics or data on enforcement actions, prosecutions, or convictions?
There is no public data in that case. Although, there is some statistics for hate crimes in general, prepared by Poland for OSCE: https://hatecrime.osce.org/poland.

1.5 Case-Law and Judicial Interpretations

What are the most significant court decisions shaping the interpretation of disinformation or hate speech laws in your country?

Decision of Constitutional Tribunal of Poland from 25 February 2014, SK 65/12 (2014) - The Constitutional Tribunal examined a motion questioning the compliance of Article 256 of the Penal Code — which bans public incitement to hatred on grounds such as nationality, race, religion, or absence of religious belief — with the Constitution. The Tribunal ruled that the limitation of freedom of expression introduced by this provision is justified and proportionate, since its purpose is to safeguard state security, public order, and the rights of other individuals.

Supreme Court of Poland, Case from 8 February 2019, No. IV KK 38/18 – Supreme Court made an interpretation of Article 256 (1) of the Polish Penal Code. On that basis it is easier to define what kind of behawior could count as a „hate speech" in criminal content in Poland: only the insult is not enough, what is importnat is to put the insult in the context, intent and public dimension.

Decision of Constitutional Tribunal of Poland from 30 September 2025 , KP 3/25— Declaring a draft hate-speech/hate-crime expansion amendment unconstitutional. In Consitutional Tribunal opinion the provision, which expanded hate-crime/hate-speech grouds (like age, gender, disability, sexual orientation) were too vague and could violate the freedom of speech. On one hand this decision showed that the limitation of freedom of speech should be introduce to

our legal system in the light of the proportionality rule, on the other hand there is still big legal gap in polish law system adressing the hate-speech matters.

Have any high-profile cases set important precedents regarding the enforcement of these laws?

No

How do courts balance the protection of society from disinformation or hate speech with the right to freedom of expression? Is the principle of proportionality the main instrument?

Yes, the principle of proportionality is the main instrument. The Constitutional Tribunal in the judgement from 6 July 2011, P12/09 decided that the court in every case uses this method to check, if the limitation of the right to freedom of expression is legal and set according to the principle of proportionality rules:

1. Usefulness (adequacy) – does the restriction of freedom of speech actually help achieve the intended goal (e.g., protection of personal rights, prevention of hatred)?
2. Necessity – are there no more lenient measures that could achieve this goal?
3. Proportionality in the strict sense – do the benefits of restricting freedom of speech outweigh the harm caused by the restriction itself?

Courts consider not only the content of the statement, but also (look e.g. Judgement of Supreme Court from 23 February 2017, I CSK 124/16):

- context (e.g., public debate, art, political commentary),
- form (whether it was offensive, provocative, or factual),
- status of the person making the statement (e.g., journalist, politician, artist),
- social consequences (whether the statement could realistically incite hatred or mislead).

1.6 Legislative Proposals (Including Those Not Passed)

Have there been recent legislative proposals aimed at combating disinformation or hate speech? If so, what did they entail?

Yes, there have been recent legislative proposals aimed at combating disinformation and hate speech.

Hate Speech

- Sejm Paper No. 876 (available at: https://www.sejm.gov.pl/sejm10.nsf/PrzebiegProc.xsp?nr=876)

  The proposal seeks to extend protection against hate speech and hate crimes motivated by discrimination on the grounds of disability, age, gender, and sexual orientation.
  It aims to:
  • Supplement the list of aggravating circumstances under Article 53 § 2a point 6 of the Criminal Code,
  • Expand the scope of offences defined in Articles 119 § 1, 256 § 1, and 257 of the Criminal Code to include discrimination based on disability, age, gender, and sexual orientation.
  The bill was passed by the Parliament, but the President refused to sign it, effectively stopping the legislative process.

Disinformation ("Fake News")

- Sejm Paper No. 746 (Sejm IX term) – a draft amendment to the Act on Preventing and Combating Infections and Infectious Diseases in Humans. The proposed new Article 49a provided that:

"Whoever, during a state of epidemic, contrary to current medical knowledge, publicly denies a threat to public health or questions its existence, encourages or incites the non-implementation or non-application of procedures ensuring protection against infections and infectious diseases, shall be subject to a fine or a restriction of liberty." However, the legislative work on this proposal was not continued, and the bill did not pass.

Were there any proposals that did not pass? If yes, what were the main reasons for their rejection or withdrawal?

Yes.

Hate speech: Sejm Paper No. 876 – the bill was passed by the Parliament but the President refused to sign it, so it did not enter into force.

Disinformation (fake news): Sejm Paper No. 746 – a parliamentary proposal to amend the Act on Preventing and Combating Infections and Infectious Diseases in Humans (Sejm IX term). Legislative work on the proposal was not undertaken.

Did these proposals encounter notable opposition or controversy? If so, from which stakeholders?

Both proposals encountered opposition from conservative and right-wing groups, including political circles linked to Law and Justice (Prawo i Sprawiedliwość), Radio Maryja, and Confederation (Konfederacja). These groups argued that the initiatives could limit freedom of speech and introduce censorship, claiming that the hate speech proposal sought to impose ideological restrictions or privilege certain groups, particularly in relation to LGBT+ protections.

1.7 Role of Online Platforms and Intermediaries

Are there specific obligations (solely from state legislation, not enforced by EU law) placed on social media companies or digital platforms to monitor and remove disinformation or hate speech?

No, there are no specific obligations under national legislation (outside EU law) that require social media companies or digital platforms to monitor or remove disinformation or hate speech.

Any regulation of online content in Poland in this area primarily results from EU legislation, such as the Digital Services Act (DSA). Polish national law does not impose additional or independent obligations on online platforms beyond those EU-level requirements.

What is the liability regime for internet service providers or online platforms in your jurisdiction?

In the scope of hate speech: although the Polish Penal Code provides for liability for hate crimes (e.g. Penal Code Article 256, Article 257), the Act on Electronic Services does not oblige platforms to actively monitor and remove hate speech as such.

In the field of disinformation: there is no special provision in Polish national law (apart from general criminal or civil provisions) that would impose on platforms the obligation to detect and remove disinformation content (false information) from the point of view of national law.

Have any landmark cases or regulatory actions been taken against major tech platforms under these rules?

No

1.8 International and Regional Considerations

Has your country ratified or adopted any international conventions or regional directives relevant to disinformation or hate speech?

Poland is a part of international human rights conventions e.g. Covenant on Civil and Political Rights, Convention on the Elimination of All Forms of Racial Discrimination, European Convention on Human Rights, Council of Europe Convention on preventing and combating violence against women and domestic violence. But they are not mentioning the hate speech or disinformation, as they were created and ratified some time ago. Only on the base of general provisions we can seek for the protection from hate speech and disinformation.

On the other hand Poland is a party of *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems* (ETS No. 189), which was ratified in 2015.

How do these international obligations influence domestic legislation and case-law?

Not applicable

Are there any ongoing discussions about aligning national law with regional or global standards?

Yes. There is a discussion about the necessity to amend our Polish Criminal Code, especially articles 119, 256 and 257 by extension the hate crimes motives e.g. to add to those provisions new motives like: sexual orientation, age, disability, identity. Unfortunately, the draft of amendment was recognize by Polish Constitutional Tribunal as unconstitutional. In opinion of Polish Constitutional Tribunal the provisions were too broad and unclear, so it didn`t realize the proportionality rules, if it comes to limitation of freedom of speech.

1.9 Practical Challenges and Enforcement Gaps

Is there a notable gap between the laws on paper and the practical enforcement?

No

Are there examples of under-enforcement or over-enforcement in practice?

No

2
ROLE OF AUTOMATIZATION AND AI IN CONTENT REGULATION

Have there been legal cases around deep fakes, synthesized speeches of politicians, etc.?

Yes. There were a case about Polish billionaire Rafał Brzkoska, the owner of InPost Company, who won with Meta over an argument about deep fakes, which used his and her wife images and were published on Meta pages. A Polish court decided to issue a protective measure in the form of a ban on publishing deepfakes featuring Brzoska and his wife on portals owned by Meta. Meta decided to appeal this decision, but after some time withdrew and the ban was upheld.

2.1 Legal Recognition and Definitions

Does your national legislation specifically define or recognize deep fakes or other AI-generated content (e.g., synthetic media)?

No. But, as the rest of European Union countries Poland uses the definition from Article 3 point 60 of AI Act.

Are there any legal provisions that explicitly address the creation, dissemination, or misuse of AI-generated content?

No

2.2 Criminal and Civil Liability

Which criminal or civil offences (if any) apply to the production or distribution of deep fakes or similar synthetic media?

Under the Penal Code(Kodeks karny)), for example: the offence of identity theft (art. 190a) may apply when someone impersonates another person, uses their likeness or data, and causes material or personal damage. This can cover cases of deep-fake videos or audio impersonations of public persons.

Under the data protection law (Ustawa o ochronie danych osobowych) misuse of a person's image or biometric (identification) data can trigger liability. For example, in a reported case where AI-generated altered images of a minor were distributed, it triggered investigation under personal-data law.

Under copyright & related rights law (Ustawa o prawie autorskim i prawach pokrewnych) and IP law: Polish law is clear that purely AI-generated works (without sufficient human creative input) are not eligible for copyright protection. That doesn't regulate the misuse of such work per se, but it shows the gap in protective regulation.

Have any cases been prosecuted under existing laws (e.g., defamation, identity theft, fraud) rather than new legislation targeting AI-generated content?

Yes, the case of Brzoska v. Meta - Provincial Administrative Court in Warsaw (there is no public record about the signature of court decision): Source: https://www.well.pl/life/148/meta_kapituluje_przed_rafalem_brzoska_prezes_inpostu_odnosi_sukces_w_walce_z_technologicznym_gigantem,18146.html

2.3 Preventive Measures and Oversight

Are there requirements for AI developers or platform operators to label or disclose AI-generated content?

No at the national level. All limitations for AI developers or platform operators are results of AI Act.

Have any policy initiatives or industry self-regulation measures been introduced to mitigate harms associated with deep fakes?

1. Urząd Ochrony Danych Osobowych (UODO) -
The Polish Data Protection President has publicly called for new legislation specifically addressing the dissemination of harmful deep-fakes. It emphasises that current rules (on data protection, image rights, etc.) are insufficient for the "new dimension" of AI-generated content. The proposal includes obligations for platforms to detect/label synthetic content and for quicker removal of harmful materials. This shows a *policy-level* step (not yet fully law) aimed at deep-fakes.
2. International Commitments- Poland announced a will to join to the Global Declaration on Information Integrity Online (a Canadian–Dutch initiative) to

combat disinformation, which includes addressing synthetic and manipulated content.

This reflects policy direction and commitment, though again not a domestic binding regulation yet.

Are there any mandatory or voluntary codes of practice for social media platforms regarding AI-generated content?

Not that one established on national level. But Poland would like to join the codes of practice, which are developing on international level e.g. Code of Practice for General-Purpose AI.

2.4 Impact on Political Processes and Elections

Have there been instances where deep fakes or AI-generated speeches impacted election campaigns, political debates, or voter perceptions?

There were some examples of deepfakes, which were used during election campaigns, but there were no proof about theirs impact on the results of election. E.g. the deepfake generated by Platforma Obywatelska in campaigne election in 2023, when they generated by AI speech of previous Prime Minister Mateusz Morawiecki. There is no data, how much that deepfake influenced the results of elections.

Source: https://www.rp.pl/wybory/art38999941-po-wykorzystala-ai-do-stworzenia-glosu-morawieckiego-w-spocie-wyborczym

How do electoral regulations or campaign laws address the use of AI-generated media (e.g., transparency rules, disclaimers)?

Not applicable. Polish electoral regulations doesn`t address the issue of AI-generated media.

2.5 Future Outlook and Emerging Trends

Are there legislative proposals pending or under discussion that aim to address deep fakes or AI-generated disinformation more explicitly?

Yes. Polish data protection authority President of UODO (Urząd Ochrony Danych Osobowych) proposed the legislative changes to combat harmful deepfakes, as current general provisions didn`t play its role to protect from deepfake and AI-manipulated media risk. Moreover, Poland plans to introduce national "Act on AI systems" to implement the EU AI Act , but it is more about AI governance, transparency, risk classification, rather than explicitly targeted at deepfakes or disinformation alone.

3
THE PROHIBITION OF CENSORSHIP AND ITS IMPACT ON REGULATING INTERNET CONTENT AND DISINFORMATION

3.1 Constitutional and Legislative Framework

Does your country's constitution or primary legislation explicitly prohibit censorship? Are there exceptions or limitations to the prohibition on censorship (e.g., national security, public order)?

Article 54 of Constitution of the Republic of Poland

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 prohibited. Statutes may require the receipt of a permit for the operation of a radio or television station.

Censorship before publication is *always unconstitutional* (TK judgment K 9/11, 20 July 2011). Post-factum sanctions must be narrowly tailored and proportionate.

Article 31 (3) of Polish Constitution

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.

Emergency exceptions: Temporary and regulated under the Constitution (Arts. 228–234).

3.2 Judicial Interpretations and Key Cases

What major court decisions have clarified the boundaries of censorship, particularly in relation to online speech?

Decision of Constitutional Tribunal from 23 March 2006, K 4/06 - the Tribunal held that state interference in the media (including in broadcasting) is permissible only

in exceptional circumstances and must be duly justified. Media regulation (including online media) must safeguard pluralism, independence, and cannot become a tool of censorship.

Have any pivotal judgments addressed the tension between prohibiting censorship and controlling disinformation?

No.

3.3 Scope and Enforcement

Which authorities or regulatory bodies are responsible for enforcing the prohibition on censorship?

1. Constitutional Tribunal - determines the compliance of legal acts with the provisions of the Polish Constitution;
2. Ordinary courts – they can control if any restriction of expression were: grounded in law, necessary and proportionate, doesn`t amount to prior restraint;
3. KRRiT (the National Council of Radio Broadcasting and Television) – this body ensures pluralism of media and also has some competence, which allows issue sanctions after broadcaster if laws are violated;
4. The Chef of Internal Security Agency – he could order removal of some terrorist online content;
5. Ombudsman – monitors the law and also could intervenes in some cases according to Polish law.

How do these bodies reconcile the prohibition with the need to remove unlawful or harmful content (e.g., hate speech, false information)?

Constitutional Tribunale and Ombudsman don`t remove unlawful or harmful content per se. The do not have competences for that. They more protect from the situations when those kind of content could show up. The ordinary courts and National Broadcasting Council on the other hand have the measure, which help to remove the unlawful or harmful content from the public sphere. In the case of courts it is their decisions and judgements. Courts usually apply the proportionality rule, so before they order to remove some materials or they prohibited to publish some materials, they need to do the proportionality test and check, weather the limitation of freedom of expression is: grounded in law,

necessary and proportionate, doesn`t amount to prior restraint. On the other hand, National Broadcasting Council could put a sanctions, when broadcaster already violated law and put some unlawful or harmful content in broadcast.

There is an amendment to The Act on Anti-Terrorist Activities and the Act on the Internal Security Agency and the Foreign Intelligence Agency from 18th October 2024, provides, among other things, that the head of the Internal Security Agency will be the authority competent to issue orders to remove content or prevent access to it.

What measures ensure that internet regulations do not amount to de facto censorship?

Proportionality test.

3.4 Practical Outcomes and Challenges

Are there instances where the prohibition of censorship resulted in the inability to remove content widely considered harmful or misleading?
No

Conversely, are there examples of state overreach where content was restricted under the guise of public interest, raising censorship concerns?
Yes, the case SIN v. Facebook. Meta removed the profiles and groups of SIN (Społeczna Inicjatywa Narkopolityki) without giving a cause and without the opportunity to appeal. The Polish court decided that Meta violated the freedom of speech and also the good name of SIN.

Source: https://en.panoptykon.org/win-against-facebook-giant-not-allowed-censor-content-will?utm_source=chatgpt.com

3.5 Future Outlook

Are there ongoing discussions about refining or reinterpreting the prohibition on censorship to account for evolving digital challenges?

No

What emerging technologies (e.g., AI-driven content moderation) might influence future debates on censorship and disinformation regulation?

Probably the deepfakes, as it is not only a threat to individual rights, but also a threat to democracy and safety of the country.

4
NATIONAL REGULATION OF INTERNET CONTENT

Especially website blocking, social media/platforms regulation, not limited solely to EU-based regulation; legislation, case law and effectivity analysis.

4.1 Legislative Framework

What laws or regulations govern the blocking of websites and the regulation of social media/platforms in your country?

Social Media Regulation

Currently (as of 2025), Poland does not have a specific law governing social media platforms or online services.

The government attempted to introduce the so-called *"Freedom of Speech Act on the Internet"* between 2021–2022 (*Projekt ustawy o ochronie wolności słowa w internetowych serwisach społecznościowych*, draft of 15 January 2021, submitted on 22 January 2021 to the Chancellery of the Prime Minister for inclusion in the legislative agenda*), but the legislative work was suspended, and the act was never adopted.

At present, regulation of online platforms in Poland primarily follows EU law, particularly the Digital Services Act (DSA).

Website Blocking

Website blocking is governed by several sector-specific laws:

1. Telecommunications Law (*Prawo telekomunikacyjne*, Journal of Laws 2004 No. 171, item 1800, as amended)
    - Article 180(1): Telecommunications operators must promptly block telecommunication connections or information transmissions upon request of authorized bodies (court, prosecutor, Police, Internal Security Agency, or Central Anti-Corruption Bureau) when such communications threaten national defense, state security, or public order and safety.

2. Act of 28 July 2023 on Counteracting Abuse in Electronic Communications
    - Allows agreements between the President of UKE, the Minister for Digital Affairs, NASK (Research and Academic Computer Network – National Research Institute), and telecommunications providers to maintain a “warning list” of fraudulent websites.
    - Domains aiming to deceive users or obtain their personal data unlawfully may be added to this list.
    - CSIRT NASK manages the list, and telecom operators who are parties to the agreement may block access to the listed websites.
3. Act on Gambling (consolidated text: Journal of Laws 2023, item 227; 2024, item 1473)
    - Article 15f establishes the Register of Domains Used for Illegal Gambling (the “blacklist”), maintained by the Minister of Finance.
    - Internet Service Providers (ISPs) are obliged to block access to websites listed in this register.
4. Code of Criminal Procedure (KPK)
    - Article 218a § 4: When electronic content constitutes a criminal offence (e.g., child pornography – Articles 200b, 202 §§ 3–4b CC; terrorist content – Article 255a CC; drug-related crimes – Chapter 7 of the Anti-Drug Act), a court or prosecutor may order its removal. The order is directed to entities such as telecom providers, online service operators, or digital service providers, who must execute the blocking or removal.
5. Civil Procedure Code (KPC)
    - Article 730 and following: Courts may issue interim injunctions to protect rights (e.g., intellectual property, personal rights, defamation, unfair competition). Such injunctions can include blocking access to specific websites or online content that infringes these rights.
6. Consumer Protection Regulation (EU Regulation 2017/2394)

- Implemented nationally via the Office of Competition and Consumer Protection (UOKiK), allowing cooperation between authorities to block or restrict access to websites violating consumer protection laws.

4.2 Scope of Website Blocking

Under what circumstances can websites be blocked (e.g., illegal content, piracy, national security concerns)?

Websites in Poland can be blocked only under specific legal circumstances defined by national legislation. The main grounds for blocking are related to national security, public safety, protection of minors, prevention of crime, and consumer protection.

National Security and Public Order

- Article 180(1) of the Telecommunications Law (*Prawo telekomunikacyjne*, Journal of Laws 2004 No. 171, item 1800, as amended*) Telecommunications operators must block communications or transmissions on request of authorized bodies (e.g., court, prosecutor, Police, Internal Security Agency, CBA) when such connections may threaten national defense, state security, or public safety and order.

Child Pornography, Violence, and Terrorism

- Article 218a § 4 of the Code of Criminal Procedure (*Kodeks postępowania karnego*)
  Courts or prosecutors may order the removal or blocking of online content that constitutes a criminal offence, including:
  • Pornographic content involving minors or containing acts of violence or animal abuse (Articles 200b and 202 §§ 3–4b of the Criminal Code),
  • Content that may facilitate terrorism-related crimes (Article 255a of the Criminal Code),
  • Content related to drug offences (Chapter 7 of the *Act on Counteracting Drug Addiction*).

Illegal Gambling

- Article 15f of the Gambling Act (*Ustawa o grach hazardowych*, consolidated text: Journal of Laws 2023, item 227; 2024, item 1473)
  The Minister of Finance maintains the Register of Domains Used for Illegal Gambling, and internet providers (ISPs) are legally obliged to block access to websites listed in this register.

Fraudulent and Phishing Websites

- Article 20 of the Act of 28 July 2023 on Counteracting Abuse in Electronic Communications
  To protect internet users from phishing and fraudulent websites designed to obtain personal data or cause financial loss, a warning list of dangerous domains is maintained by CSIRT NASK.
  Telecommunications operators who are party to the relevant agreement may block access to these domains.

Civil Law Proceedings

- Article 730 of the Civil Procedure Code (*Kodeks postępowania cywilnego*)
  Courts may issue interim injunctions to "secure the claim," which can include blocking access to websites that infringe intellectual property rights, personal rights, or consumer protection laws.
  The law does not specify the types of technical measures to be used.

Consumer Protection and Deceptive Practices

- EU Regulation 2017/2394 on cooperation between consumer protection authorities (*CPC Regulation*), enforced in Poland by the Office of Competition and Consumer Protection (UOKiK), allows blocking or restricting access to websites that violate consumer rights or engage in unfair commercial practices.

Could it be said that the legislation on website blocking leaves a lot of discretion to the blocking authority, and so the provision of the law is very broad?

Yes — Polish legislation on website blocking leaves significant discretion to the authorities, and in some cases, the legal provisions are indeed broad and vaguely defined.

For example, Article 180 of the Telecommunications Law allows authorized bodies such as the Police, Internal Security Agency (ABW), or Military Counterintelligence Service (SKW) to request the blocking of communications or information transmissions when they pose a threat to "national security" or "public safety." These concepts are not precisely defined in the law, leaving room for wide interpretation by the authorities.

Moreover, in some cases — such as the Register of Domains Used for Illegal Gambling maintained by the Minister of Finance — blocking decisions are administrative in nature and do not require prior judicial authorization. This further expands the discretionary power of administrative bodies in determining which websites are restricted.

Is it conceivable that a court or administrative body would block a website on an ad hoc basis, on the basis of a very general mandate? E.g. interim measures in litigation.

Yes, it is conceivable that a court or administrative body in Poland could order the blocking of a website on an ad hoc basis, relying on a general legal mandate rather than a specific, narrowly defined rule.

1. Civil Procedure – Interim Measures (Środek zabezpieczający)

Under the Polish Code of Civil Procedure (Kodeks postępowania cywilnego), courts may issue interim injunctions to secure claims in various types of cases — including intellectual property, defamation, unfair competition, and consumer protection.

- The law does not specify what types of measures can be imposed, stating only that the injunction should "secure the claim."
  This gives courts broad discretion to order:
  • Temporary blocking of a website,

• Removal of specific online content,
• Restriction of access to a platform or online service,
even if there is no explicit provision in civil law regulating such measures.

2. Criminal Procedure – Blocking and Seizure (k.p.k.)

Under Articles 217c and 218a of the Code of Criminal Procedure (Kodeks postępowania karnego), a criminal court or prosecutor may order:

- The seizure,
- Blocking, or
- Securing of IT systems, including websites, servers, or domain names.

These provisions are general and open to interpretation, and are typically applied to:

- Protect evidence,
- Prevent the continuation of a crime, or
- Stop further harm to victims or the public.

3. Administrative Context – Gambling and Fraud Prevention

- Under Article 15f of the Gambling Act, once a domain is entered into the Minister of Finance's blacklist (Register of Domains Used for Illegal Gambling), internet providers are obliged to block access.
- Under the Act of 28 July 2023 on Counteracting Abuse in Electronic Communications, telecom operators may voluntarily block access to domains included on the "warning list" managed by CSIRT NASK, which identifies fraudulent or phishing websites.

Who has the authority to order or implement website blocking (e.g., courts, government agencies, telecom regulators)?

Authority	**Legal Basis**	**Scope of Blocking**
Courts (civil and criminal)	Code of Civil Procedure, Code of Criminal Procedure	Interim measures, seizure of domains or IT systems during proceedings
Prosecutor	Code of Criminal Procedure (Art. 218a)	Temporary seizure or blocking during investigations
Minister of Finance	Gambling Act (Art. 15f)	Maintains the *Rejestr domen zakazanych* (Blacklist of Illegal Gambling Sites); ISPs are legally required to block domains on this list
Security Services (Police, ABW, SKW, CBA)	Telecommunications Law (Art. 180)	Can require operators to provide access to data or implement technical measures, though this is more focused on surveillance rather than direct website blocking
UOKiK (consumer protection & DSA)	DSA	The Office of Competition and Consumer Protection does not order the blocking of an ISP, but may formally order a platform to remove content or block an account.

Could it be said that the website blocking bodies are well staffed for this agenda?

It could be said that some website-blocking bodies in Poland are relatively well staffed and equipped, while others lack specialized technical capacity.

- The Minister of Finance operates a specialized unit responsible for maintaining the Register of Domains Used for Illegal Gambling and ensuring that Internet Service Providers (ISPs) comply with blocking requirements. This system is focused, institutionalized, and functions effectively.

- Law enforcement agencies such as the Police, Internal Security Agency (ABW), and Central Anti-Corruption Bureau (CBA) have dedicated cybercrime units and teams specialized in digital evidence handling and online investigations, allowing them to effectively manage blocking requests or technical coordination in criminal cases.

- Courts, however, generally lack dedicated technical expertise concerning internet infrastructure and website blocking mechanisms. Judges typically rely on expert opinions, as well as inputs from prosecutors, law enforcement, or external specialists, when making decisions in this area.

In summary, administrative and enforcement bodies (e.g., Ministry of Finance, law enforcement) are better equipped and specialized, while courts have limited technical capacity and depend on external expertise for implementing or assessing website-blocking measures.

Is there a transparent process or published criteria for determining which sites get blocked?

No, there is no fully transparent or uniform process for determining which websites are blocked in Poland, and the criteria are not always publicly available.

In most cases, blocking decisions are made by competent authorities (such as courts, prosecutors, or the Minister of Finance) under specific legal acts, but the procedures and criteria are not standardized or openly published.

- In the case of the gambling blacklist maintained by the Minister of Finance, the list of blocked domains is public, but the decision-making process and criteria for inclusion are not transparent, and affected entities have limited procedural tools to verify or appeal the blocking.

- For security-related blocking (under the Telecommunications Law, Art. 180) or criminal proceedings, decisions are made by law enforcement or judicial authorities based on general terms such as *"national security"* or *"public order"*, which allows broad discretion and lacks detailed, publicly available guidance.

- Individuals or entities whose websites are blocked generally have restricted legal remedies to challenge or review the decision, especially when the blocking results from administrative or law enforcement actions.

In summary, the website blocking process in Poland lacks transparency, and there are no clear, published criteria governing which sites may be blocked or how such decisions can be independently reviewed.

4.3 Implementation and Enforcement

How is website blocking technically enforced (e.g., DNS blocking, IP blocking, URL filtering)?

Website blocking in Poland is technically enforced through different mechanisms, depending on the legal basis and responsible authority. The degree of transparency and oversight varies significantly between systems.

1. Gambling Blacklist – DNS and Domain-Level Blocking

Legal basis: *Gambling Act* (Art. 15f)

Authority: *Minister of Finance*

- The Minister of Finance maintains a public register called the *Rejestr Domen Służących do Oferowania Gier Hazardowych Niezgodnie z Ustawą*
  (Register of Domains Used for Offering Gambling Games in Violation of the Law), available at hazard.mf.gov.pl

2. Courts and Prosecutors – Case-by-Case Blocking

Legal basis: *Code of Civil Procedure* (Art. 730) and *Code of Criminal Procedure* (Arts. 217c, 218a)

Authorities: Civil and criminal courts, prosecutors

- There is no centralized list of websites blocked via judicial or prosecutorial orders.
- The technical methods (DNS blocking, IP blocking, URL filtering, or content removal) depend on the court's or prosecutor's order and cooperation with hosting providers or telecom operators.
- Such measures are often confidential, particularly in criminal proceedings, and not subject to public disclosure.
- Parties to the proceedings may be notified, but the general public has no visibility into which websites are blocked or for what reasons.

3. Security and Law Enforcement Services – Confidential Blocking Requests

Legal basis: *Telecommunications Law* (Art. 180)

Authorities: *Police, Internal Security Agency (ABW), Military Counterintelligence Service (SKW), Central Anti-Corruption Bureau (CBA)*

- These agencies can request blocking of telecommunications transmissions or data flows when necessary to protect national defense, state security, or public order.
- Such requests and their implementation are classified and not publicly reported.
- The technical enforcement method is not detailed in the law but may involve IP blocking, DNS filtering, or network-level restrictions imposed by telecom operators.
- Because these measures are executed under broad mandates and without public oversight, their transparency and accountability are limited.

Are there procedural safeguards (e.g., judicial warrants, due process) before blocking is executed?

Legal basis	Procedural safeguard?
Courts (civil & criminal)	Yes — Blocking can only occur via judicial decision (interim measure or seizure). Parties have access to procedural rights, including appeals and hearings.
Prosecutor (k.p.k.)	Limited — Prosecutor can order seizure/blocking during investigations but this must be later approved by the court.
Minister of Finance (Gambling blacklist)	No full judicial safeguard — Blocking is administratively imposed. Operators are notified only after entry into the blacklist and may challenge it after the fact in court.
Security services (ABW, Police, SKW)	Mixed — Actions are based on national security clauses. Often these are non-transparent and court control is weak or delayed.
UOKiK (consumer protection & DSA)	Yes — Decisions must follow administrative procedure. The entity can contest them before court (Sąd Ochrony Konkurencji i Konsumentów). However, UOKiK cannot order ISPs to block websites.

Do the owners or operators always have the possibility to prevent the blocking of websites, e.g. are they given a period of time to correct illegal content?

Owners or operators of websites do not always have the opportunity to prevent blocking, and the possibility to correct or remove illegal content depends on the legal context and the authority involved.

- In civil proceedings (e.g., copyright, defamation), courts often allow parties to voluntarily remove or correct the content to avoid blocking.

- In UOKiK procedures, correction is usually the primary remedy before more severe measures.
- In criminal proceedings, owners may not be offered such an opportunity if the blocking is imposed for evidentiary purposes or to prevent ongoing crimes.
- In the gambling blacklist, there is no formal grace period — once added to the register, the blocking applies immediately. Only after inclusion can the owner appeal to the court.

Do the blocking authorities differentiate between blocking an entire website and blocking only part of a website?

No, the blocking authorities in Poland do not formally differentiate between blocking an entire website and blocking only part of a website. The relevant legislation is vague on the scope and proportionality of blocking measures, and the technical and procedural practices vary depending on the authority involved.

1. General Situation

- Polish law does not specify whether blocking should target an entire domain, a subpage, or specific content.
- As a result, broad or domain-level blocking is often used, even when the issue concerns only part of a website.
- There is no binding requirement for authorities to apply the least restrictive measure or to limit blocking to specific URLs or subdomains.

2. Civil Proceedings

- In civil cases (e.g., copyright or defamation), courts could theoretically order partial blocking, such as removing a single article, image, or URL.
- However, in practice, the technical implementation by internet providers or hosting services often results in blocking the entire domain, since it is simpler and easier to enforce.

3. Gambling Blacklist (Minister of Finance)

- Under Article 15f of the Gambling Act, blocking applies to entire domain names listed in the Register of Domains Used for Illegal Gambling.
- Partial blocking (e.g., subpages) is not practiced — the system is domain-based.
- The law allows affected entities (e.g., website operators, telecom providers, or domain owners) to file an objection to the Minister of Finance within two months of being listed.
    - The Minister must then issue a decision within 14 days, either maintaining or removing the domain from the register.

4. Security and Intelligence Services (ABW)

- Under Article 32c of the Act on the Internal Security Agency (ABW), website blocking may be ordered for national security reasons.
- The law allows for:
    1. Ordering blocking (Art. 32c(1)),
    2. Emergency blocking with approval from the Prosecutor General (Art. 32c(4)),
    3. One-time extension of blocking for up to three months (Art. 32c(7)).
- However, only the Head of ABW and the Prosecutor General have the right to appeal court decisions on such blocking (Art. 32c(10)).
- Website owners or operators have no legal mechanism—even after the fact—to challenge or verify the legitimacy of the blocking.

5. Fraud and Phishing (Act on Counteracting Abuse in Electronic Communications)

- The warning list managed by CSIRT NASK also functions at the domain level.
- Telecom providers may voluntarily block entire domains listed as fraudulent or phishing sources; partial blocking is not used in practice.

How is the delivery of these warrants to other countries ensured?

Case Type	Cross-border tool
Civil	Brussels I bis (Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, *OJ L 351*), Hague Service Convention
Criminal	European Investigation Order (EU), MLATs (non-EU)
Administrative (gambling)	Polish ISPs block, no foreign delivery
Platform Regulation	DSA cross-border orders via UOKiK

4.4 Transparency and Accountability

Are authorities required to publish lists of blocked websites and provide justifications for blocking decisions?

Institution	Is there a public list?	Justification provided?
Minister of Finance (gambling)	Yes	Category-based (illegal gambling)
Courts (civil & criminal)	No	In individual rulings only
Prosecutor	No	In procedural documents only
Security services	No	Classified or internal use

UOKiK (DSA role)	Partial	Yes, in decisions to platforms and transparency reports
CERT	Yes	No

Do affected website owners, users, NGOs or public have avenues to challenge blocks or content removals before courts?

Actor	Challenge available?	Notes
Website owners	Yes	Court and administrative proceedings possible
Platform operators	Yes	Administrative courts, civil courts, DSA procedures
Users	Limited	Mostly indirect, unless personal rights are affected
NGOs	Limited	Can act indirectly or through public interest litigation Intervene in administrative or judicial proceedings if they represent consumer or freedom of expression interests.
Public	Generally no	No general right to challenge blocking unless directly affected

Do affected website owners, users, NGOs or public have avenues to challenge blocks or content removals before (administrative) bodies?

Actor	Challenge available?	Notes
Website owners	Yes	Court and administrative proceedings possible
Platform operators	Yes	Administrative courts, civil courts, DSA procedures
Users	Limited	Mostly indirect, unless personal rights are affected
NGOs	Limited	Can act indirectly or through public interest litigation
Public	Generally no	No general right to challenge blocking unless directly affected

Yes — in Poland, some avenues exist for website owners, users, or organizations to challenge blocking or content removal, but the scope and effectiveness of these remedies vary greatly depending on the legal basis for the blocking. In several contexts, appeals are allowed only after blocking takes effect, and in others, no formal procedure is available at all.

1. Gambling Blacklist (Minister of Finance)

Legal basis: *Gambling Act, Art. 15f*

- Website owners or domain holders can:
    - File a request for removal of their domain from the gambling register.

    - If the request is refused, lodge a complaint with the Voivodeship Administrative Court (WSA).
    - Further appeal to the Supreme Administrative Court (NSA) is possible.
- However:
    - Blocking is imposed immediately after inclusion in the register.
    - Appeals have no suspensive effect, so the website remains blocked throughout the proceedings.

2. Court-Imposed Blocking (Civil and Criminal Cases)

Legal basis: *Code of Civil Procedure* and *Code of Criminal Procedure*

- In both civil and criminal cases, the website owner, platform operator, or other parties can:
    - Challenge interim measures or blocking orders before the same court that issued them.
    - Appeal decisions through ordinary legal remedies (appeal or interlocutory appeal).
- These procedures are judicial and formal, providing access to review and due process.
- However, foreign or non-party website operators may face difficulties participating effectively if they are not notified or lack local representation.

3. Prosecutor-Imposed Blocking During Investigations

Legal basis: *Article 218a of the Code of Criminal Procedure*

- Blocking ordered by the prosecutor during investigations is considered a temporary security measure and must later be approved by a court.
- The affected party can challenge the blocking through standard criminal procedures — for example, by filing a complaint to the court or appealing decisions once formally notified.

- In practice, foreign website owners may have limited ability to contest such decisions due to lack of notice or jurisdictional constraints.

4. Security Services (ABW, SKW, Police)

Legal basis: *Telecommunications Law (Art. 180)* and *Act on the Internal Security Agency (Art. 32c)*

- Blocking by security or intelligence services is generally non-transparent and classified.
- There is no clear or direct procedure for website owners or users to challenge such measures.
- In theory, an affected entity could file a civil action against the State Treasury for violation of property or freedom of expression, but this would be a complex, lengthy, and uncertain process.
- Under the ABW Act, only the Head of ABW and the Prosecutor General have the right to appeal court orders related to blocking — not the affected website owners.

5. UOKiK (Consumer Protection and Platform Regulation)

Legal basis: *Act on Competition and Consumer Protection* and *Digital Services Act (DSA)*

- Entities affected by UOKiK decisions (e.g., platforms ordered to remove content) can:
  • File an appeal to the Court of Competition and Consumer Protection (SOKiK).
  • Platforms and providers have full access to judicial review.
- End-users or NGOs may participate if they have legal standing or are admitted as amicus curiae in proceedings.

6. List of Warnings for Dangerous Sites (Act on Counteracting Abuse in Electronic Communications, 2023)

Legal basis: *Article 21 of the Act of 28 July 2023*

- A domain owner whose website is placed on the warning list managed by CSIRT NASK can file an objection to the President of the Office of Electronic Communications (UKE).
- The President of UKE then reviews the objection and decides whether to maintain or remove the domain from the list.

Does the website blocking mechanism ensure that the blocking is always temporary?

Polish law does not guarantee that all website blocking measures will be temporary.
The duration of blocking depends on the legal basis and type of authority involved. While civil-law blocking is inherently time-limited, administrative and security-related measures can last indefinitely unless specifically reviewed or challenged. There are no general statutory obligations for periodic review or automatic expiry ("sunset clauses") of blocking decisions.

1. Gambling Blacklist (Art. 15f Gambling Act)

- Blocking is formally indefinite. Once a domain is entered into the *Register of Domains Used for Illegal Gambling*, it remains blocked until the Ministry of Finance removes it.
- There are no automatic time limits or periodic reviews.
- The domain owner must actively request removal or challenge the decision before an administrative court (WSA → NSA).
- If the entity takes no action, the block can last indefinitely.

2. Court-Ordered Blocking (Civil and Criminal Cases)

- Civil cases:
    - Blocking imposed through interim injunctions (*środki zabezpieczające*) is temporary by nature, lasting until the court issues a final judgment.
    - After the case is resolved, the court must decide whether to:
        - Lift the block, or

        - Make it permanent (e.g., by prohibiting operation of a particular website).

- Criminal cases:
    - Blocking (e.g., seizure of domains or IT systems) is also provisional, but can last:
        - Throughout the investigation,
        - Until the end of the trial,
        - Or longer, if the court orders continuation for evidentiary or preventive reasons.
    - No strict statutory time limits apply — it is left to the court's discretion.

3. Administrative Actions by UOKiK (Consumer Protection / DSA Enforcement)

- Blocking measures are typically corrective and temporary.
    - UOKiK focuses on removal of unlawful content or cessation of unfair commercial practices.
    - Once compliance is achieved, the measure should be lifted.
    - Duration depends on cooperation by platforms or businesses, rather than a fixed legal timeframe.

4. Security Services (Police, ABW, SKW)

- Blocking imposed under Telecommunications Law (Art. 180) or national security laws is often open-ended.
- Such restrictions can last as long as the authority considers the threat unresolved.
- There are no automatic expiry rules or mandatory re-assessment procedures.

- Judicial review may occur only if the matter becomes part of a formal court proceeding.

5. List of Warnings for Dangerous Sites (Act on Counteracting Abuse in Electronic Communications, 2023)

- Entries on the warning list are time-limited to six months.
- If the domain is removed from the list or the entry expires, access to the website should be restored.
- This is one of the few mechanisms with a defined duration for blocking.

What mechanisms exist for independent review or oversight of blocking actions and platform moderation practices?

In Poland, independent review and oversight of website blocking and platform moderation practices exist primarily through judicial and administrative mechanisms, but the extent and timing of oversight vary depending on the type of action and the authority involved.

Judicial Oversight (Courts)

- Civil and Criminal Blocking Orders:
    - All court-imposed blocking (interim measures, final injunctions, criminal seizures) is subject to judicial control, meaning:
        - Parties may appeal against interim blocking.
        - There is a possibility of judicial review during or after the proceedings.
    - Courts act as the main independent oversight of content restrictions imposed during litigation.

Administrative Court Control (for administrative blocking)

- Minister of Finance's Gambling Blacklist:
    - Website owners can challenge inclusion in the blacklist to:

        - Voivodship Administrative Court (Wojewódzki Sąd Administracyjny)
        - Then to the Supreme Administrative Court (Naczelny Sąd Administracyjny)
    - This provides an independent review of the legality of the block.
    - BUT → the blacklist applies immediately and is only reviewed post-factum, after blocking is already in effect.

UOKiK and Platform Moderation (under DSA & Polish Consumer Law)

- Since 2024, under the Digital Services Act (DSA):
    - UOKiK acts as Poland's Digital Services Coordinator (DSC).
    - Platforms (e.g., social media, marketplaces) must:
        - Implement transparent complaint-handling systems for users.
        - Provide internal redress mechanisms for moderation decisions.
        - Allow users and content providers to appeal to an out-of-court dispute settlement body.
- UOKiK also has powers to:
    - audit platforms for their moderation practices.
    - Issue orders and conduct inspections of platforms' procedures.
- The DSA additionally establishes:
    - Annual transparency reports by platforms and UOKiK.
    - Judicial review of UOKiK's decisions before SOKiK (Court of Competition and Consumer Protection).

Oversight of Security Services

- ABW, Police, and other agencies have limited external oversight:
    - In theory, actions affecting fundamental rights are reviewable by courts if a party challenges them.
    - However, there is no automatic or ex ante independent oversight of measures like technical restrictions or access limitations for national security purposes.

List of Warnings for Dangerous Sites- Yes, by President of the Office of Electronic Communications

4.5 Impact and Effectiveness

Have any studies or official reports evaluated the effectiveness of website blocking or social media regulations in reducing unlawful or harmful content?

- Raport roczny CSIRT KNF (Computer Security Incident Response Team, Commision of Financial Suspension) - https://www.knf.gov.pl/knf/pl/komponenty/img/Raport_Roczny_CSIRT_KNF_2024_93226.pdf
- Raport roczny 2024 z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego internetu, Państwowy Instytut Badawczy NASK - https://cert.pl/uploads/docs/Raport_CP_2024.pdf

However — these reports focus mainly on cyber-security threats (phishing, malware, fraud) rather than specifically evaluating the impact of website-blocking laws or social media regulations on hate speech or disinformation.

So while they show steps taken and scale of blocking, they do not comprehensively assess how effective the laws or platform regulations are in reducing unlawful or harmful content (in the sense of disinformation/hate speech).

How do blocked entities or individuals typically respond (e.g., mirror sites, VPN usage), and does this undermine the intended impact?

Mirror sites / alternative domains

This is by far the most common and immediate response.

- Blocked websites (especially in gambling, piracy, or fraud sectors) often:
    - Register new domains with small variations (e.g., example1.pl, example.biz, examp1e.net)
    - Use foreign TLDs outside .pl (like .com, .to, .ru, .xyz)
    - Rely on dynamic DNS or redirection services to constantly shift IP addresses and URLs.

Effect:

- This quickly circumvents national blocking — especially if the enforcement is based on static blacklists (like the gambling blacklist).
- ISPs and regulators must then play “whack-a-mole”, constantly updating lists.

2. VPNs (Virtual Private Networks) and proxy servers

Widely used by users, especially tech-savvy individuals.

- Users route their traffic through foreign servers to bypass Polish ISP-level blocks.
- Easy to do with free or commercial VPN apps (e.g., NordVPN, ProtonVPN, Psiphon).
- Common in access to:
    - Banned gambling or streaming sites
    - Politically sensitive or geo-restricted content

Effect:

- Makes blocking ineffective at the user level, especially where no deep packet inspection (DPI) is used.

3. Encrypted DNS (DoH, DoT) and alternative resolvers

- DNS-over-HTTPS (DoH) and DNS-over-TLS (DoT) encrypt DNS queries.

- Users configure browsers (e.g., Firefox, Chrome) or routers to use non-Polish DNS resolvers (like Cloudflare 1.1.1.1 or Google DNS 8.8.8.8).

Effect:

- Completely bypasses Polish ISP DNS filtering (which is the usual method of implementing blocks).
- Makes DNS-based blocking trivial to circumvent.

4. Minimal impact in criminal or malicious sectors

- In cases involving phishing, fraud, and serious cybercrime:
    - Blocking has only temporary impact — operators are prepared to shift to new infrastructure quickly.
    - Many use botnets, fast-flux networks, or bulletproof hosting outside Poland/EU.

Effect:

- Blocking slows them down, but does not stop operations unless coordinated with law enforcement takedowns.

Does this undermine the intended impact of blocking?

Yes — in many cases.

- Blocking is symbolic or deterrent rather than technically bullet

How do ISPs, platform operators, or tech companies influence the shaping of internet regulation?

1. Through Industry Associations and Consultations

Major tech stakeholders act collectively through associations:

- PIIT – *Polska Izba Informatyki i Telekomunikacji*
  Represents ISPs, telcos, and IT firms. Provides opinions on legislative drafts (e.g., Telecommunications Law, blocking powers).

- Lewiatan, ZIPSEE, ZPP – business organizations representing digital service providers and startups.
- Chambers of Commerce (e.g., KIG, KIPR) also participate in public hearings or consultations organized by ministries or Parliament.

Direct lobbying and position papers

Big tech firms (Google, Meta, Amazon) often submit:

- Position papers in response to legislative drafts
- Lobby government agencies, including the Ministry of Digital Affairs, UKE, UOKiK, and members of Parliament.

3. Participation in regulatory sandbox or expert working groups

In some areas, tech companies are invited to:

- Take part in regulatory sandboxes (e.g., fintech, digital ID)
- Join expert panels with government agencies (e.g., with UKE or NASK in cybersecurity)

4.6 Emerging Trends and Future Outlook

Are there any recent or upcoming legislative proposals that aim to broaden or narrow website blocking or social media regulation?

In March 2025, the Deputy Prime Minister of Poland announced the government's determination to implement a plan to tax large technology companies, despite opposition from the United States. The aim of this tax is to cover the profits earned by major tech firms operating in Poland and to support the development of Polish technology companies. However, the details of the plan have not yet been published on official government websites[5].

[5] https://www.infor.pl/twoje-pieniadze/podatki/6883744,podatek-od-big-techow-daje-milionowe-zyski-ale-jest-problem-natury-po.html

The Polish government has approved a major amendment to the Act on the Provision of Electronic Services, a legal framework that will implement the EU's Digital Services Act (DSA) domestically[6].

The amendment gives Polish authorities and online platforms a legal, fast-track procedure to block illegal content (like human trafficking, identity theft, child exploitation, and online fraud). It also creates a formal appeals process for users whose posts are removed and divides oversight among three institutions:

- UKE – Office of Electronic Communications (Digital Services Coordinator)
- UOKiK – Office of Competition and Consumer Protection (for e-commerce platforms)
- KRRiT – National Broadcasting Council (for video-sharing platforms)

4.7 Practical and Ethical Considerations

Have concerns been raised about over-blocking (collateral censorship) or chilling effects on legitimate speech?

- Fundacja Panoptykon – multiple position papers and legal analyses
- Helsińska Fundacja Praw Człowieka – reports on digital rights and freedom of expression

1. Gambling blacklist (Art. 15f Gambling Act)

- Entire domains are blocked once added to the blacklist, without distinction between legal and illegal content hosted under the same domain.
- No court order is required, and there's no suspensive effect of appeal.

2. New "List of Warnings" (2023 Anti-Abuse Law)

- Domains used for fraud or phishing may be blocked by ISPs at the request of CSIRT NASK.

[6] https://www.prawo.pl/biznes/rzad-przyjal-projekt-ustawy-ws-blokowania-nielegalnych-tresci-w-internecie,535050.html

- However, the decision is not always reviewed by a court and may affect entire domains based on automated classifications or reports.

5
NATIONAL IMPLEMENTATION OF RELEVANT EU REGULATIONS CONCERNING INTERNET CONTENT

Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online

Regulation (EU) 2022/2065 (DSA)

(It is also possible to refer to other relevant European legislation.)

5.1 Transposition and Legislative Adaptation

Has your country adopted or adapted any national legislation to comply with Regulation (EU) 2021/784 on terrorist content online?

Poland has granted the head of the Internal Security Agency powers under which he can order hosting service providers to remove specific content that violates the principles regulated by Regulation EU 2021/784. It is an effect of the adoption of the Act of 18th October 2024, amending the Act on Counter-Terrorism Activities and the Act on the Internal Security Agency and the Foreign Intelligence Agency [article Art. 26c (1) and (3)] (Ustawa z dnia 18 października 2024 r. o zmianie ustawy o działaniach antyterrorystycznych i ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu).

What specific laws or regulations have been enacted or amended to align with the DSA (Regulation (EU) 2022/2065)?

The Act of 18th October 2024, amending the Act on Counter-Terrorism Activities and the Act on the Internal Security Agency and the Foreign Intelligence Agency

5.2 Institutional Responsibilities

Which national authority or authorities are responsible for overseeing and enforcing compliance with the terrorist content regulation?

Internal Security Agency (ABW) is responsible for that on a ground of mentioned aboved amendment. Also on that ground the TCO Contact Point were established, it is a special unit of ABW – CAT ABW Centrum Antyterrorystyczne ABW.

Similarly, which body (or bodies) monitors and enforces the Digital Services Act in your jurisdiction?

As Poland has not fully fulfilled the obligations from DSA, the Prime Minister temporally nominated Office of Electronic Communications (UKE) as an body which supposed to monitors and enforces DSA (Digital Services Coordinator).

Have any new regulatory agencies or units been created to handle these mandates?

Yes, CAT ABW - new unit of Internal Security Agency.

5.3 Obligations for Hosting Service Providers

Under Regulation (EU) 2021/784, how are hosting service providers required to remove or disable terrorist content?

On a base on an order of the Head of the Internal Security Agency - (article Art. 26c (1) and (3) of the Act of 18th October 2024, amending the Act on Counter-Terrorism Activities and the Act on the Internal Security Agency and the Foreign Intelligence Agency.

Are there specific timeframes for removal (e.g., the one-hour rule) and how are these enforced in practice?

The timeframes are establish in the Head of Internal Security Agency order.

Regarding the DSA, what additional obligations (e.g., risk assessments, transparency reports) must online platforms fulfill in your country?
Not applicable

5.4 Notification and Removal Procedures

What procedures or protocols must authorities follow when issuing removal orders for terrorist content?

Article 26c of the Act of 18th October 2024, amending the Act on Counter-Terrorism Activities and the Act on the Internal Security Agency and the Foreign Intelligence Agency:

1. The Head of the Internal Security Agency (ABW) supervises the implementation of the special measures referred to in Article 5 paragraphs 1-3 of Regulation 2021/784 by:

1) inspecting the special measures taken by the hosting service provider, including their compliance with Article 5 paragraphs 2 and 3 of Regulation 2021/784;

2) issuing written recommendations to the hosting service provider aimed at eliminating any identified irregularities and adapting its operations to the provisions of Regulation 2021/784.

2. When carrying out the activities referred to in paragraph 1, an authorized officer of the ABW has the right to:

1) enter the premises of the inspected facilities used to provide hosting services;

2) request explanations from the hosting service provider and access to technical and operational documentation resulting from the application of the special measures, or to inspect such documentation.

How do national courts or administrative bodies review such orders to ensure they are lawful and proportionate?

The orders are issued with the court control procedure. Orders are treated as administrative decisions, so the body addressed to review such orders are the administrative courts. In that type of cases the mentioned below procedures are used:

Article 26d. 1. The order to remove or establish an infringement referred to in Article 4 paragraphs 3 and 4 of Regulation 2021/784 shall be issued by way of an administrative decision. To proceedings in these matters, to the extent not regulated in Regulation 2021/784 and this Act, the provisions of Article 6, Article 7, Article 7b, Article 8, Article 12, Article 14, Article 16, Article 24, Article 26 § 1 and 2, Articles 28–30, Article 32, Article 33, Article 35 § 1, Article 50, Articles 54–56, Articles 63–65, Article 72, Article 75 § 1, Article 77, Article 39, and Article 40 shall apply. 97 § 1 item 4 and § 2, Article 104, Article 105 § 1, Article 112, Article 113 § 1, Articles 156–158, Article 217 and Article 268a of the Act of 14 June 1960 - Code of Administrative Procedure (Journal of Laws of 2024, item 572).

Under the DSA, how are notice-and-action mechanisms implemented, and are there clear guidelines for both users and platforms?

Not applicable

5.5 Sanctions and Penalties

What sanctions or penalties can be imposed on service providers for non-compliance with Regulation (EU) 2021/784?

Article 26f. 1. A hosting service provider that fails to comply with the obligation referred to in Article 3 paragraph 3 or 6, Article 4 paragraph 2 or 7, Article 5 paragraphs 1-3, 5 or 6, Article 6, Article 7, Article 10, Article 11, Article 14 paragraph 5, Article 15 paragraph 1, or Article 17 of Regulation 2021/784 shall be subject to a fine.

2. The fine referred to in paragraph 1 shall be imposed by the Head of the Internal Security Agency by way of an administrative decision, taking into account the conditions and circumstances specified in Article 18 of Regulation 2021/784, in the amount of up to 4% of the total turnover achieved by the hosting service provider in the previous financial year.

3. The decision referred to in paragraph 2 is final. 4. Funds from the fines referred to in paragraph 1 constitute state budget revenue.

Under the DSA, are there specific ranges of fines or penalties that apply to infringements in your country?

Not applicable

Have there been any notable enforcement actions or penalties imposed so far?

No.

5.6 Scope and Application

Are all online platforms equally subject to these regulations, or do smaller platforms and start-ups have different obligations?

This solution has been not predicted in the text of Act.

Does your country apply any specific exemptions or streamlined procedures for non-profit platforms, academic repositories, or other niche services?

No.

5.7 Judicial Review and Legal Challenges

Have there been any court cases challenging the implementation or scope of Regulation (EU) 2021/784 in your jurisdiction?

None so far

What arguments—constitutional, procedural, or otherwise—have been raised in these challenges?

Not applicable

5.8 Transparency and Reporting

Do authorities or platforms publish reports on the volume of terrorist content removed under Regulation (EU) 2021/784?

They are obliged to, but Poland didn`t meet this expectations.

Under the DSA, what transparency requirements exist for service providers (e.g., content moderation reports)?

Not applicable

How accessible is this information to the public or civil society watchdogs?

For now this information is not accessible at all.

5.9 Cooperation with Other Member States and EU Bodies

Is there any formal mechanism for cooperation between your national authorities and other EU member states in enforcing these regulations?

Yes, the UEK was nominated by Prime Minister as a temporary Digital Services Coordinator, which is responsible for the effective exchange of information with the European Commission, the European Digital Services Council and counterparts from other countries.

How do EU-level entities (e.g., the European Commission, Europol) coordinate or facilitate the exchange of best practices?

"For first, the Digital Services Coordinators were appointed or will be appointed in every EU country. For second, on the ground of DSA the European Commission is obliged to create the expert group, which will provide evidence-based information and specific expertise on online user safety, aiding in the enforcement of the regulation (article 64 of the DSA).

The European Cybercrime Centre (EC3) was set up by Europol to strengthen the law enforcement response to cybercrime in the EU.

EC3 offers operational, strategic, analytical and forensic support to Member States' investigations. For each of the cybercrime types mentioned above, EC3:

- *serves as the central hub for criminal information and intelligence;*
- *supports operations and investigations by Member States by offering operational analysis, coordination and expertise;*
- *provides highly specialised technical and digital forensic support capabilities to investigations and operations;*
- *provides support to EU crisis management structures, within the scope of Europol's mandate, and facilitates the operational, technical and strategic collaboration between law enforcement agencies (LEAs) and other relevant cyber communities and EU institutions, bodies and agencies (e.g. Eurojust, EEAS, ENISA, CERT-EU, Commission, Council, etc.);*
- *provides 24/7 operational and technical support to LEAs for immediate reaction to urgent cyber incidents and/or cyber crises via stand-by duty and the EU Law Enforcement Emergency Response Protocol (EU LE ERP);*
- *hosts and facilitates the efforts of the Joint Cybercrime Action Taskforce (J-CAT) in combating cybercrime;*
- *supports training and capacity-building, in particular for the relevant authorities in Member States;*
- *provides a variety of strategic analysis products that enable informed decision-making on combating and preventing cybercrime;*

- *provides a comprehensive outreach function connecting law enforcement authorities tackling cybercrime with the private sector, academia and other non-law enforcement partners;*

- *contributes to the preparation and delivery of standardised prevention and awareness campaigns and activities in the cybercrime-mandated areas.*

Operational highlights

- *Operation Eastwood, coordinated by Europol and Eurojust, targeted the cybercrime network NoName057(16), taking the group's central infrastructure offline and disrupting an attack-infrastructure consisting of over one hundred computer systems worldwide.*

- *In May 2025, Operation Endgame resulted in 21.2 million EUR in cryptocurrency seized, as well as the takedown of 300 worldwide malware servers, the neutralisation of 650 domains, and the arrest warrants against 20 targets, dealing a direct blow to the ransomware kill chain.*

- *A global Crackdown on Kidlix a major child sexual exploitation platform with over 2 million users, took place in April 2025, leading to 79 arrests and 1400 identifications. Operation Stream has been the largest operation ever handled by Europol's experts in fighting child sexual exploitation, and one of the biggest cases supported by the law enforcement agency in recent years.*

- *The No More Ransom project, which was launched in 2016 with the goal to help victims of ransomware retrieve their encrypted data without having to pay the criminals, now counts with over 200 partners. The portal is available in 38 different languages and offers 157 tools capable of decrypting over 180 different types of ransomware. To date, the No More Ransom Initiative has seen more than 10 million downloads of available tools and has assisted millions of victims worldwide".*

Source of cite: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Have there been cross-border cases that required joint enforcement efforts?

No.

5.10 Impact on Freedom of Expression and Privacy

Have concerns been raised that the fast removal requirements under Regulation (EU) 2021/784 might lead to over-removal or censorship?

Such concerns have arisen. However, Polish law has created mechanisms to control the removal of unlawfully harmful content, which allows for the possibility of challenging the order of the Head of the Internal Security Agency and subjecting the decision to judicial review.

Under the DSA, how are fundamental rights—such as freedom of expression and data protection—safeguarded in your national implementation?

Not applicable

What oversight or appeal mechanisms exist for content creators or users affected by removals?

The Act on Anti-Terrorist Activities and the Act on the Internal Security Agency and the Foreign Intelligence Agency from 18th October 2024:

Article 26d

4. A hosting service provider against whom the Head of the Internal Security Agency has issued a removal order, or a content provider whose content is covered by a removal order, has the right to file a complaint against this order with an administrative court within 30 days of the date of:

1) its delivery in the manner referred to in Article 3(5) of Regulation 2021/784 – in the case of a hosting service provider;

2) receipt of the information referred to in Article 11(1) of Regulation 2021/784 – in the case of a content provider.

5. A hosting service provider or content provider in respect of whom the Head of the Internal Security Agency issued a decision referred to in Article 4 paragraph 4 of Regulation 2021/784 has the right to file a complaint against this decision with an administrative court within 30 days of receiving notification of this decision.

6. A hosting service provider in respect of whom the Head of the Internal Security Agency issued a decision referred to in Article 5 paragraphs 4, 6, or

7 of Regulation 2021/784 has the right to file a complaint against this decision with an administrative court.

7. Complaints referred to in paragraphs 4–6 may be considered under the simplified procedure referred to in Article 120 of the Act of 30 August 2002 – The Code of Administrative Court Procedure (Journal of Laws of 2024, item 935), unless the party requests a hearing and the court determines that all circumstances of the case have been sufficiently clarified and that a hearing is unnecessary. The provisions of Article 122 of the Act of 30 August 2002 – The Code of Administrative Court Procedure shall apply.

5.11 Comparisons with Other Jurisdictions

If relevant, do lawmakers or regulators reference how other EU member states are implementing these regulations?

No

Are there notable differences in how your country addresses terrorist content or digital services obligations compared to neighboring states?

Not applicable

6
THE ROLE OF THE ADMINISTRATOR OF THE NATIONAL TOP-LEVEL DOMAIN (.CZ/.SK/.PL/.HU)

6.1 Institutional Setup and Governance

Which entity (public, private, or non-profit) administers the national top-level domain (TLD) in your country?

The national top-level domain (TLD) ".pl" in Poland is administered by the Research and Academic Computer Network – National Research Institute (Naukowa i Akademicka Sieć Komputerowa, NASK – Państwowy Instytut Badawczy).

NASK was established on 14 December 1993 by order of the Chairman of the Committee for Scientific Research (Order No. 5/93, Official Journal of the KBN No. 7, item 33). Since 1 October 2010, it has operated as a state research institute under:

- the Act of 30 April 2010 on Research Institutes (Journal of Laws No. 96, item 618),
- the Act of 30 April 2010 introducing reforms to the science system, and
- the Regulation of the Council of Ministers of 7 June 2017.

Domain registration under the ".pl" TLD is carried out through accredited registrars participating in the Partner Programme, which was launched by NASK in December 2002.

How is this administrator selected or designated (e.g., through a government contract, regulatory framework, or historical precedent)?

The administrator of Poland's national top-level domain ".pl" — NASK (Research and Academic Computer Network – National Research Institute) — was designated primarily through historical precedent and international technical delegation, rather than a formal government tender or specific statutory act.

What legal or regulatory instruments define and govern the role of this TLD administrator?

The legal and regulatory framework governing NASK's role as the ".pl" TLD administrator is defined by a combination of technical delegation, internal regulations, and general legal acts:

Technical Delegation by IANA/ICANN

- The Internet Assigned Numbers Authority (IANA) officially delegates the management of the ".pl" TLD to NASK.
- The delegation is recorded in the IANA Root Zone Database: https://www.iana.org/domains/root/db/pl.html

Internal Regulation – NASK Domain Name Regulations

- The ".pl" Domain Name Regulations (*Regulamin nazw domeny .pl*) issued by NASK on 18 December 2006 (as amended, current version effective from 1 December 2015) specify:
    - The terms and conditions for registering and maintaining domain names under ".pl".
    - The rights and obligations of domain holders and registrars.
    - The procedures for resolving disputes and terminating domain service agreements.

General Legal Framework

- NASK operates as a state research institute under the Act of 30 April 2010 on Research Institutes (Journal of Laws No. 96, item 618).
- This act provides the general legal basis for NASK's activities as a public entity responsible for information and communication technologies in Poland.
- In summary, NASK's role as the ".pl" domain administrator is based on international technical delegation (IANA) and its own internal regulations,

supported by its status as a public research institute under Polish law, rather than by a dedicated national statute.

6.2 Responsibilities and Mandate

What are the core functions of the TLD administrator (e.g., domain name registration, policy enforcement, dispute resolution)?

Legal Basis: *Regulations for .pl Domain Names* (*Regulamin nazw domeny .pl*) of 18 December 2006 (as amended, currently in force since 1 December 2015).

Under this internal regulation, the Research and Academic Computer Network – National Research Institute (NASK) performs the following functions as the administrator of the ".pl" top-level domain:

- Registration and Maintenance of Domain Names- NASK provides services related to the registration and ongoing maintenance of domain names under the ".pl" TLD. This includes creating new domain entries and ensuring their technical continuity.
- Administrative and Technical Management- NASK manages subscriber data and operates the information systems necessary to process and maintain domain registrations and associated technical records.
- Cooperation with Partners (Registrars)- NASK concludes cooperation agreements with accredited partners (registrars), who act as intermediaries in the process of domain name registration and management within the ".pl" domain.
- Setting Technical Registration Requirements- NASK defines the technical requirements for domain names, including permissible characters

Does the administrator have any responsibilities related to content regulation or oversight of hosted websites?

Based on the "Abuse Prevention Policy for .pl Domain Names" (*Polityka przeciwdziałania nadużyciom z wykorzystaniem nazw w domenie .pl*, DNS.pl, 2019), NASK has limited but important responsibilities related to addressing illegal or harmful activities conducted through ".pl" domain names.

However, NASK is not a content regulator or censorship authority — it does not monitor, moderate, or assess website content for legality or accuracy. Its role is strictly technical and reactive, focused on maintaining the security and stability of the DNS system.

Key Responsibilities under the Abuse Prevention Policy:

- Scope of Action -The policy declares NASK's commitment to act *"in cases of detected illegal or dishonest practices involving .pl domain names that may threaten the security or stability of the DNS system or Internet users."* (Section 2)
- Grounds for Intervention- NASK may intervene when a domain is used for activities such as:
    - Phishing, malware distribution, or impersonation (spoofing),
    - Violations of DNS security principles,
    - Large-scale fraud (e.g., fake online stores or scams).
- Possible Measures Taken by NASK
    - Temporary suspension of domain delegation (blocking the website's operation),
    - Contacting the domain holder (subscriber) to clarify or resolve the issue,
    - Notifying competent authorities, such as the Police, CERT Polska, or the Internal Security Agency (ABW), when criminal or harmful activity is suspected.

6.3 Registration Policies

What rules or policies govern the registration of domain names under the national TLD (e.g., residency requirements, trademark considerations)?

You don't have to be a Polish entity to register a name in a national domain. According to the latest NASK report, "The .pl Domain Name Market," over 90% of .pl domain name registrants are located in Poland, but registrations from

Germany, the USA, and the Netherlands also occur. Name registration is based on the first-come, first-served principle.

NASK does not check whether a domain name violates trademarks or other IP rights at the time of registration.- No prior verification of trademark rights

Domain names must meet technical conditions, such as: Contain 1–63 characters, Use allowed characters: a–z, 0–9, hyphen ("-"), Must not start or end with a hyphen.

There is no published list of banned words, but NASK can reject names that: Violate technical rules, Are reserved or system-critical (e.g., *.gov.pl*, *.edu.pl* under managed subdomains), Are used in bad faith or cause system instability (e.g., phishing, spoofing).

Trademark or name-right disputes are not handled by NASK itself, but can be resolved via:

- Court proceedings,
- Or arbitration at one of the following:
    - Sąd Polubowny przy PIIT (Arbitration Court at the Polish Chamber of Information Technology and Telecommunications),
    - SAiP przy KIG (Court of Arbitration at the Polish Chamber of Commerce).

Rule	Applies?
Polish residency required?	No
First-come, first-served?	Yes
Trademark protection checked?	No
Technical format rules?	Yes

Content restrictions (e.g., banned words)?	Partially
Dispute resolution via arbitration or court?	Yes

Are there restrictions or special requirements for certain types of domain names (e.g., government domains, restricted sectors)?

Yes — under the .pl national TLD, while most domain names are open for public registration, there are restrictions or special requirements for certain types of domains, particularly those involving government, education, or special-use subdomains.

-.gov.pl – Reserved for Polish public administration and state institutions.
Must be requested through official procedures, typically coordinated with NASK and appropriate ministries.

- .mil.pl – Reserved for the Ministry of National Defence and Polish Armed Forces.

- .edu.pl – Managed separately for educational institutions (universities, schools, etc.) with eligibility requirements.

Does the administrator have a public policy document or guidelines outlining registration procedures and dispute resolution processes?

Yes, the .pl domain administrator (NASK) provides clear, publicly available policy documents and guidelines that outline:

1. Registration procedures
2. Dispute resolution processes
3. Registrant responsibilities and rights

These are all published on NASK's official website: https://dns.pl

6.4 Dispute Enforcement

Under what circumstances can the administrator revoke or suspend a domain name?

It is regulated by the .pl Domain Name Regulations as of 18th December 2006. The first general reason is under Article 25 of this document, which states that: *Irrespective of the reasons specified in other articles of these Regulations, the NASK can terminate the Agreement without the notice if the provisions of the Regulations have been infringed by the Subscriber.*

The article 27 of this document is more specified: *When NASK has determined that the Maintenance of the Domain Name causes, may cause or affect the emergence or development of danger of security and stability of global domain name system or the .pl Domain, NASK shall be authorized to suspend the Maintenance of the Domain Name or Change of Delegation.*

Source of cite: https://www.dns.pl/en/pl_domain_name_regulations

6.5 Collaboration with Government and Law Enforcement

Does the TLD administrator coordinate with government agencies or law enforcement in addressing illegal online activities (e.g., court orders to suspend domains)?

The TLD administrator is an independent body from government agencies and operates independently of them. However, any situations (including infringement reports and court orders) that violate the .pl Domain Name Regulations as of December 18, 2006 may result in domain suspension or deletion.

Are there formal procedures or agreements (memoranda of understanding) in place to facilitate this cooperation?

Not aware of any.

Have there been notable cases in which the TLD administrator took action against domain owners at the government's request?

Not aware of any. Nevertheless, according to annual reports, the Scientific and Academic Computer Network (NASK) is deleting some domains registered under the .pl domain. These deletions are largely due to domain failures, but they also

include instances where domains are deleted for violations of NASK regulations. It's worth noting that NASK has effectively blocked the operation of dozens of domains used to distribute malware and spam. It is worth to pointed out that there were one nobel case, but led only by NASK without government`s request, when NASK cancelled the agreement with Domain Silver Inc., which was responsible for handling malicious web addresses.

6.6 Transparency and Accountability

Are domain holders or the public able to appeal or challenge decisions made by the TLD administrator?

Yes. Decision of NASK could be challenge in front of polish courts on general rules. Furthermore, within NASK was established an Arbitration Court addressed to the issues, when the Subscriber has infringed the rights of third person by entering into or performing the Agreement.

6.7 Economic and Market Considerations

Are registration fees or other costs regulated by the government, or set independently by the TLD administrator?

The fees are set by NASK, the rates are public and you can easly check it at website: https://www.dns.pl/cennik_dla_rejestratorow

7
INDEPENDENT OVERSIGHT MECHANISMS

The role of ombudsman institutions, national human rights bodies, and other watchdogs

7.1 Institutional Mandates and Legal Foundations

Which institutions in your country serve as independent oversight mechanisms, such as ombudsman offices or national human rights commissions?

Polish Constitution established two constitutional bodies responsible for human rights protection: The Commissioner for citizens' rights and The Commissioner for children`s rights.

Under what legal or constitutional provisions are these institutions established, and how is their independence safeguarded?

The Commissioner for citizen`s rights is constitutional body, established in Polish Constitution from 2th April 1997 in article 208. He is responsible for ensuring the implementation of human and civil rights and freedoms on the territory of Poland. He is nominated by the Sejm with approval of the Senat, but he is independent and out of the power division. All goals and obligations are regulated in statutory act: Act from 15 July 1987 on the Commissioner for Human Rights.

The second body is The Commissioner for children`s rights. This institution was established by article 72(4) of Polish Constitution from 2th April 1997. All competences are described in additional statutory act.

Do their mandates explicitly cover digital rights, freedom of expression online, or the regulation of online content?

No. The protection in that areas is the result of an interpretation that expands already existing fundamental rights.

7.2 Scope of Authority and Responsibilities

What types of complaints or issues can be brought to these oversight bodies (e.g., alleged censorship, violations of online privacy, hate speech)?

In general The Commissioner for Human Rights takes action (Article 9 - Act from 15 July 1987 on the Commissioner for Human Rights):

1) at the request of citizens or their organizations;

2) at the request of local government authorities;

2a) at the request of the Ombudsman for Children;

2b) at the request of the Ombudsman for Small and Medium-sized Enterprises;

3) on his own initiative.

Do these institutions have the power to issue legally binding decisions, recommendations, or only advisory opinions?

When the Commissioner for Human Right decide to take an action they can:

Article 14 Act from 15 July 1987 on the Commissioner for Human Rights

After examining the case, the Commissioner may:

1) explain to the applicant that he/she has not found a violation of human and civil rights and freedoms;

2) refer a motion to the body, organization, or institution in whose activities he/she has found a violation of human and civil rights and freedoms;

such a motion may not violate judicial independence;

3) submit a motion to the body superior to the entity referred to in point 2 to apply measures provided for in the law;

4) request the initiation of proceedings in civil cases, as well as participate in any ongoing proceedings – with the rights of a prosecutor;

5) request the initiation of preparatory proceedings by a duly authorized prosecutor in cases concerning crimes prosecuted ex officio;

6) request the initiation of administrative proceedings, file complaints with the administrative court, and participate in these proceedings – with the rights

of a prosecutor;

7) file a motion for punishment or for the annulment of a final

decision in proceedings concerning petty offences, under the terms and procedures specified in separate regulations;

8) file a cassation appeal or extraordinary appeal against a final judgment, under the terms and procedures specified in separate regulations.

The Commissioner for Human Right also can:

Article 16 Act from 15 July 1987 on the Commissioner for Human Rights

1. In connection with the cases under consideration, the Commissioner may submit assessments and proposals to the relevant authorities, organizations, and institutions aimed at ensuring effective protection of human and civil rights and freedoms and improving the process of resolving their cases.

2. The Commissioner may also:

1) submit motions to the relevant authorities to undertake legislative initiatives or to issue or amend other legal acts in matters concerning human and civil rights and freedoms and freedoms;

2) submit motions to the Constitutional Tribunal in matters referred to in Article 188 of the Constitution;

3) declare participation in proceedings before the Constitutional Tribunal and participate in such proceedings;

4) submit motions to the Supreme Court to adopt a resolution aimed at clarifying legal provisions that raise doubts in practice or whose application has led to discrepancies in case law. 3. If the Commissioner submits an application to the Constitutional Tribunal referred to in paragraph 2, point 2, he or she shall inform the Commissioner for Children's Rights thereof if the application concerns the rights of the child.

How do they prioritize or select cases related to digital rights or internet regulation?

There are no rules about that.

7.3 Complaints and Redress Mechanisms

How can citizens, NGOs or persons affected file complaints regarding internet-related grievances (e.g., blocked websites, content takedowns)?

If the issue concerns illegal or harmful online content (for example, child sexual abuse material, hate speech, obviously illicit content) it could be reported via the national hotline Dyżurnet.pl (run by NASK) which receives such notifications and forwards them to relevant providers or authorities.

If the content were wrongfully removed or blocked by a platform the complaint could be submit on the ground of platform internal regulations.

If this is about digital-accessibility or public sector website issues there is possibility to complain to UOKIK(Urząd ochrony konkurencji i konsumenta).

At least the complain could be submit to the civil court.

Are these processes user-friendly, accessible online, or free of charge?

It depends. If the complaint is made to the platform it is usually free, but when you could go to proceeding you need to pay the fee.

What remedies (e.g., compensation, policy recommendations, sanctions) can these institutions provide or recommend?

Not applicable

7.4 Interaction with Government and Legislators

Are ombudsman or human rights bodies consulted during the legislative process on laws affecting internet governance or digital rights?

Yes, they can share their insight.

Do they issue formal opinions or recommendations to government entities, and are these taken into account?

There is no obligation to consult the Commissioner for Human Rights, but on the ground of Article 16 (2) Act from 15 July 1987 on the Commissioner for Human Rights the Commissioner can submit motions to the relevant authorities to undertake legislative initiatives or to issue or amend other legal acts in matters concerning human and civil rights and freedoms and freedoms.

Have their recommendations ever led to significant changes in internet-related legislation or regulation?

No examples in this area.

7.5 Case Studies and Notable Interventions

Can you provide examples of significant cases where these institutions intervened to address online censorship, disinformation, or hate speech?

The opinion of the Commissioner for Human Rights of 9 January 2025 ("II.510.345.2024.MW/PZ") was addressed to the Chairwoman of the Special Committee for Changes in Codifications, in connection with the government draft act amending the Penal Code (form no. 876). In this opinion, the Commissioner for Human Rights responded positively to the proposal to expand the list of grounds for hate crimes to include disability, age, gender and sexual orientation, but at the same time expressed reservations about some of the draft solutions. The Constitutional Tribunale ruled that the proposed changes are uncostitutional.

The opinion of the Commissioner for Human Rights of 26 October 2021 (VII.564.94.2021.AMB) was adressed to the Ministry of Justice. The Commissioner for Human Rights issued an opinion on "internet freedom" — including in the context of content moderation, the user's right to appeal, issues related to hate speech and internet regulation.

Were their interventions successful, and did they lead to policy changes, legal reforms, or compensation for victims?

Not applicable

What challenges did they face (e.g., resistance from governmental bodies, lack of cooperation from digital platforms)?

Not applicable

7.6 Effectiveness and Criticisms

How do stakeholders (e.g., civil society, media, academia) perceive the effectiveness of these independent oversight mechanisms in protecting online rights?

The Commissioner for Human Rights does not have competence to intervene in many cases of online rights, especially those involving private-sector digital platforms (e.g., account removals by social-media companies). What Commissioner can do is to join

Have there been criticisms or concerns regarding their impartiality, resources, or scope?

Civil society reports note that despite its role, the RPO's resources, mandate and capacity may not fully match the growing digital-rights challenges (e.g., surveillance, profiling, data-driven services). While the RPO raises issues, some critiques suggest it lacks sufficient enforcement power or systemic influence when platform governance or digital regulation is involved. The institutional gap between state actors and private digital intermediaries is noted.

Source: https://siecobywatelska.pl/wp-content/uploads/2024/05/RoLR_word-1.pdf

Do they face budgetary or political constraints that limit their ability to address digital rights issues effectively?

Not really. It is more about the competences and accessible measures.

7.7 Future Outlook and Reform

Are there ongoing discussions about reforming or expanding the mandates of these institutions to better address internet governance and digital rights challenges?

Yes. Look at the common report of NGO`s: https://siecobywatelska.pl/wp-content/uploads/2024/05/RoLR_word-1.pdf

How might emerging technologies (AI, automated content moderation) influence the need for stronger or more specialized oversight?

There is a feeling of lack of the adequate measures to combat the disinformation and hate speech and regulate the private sector of digital platforms. So the development of new technologies could cause a necessity of applying new provision, which would fulfill all the mentioned above gaps in national legal system.

Are there proposals to create new institutions or strengthen existing ones to address the complexities of the digital environment?

Yes, in the context of implementation of DSA obligations. There is a discussion to create Freedom of Expression Council to guarantee the protection of freedom of expression in the context of new regulations and limitations. The main competences of FEC:

- receiving and reviewing appeals against decisions by online platforms,

- supervising platforms' compliance with the obligations arising from the DSA (including content removal and restoration procedures),

- protecting freedom of speech and the right to information in the process of online content moderation,

- cooperating with national and European regulatory authorities and fulfilling a monitoring role in this regard.

7.8 Comparisons and Best Practices

Do your country's oversight bodies benchmark against international best practices or models from other jurisdictions?

There is no detailed information, only one page of Ministry of Digital Affairs was mentioned that during the preparation of draft of the act implementing DSA, other countries solutions have been taken under consideration.

Source: https://www.gov.pl/web/cyfryzacja/kolejny-wazny-etap-wdrozenia-aktu-o-uslugach-cyfrowych-w-polsce?utm_source=chatgpt.com

Are there examples of pioneering or innovative approaches taken by these institutions that could be emulated elsewhere?

No

How does your country's independent oversight framework compare with regional or international standards (e.g., Council of Europe recommendations, UN guidelines)?

Poland is still working on reach to international and European Union standards. There is still not fulfilled obligations from DSA.