SPECIAL EDITION NO. 2

dot.pl

NASK

dot.pl

SUMMARY REPORT 2024

SPECIAL EDITION NO. 2

WARSAW, MAY 2025

ISSN 3071-673X

mail.pl
com.pl
aid.pl
auto.pl
atm.pl
edu.pl
agro.pl
gmina.pl
mil.pl
info.pl
targi.pl
gsm.pl
mil.pl
miasta.pl
media.pl
realestate.pl
shop.pl
net.pl
kolobrzeg.pl
nieruchomosci.pl
szkola.pl
org.pl
sklep.pl
sos.pl
travel.pl
gniezno.pl
turystyka.pl
nom.pl

Table of Contents

Introduction

The Internet is inherently cross-border in nature, and existing national legal frameworks have proven insufficient for the provision of digital services across the entire European Union. This applies not only to services offered within the EU's digital single market but also to those provided by entities based outside of it. The limited effectiveness of previous regulations has impacted the ability to ensure both security and a consistent level of protection for the rights of EU citizens and businesses operating online.

In 2024, the harmonization of conditions for the development of innovative, cross-border digital services—while maintaining a safe online environment—became a reality at the EU level. New legislation has revolutionized the existing rules governing the digital services market. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act, or DSA) complements existing sector-specific regulations. According to the EU legislator, it does not affect the application of existing Union laws governing particular aspects of information society services, where these laws apply as lex specialis.

However, the DSA applies to service providers to the extent that no more specific provisions—such as those set out in the Audiovisual Media Services Directive or other EU acts like the Regulation on addressing the dissemination of terrorist content online—are in force. It also draws on the 2018 Commission Recommendation on illegal content online (C(2018) 1177 final) and the EU Internet Forum's work on terrorist content.

The DSA introduces several important provisions:

(a) mechanisms to counter illegal goods, services, and content online, including user reporting systems and, for platforms, cooperation with "trusted flaggers";

(b) new obligations regarding the traceability of business users on online marketplaces;

(c) effective safeguards for users, including the right to contest content moderation decisions;

(d) far-reaching transparency measures, particularly regarding recommendation algorithms;

(e) obligations for very large platforms to prevent the misuse of their systems, conduct risk assessments, and undergo independent audits;(f) requirements for major platforms to grant researchers access to key data for studying online risks;

(g) a supervisory structure reflecting the complexity of the online ecosystem—national authorities will play a leading role, supported by the new European Board for Digital Services, while the European Commission will exercise enhanced oversight over very large platforms.

The new rules primarily apply to intermediaries—digital service providers. The regulation emphasizes that platforms reaching more than 10% of Europeans (around 45 million users) are also subject to these obligations. Many of these duties are aimed specifically at combating illegal content online.

The DSA uses the term “illegal content” but does not define it exhaustively. According to Article 3(h), „illegal content” refers to any information that, by itself or by reference to an activity—including the sale of products or the provision of services—is not compliant with Union law or the law of any Member State that complies with Union law, regardless of the subject matter. This means the classification of content as illegal will depend on the value system adopted by the Member State concerned, except where harmonized definitions apply.

This new regulatory reality significantly alters the functioning of the digital services single market and will ultimately reshape the broader digital environment. That is why this report not only presents the latest data and trends related to online activity, but also explores compelling research findings about what users and experts consider illegal content and how they assess fundamental values—such as the balance between freedom and security. These questions lie at the heart of today’s most pressing issue: how the digital world is evolving.

We invite you to join the discussion!

PART I

The .pl Domain Name Market

Facts and Figures

almost **2.59 mln** million active names in the .pl domain

2.26 names per subscriber

over **767** thousand new names

over **2** thousand new registrations per day

189 .pl domain registry partners

over **1.8 mln** renewed names

over **1.1 mln** subscribers

64.42 % of subscribers are organizations

almost **485** thousand names secured with DNSSEC

35.58 % of subscribers are individuals

over **8** thousand new option registrations

almost **2** thousand renewed options

almost **151** thousand transfers

Copyright by NASK

Ranking of European Domain Registries

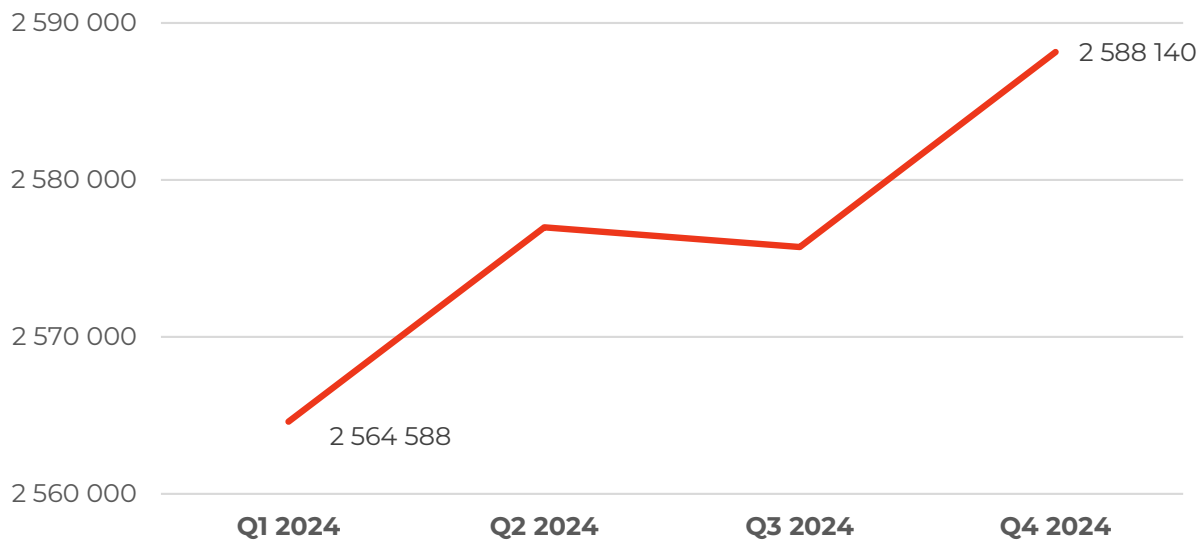
	.de	Germany	17 684 865
	.uk	United Kingdom	10 260 979
	.nl	Netherlands	6 175 615
	.fr	France	4 216 306
	.it	Italy	3 495 034
	.pl	Poland	2 588 140
	.es	Spain	2 094 791
	.be	Belgium	1 718 090
	.cz	Czech Republic	1 485 493
	.se	Sweden	1 456 166

Copyright by NASK

Domain Services

Number of .pl Domain Names Maintained

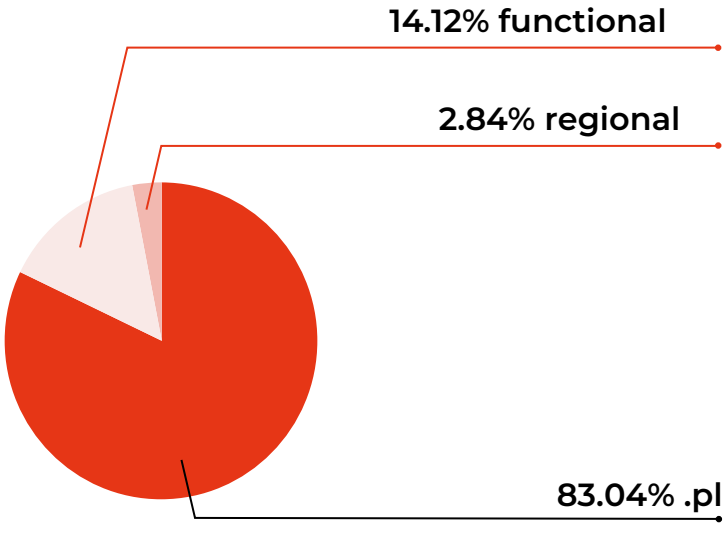
In 2024, the number of active .pl domain names in the DNS increased by **41 733**, representing an annual growth rate of **1.64%**.



Copyright by NASK

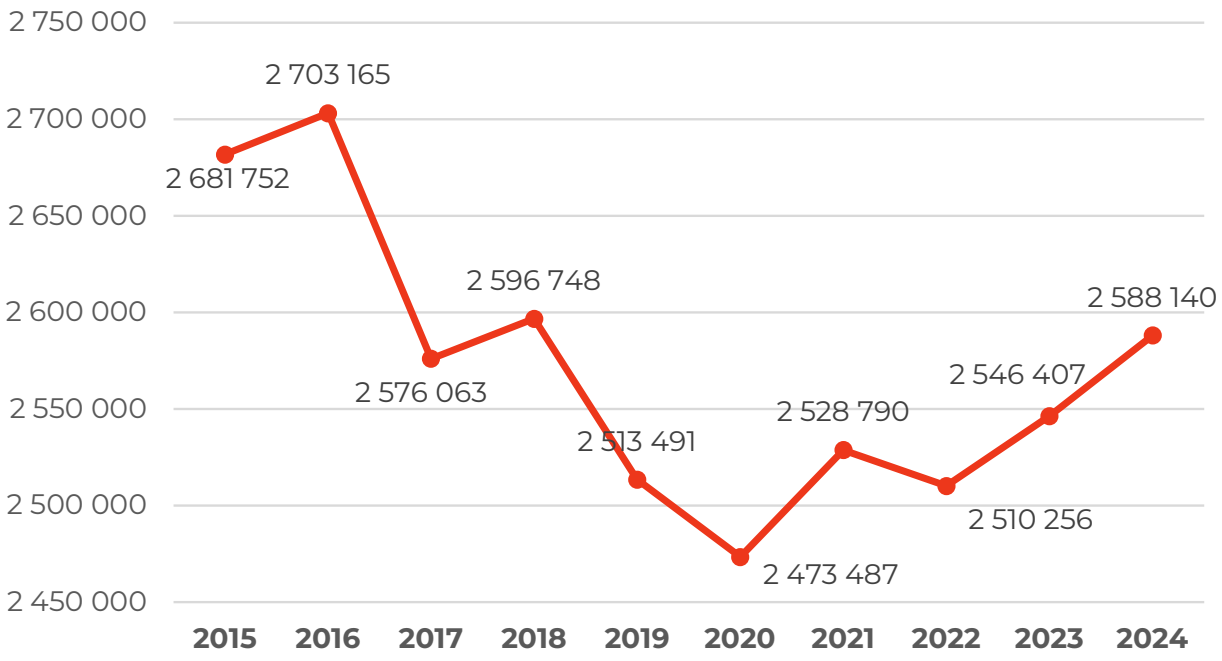
Active .pl Domain Names in the DNS by Zone Type

Names registered directly under the .pl domain, under functional domains (e.g., com.pl, net.pl, etc.), and under regional domains (e.g., waw.pl, slask.pl, etc.).



Copyright by NASK

Number of .pl Domain Names in the DNS, 2015–2024



Copyright by NASK

Number of .pl Domain Name Registrations

Year 2024

number of registrations
767 058

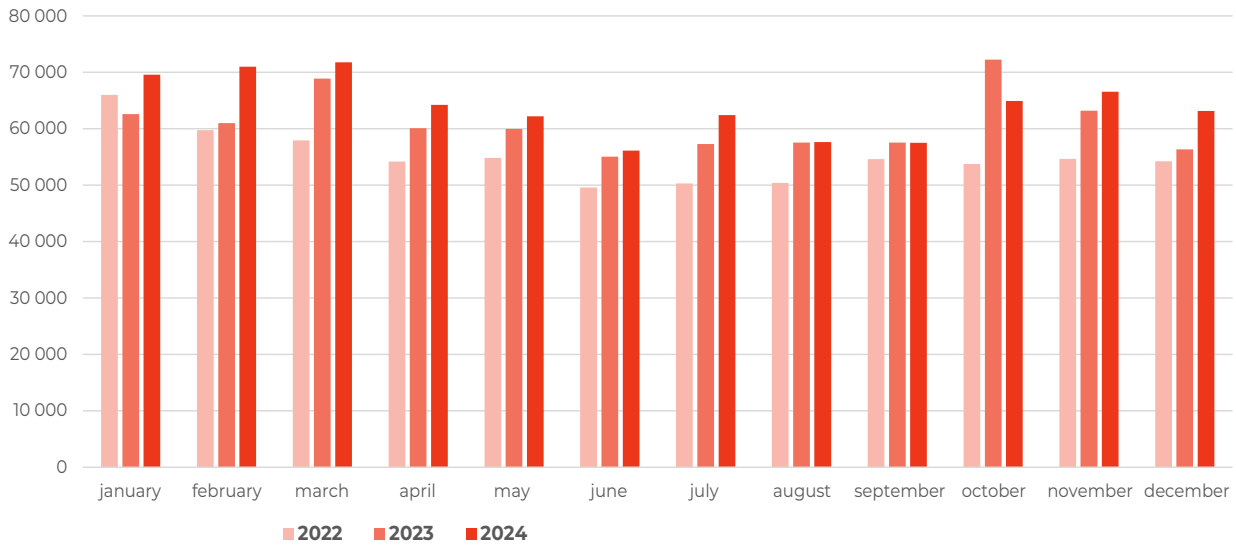
average daily number of name registrations
2 096

the most domains were registered in March
71 758

the fewest domains were registered in June
56 117

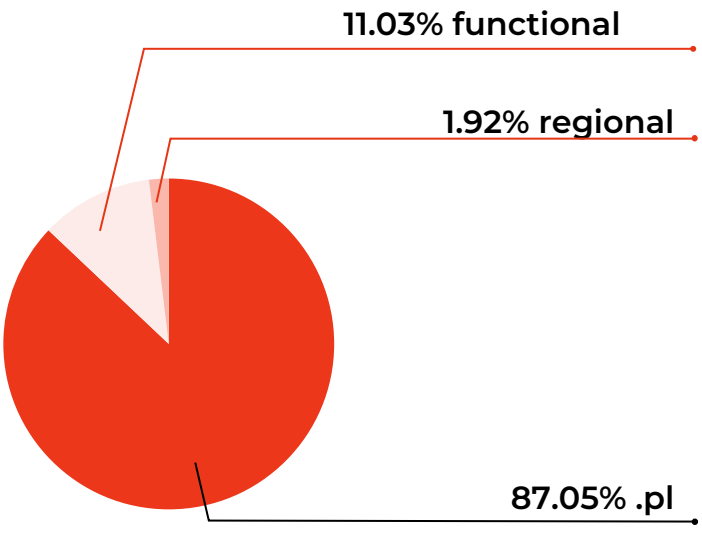
Copyright by NASK

Number of .pl Domain Name Registrations



Copyright by NASK

.pl Domain Name Registrations by Zone Type



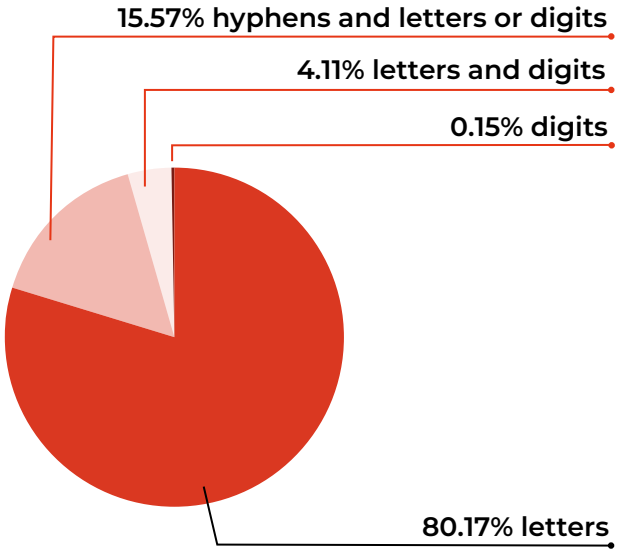
Breakdown of Domain Names Registered Directly under .pl, Functional Domains (e.g., com.pl, net.pl, etc.), and Regional Domains (e.g., waw.pl, slask.pl, etc.)

Copyright by NASK

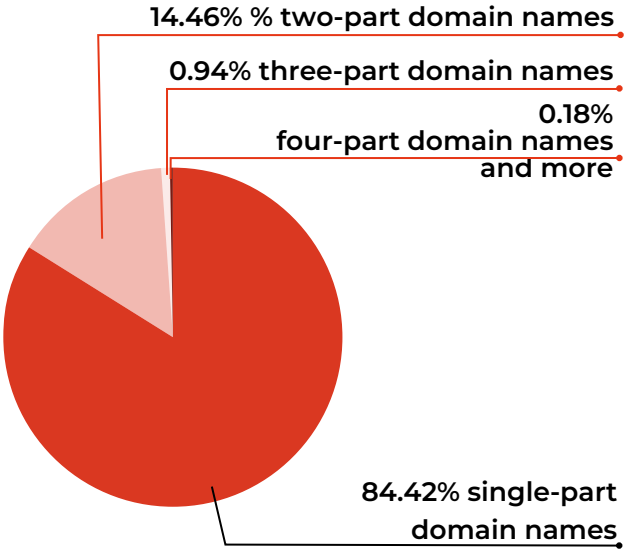
Structure of .pl Domain Names

At the end of 2024, the average number of characters used in .pl domain names was 10.94. A total of 9 .pl domain names reached the maximum length of 63 characters.

The most common were nine-character domain names, with 233 099 registered in the registry. The maximum number of segments (words) in a single domain name recorded at the end of 2024 was 11.

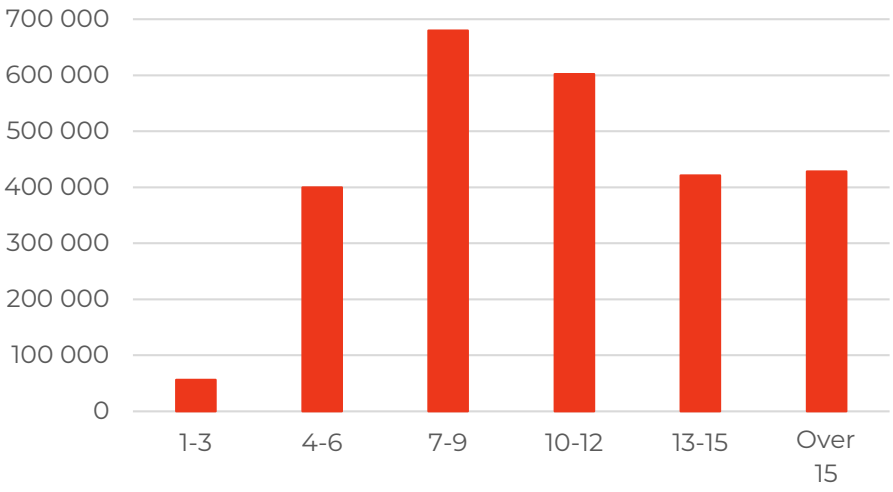


Characters in .pl Domain Names, 2024



Number of Segments in .pl Domain Names, 2024

Copyright by NASK

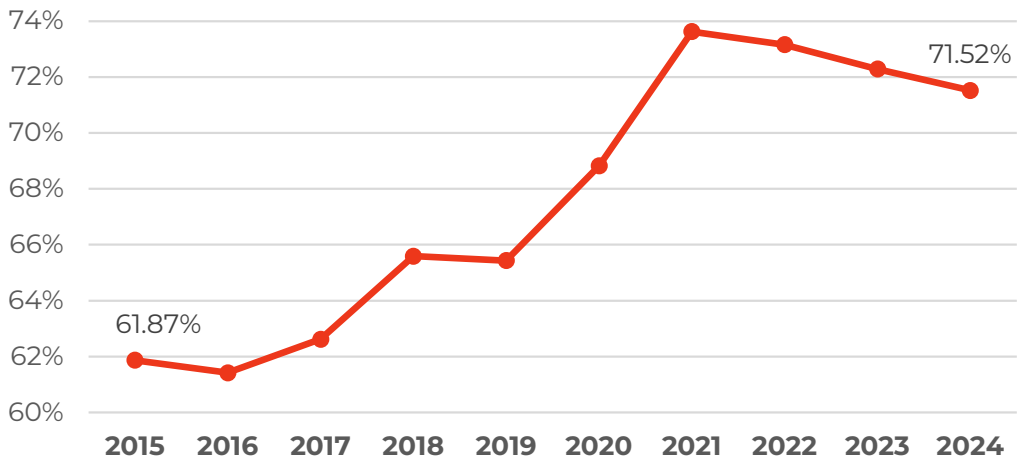


Number of Characters in .pl Domain Names, 2024

Copyright by NASK

Renewals of .pl Domain Names for the Next Billing Period

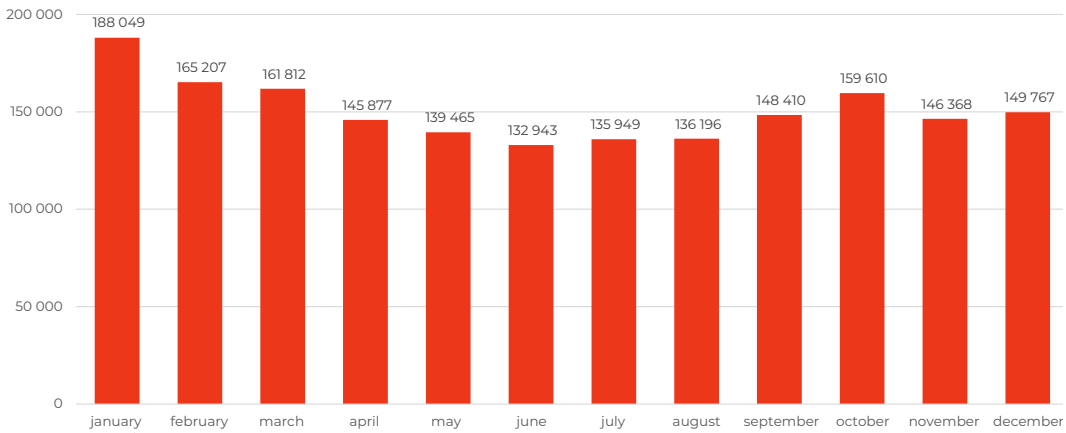
Years 2015–2024



Renewal Rate of .pl Domain Names, 2015–2024

Copyright by NASK

Year 2024

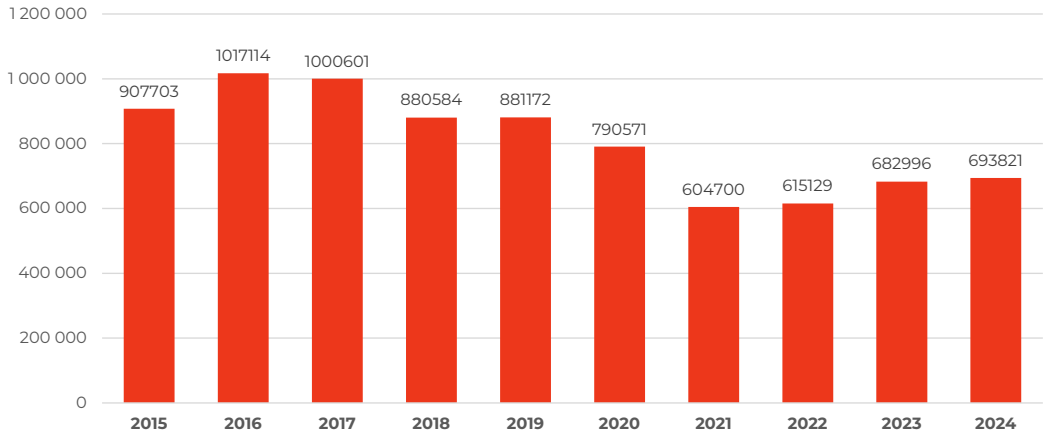


Number of Renewed .pl Domain Names, 2024

Copyright by NASK

Number of Non-Renewed .pl Domain Names

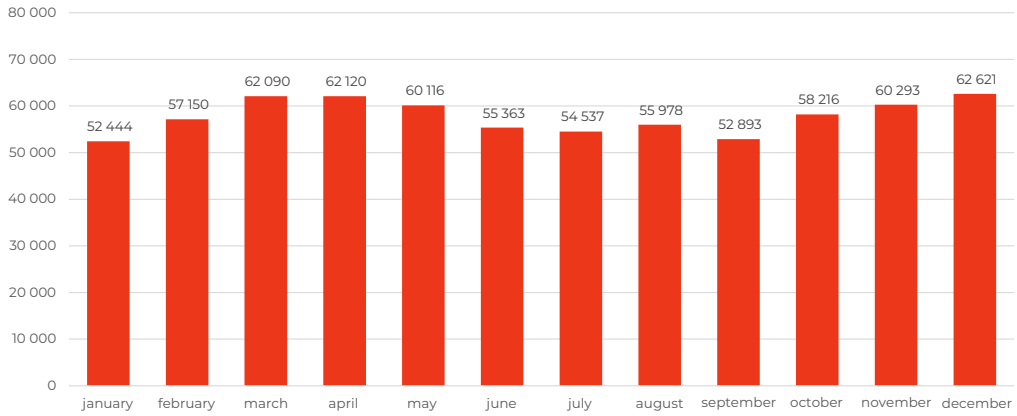
Years 2015–2024



Number of .pl Domain Names Released Due to Non-Renewal, 2015–2024

Copyright by NASK

Year 2024

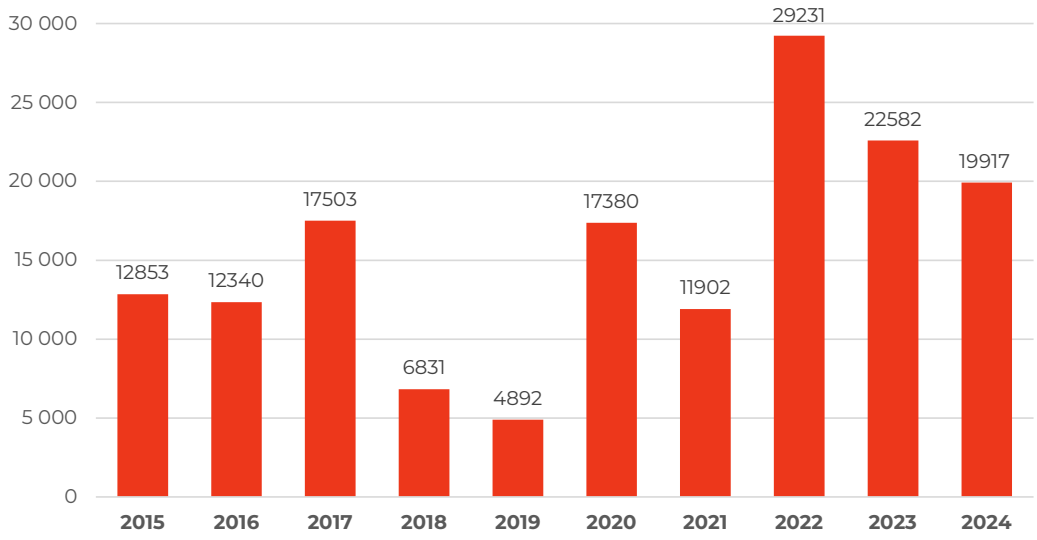


Number of .pl Domain Names Released Due to Non-Renewal, 2024

Copyright by NASK

Number of Deleted .pl Domain Names

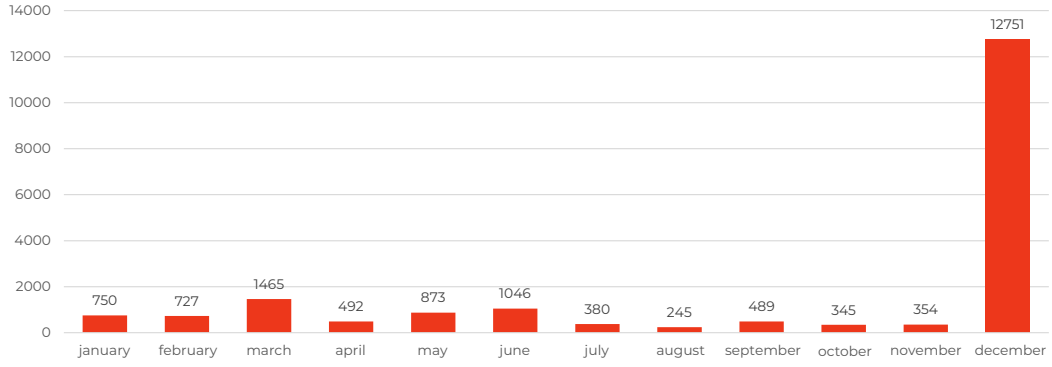
Years 2015–2024



Number of .pl Domain Names Released After Prior Deletion, 2015–2024

Copyright by NASK

Year 2024

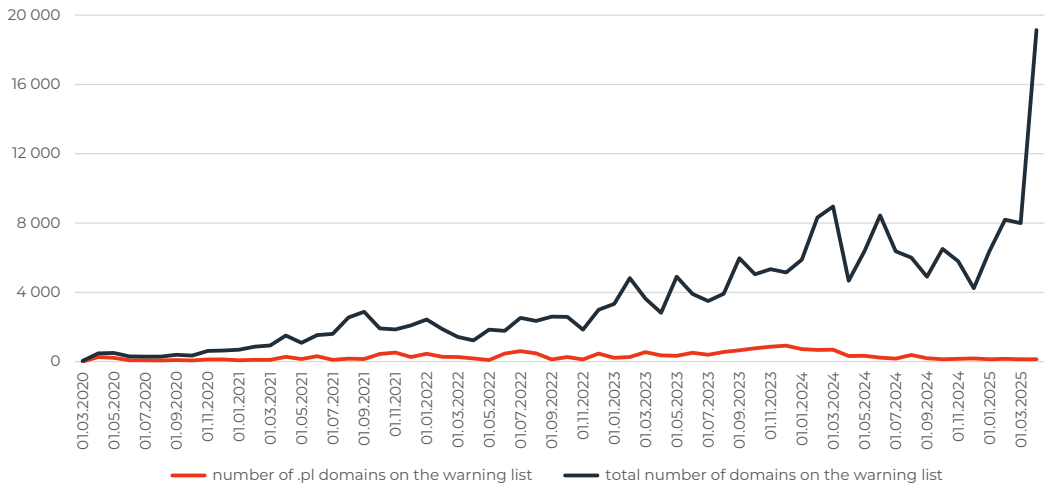


Number of .pl Domain Names Released After Prior Deletion, 2024

Copyright by NASK

Number of Domains Blocked by CERT Polska

Years 2020–2024



Number of Domains Blocked by CERT Polska, 2020–2024

Copyright by NASK

Year 2024

In 2024, .pl domains accounted for 5.51% of all domains on the warning list of dangerous websites. Compared to 2023, this represents a drop of more than half, due in part to the improvement of the domain blocking process within the .pl zone, introduced in February 2024.

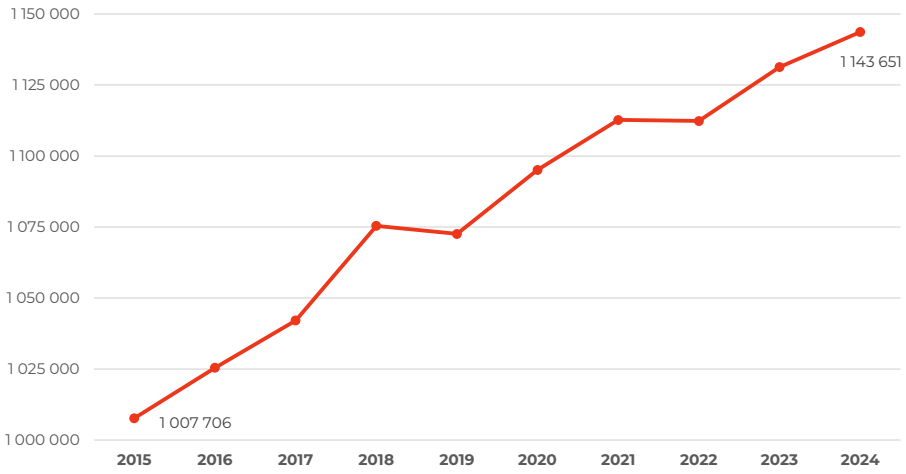
.com	35 312	.sbs	1 358
.xyz	4 724	.online	1 262
.pl	4 213	.info	1 165
.top	4 029	.lol	906
.shop	2 136	.pro	865
.site	1 977	.lat	677
.click	1 865	.pics	640
.cfd	1 666	.rest	549
.net	1 581	.eu	529
.org	1 503	.store	524

Top 20 registries whose domains were added to the CERT Polska warning list for dangerous websites, 2024

Copyright by NASK

Services for .pl Domain Name Registrants

Number of .pl Domain Name Registrants



Number of Registrants, 2015–2024

Copyright by NASK

12 319 Number of Registrants Who Joined in 2024

181 223 Number of .pl Domain Name Registrant Changes in 2024

2.26 Average Number of .pl Domain Names per Registrant

64.42% Registrants as Organizations

35.58% Registrants as Natural Persons

Copyright by NASK

Location of .pl Domain Name Registrants

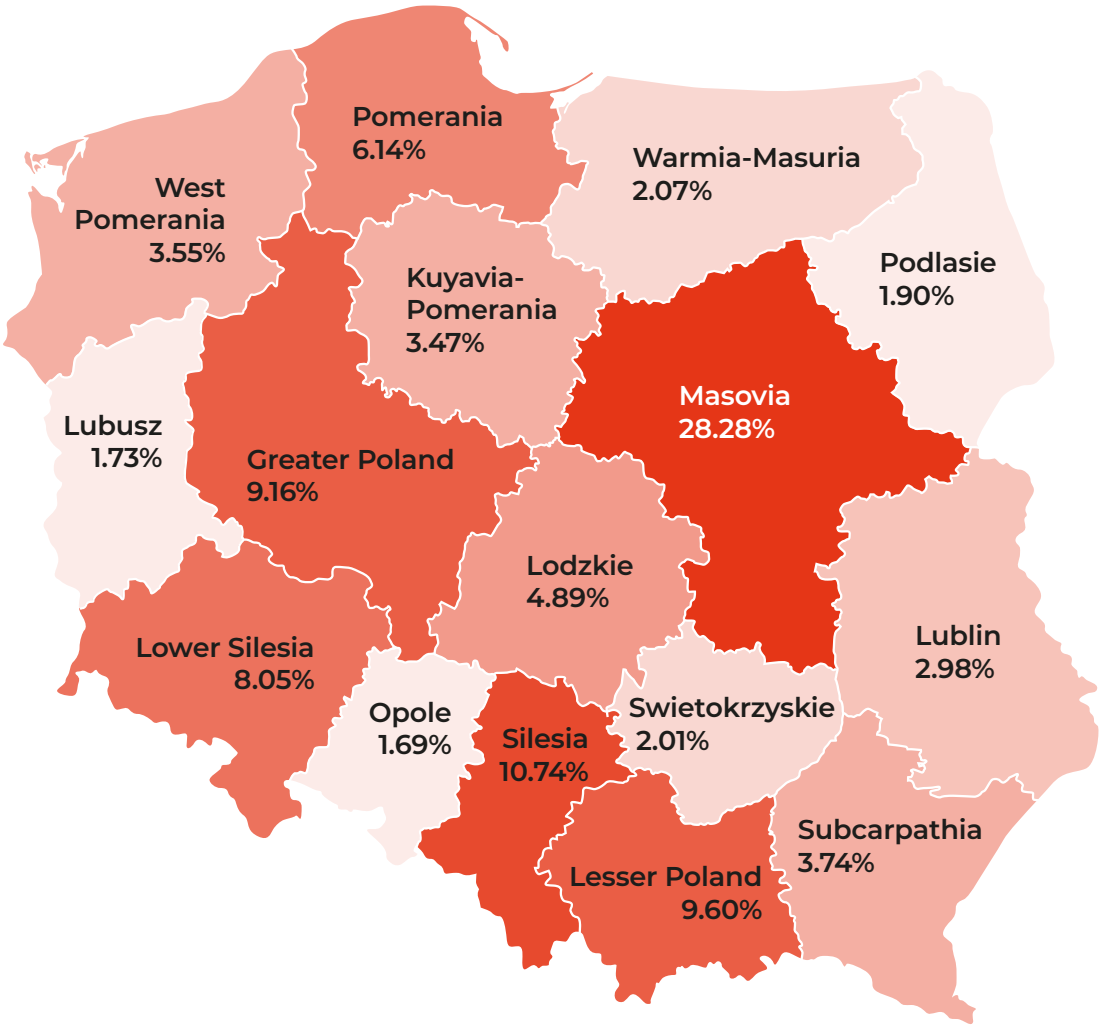
90.68% .pl Domain Names Present in the DNS at the End of 2024 Maintained for Polish Registrants

28.28% Domain names were registered to individuals and organizations from the Mazowieckie Voivodeship, with as many as 20.69% originating from Warsaw.

Nearly half of all registrants from Poland were users of domains from the following voivodeships:

28.28%	Masovia
10.74%	Silesia
9.60%	Lesser Poland

Copyright by NASK



Location of Registrants in Poland by Voivodeship, 2024

Copyright by NASK

Statements from .pl Domain Registry Partners

Aftermarket.pl Limited

From the unique perspective of a registrar closely involved in the secondary domain market, we can say that 2024 was a good year for the .pl domain. Compared to 2023, the number of new .pl domain registrations on our platform increased by 10%, while the number of renewals grew by 7%. This reflects the steadily growing interest of Poles in having an online presence. The .pl domain is their natural first choice when creating their own website address.

Undoubtedly, promotional campaigns by the .pl domain registry also contributed to the increase in registrations and renewals, encouraging registrars to explore new ways of promoting these domains. While some entities limited their marketing activities to simple price reductions, 2024 also brought several interesting and creative promotional efforts, which led to improved performance.

The secondary domain market also saw similar growth — the total value of domain sales on the Aftermarket.pl platform rose by 6% compared to the previous year. This shows increasing awareness that a good website address is a key element of an effective online marketing strategy, prompting end users to invest in valuable domain names.

Third-level .pl domains — both functional and regional — continue to decline in significance. Once attractive due to lower prices, their numbers have been steadily decreasing since registration costs were equalized with second-level domains. Their share in our platform's total registrations fell by as much as 15%, indicating that when offered domains at the same price, users clearly prefer second-level options.

IDN domains also remain marginal in the overall number of registrations. The idea of registering domains with Polish characters still hasn't reached the awareness of the average internet user. Many people are unaware that such domains exist or that they must be registered or purchased separately, effectively doubling the cost.

A continuing challenge is increasing interest in Polish domains among foreign entities. Although the .pl extension is one of the most popular in Europe, it is still registered almost exclusively by residents of Poland. The share of foreign entities in .pl domain registrations is low — even lower in the case of purchases on the secondary market. It seems the Polish market remains too unfamiliar or "exotic" for international buyers.

OVH SAS

The Polish domain market is developing dynamically, with users increasingly opting for solutions that offer not only competitive pricing but also a high level of security, management automation, and top-tier technical support. OVHcloud meets these needs by offering comprehensive domain registration and management services, including DNSSEC security, which protects against cryptographic cyberattacks such as “man-in-the-middle” attacks and DNS data tampering.

We are also pleased that the use of local, European providers contributes to the development of the domestic market. There is growing demand for stable services, especially those powered by artificial intelligence, which translates into increased use of cloud resources — such as our public cloud and ready-made solutions that support AI implementation in companies and organizations, including training LLM models.

As one of NASK’s key partners, we continue to be the largest operator with a broad portfolio that includes a wide range of artificial intelligence, cloud, hosting, and domain registration services, meeting the expectations of both small businesses and large enterprises — comments Robert Paszkiewicz, VP, Central and Eastern Europe, OVHcloud.

Home.pl S.A.

The beginning of 2025, which marks two important anniversaries in domain history — the 40th anniversary of the registration of the first .com domain and the 35th anniversary of the creation of the .pl domain — is a fitting moment to assess the market.

Starting with the .pl domain, it is clear that 2024 was another successful year, further strengthening its decades-long position as the preferred domain among Polish registrants. This is also reflected in the .pl renewal market, which, year after year — and 2024 was no exception — continues to mature and stabilize. The high renewal rate confirms that choosing a .pl domain is usually a long-term investment, with registrants valuing its reliability.

Market analysis also shows that business clients are increasingly aware of the importance of having their own website to showcase their services and products online. Despite the rapid development and expansion of social media, owning an independent website remains a priority. Notably, we are also seeing greater customer awareness in terms of security. This is evident in the growing trend of purchasing complementary services — particularly those enhancing security, such as SSL certificates — along with domain registrations. We observe this trend with great satisfaction, as at home.pl we dedicate significant effort to educating our clients on cybersecurity.

The aforementioned interest among clients in having their own website is naturally connected to the domain name. In this regard, an important challenge we observe is that most “catchy” and “simple” names are already taken. In such cases, there are at least two possible solutions: purchasing a domain from the secondary market or using modern tools, such as AI-powered search engines, which help clients find the ideal — sometimes unexpected — domain name. Both of these services are part of the home.pl portfolio.

After a successful 2024, we look to the future with optimism, believing that the .pl domain will remain the first choice for Poles — both for personal and commercial use.

nazwa.pl sp. z o.o.

The year 2024 confirmed a clear trend in the domain market: today, the real use of internet addresses matters more than acquiring them for investment purposes. Companies increasingly treat domains as a key element of their business strategy, particularly in the growing e-commerce sector. In this process, **nazwa.pl** plays a vital role by providing modern cloud services and supporting businesses in establishing their online presence.

As part of the NetArt Group, we observe the domain market both locally and globally. In Poland, the .pl extension consistently remains the primary choice for companies and private users. Its stability, prestige, and recognition make it a popular option among entrepreneurs. At the same time, we’re witnessing a global rise in the importance of **nTLDs (new gTLDs)**, which are gaining traction especially among startups and the creative industries. While traditional extensions like .com continue to dominate, more and more companies are recognizing the potential of new domain types tailored to specific business profiles.

Recent years have seen a significant increase in the number of companies operating websites and online stores based on advanced cloud services. Businesses are consciously choosing domains that are actively used in operations rather than being parked or held for resale. This reflects a modern approach to building an online presence—where not just the registration of a domain matters, but its practical application in day-to-day business activities.

Awareness of online threats continues to grow each day. Companies are eager to protect their brands by registering multiple domain variants and investing in technologies such as **DNSSEC**. Business clients are actively seeking protection against phishing attacks and domain hijacking, placing strong emphasis on digital security. At **nazwa.pl**, we actively support these efforts by delivering comprehensive solutions that help companies operate online both effectively and securely.

cyber_Folks S.A.

cyber_Folks™

Poland maintains a strong position in the European country-code domain market, ranking 6th in terms of the number of registered domains with the .pl extension — around 2.6 million. This places Poland consistently among the top ten European countries and confirms its leadership in the Central and Eastern European region.

Analyzing the number of domains per company — which in Poland stands at approximately 1.04 domains per company — reveals a moderate level of business activity online. For comparison, the average in Germany is 5.4 domains per company, and in the Netherlands, 3.3, indicating considerable growth potential in Poland, particularly among SMEs. On the other hand, Poland scores higher than France (0.66), suggesting ongoing digitalization of domestic businesses.

In 2024, the number of registered .pl domains increased by 2.3% year-on-year. While the growth rate was not the highest in Europe, this steady rise confirms user trust in the .pl domain as a fundamental online presence tool. It remains the most frequently chosen extension on the Polish market, further strengthened by a high renewal rate and improving service quality.

This past year also saw growing interest in domains tailored to e-commerce. The rapid expansion of online trade has led businesses to seek addresses that are not only memorable but also SEO-optimized. This trend aligns perfectly with treating the domain name as an integral part of brand identity. Entrepreneurs increasingly choose names that reflect their business and communicate its values.

Greater interest in domain names also corresponds with rising awareness of the need for protection. According to research by cyberFolks, 16% of entities registered domains for brand protection purposes. As domain names grow in value, more companies are securing themselves against cybersquatting and dishonest practices. Business owners are registering various versions of their domains across different extensions to prevent domain hijacking. The rise in phishing attacks and fraudulent websites impersonating well-known brands only underscores the importance of domain protection as part of a company's broader strategy. Increasingly, businesses view their domain names as equal in importance to their brand name, logo, or visual identity.

In summary, Poland remains a significant player in the European domain market, with a strong regional position and stable growth. At the same time, there is still substantial development potential — especially in activating small and medium-sized enterprises and leveraging the opportunities offered by diversified domain extensions.

DD sp. z o.o.

Last year, nearly 700,000 .pl domains were not renewed for another term. Our statistics show that approximately 20% of those domains were re-registered shortly after being deleted. These may include valuable names due to their history, search engine ranking, or usefulness in SEO. Others may simply have appealing names that were previously unavailable but found new use after deletion.

Our platform is one of the few in Poland that supports the so-called secondary domain market. We capture domains on behalf of our clients — registering names immediately after they are removed from the registry. Our clients primarily include small and medium-sized enterprises, SEO agencies, and IT professionals.

In 2024, our service recorded a 60% increase in domain registrations compared to 2023. The first months of the current year confirm this trend. We are seeing growing interest in specialized services such as domain catching and the management of large domain portfolios. We provide tools that enable easy administration and maintenance of hundreds or even thousands of domains within a single portfolio. Our professional yet individualized approach allows us to adapt to the specific needs of each client.

In 2025, we will continue to actively participate in the .pl Domain Registry (NASK) programs aimed at promoting and developing the .pl domain market. The .pl extension remains the undisputed leader and the primary choice for entities doing business in Poland.

LH Sp. z o.o.

We consider 2024 to be a very successful year at LH.PL. We increased the number of newly registered domains, with the .pl domain still accounting for the vast majority of registrations. We continue to observe growing interest from companies in building their online visibility, which has also positively impacted our other product offerings. We remain committed to our strategy, where customer service quality, security, and the stability of digital services are our top priorities. In 2024, we successfully passed audits of our ISO 9001 and 27001 systems, confirming both quality and a high level of security.

As in the previous year, our security department noted an increased number of cyberattacks — for example, phishing. An increasing number of domains, including .pl domains, are being registered specifically for phishing attempts. We have improved our solutions to minimize the risks associated with this trend.

The year 2024 was marked by a focus on security. Like other registrars and hosting providers, we are closely following developments related to the National Cybersecurity System and preparing for the implementation of **NIS2**.

Despite the challenges, we are definitely satisfied with the results LH.PL achieved in 2024. We are ready for further growth and future challenges in pursuit of our mission to ensure uninterrupted online operations for our clients.

DOMENY.TV MSERWIS Sp. z o.o.

The year 2024 was a period of stabilization for us. We did not observe a significant increase in Polish domain registrations. However, we did record a 4.77% increase in renewals. This clearly indicates growing user loyalty to their existing Polish domain names and a willingness to maintain them long-term. We continuously monitor these changes and adapt our services to provide the best possible support to our clients in managing their online addresses.

The .pl domain remains the undisputed leader — it accounts for as much as 67.4% more registrations with us than all other domain extensions combined. At the same time, we offer the largest number of domain extensions available for registration in Poland — currently as many as 1114 different extensions.

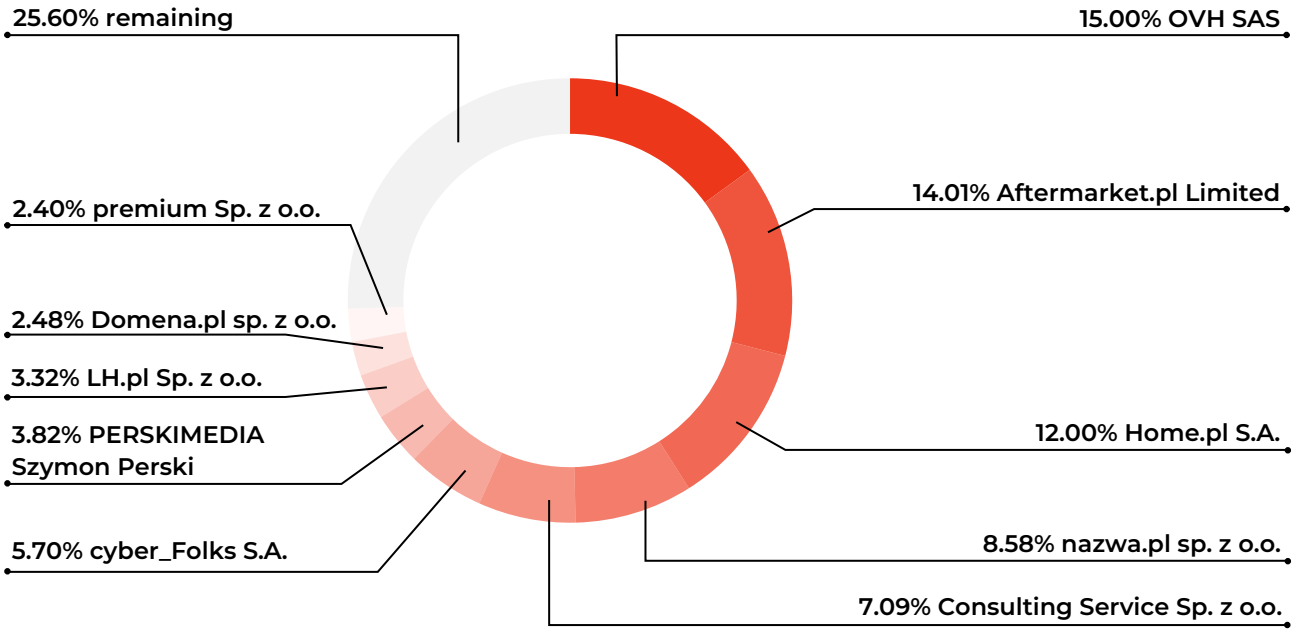
In 2024, to meet client needs in the area of creative naming, we expanded our naming e-book, which offers guidance on how to create attractive and effective domain names.

We are also seeing increasing interest in security-related topics, including DNSSEC and maximum protection for both domain names and admin panels. In response, we continue to promote two-factor authentication (2FA) and other tools and mechanisms that help our clients maintain full control and security over their domain assets.

All of these initiatives and improvements allow us to continuously raise the quality of our services and respond to the changing needs of the market. We value the trust of our clients and support them in every aspect of domain management.

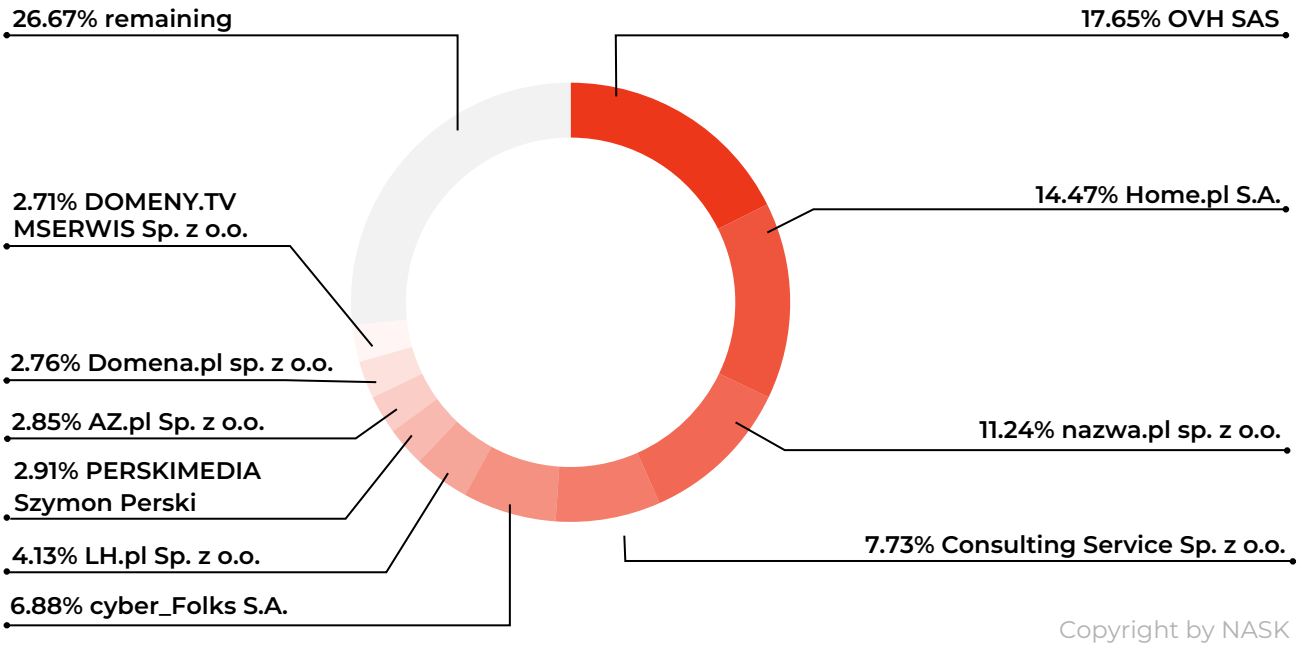
Structure of the .pl Domain Name Market

Percentage Share of Partners in .pl Domain Name Management, 2024



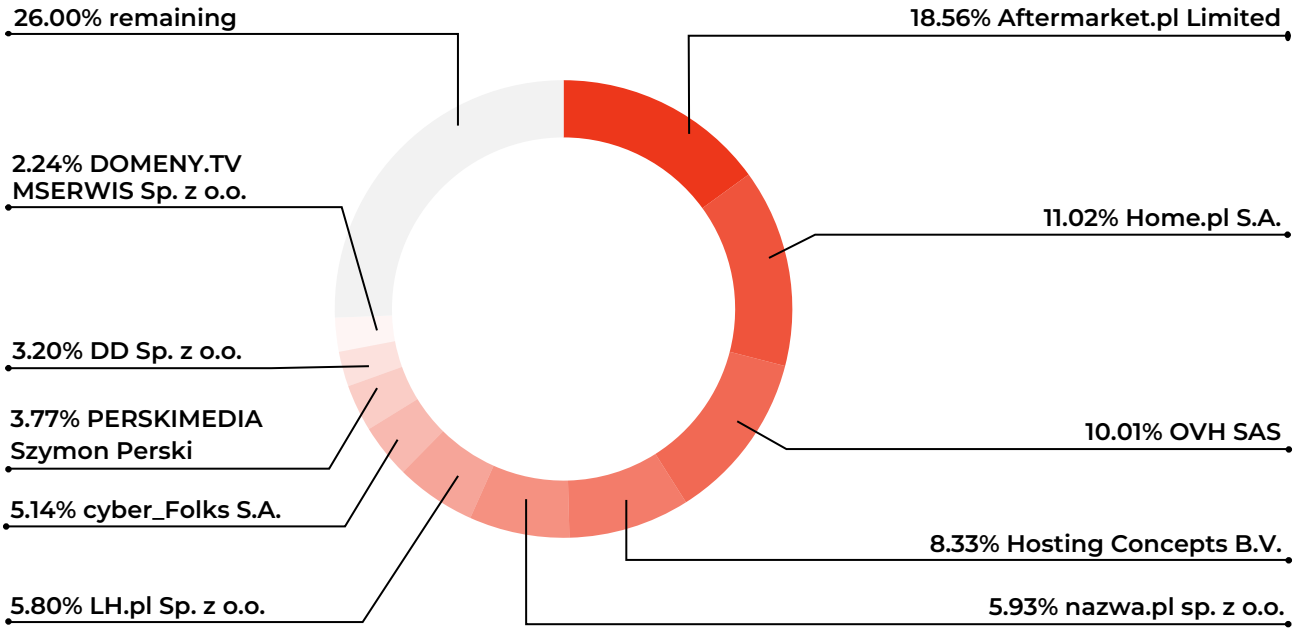
Copyright by NASK

Percentage Share of Partners in .pl Domain Name Registrant Services, 2024



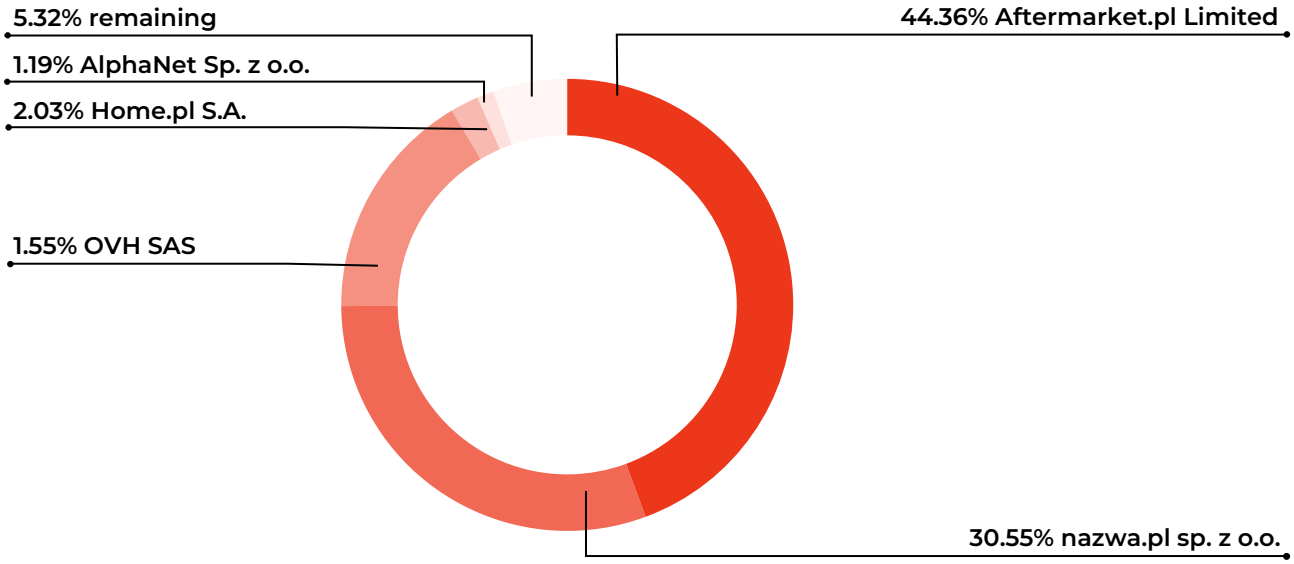
Copyright by NASK

Percentage Share of Partners in .pl Domain Name Registrations, 2024



Copyright by NASK

Share of Partners in Managing .pl Domain Names Secured with DNSSEC, 2024



Copyright by NASK

PART II

Report on the Study of Illegal Content on the Internet

Information about the study

In this year's report of the .pl domain registry, we present a study conducted in collaboration with the Kozminski University and the National Chamber of Electronics and Telecommunications (KIGEiT), dedicated to illegal content on the Internet.

This time, we asked two groups of respondents for their opinions. The first group consisted of a representative sample of Polish citizens. The aim of the study was to assess their knowledge of illegal content on the Internet, their personal experiences with such content, and to verify their understanding of the law, the effectiveness of reporting illegal content, and the protection of digital identity. The results of this nationwide survey will be used to develop recommendations for public institutions and non-governmental organizations, which may help improve education and enhance the protection of Internet users in Poland.

The second group of respondents consisted of 16 registrars—business partners cooperating with NASK-PIB as part of the NASK Partnership Program. The selection of representatives from this sector was deliberate due to the expert nature of the study. Their insights on illegal content on the Internet further enriched this report. The conclusions gathered from the registrars provided an industry perspective, allowing for a better understanding of the challenges faced by the domain registration sector and supporting the development of more effective public policy recommendations in the areas of cybersecurity and user protection on the Internet.

RESEARCH SAMPLE

- A representative sample of Polish women and men aged 18 and above (by gender, age, voivodeship, size of place of residence, and education level). Sample size: N=1083
- A group of 16 experts – business partners cooperating with NASK-PIB as part of the Partnership Program

RESEARCH PERIOD

- November – December 2024

RESEARCH METHODOLOGY

- Online survey (CAWI) conducted with a representative sample of Polish citizens and NASK-PIB business partners
- The study was carried out using the ReaktorOpinii.pl research panel, owned by the Accorp Sp. z o.o. group

Research Questions

1. In your opinion, what types of online content are illegal?
2. How often do you encounter the following types of content on the Internet?
3. Have you ever come across content on the Internet that you consider illegal?
4. Where on the Internet do you most often encounter illegal content?
5. In your opinion, who can be notified when illegal content is found online?
6. What actions do you take when you come across illegal content on the Internet?
7. Do you believe that reporting illegal content can lead to its removal?
8. Do you think that the presence of illegal content on the Internet has a negative impact on society?
9. In what way, in your opinion, does the presence of illegal content on the Internet negatively affect society?
10. Do you believe that new technologies (such as artificial intelligence) support the detection of illegal content online?
11. Do you believe that new technologies (such as artificial intelligence) support the removal of illegal content online?
12. In your opinion, do social media platforms (e.g., Facebook, Instagram) effectively remove illegal content?
13. In your opinion, which is more effective in combating illegal content on the Internet — removing the illegal content or blocking the account of its author?

14. Are you concerned about freedom of speech in relation to the automatic removal of content suspected of being illegal?

15. Do you believe that certain harmful content (e.g., controversial political, religious, or philosophical opinions, or controversial works of art intended to draw attention to an important social issue) should be legal if they comply with freedom of speech principles?

16. Are you concerned that your digital identity (i.e., information representing you online) could be compromised?

17. What type of online aggression do you think is the most common?

18. In the past 12 months, have you been subjected to online aggression—for example, someone posting something negative or offensive about you online?

19. Where on the Internet were you exposed to aggression?

20. In the past 12 months, have you witnessed someone else becoming a victim of online aggression—such as someone posting something negative or offensive about another person?

21. Where on the Internet did you notice someone else becoming a victim of aggression or violations online?

22. Do you refrain from expressing your opinion online for fear of becoming a victim of digital aggression?

23. In your opinion, is it easy to find information about what constitutes illegal content on the Internet?

24. In your opinion, is it easy to find information about the legal regulations regarding illegal content on the Internet?

25. How do you assess the effectiveness of legal regulations in combating illegal content on the Internet?

Key Findings from the Study:

1. Polish people generally recognize illegal content well; however, some areas like disinformation and discrimination are less frequently associated with legal violations.

2. Social media is the main place where people encounter illegal content, but many Poles do not know where to report it.

3. Despite awareness of the risks, nearly half of Poles take no action against illegal content.

4. New technologies, including AI, are seen as potentially helpful, but many people have no opinion on their role.

5. Over half of Poles believe that controversial content should be legal if it falls within the boundaries of freedom of speech.

6. Fear of online aggression limits freedom of expression, negatively affecting public debate on the Internet.

7. Poles are skeptical about the effectiveness of laws and social media platforms in combating illegal content.

8. Hate speech and ridicule are the most common forms of online aggression.

9. Fear of aggression reduces online activity—many avoid commenting or expressing opinions.

10. Poles show high awareness of threats, especially concerning the protection of children, personal data, and terrorist content.

11. Older and better-educated individuals more often identify a wider range of illegal content types, which may indicate greater legal knowledge and experience in risk assessment.

Illegal Content on the Internet

Research Findings in Numbers

Gender

WOMEN:

- More often perceive the negative impact of illegal content on society (92%).
- More often avoid expressing their opinions online (30%).
- Believe that both methods (removing illegal content or blocking the author's account) are equally effective (49%).
- Most frequently choose social media and website administrators as the place to report illegal content (56%).
- In their opinion, the second most common form of online aggression is mocking others (64%).
- More often recognize cyberbullying (harassment, humiliation, intimidation) than other forms of aggression (51%).

MEN:

- More often encounter illegal content on the Internet (47%).
- More often have personally experienced aggression online (13%).
- Frequently do not respond to illegal content online (53%).
- Are more convinced of the effectiveness of new technologies in combating illegal content on the Internet (51%).
- Believe that blocking the author's account is a more effective method of combating illegal content (39%).
- More often express concerns about the automatic removal of suspicious content (40%).
- Believe that controversial content should remain legal if it aligns with the principles of freedom of speech (57%).
- Consider it easy to find information about illegal content on the Internet (49%).

Age

- Young people aged 18–29 most frequently encountered illegal content online (61%).
- People aged 18–39 most often express concerns about the automatic removal of suspicious content (43%).
- Individuals aged 18–29 most often face online discrimination based on race, religion, or sexuality (56%).
- Primarily young people aged 18–29 have witnessed aggression on the Internet (60%).
- People aged 18–29 (58%) and 30–39 (57%) believe it is easy to find information about illegal content online.
- • People aged 18–29 (56%) and 40–49 (56%) believe that finding information about laws related to illegal online content is easy.
- People aged 30–39 are particularly exposed to illegal content through streaming platforms (43%).
- People aged 40–49 identified messaging apps as the main source of illegal content (35%).
- Individuals aged 40–49 most frequently notice conflict provocation and the spread of disinformation (cybertrolling) (57%).
- People aged 50–59 strongly believe in reporting illegal content to institutions that can facilitate its removal (80%).
- People over the age of 70 believe that blocking the author's account is a more effective way to combat illegal content online (44%).

Education

People with higher education:

- More often encounter illegal content on the Internet (47%).
- Are more frequently exposed to illegal content through streaming platforms (41%).
- Most often choose social media and website administrators as the place to report illegal content (59%).
- More often perceive the negative impact of illegal content on society (94%).
- Are more frequently convinced of the effectiveness of new technologies in combating illegal content online (51%).
- Most often believe that both methods (removing illegal content or blocking the author's account) are equally effective (52%).
- Believe that controversial content should remain legal if it complies with the principles of freedom of speech (59%).
- Most frequently express concerns about digital identity violations (67%).
- Have most often witnessed aggression online (49%).
- Believe that the most common form of online aggression is hate speech (75%).
- Most frequently notice conflict provocation and the spread of disinformation (cybertrolling) online (57%).
- Often avoid expressing their opinions online (32%).

People with secondary or lower education:

- More often have personally encountered aggression online (13%).
- Believe that exposure to illegal content does not negatively affect society (6%).
- Are less likely to express concerns about digital identity violations online.
- People with secondary and lower education have less often witnessed aggression online.
- Individuals with less than secondary education consider the current legal regulations for combating illegal content on the Internet to be effective (24%).

PhD, habil. Monika Dorota Adamczyk
prof. KUL
Professor at KUL –
Department of Human Rights and Social Work
Institute of Sociological Sciences
Faculty of Social Sciences
John Paul II Catholic University of Lublin

EXPERT COMMENT

Analyzing the results of the report „Poles Regarding Illegal Content on the Internet," it is impossible to overlook the broader social context in which we operate — the context of Society 5.0. This is a concept of a highly digitized reality where digital technology — from the Internet, through artificial intelligence, to the Internet of Things — permeates all spheres of life, from work to social relationships, education, and leisure. In such an environment, not only does access to content (both legal and illegal) become widespread, but it also becomes impossible to fully disconnect from the digital world. The Internet is no longer an alternative space — it is an integral part of our daily lives, shaping the identities of individuals and communities.

The presence of this digital dimension is felt most strongly by representatives of Generations Y (Millennials), Z, and Alpha — generations „immersed in screens." The report's data clearly show that people aged 18–29 are the most exposed to illegal content — as many as 61% of them have encountered it on the Internet. Moreover, this group most frequently experiences discrimination based on race, religion, or sexuality (56%), as well as aggression (60%). This not only testifies to the digital activity of this group but also highlights their particular vulnerability to symbolic violence and the instability of social norms in the online space

Generation X (currently people aged 40–59) is also increasingly recognizing the dark side of the digital world. This age group most often notices phenomena such as trolling (57%) and the spread of disinformation, with people aged 40–49 identifying messaging apps as the main source of illegal content (35%). This points to the need to increase vigilance and media education also among generations that entered the digital world later than their younger peers.

In the case of the oldest age groups (60+, especially 70+), there is a prevailing belief that effective measures should be repressive in nature — for example, blocking the accounts of authors of illegal content (44%). This perspective aligns closely with the concept of social control, typical of the Baby Boomer generation, which was raised in entirely different communication conditions and now faces the challenge of adapting to a world whose rules are often unclear and constantly changing.

Differences in the perception of and reactions to illegal content are also noticeable at the level of education. People with higher education demonstrate greater awareness of the risks and more often

recognize a negative impact of this content on society (94%) and more frequently report it to administrators (59%). Importantly, they are also more convinced of the effectiveness of new technologies in combating illegal content (51%), although at the same time they fear violations of their digital identity (67%) and often refrain from expressing their opinions online (32%). Here, we are dealing with a paradoxical phenomenon of digital ambivalence — technology provides a sense of security but simultaneously causes anxiety.

Particularly interesting are the gender differences. Women show greater sensitivity to symbolic violence — they more often notice cyberbullying (51%) and mocking (64%), and they also more frequently avoid expressing themselves online (30%). Men, on the other hand, are more convinced of the effectiveness of technology, but simultaneously more often ignore illegal content (53%), which may indicate attitudes of indifference or normalization of aggression in the digital space.

In Society 5.0, where the boundaries between what is "real" and what is "virtual" become fluid, illegal content on the Internet ceases to be merely a "technical problem." It becomes a social, cultural, and ethical challenge that requires multi-level actions — from digital education and legal regulations to the development of empathy and responsibility online. Escaping the Internet is not possible — only the development of mature digital competencies will allow for conscious and responsible use of its resources.

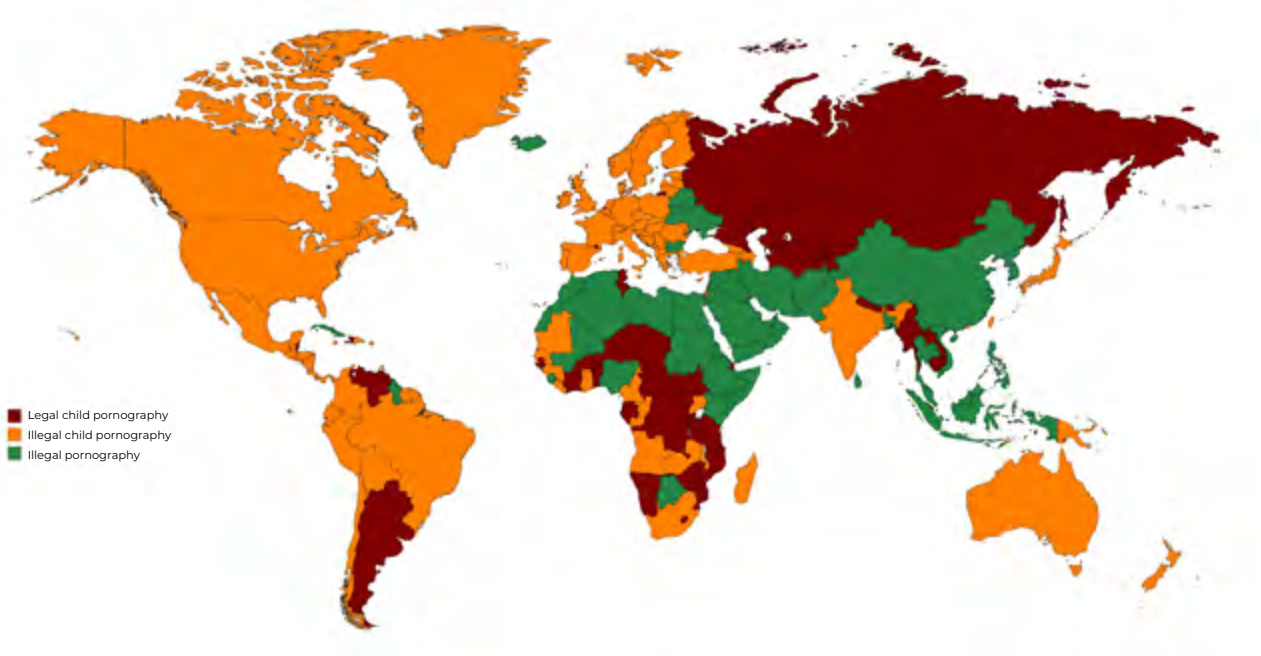
Personal experiences with illegal content

Does growing awareness of the existence of illegal content on the Internet make us feel safer online?

What types of content on the Internet do you consider illegal?
Sample size: N=1083

Most commonly identified illegal content

At the top of the list is child pornography (93%). It is widely accepted across Europe, both socially and legally, that child pornography is illegal content. However, as shown in the chart below, such content is not universally recognized as illegal worldwide. There are also very high indications for violations of personal data (85%) and terrorist content (84%).



Legality of child pornography worldwide, Source: TECHPEDIA, https://www.techpedia.pl/index.php?str=tp&no=32622

Legal and Ethical Issues

A significant proportion of respondents (80%) recognize intellectual property infringement as illegal content. This reflects a growing awareness of copyright protection; however, there may still be differences in interpreting exactly what constitutes illegal content.

Content Related to Hate Speech and Discrimination

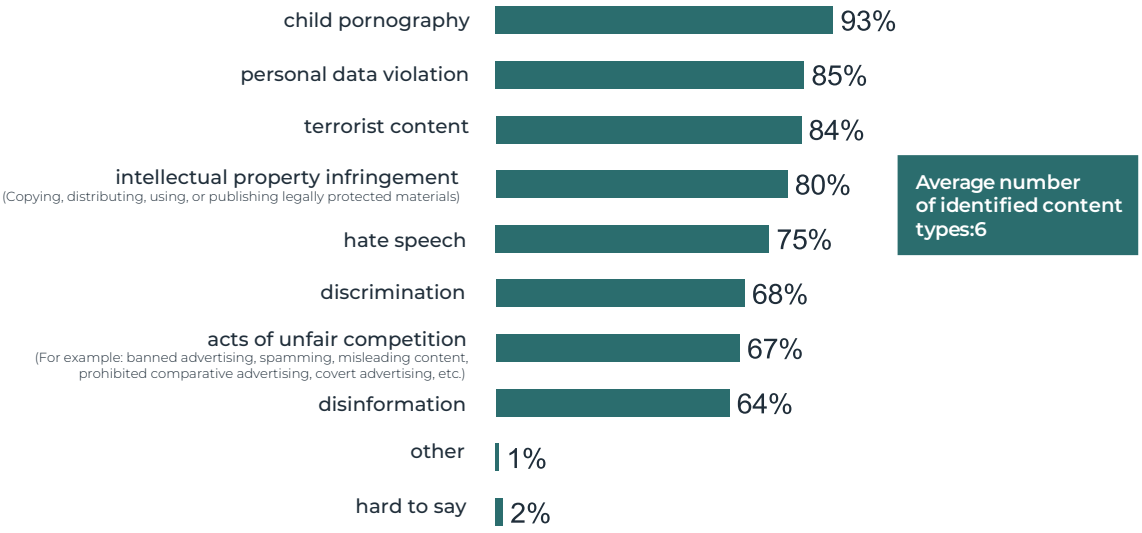
Hate speech (75%) and discrimination (68%) are often considered illegal; however, the slightly lower response rates compared to other categories may result from varying legal regulations and personal interpretations of freedom of speech.

Disinformation and Unfair Competition

Disinformation was identified by 64% of respondents, suggesting that society increasingly perceives it as a threat, although it is not always clearly associated with illegality. It is worth noting that, according to last year's report by the Digital Poland Foundation, "Disinformation Through the Eyes of Poles," there remains a high level of disinformation in Poland — 91% of Poles strongly agreed with at least one of the false statements surveyed (Digital Poland Foundation, Disinformation Through the Eyes of Poles, 2024 Edition). Unfair competition acts (67%) also ranked high, which may be due to growing consumer awareness and issues related to false advertising and covert advertising.

Interestingly, the experts we surveyed indicated a different hierarchy. As in the nationwide study, child pornography ranked first, but second place was taken by acts of unfair competition. These were followed by: intellectual property infringement, terrorist content, disinformation, and only in sixth place — personal data violations. These differences are most likely due to the specific nature of the industries in which the experts operate.

Illegal Content According to Respondents



The study showed that Poles have a high awareness of illegal content on the Internet, although their assessments vary depending on the category. The most frequently identified illegal content includes child pornography, personal data violations, and terrorist content. Legal and ethical issues, such as intellectual property infringement, were also pointed out by the majority of respondents, indicating a growing awareness of copyright protection. Slightly greater discrepancies appeared regarding hate speech and discrimination, which may result from differing interpretations of freedom of speech. In the areas of disinformation and acts of unfair competition, there is a noticeable increase in social awareness of the threats, although not everyone unequivocally perceives them as illegal. These findings are confirmed by other studies, such as the report by the Digital Poland Foundation, which highlights a high level of disinformation in Poland. Interestingly, experts assess the hierarchy of threats somewhat differently. Although child pornography remains in first place, acts of unfair competition rank second, ahead of intellectual property infringements and terrorist content. Personal data violations, which ranked second in the general survey, were placed only sixth by experts, which may be due to the specific nature of the industries they work in.

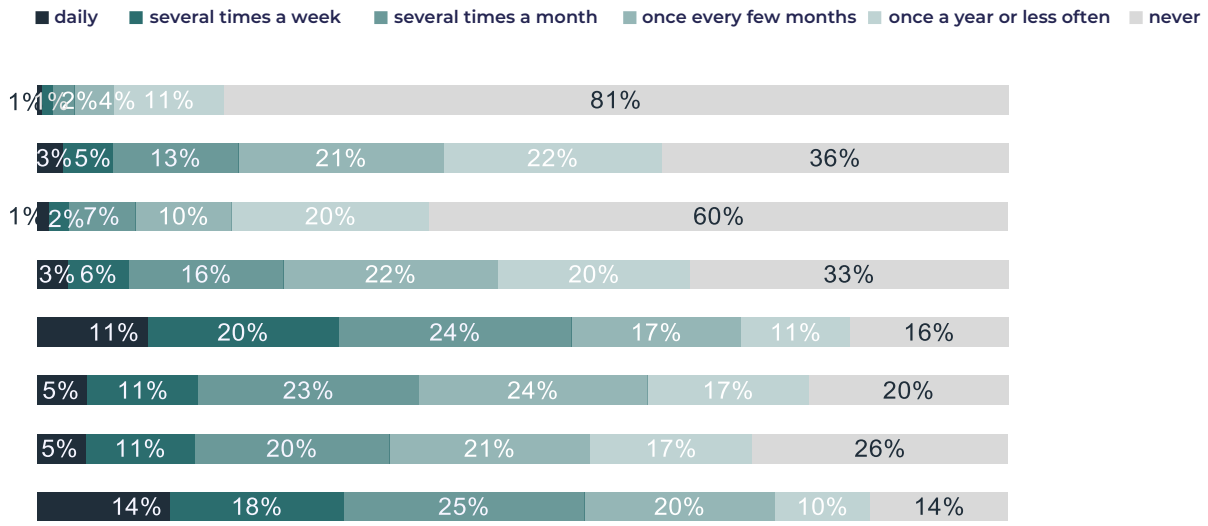
FREQUENCY OF EXPOSURE TO ILLEGAL CONTENT

How often do you encounter the following types of content on the Internet?
Sample size: N=1083

Most respondents declare that they rarely encounter illegal content. In many categories, answers such as „never" or „once a year or less" dominate, suggesting that most users seldom come across content considered illegal. The types of content with the highest exposure (at least several times a month) are disinformation and hate speech, which often appear on social media and internet forums.The least frequently encountered are those types most commonly recognized by respondents as illegal, such as child pornography — as many as 81% of respondents have never encountered it, and only 4% reported encountering it several times a month.

There are differences in the perception of illegal content — some people may not be aware that certain content is illegal or simply do not recognize it as unlawful, which may affect the survey results.

Frequency of Exposure to Illegal Content



The study shows that the most frequently encountered content relates to disinformation, hate speech, and discrimination, while the most obvious legal violations, such as child pornography or personal data breaches, are rarely noticed by the average Internet users. The high frequency of exposure to certain categories of content suggests the need to raise user awareness and to intensify educational and regulatory efforts.

EXPERIENCE WITH ILLEGAL CONTENT ON THE INTERNET

Have you ever come across content on the Internet that you consider illegal?
Sample size: N=1083

The study shows that 42% of respondents admitted to encountering content online that they considered illegal. At the same time, 36% of people, despite being presented with a definition of illegal content at the start

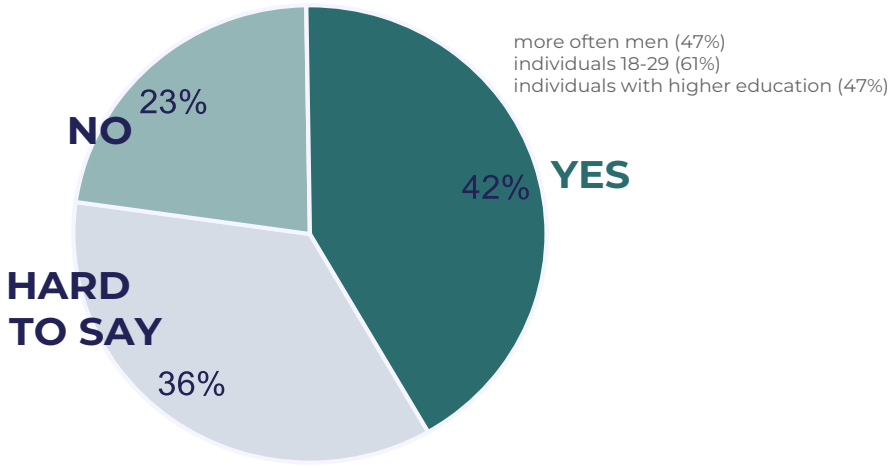
of the survey are not sure whether they have encountered such materials which may indicate ambiguity in the definition of illegal content in the respondents' perception or a lack of knowledge on the subject. 23% of respondents stated that they have never come across illegal content.

The experts we surveyed, however, had no doubts, almost unanimously confirming contact with illegal content on the Internet. Only one out of sixteen was unable to provide a clear answer to this question. This indicates a much greater knowledge of illegal content among people professionally involved with the Internet

The demographic analysis of the entire Polish population shows that men (47%), young people aged 18–29 (61%), and individuals with higher education (47%) more often encounter illegal content. This may suggest that younger groups of Poles and more educated individuals are more active on the Internet and more frequently come across various forms of illegal content, for example on social media, news websites, or discussion forums.

Experience with illegal content on the Internet

Have you ever come across content on the Internet that you consider illegal?
Base: Total N=1083



One of the key findings of the study is that a significant number of people, despite initially declaring knowledge on the subject, are unable to clearly identify what constitutes illegal content, whether they have encountered illegal content, which may indicate the need for greater user education on how to recognize and report such materials.

PLACES OF EXPOSURE TO ILLEGAL CONTENT

Where on the Internet do you most often encounter illegal content?
Sample size: N=462 (Individuals who have ever come across illegal content online)

The majority of respondents (78%) identified social media platforms (e.g., Facebook, Instagram) as the main source of such content. This may be due to the broad reach of these platforms, the ease with which content can be shared, and the challenges associated with moderating it.

In second place were internet forums (47%), where illegal content was more frequently encountered by individuals with higher education (56%). This may suggest that more educated people use forums as a source of information and opinion exchange, where disinformation and illegal content may be more difficult to detect.

Streaming platforms (e.g., YouTube) rank third (32%)—here, individuals aged 30–39 (43%) and those with higher education (41%) are particularly exposed to illegal content. This may be due to content recommendation algorithms and the difficulty of quickly removing materials that violate the law.

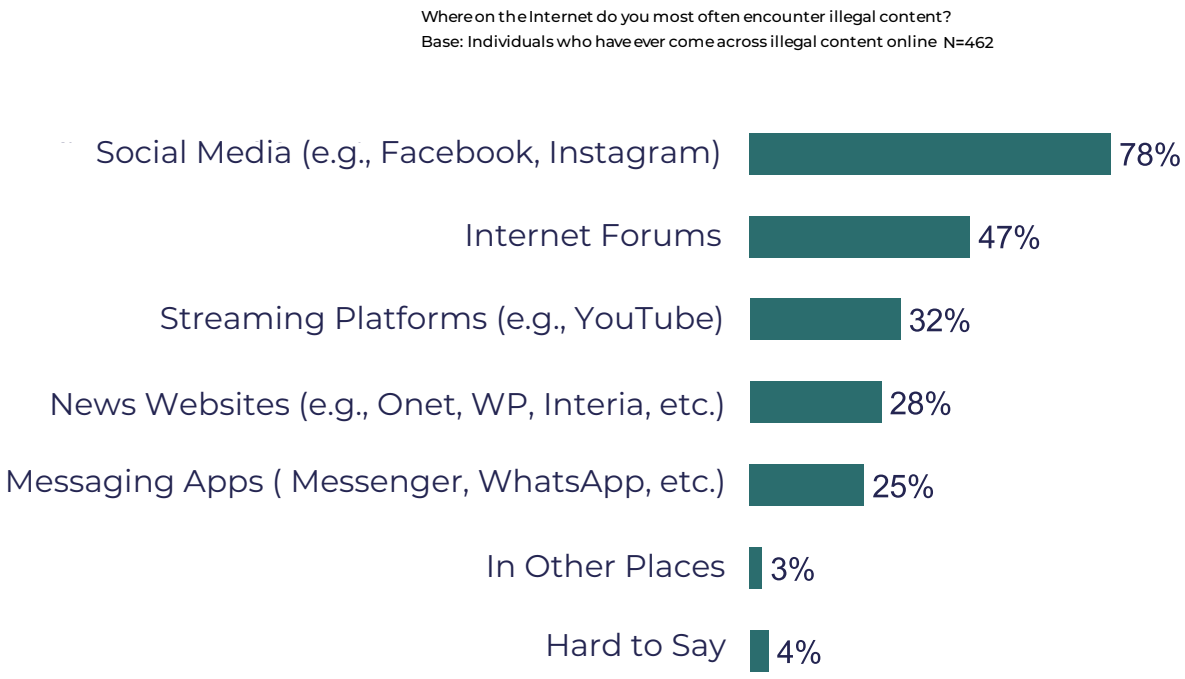
News websites (e.g., Onet, WP, Interia) were indicated by 28% of respondents, with higher-educated individuals reporting this more frequently (36%). This may suggest the presence of illegal content in comment sections or opinion articles.

Messaging apps (e.g., Messenger, WhatsApp) were indicated by 25% of respondents, mainly individuals aged 40–49 (35%). This may indicate that private groups and chats are also used to spread illegal content, making it more difficult to moderate.

Only 3% of users indicated other sources, and 4% had difficulty clearly identifying where they had encountered illegal content on the Internet.

Interestingly, the control group of experts from the internet-related industry established a different hierarchy of places where illegal content is encountered online. As with the general Polish population, social media ranked first (15 mentions), but streaming platforms came second (9 mentions), followed by internet forums (6) and news websites (5). Messaging apps were indicated as the least frequent source. This is likely due to the different ways in which people who work with the Internet on a daily basis use it.

Places of Exposure to Illegal Content



The most important factors influencing the most frequent exposure to illegal content in specific sources:

Social media:

- A huge number of users and ease of content publication.
- Ease of spreading misinformation and fake news.
- Complexity of moderation mechanisms.
- Anonymity and difficulty in law enforcement.

Streaming Platforms:

- Long response times to reports.
- Easy accessibility and lack of effective live moderation.
- Circumvention of security measures and moderation algorithms.

Internet Forums:

- Less restrictive moderation.
- Operation within the „Dark Web."
- Users exchanging instructions on how to circumvent the law.

News Websites:

- User comments.
- Publication of controversial materials.
- Advertising and clickbait content.

Messaging Apps:

- Lower accidental exposure.
- Message encryption.
- Lack of publicly accessible content.

Social media are the most common source of illegal content—almost all respondents identified Facebook, Instagram, and similar platforms as the places where they most frequently encounter content that violates the law.

These results highlight the need for better regulation of online content, strengthening tools for reporting violations, and increasing user awareness about responsible use of the digital space.

Possible consequences of widespread exposure to illegal content:

1. **Disorders of psychological and emotional development**

- Exposure to pornographic content, especially at a young age, may lead to:
  - Abnormal psychosexual development,
  - Formation of inappropriate sexual behavior patterns,
  - False beliefs about one's own body.
- Negative impact on the sexual aspect of life.

2. **Increase in aggression and antisocial behavior**

- Exposure to violent content may:
  - Encourage aggressive behaviors,
  - Reinforce hostility towards peers, vulnerable individuals, or people of different nationalities and religions.

3. **Desensitization to violence and pathological behaviors**

- Frequent exposure to violent materials may:
  - Lead to indifference toward aggression and brutality,
  - Increase tolerance for violence in real life.

4. Anxiety, worry, and decreased sense of security

- Children and adolescents exposed to harmful content may:
  - Experience negative emotions such as anxiety and worry,
  - Feel a reduced sense of safety,
  - Suffer from worsened mood and mental state.

5. Risky behaviors and moral degradation

- Exposure to illegal content may:
  - Lead to behaviors that conflict with social norms,
  - Increase the tendency toward risky actions,
  - Cause moral degradation and loss of ethical values.

6. Privacy violations and fraud

- Online interactions may result in:
  - Fraudulent acquisition of personal data, login credentials, passwords, or money,
  - Exposure to financial and reputational consequences.

7. Legal problems

- Engaging with scammers or participating in illegal file sharing may lead to:
  - Charges of legal violations,
  - Legal consequences such as fines, civil liability, or criminal proceedings.

8. Internet addiction

- Excessive use of the Internet, especially in the context of accessing illegal content, may lead to:
  - Addiction to the web and its content,
  - Negative impact on personal life, education, and work,
  - Reduced control over time spent online, which can result in neglecting responsibilities and interpersonal relationships.

Source: J. Piechna, Szkodliwe treści Internecie. Nie akceptuję, reaguję! Poradnik dla rodziców, NASK, Warszawa 2019, https://cyberprofilaktyka.pl/publikacje/Szkodliwe%20tre%C5%9Bci%20w%20Internecie_www

AWARENESS OF WHERE TO REPORT ILLEGAL CONTENT

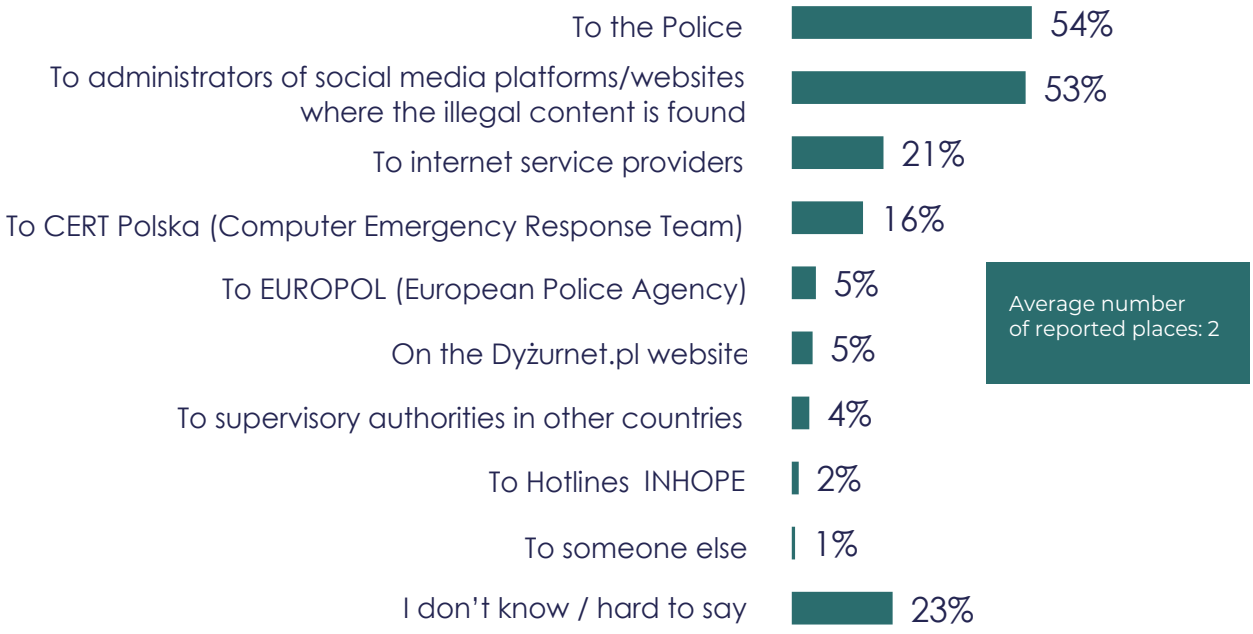
Who do you think can be reported to when encountering illegal content on the Internet?

Sample size: N=1083

The study results show a wide variety of actions taken when encountering illegal content on the Internet. The most commonly chosen reporting methods indicate a preference for solutions available at the platform level and national institutions. At the same time, some respondents do not take any action, and international tools such as Europol or INHOPE are not used at all.

Poles most often indicate the Police (54%) as the institution to which illegal content can be reported. This may suggest that most people associate reporting such content with official law enforcement agencies. Administrators of social media platforms and websites took second place (53%), with women (56%) and individuals with higher education (59%) indicating them more frequently. This reflects growing awareness that these services are obligated to moderate and remove illegal content. Internet service providers were identified by 21% of respondents, suggesting that their role in combating illegal content is not widely recognized. Even lower recognition was given to CERT Polska (16%), Europol (5%), the Dyżurnet.pl website (5%), supervisory authorities in other countries (4%), and INHOPE hotlines (2%) — despite these institutions being involved in cybersecurity and combating internet crime.

Awareness of where to report illegal content



The study results indicate that most respondents are aware of various institutions involved in combating illegal content on the Internet; however, reporting preferences are strongly focused on national entities such as CERT Polska, internet service providers, and the Police. International institutions and specialized reporting platforms like Europol, INHOPE, or Dyżurnet.pl remain largely overlooked, which may reflect their low recognition among users..

For comparison, the group of experts we studied—Internet specialists—identified CERT Polska as the primary institution to report illegal content online. Internet service providers were ranked second, while the Police and platform administrators tied for third place. This reflects their significantly greater knowledge in this area compared to the general Polish population.

The CERT Polska team operates within the structures of NASK – the National Research Institute, which conducts scientific research, manages the .pl domain registry, and provides advanced ICT services. As CSIRT NASK (the National Computer Security Incident Response Team), it is responsible, among other things, for:

- Monitoring cybersecurity threats and incidents at the national level;
- Sharing information about incidents and risks with entities in the national cybersecurity system;
- Issuing alerts about identified cybersecurity threats;
- Responding to reported incidents;
- Classifying incidents, including serious and significant incidents as critical incidents, and coordinating the handling of critical incidents;
- Monitoring cybersecurity threat indicators;
- Developing tools and methods for detecting and combating cybersecurity threats;
- Conducting activities aimed at raising awareness in the field of cybersecurity.

Source: Cert.pl, https://cert.pl/en/about-us/

It is surprising that as many as 23% of respondents do not know or cannot identify the appropriate place to report illegal content, highlighting the need to increase education about available reporting mechanisms and the relevant authorities responsible for combating such issues online. The average number of reported places was 2, meaning most people could name only one or two reporting sources, which may suggest limited knowledge in this area.

WHAT CAN BE DONE?

- **Digital education and social campaigns** – It is essential to raise awareness about the role of institutions involved in combating illegal content on the Internet.
- **Promoting Dyżurnet.pl and other national reporting mechanisms** – The lack of reports may stem from a lack of knowledge about the existence of such tools.
- **Building trust in law enforcement agencies** – Efforts are needed to convince users that reporting to the Police or Europol can yield effective results.
- **Encouraging action against illegal content** – Campaigns emphasizing that every intervention matters in the fight against cybercrime.

ACTIONS TO TAKE WHEN ENCOUNTERING ILLEGAL CONTENT

What actions do you take when you encounter illegal content on the Internet?
Sample size: N=462 (People who have ever come across illegal content online)

The study on reactions to illegal content on the Internet reveals significant trends in user behavior and highlights the most commonly used reporting methods. The results indicate that users prefer to report illegal content directly on internet platforms or to national cybersecurity institutions, while rarely using international organizations or law enforcement agencies. There is also a group of people who take no action, raising concerns about passivity in the face of online law violations.

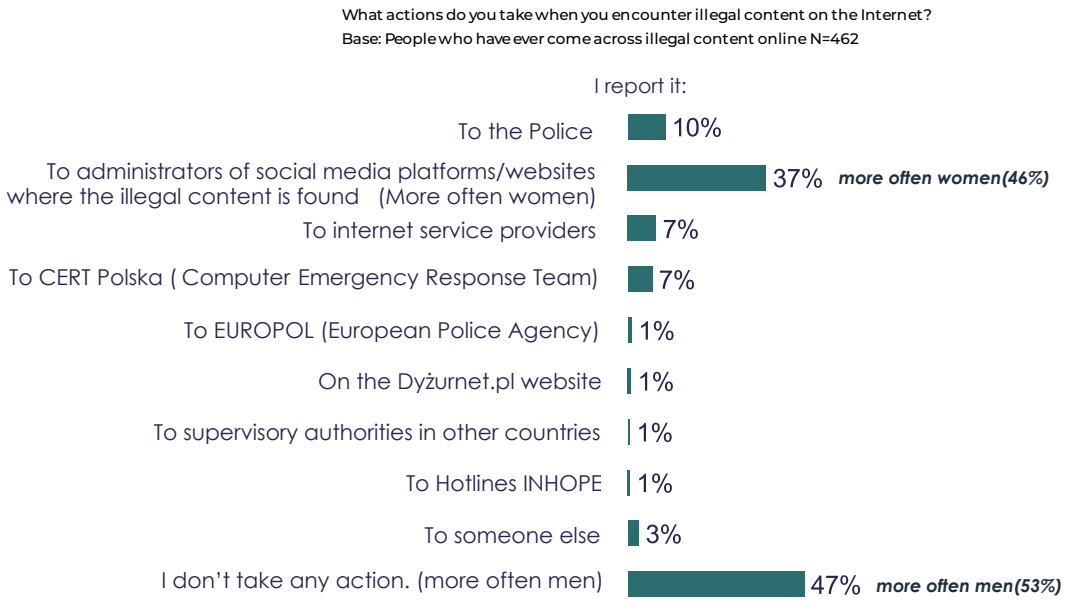
Almost half of respondents (47%) do not take any action after encountering illegal content on the Internet, indicating widespread passivity in responding to such content. This lack of response is more common among men (53%).

Only 10% of people report the illegal content they encounter, which suggests that reporting mechanisms may be insufficiently accessible or that users are unaware of how to do so. Meanwhile, 37% choose to avoid such content, a behavior more common among women (46%). This may stem from a desire to protect themselves or their loved ones from unpleasant or dangerous materials.

Other actions, such as warning other users or taking legal steps, are marginal, ranging between 1-7%. This could be due to a lack of knowledge about effective methods to counter illegal content or fear of potential consequences.

Internet experts show significantly higher activity in this area. Only three out of the sixteen experts we surveyed do not take any actions related to reporting illegal content on the Internet.

ACTIONS TO TAKE WHEN ENCOUNTERING ILLEGAL CONTENT



The results indicate a low level of active user response to illegal content online. Greater education and promotion of reporting tools are necessary to improve the effectiveness of combating such content on the Internet.

Prof. Ryszard Szpyra, PhD, habil.
Head of the Department
of Information Security
Institute of Security
International Faculty
of National Security
War Studies University, Poland

EXPERT COMMENT

In classical capitalism, effectiveness dominates over morality, because the system rewards economic efficiency and other forms of effectiveness, not ethical behavior. Many scholars, such as Zygmunt Bauman and Naomi Klein, confirm that capitalism fosters situations where ethical values are subordinated to profitability and efficiency. This is one of the main sources of the civilizational decline in good manners, personal culture, and overall ethics. The lack of widespread ostracism and the nature of modern mass communication media contribute to the spread of brutalization in social communication. Regarding the latter, it is worth mentioning the algorithms and mechanisms of social media platforms, which promote negative, emotion-provoking content, causing hate speech to „live" longer, spread faster, and attract more attention. The immense influence of the so-called "big tech" owners paralyzes politicians, making them unable to effectively regulate these platforms by law. China manages to regulate effectively, but its regulations go too far, excessively limiting human freedom. Here arises the important dilemma between the level of freedom and the level of security: increasing one decreases the other. Moreover, the nature of the Internet provides greater anonymity and lack of direct consequences for one's actions. Added to this is the ongoing ideological and civilizational struggle, as well as growing social polarization, which leads to groupthink and treating others with contempt. As society becomes accustomed to such an environment, it ceases to shock and provoke widespread opposition. Furthermore, intellectual elites—especially political elites—do not set a good example from the top. Politicians themselves propagate controversial content because it provokes emotions and thereby increases public interest. Thus, the high social passivity towards illegal content encountered on the Internet is not surprising. This passivity also stems from a low belief in the effectiveness of countermeasures and a growing conviction about the low social harm of such content, resulting from habituation to the current state of affairs. Regarding counteracting these phenomena, systemic and ad hoc actions should be undertaken. Systemic actions go beyond the scope of the discussed content. As for ad hoc actions, they are properly indicated. It seems, however, that CERT is more suited to counteracting harmful teleinformatics activities rather than combating illegal content flowing in digital information streams.

Opinions on Illegal Content on the Internet

Illegal Content on the Internet – Do You Stay Silent or Take Action?

CAN REPORTING ILLEGAL CONTENT LEAD TO ITS REMOVAL?

Do you believe that reporting illegal content to someone can lead to its removal?
Sample size: N=1083

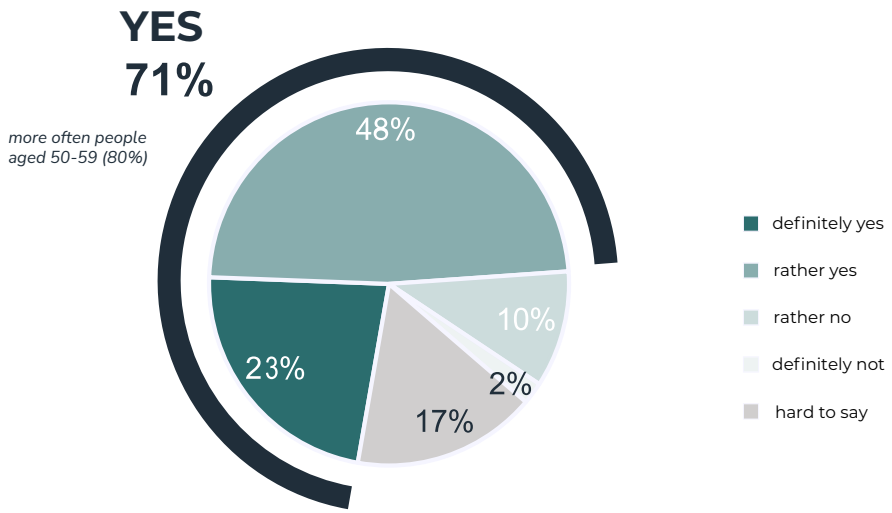
The vast majority of respondents (71%) believe that reporting illegal content can lead to its removal, including 48% who are completely certain of this and 23% who are rather confident. This belief is particularly strong among people aged 50–59, with 80% sharing this view.

However, 17% of respondents are unsure about the effectiveness of reporting, and 12% are skeptical: 10% think that reporting probably does not lead to content removal, and 2% believe it definitely has no effect.

The opinions of the experts we surveyed do not differ significantly from those of the general population.

Can reporting illegal content lead to its removal?

Do you believe that reporting illegal content to someone can lead to its removal?
Base: Total N=1083



The results suggest that respondents' awareness of the mechanisms for reporting illegal content online is relatively high, although some individuals remain uncertain about their effectiveness. This may stem from a lack of information about how online platforms operate and differences in how reports are enforced across various services.

DOES ILLEGAL CONTENT HAVE A NEGATIVE IMPACT ON SOCIETY?

Do you believe that the presence of illegal content on the Internet has a negative impact on society?
Sample size: N = 1083

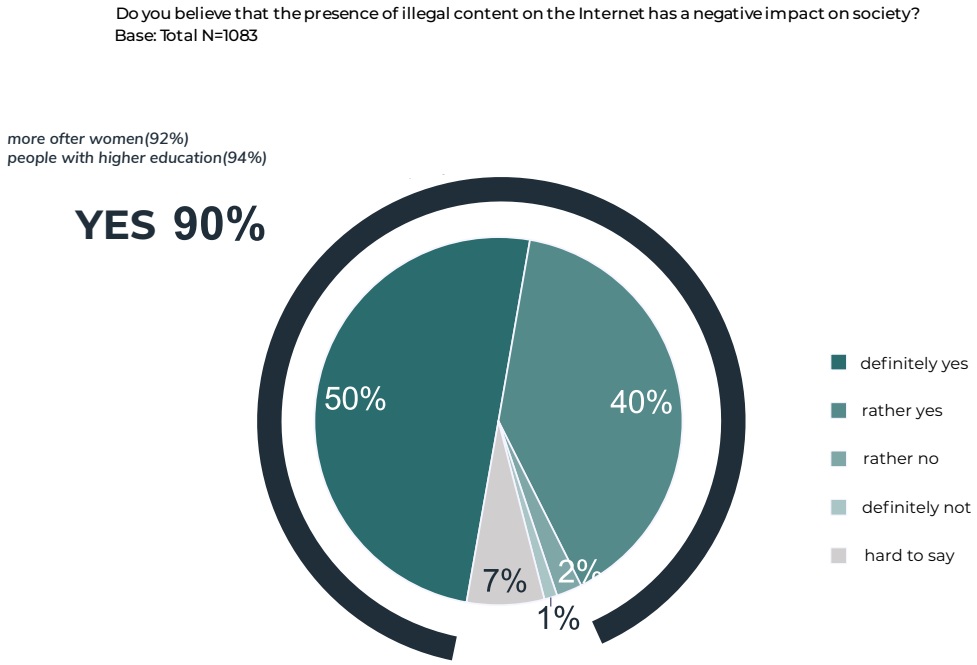
The vast majority of respondents (90%) believe that such content has a negative impact on society – including 50% who are completely certain of this and 40% who tend to share this opinion.

Only 7% of respondents are doubtful, stating that such content rather does not have a negative impact, and just 1% strongly believe there is no such impact. 2% of respondents are unable to determine their position.

The opinions of experts are consistent with the findings of the nationwide survey.

An interesting observation from the survey results is that women (92%) and individuals with higher education (94%) are more likely to perceive a negative impact. This may be due to a greater awareness of the risks associated with illegal content or more frequent exposure to reliable sources of information on the subject.

Does illegal content have a negative impact on society?



The survey shows that society largely recognizes the dangers associated with the presence of illegal content on the Internet, which indicates the need for effective regulatory and educational measures in this area.

WHAT IS THE NEGATIVE IMPACT OF ILLEGAL CONTENT ON SOCIETY?

In your opinion, how does the presence of illegal content on the Internet negatively affect society?
Sample size: N = 977 (individuals who believe that illegal content has a negative impact on society)

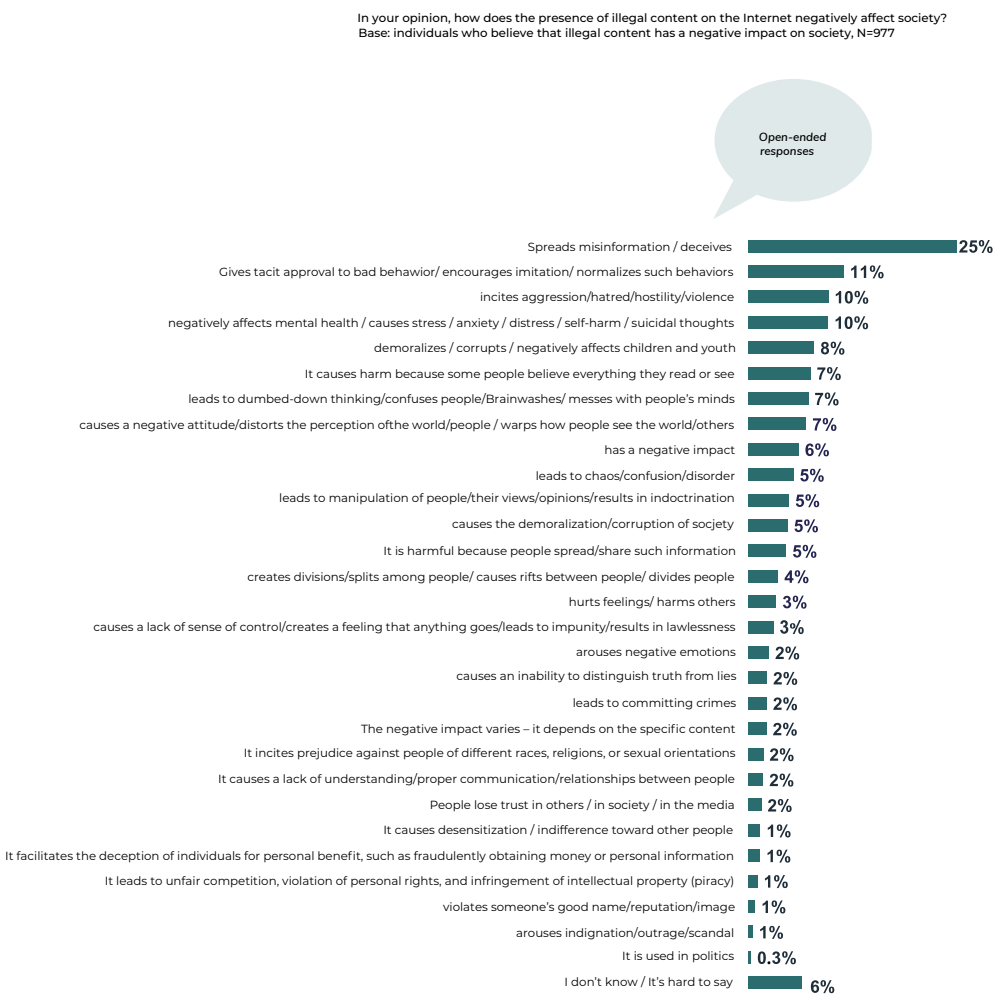
Respondents spontaneously identified various effects they believe result from the presence of such content online. The most frequently mentioned problem is the spread of misinformation and misleading people (25%). This highlights growing concerns related to fake news, information manipulation, and propaganda, which can shape public opinion and influence social and political decisions.

Other negative effects mentioned by respondents include:

- Encouraging bad behavior and normalizing pathological attitudes (11%),
- Inciting aggression, hatred, hostility, and violence (10%),
- Negative impact on mental health, leading to stress, anxiety, self-harm, and suicidal thoughts (10%).

Other significant threats are demoralization of children and youth (8%), promoting false beliefs through information manipulation (7%), and information chaos and distortion of reality perception (7%).

What is the negative impact of illegal content on society?



The survey results indicate that society recognizes the multifaceted threats associated with illegal content on the Internet – from misinformation and manipulation to negative impacts on mental health and increased aggression. This underscores the need for more effective legal regulations and greater media education, so that users can critically evaluate the content they encounter.

SUPPORT FOR NEW TECHNOLOGIES

DETECTION:

In your opinion, do new technologies (such as artificial intelligence) support the detection of illegal content on the Internet?

Sample size: N=1083

REMOVAL:

In your opinion, do new technologies (such as artificial intelligence) support the removal of illegal content on the Internet?

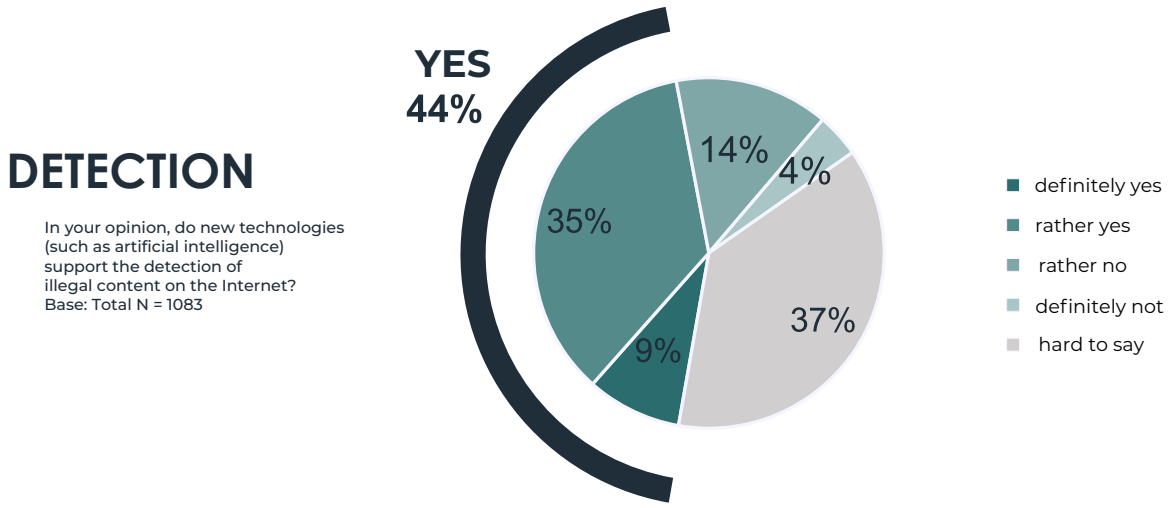
Sample size: N = 1083

1. Detection of illegal content on the Internet

44% of respondents believe that new technologies help in detecting illegal content (9% "definitely yes" and 35% "rather yes"). The groups most convinced about the effectiveness of these technologies are men (51%) and people with higher education (51%). 18% of respondents think that new technologies are not sufficiently effective in this area (14% "rather no" and 4% "definitely no"). This may suggest that users notice algorithm errors and cases where artificial intelligence fails to recognize context. Additionally, as many as 37% of respondents have no opinion, which could mean that some users lack knowledge about how content moderation algorithms work.

These results align with the opinions of the experts we surveyed.

Support for New Technologies – Detection

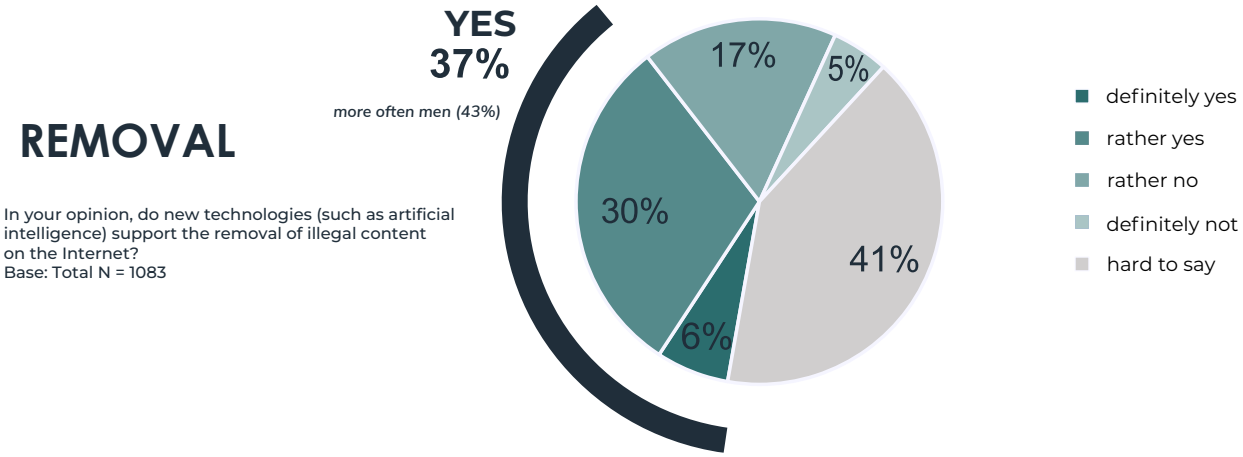


2. Removal of illegal content on the Internet

Even fewer respondents (37%) believe that technologies are effective in removing illegal content (5% chose "definitely yes" and 32% "rather yes"). This means that fewer people trust the effectiveness of removal compared to detection of illegal content. 22% think that technologies do not handle content removal well (17% "rather no" and 5% "definitely no"). This may be because, even if algorithms detect illegal content, its removal requires human intervention or the removal process takes too long, leading to perceptions of ineffectiveness. 41% of respondents selected "hard to say," which may indicate that users do not know exactly how content moderation systems work on the Internet.

The surveyed experts also had many doubts on these issues. Only 7 out of 16 experts believe that modern technologies are effective in removing illegal content on the Internet.

Support for New Technologies – Removal



44% of respondents believe that new technologies, such as artificial intelligence, effectively support the detection of illegal content, but only 37% say they effectively remove it. The majority of people are not convinced about the effectiveness of these technologies, which means the moderation process still needs improvement. This highlights the need to develop better algorithms, increase platform response speed, and ensure greater transparency in content removal decisions.

EFFECTIVENESS OF REMOVING ILLEGAL CONTENT BY SOCIAL MEDIA

In your opinion, do social media platforms (e.g., Facebook, Instagram) effectively remove illegal content?

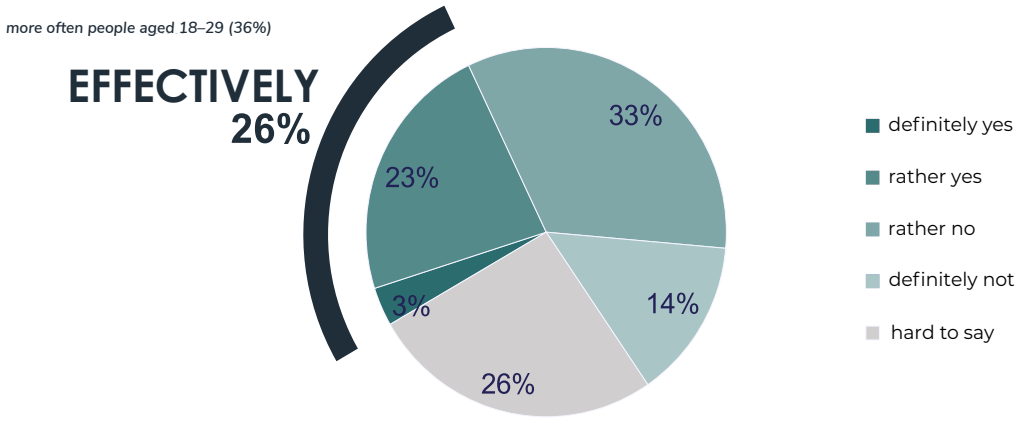
Sample size: N = 1083

Only 26% of respondents believe that social media effectively eliminate illegal content — 3% describe their actions as "definitely effective" and 23% as "rather effective." This perception is more common among the youngest age group (18–29 years). As many as 47% of respondents consider the platforms' actions ineffective — 33% rate them as "rather ineffective" and 14% as "definitely ineffective." 26% of respondents have no clear opinion and chose "hard to say."

The group of experts we surveyed is even more critical in this regard. The majority of them (12 out of 16) negatively assess the effectiveness of social media platforms in removing illegal content.

Effectiveness of Illegal Content Removal by Social Media Platforms

How do you assess the effectiveness of legal regulations in combating illegal content on the Internet?
Base: Total N=1083



These results indicate that most Poles do not trust the effectiveness of social media platforms in combating illegal content. This may be due to instances where harmful materials remain online despite user reports, or due to slow responses from platform administrators. A significant portion of respondents remain undecided, which may suggest a lack of sufficient knowledge about how platforms operate in this area. These findings point to the need for greater transparency and more effective content moderation mechanisms on social media.

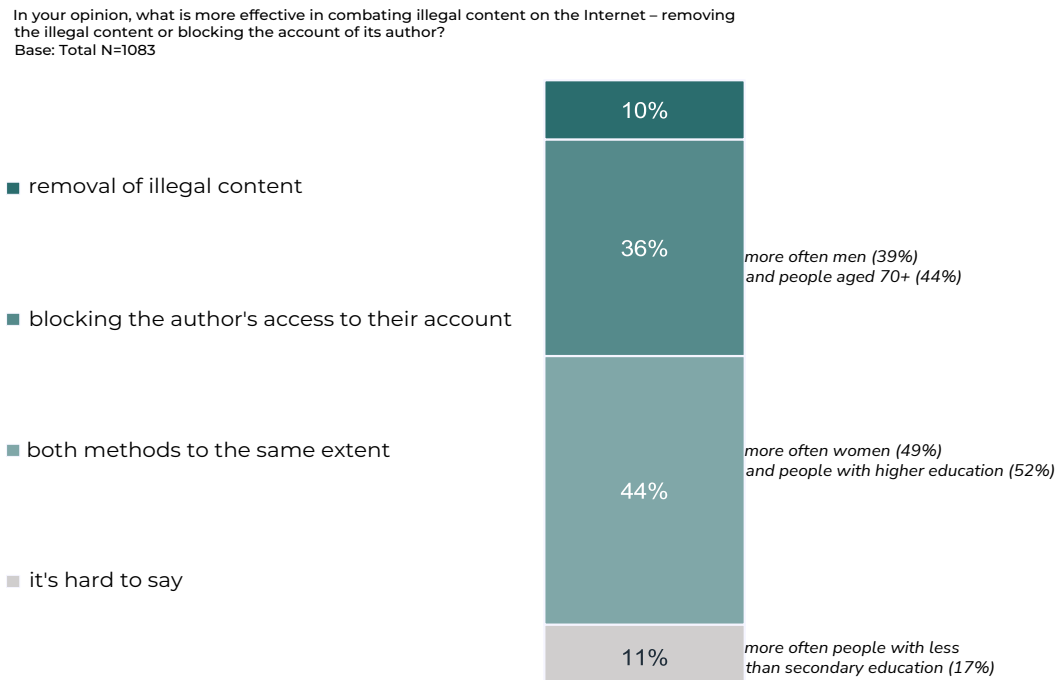
EFFECTIVENESS OF METHODS FOR COMBATING ILLEGAL CONTENT

In your opinion, what is more effective in combating illegal content on the Internet – removing the illegal content or blocking the account of its author?
Sample size: N = 1083

When it comes to the effectiveness of combating illegal content on the Internet, respondents' opinions are divided. 44% believe that both methods — removing illegal content and blocking the author's account — are equally effective. This view is more commonly expressed by women (49%) and individuals with higher education (52%). According to 36% of respondents, blocking access to the author's account is more effective. This opinion is more frequently shared by men (39%) and people over the age of 70 (44%). Only 10% believe that removing illegal content is the more effective solution, while 11% of respondents have no opinion on the matter — more often among those with less than a secondary education (17%).

Interestingly, expert opinion differs in this regard. The Internet specialists surveyed identified content removal as the most effective method of combating illegal content online, or alternatively, a combination of both approaches. Blocking access to the author's account was considered by them to be less effective.

Effectiveness of methods for combating illegal content



Most respondents believe that effective action against illegal content should combine both the removal of such materials and blocking access for their authors. Fewer people believe in the effectiveness of either method on its own, with account blocking seen as more effective than content removal alone. These results suggest that internet users expect more decisive measures against those who publish illegal content, rather than merely passive removal of its effects.

FREEDOM OF SPEECH...

...AND CONCERNS ABOUT THE AUTOMATIC REMOVAL OF SUSPICIOUS CONTENT

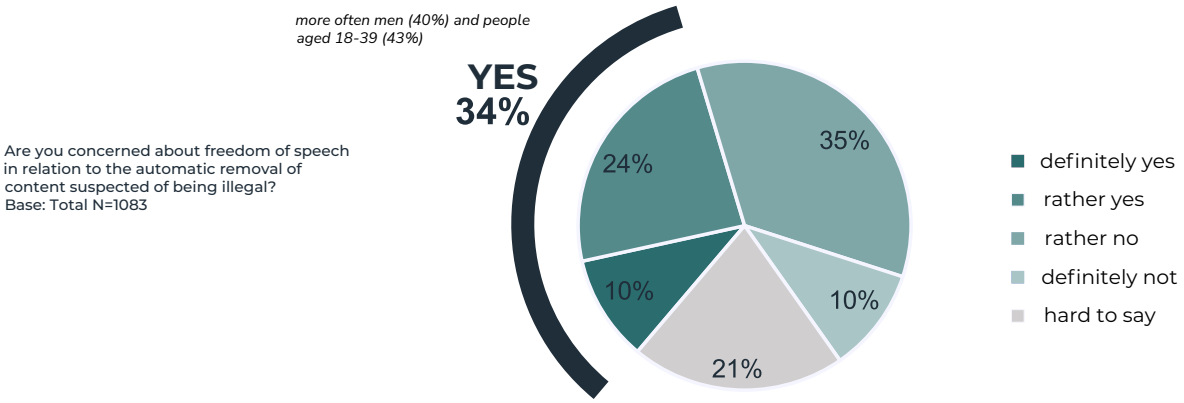
Are you concerned about freedom of speech in relation to the automatic removal of content suspected of being illegal?

Sample size: N=1083

34% of respondents in the nationwide survey are concerned that the automatic removal of content suspected of being illegal may pose a threat to freedom of speech. These concerns are most commonly expressed by men (40%) and individuals aged 18–39 (43%). At the same time, 45% of respondents do not share these concerns, while 21% have no opinion on the matter. The results suggest that although a significant portion of people recognize the risk of abuse in automatic content moderation, it is not a dominant concern within society.

Similar opinions were expressed by the experts we surveyed.

Freedom of speech... and concerns about the automatic removal of suspicious content



...AND THE LEGALITY OF CONTROVERSIAL BUT SOCIALLY IMPORTANT CONTENT

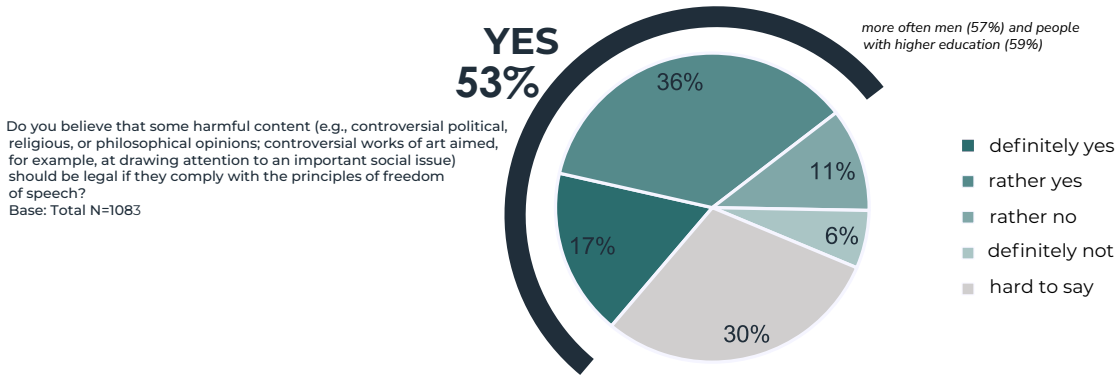
Do you believe that some harmful content (e.g., controversial political, religious, or philosophical opinions; controversial works of art aimed, for example, at drawing attention to an important social issue) should be legal if they comply with the principles of freedom of speech?

Sample size: N=1083

53% of respondents believe that controversial content (e.g., political, religious, or philosophical opinions, critical art) should remain legal if it complies with the principles of freedom of speech. This view is most commonly held by men (57%) and individuals with higher education (59%). Seventeen percent of respondents oppose such freedom of speech, while 30% have no opinion on the matter. These results show that the majority of those surveyed support the right to publish controversial content, provided it does not violate legal standards.

Even stronger supporters of the legality of controversial content—provided it complies with the principles of freedom of speech—are the Internet experts we surveyed (11 out of 16 votes).

Freedom of speech... and the legality of controversial but socially important content



Although a significant portion of society (34%) fears that automatic content removal may threaten freedom of speech, the majority do not see it as a key issue. Over half of the respondents (53%) believe that controversial but socially important content should be legal, indicating a strong commitment to the principle of freedom of speech—especially among men and those with higher education. The results suggest that while content moderation on the Internet raises some concerns, greater emphasis is placed on the right to free expression on socially significant matters. Poles do not have a clear-cut stance on concerns about freedom of speech related to the automatic removal of suspicious content — most often, do not have such concerns (nearly half), but one in three sees this as a threat, and one in five has no opinion on the matter. More likely to believe that controversial content, as long as it complies with the principles of freedom of speech, should be legal — half of the population holds this view. Only one in six disagrees, while the rest do not have a defined position.

CONCERNS ABOUT DIGITAL IDENTITY VIOLATION

Do you have concerns that your digital identity (i.e., the information representing you on the Internet) may be compromised?

Sample size: N=1083

62% of respondents express concerns about the potential compromise of their digital identity. These concerns are most commonly reported by individuals with higher education (67%), which may reflect greater awareness of cyber threats. 42% of respondents are strongly worried about digital identity breaches, while another 20% have moderate concerns.

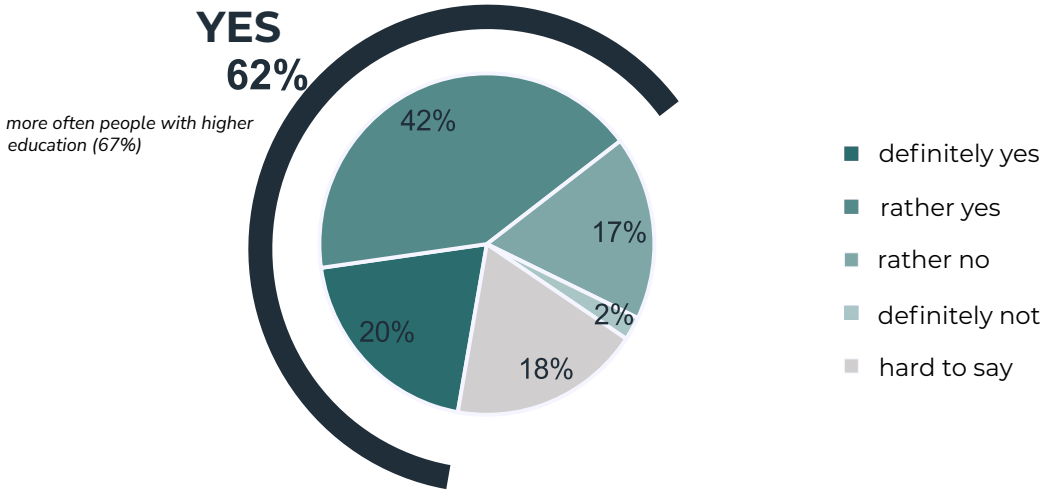
17% of respondents are rather unconcerned about their digital identity being compromised, and only 2% are firmly dismissive of such a possibility. 18% of respondents have no opinion on the matter, which may indicate a lack of knowledge or awareness about data protection risks online. The survey results indicate that the majority of respondents are aware of the risks related to breaches of their personal data and digital identity.

Experts surveyed show an even greater awareness of the risks related to identity theft on the Internet—14 out of 16 express concerns about it, while only 1 does not feel threatened.

The high level of concern among individuals with higher education suggests that those more familiar with digital technologies have a better understanding of potential threats such as identity theft, phishing, and privacy breaches by tech companies. However, nearly one-fifth of respondents still exhibit little concern, which may reflect either a lack of awareness of cyber threats or confidence in the effectiveness of their own security measures.

Concerns about digital identity violation

Do you have concerns that your digital identity (i.e., the information representing you on the Internet) may be compromised?
Base: Total N=1083



The study shows that concerns about digital identity security are widespread—most Internet users recognize the risk of their personal data being compromised. At the same time, there is a group of people who are either unaware of these threats or do not perceive them as significant. In the context of the growing number of cyberattacks, it is essential to educate the public about protecting their digital identity and using the Internet safely.

EXPERT COMMENT

Dr Agnieszka Jankowska
Member of the Board
of the Digital Poland
Foundation,
Chairperson
of the Council for Digitization

The results of the survey conducted among Polish women and men, presented in the report "Poles and Illegal Content on the Internet," provide valuable insights into public awareness, social attitudes, and societal expectations toward digital platforms and the state.

First and foremost, it is important to highlight the differences in understanding digital threats and the level of knowledge on the subject. On one hand, it is encouraging that 71% of respondents believe in the effectiveness of reporting illegal content online, as this leads to the removal of such content. On the other hand, half of Polish women and men (47%) think that online platforms are not effective enough in removing illegal content, 26% have no opinion on the matter (indicating a lack of knowledge), and 29% believe that reporting illegal content does not result in its removal.

We recognize that reporting illegal content is a key tool in combating disinformation, hate speech, and other harmful phenomena online. Respondents acknowledge the negative consequences of the presence of illegal content on the Internet, citing, among others, the spread of disinformation and false information (25%), normalization of pathological behaviors and encouragement of bad conduct (11%), as well as the stimulation of aggression, hatred, and violence, along with negative impacts on mental health (10%). These data emphasize the necessity of responding to harmful content, which requires the involvement of users, digital platforms, and the state alike. Moreover, more effective legal regulations are essential, alongside systemic prevention measures—such as broad public education in cybersecurity, cyber hygiene, and media literacy. The state should play a more active role in educating society on media skills, equipping citizens with the ability to think critically, analyze information available online, distinguish opinions from facts, and more broadly, navigate the online environment safely. This includes knowledge about what types of illegal content exist, how, and where to report them.

An interesting issue explored in this report is the matter of freedom of speech. Thirty-four percent of respondents fear that automatic removal of illegal content may violate freedom of speech, while 45% do not perceive such threats. It is worth noting that this difference may stem from a lack of full awareness about potential abuses, as well as from varying interpretations of the concept of freedom of speech in the context of technological limitations. On the other hand, 62% of respondents express concerns about violations of their digital identity, indicating a growing awareness of privacy and data security threats on the Internet. The higher level of concern among individuals with higher education suggests that better knowledge of digital technologies is linked to greater risk awareness. Nevertheless, the fact that about 20% of respondents have no opinion on the matter highlights the need for more intensive educational efforts.

Hate speech online

What are the consequences of fear of online aggression?

TYPES OF ONLINE AGGRESSION

What type of online aggression do you think is the most common?
Sample size: N=1083

The most common forms of online aggression

According to respondents, the most common form of online aggression is hate speech — 66%. This is the most frequently indicated type of aggression on the Internet, involving verbal violence against individuals or social groups. It is most often noticed by people with higher education (75%).

Mocking others — 61% — is the second most frequently mentioned form of aggression, particularly recognized by women (64%).

Provoking conflicts and spreading disinformation (cybertrolling) — 50% — is most often noticed by people aged 40–49 (57%) and those with higher education (57%).

Discrimination based on race, religion, or sexual orientation is also considered by respondents to be frequently present online (48%). This is most commonly experienced by younger people aged 18–29 (56%).

Cyberbullying (harassment, humiliation, intimidation), despite numerous social campaigns, remains a very common form of online aggression. It is noticed by as many as 46% of respondents, most often women (51%).

Respondents also mention doxxing (publishing private information to intimidate or embarrass) — 43%, dogpiling (group aggression) — 32%, and the phenomenon of online outrage — 19%.

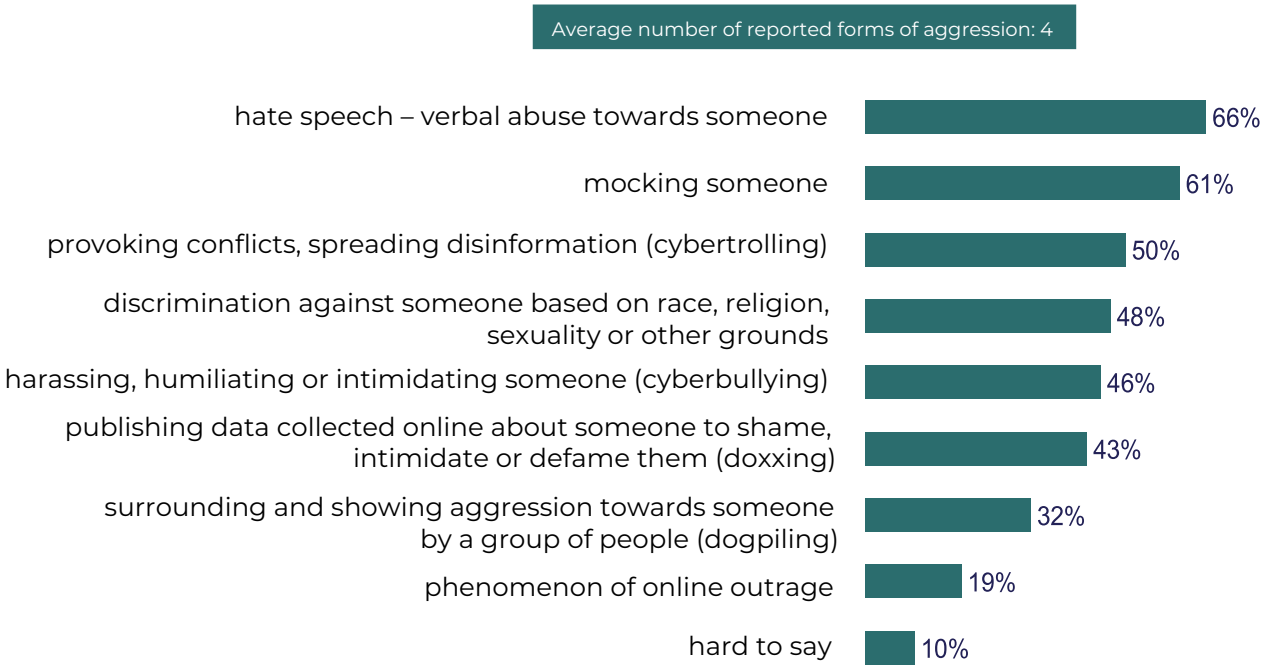
Only one in ten Poles declares that they have personally experienced online aggression directly targeting them. Such incidents most often occurred on social media platforms.

Almost half of the population (43%) states that they have witnessed online aggression aimed at someone else. This too most frequently took place on social media.

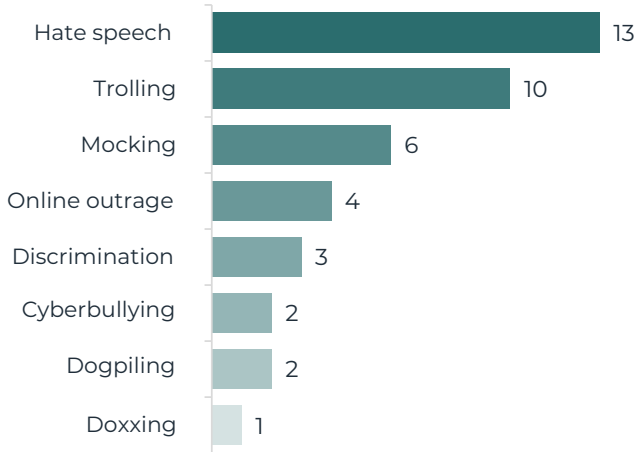
The experts we surveyed most often identified trolling (provoking conflicts and spreading disinformation) as the most common form of online aggression, with 13 mentions. Hate speech came in second with 11 mentions, followed by mocking with 10. Discrimination and harassment (7 mentions) and the phenomenon of online outrage (5 mentions) were ranked next..

TYPES OF ONLINE AGGRESSION

What type of online aggression do you think is the most common?
Sample size: N=1083

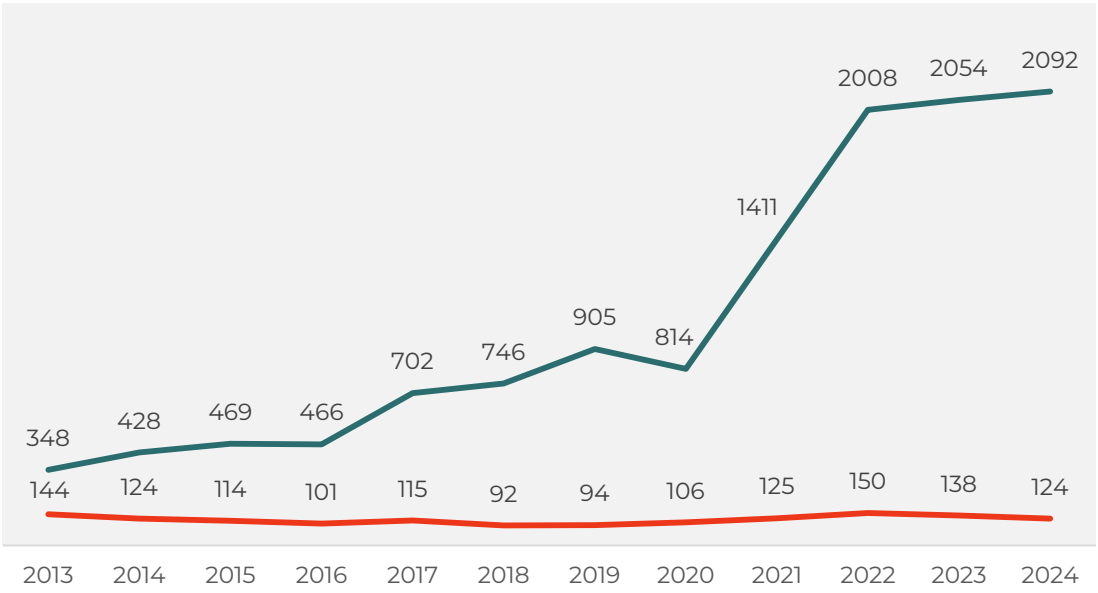


The most commonly reported forms of aggression were hate speech — 13 mentions, trolling (provoking conflicts, disinformation) — 10, and mocking — 6. Fewer respondents observed online outrage — 4, discrimination (based on race, religion, sexual orientation, or other grounds) — 3, bullying and dogpiling — 2, and violations of privacy (doxxing) — 1.



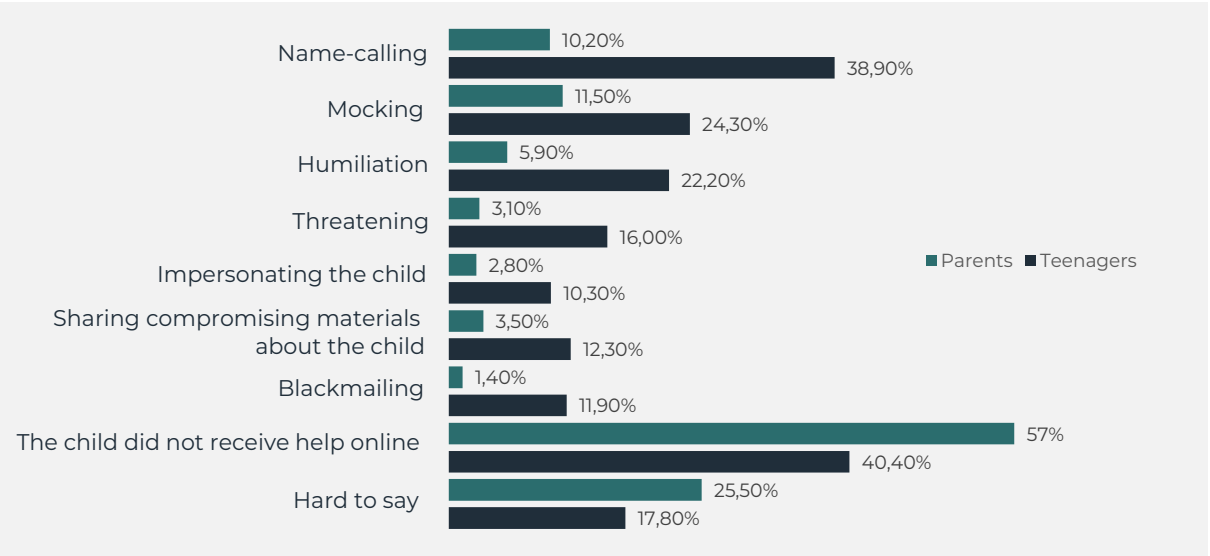
The above research results indicate a strong need for regulation and content moderation — the high prevalence of hate speech and trolling highlights the necessity for more effective actions by online platforms. Digital education is also essential, as internet users themselves should be aware of the consequences of cyberbullying and privacy violations. The noticeable increase in online aggression calls for social and legal intervention to counteract the growing problems related to harassment and disinformation.

Number of suicide attempts and suicide attempts resulting in death in the 13–18 age group.



Source: Summary by the portal ciekaweliczby.pl based on data from the Police

Comparison of teenagers' declarations about experiencing violence on the Internet with their parents' awareness of the issue.



Source: NASK, Teenagers 3.0. Report from a nationwide study of students and parents.

PERSONAL EXPERIENCE WITH AGGRESSION ON THE INTERNET

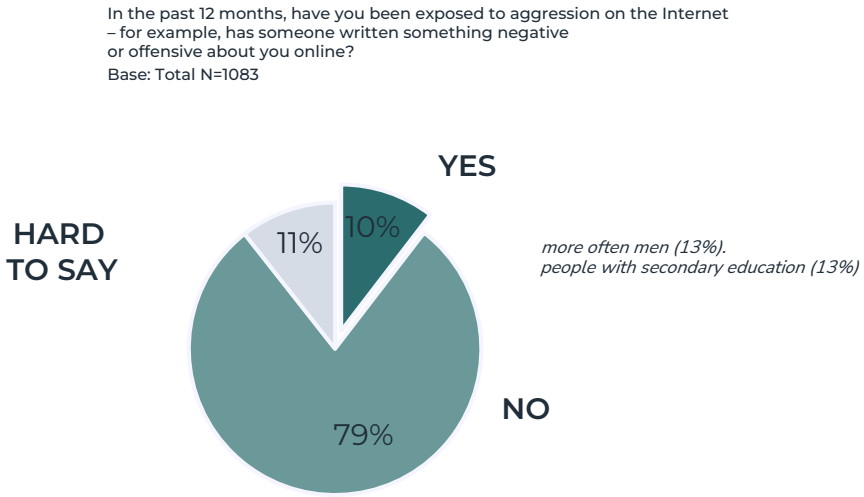
In the past 12 months, have you been exposed to aggression on the Internet – for example, has someone written something negative or offensive about you online?
Sample size: N=1083

- 10% of respondents experienced aggression on the Internet – this was more common among men (13%) and individuals with secondary education (13%).
- 79% answered "no," which means that the vast majority of respondents either did not experience online aggression or were not aware that such a situation had occurred.
- 11% were unsure whether they had experienced aggression, suggesting that some cases may be difficult to clearly assess.
- Slightly more often, the experts we surveyed reported experiencing online aggression (4 out of 16). None of them had difficulty identifying aggressive behavior on the Internet.

The low percentage of individuals experiencing aggression (10%) may suggest that the problem is not widespread, or that users avoid situations that could lead to online attacks. This low result may also be influenced by the fact that the study was conducted among adult Internet users, whereas it is children and teenagers who use the Internet most frequently and actively. In this age group, the percentage of those experiencing aggression would very likely be much higher. This is confirmed by the World Health Organization's studies conducted every four years.

79% of respondents had not encountered online aggression, which may indicate effective content filtering by platforms or a conscious effort to avoid controversial discussions. 11% of respondents were unable to answer the question, which may suggest a lack of clear definitions of online aggression or a low level of awareness about cyberbullying.

Personal experience with aggression on the Internet



There is no doubt that the problem of online aggression exists, although according to the above survey results, it affects a relatively small group of users. Men and individuals with secondary education report experiencing online aggression more frequently — this may be due to their greater activity in certain online spaces. It is important to educate users about the various forms of online aggression and how to respond to them, especially since some people are unable to clearly assess whether they have been victims of such behavior.

ENCOUNTER WITH SUCH AGGRESSION

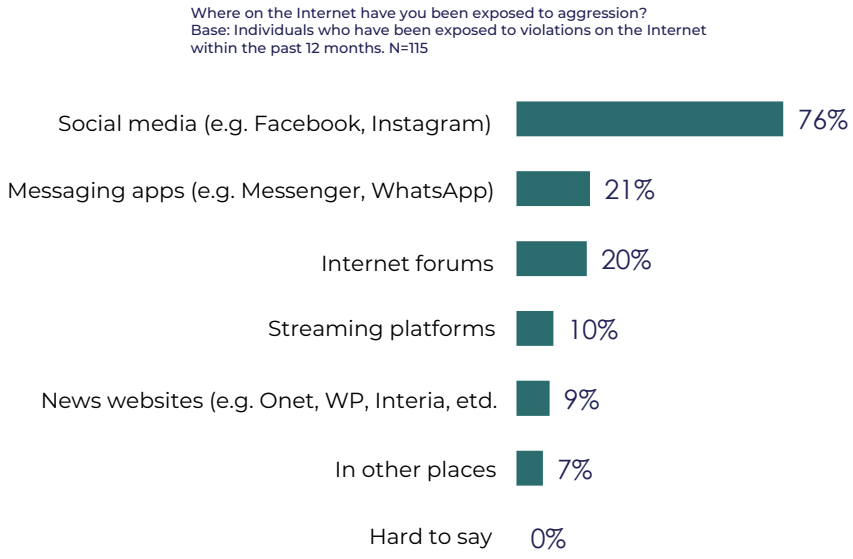
Where on the Internet have you noticed someone else becoming a victim of aggression/violations online?

Basis: Individuals who witnessed aggression on the Internet. Sample size: N=478

Social media are by far the most common place where people encounter online aggression – as indicated by 76% of respondents. This is by far the highest result, showing that public spaces on social media are particularly susceptible to negative interactions. To a somewhat lesser extent, aggression is also present on messaging apps and internet forums (21% experienced aggression on messaging apps such as Messenger or WhatsApp, and 20% encountered it on internet forums).

Experts pointed to the same platforms.

Place of encountering such aggression



These results suggest that aggression also occurs in more closed online spaces, but on a smaller scale than on social media. A much smaller number of aggression cases take place on streaming platforms and news websites (10% pointed to streaming platforms, e.g., YouTube, while 9% experienced aggression on news websites, e.g., Onet, WP, Interia). This means that in spaces primarily focused on content consumption (videos, news), aggression is less common than in interactive environments. Interestingly, none of the respondents had difficulty identifying the online spaces where aggression can be encountered. Respondents are aware of where they have experienced aggression, which suggests that the problem is real to them and well recognized.

Social media – the dominant source of illegal content (e.g., Facebook, Instagram, Twitter, TikTok) – why?

- Massive number of users and ease of content publication – social media is a dynamic environment where users publish huge amounts of material in real-time. Not all of it is effectively moderated.
- Spread of disinformation and fake news – social media platforms are one of the main channels for disseminating false information.

- Complexity of moderation mechanisms – although platforms have tools to detect and remove illegal content, their effectiveness is limited. Automated algorithms for detecting violations are often insufficient, and manual moderation cannot keep up with the scale of the problem.
- Anonymity and difficulty in law enforcement – users can create fake accounts, share materials, and then delete them before administrators detect them.

BEING A WITNESS TO AGGRESSION ON THE INTERNET

In the past 12 months, have you witnessed someone else becoming a victim of aggression on the Internet – for example, someone writing something negative or offensive about someone online?

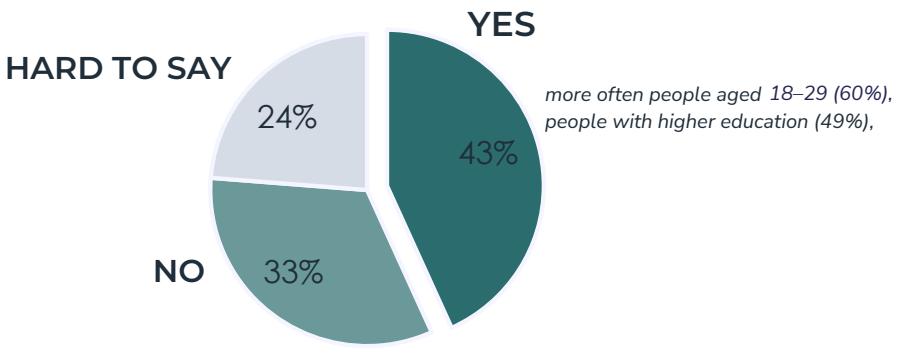
Sample size: N=108

Almost half (43%) of respondents witnessed aggression on the Internet, especially among younger people (18–29 years old) – 60%, and those with higher education (49%). However, as many as 33% did not notice such cases, and 24% had difficulty determining whether something was aggression or not. This may be due to lower activity on social media among older people, avoidance of toxic content, or a different definition of online aggression. 24% of respondents selected "Hard to say," suggesting that it is not always easy to clearly recognize aggression on the Internet. This may result from unclear boundaries between a joke and offensive content or a lack of awareness about hate speech.

Experts encountered aggression much more frequently (or were able to clearly define it) – 13 out of 16 respondents indicated this. Only one person stated that they had not observed aggression on the Internet in the past 12 months, and two had difficulty answering this question.

Being a witness to aggression on the Internet

In the past 12 months, have you witnessed someone else becoming a victim of aggression on the Internet – for example, someone writing something negative or offensive about someone online?
Base: Total N=108



This highlights the need for educational and systemic actions to increase awareness and improve the effectiveness of responses to online aggression.

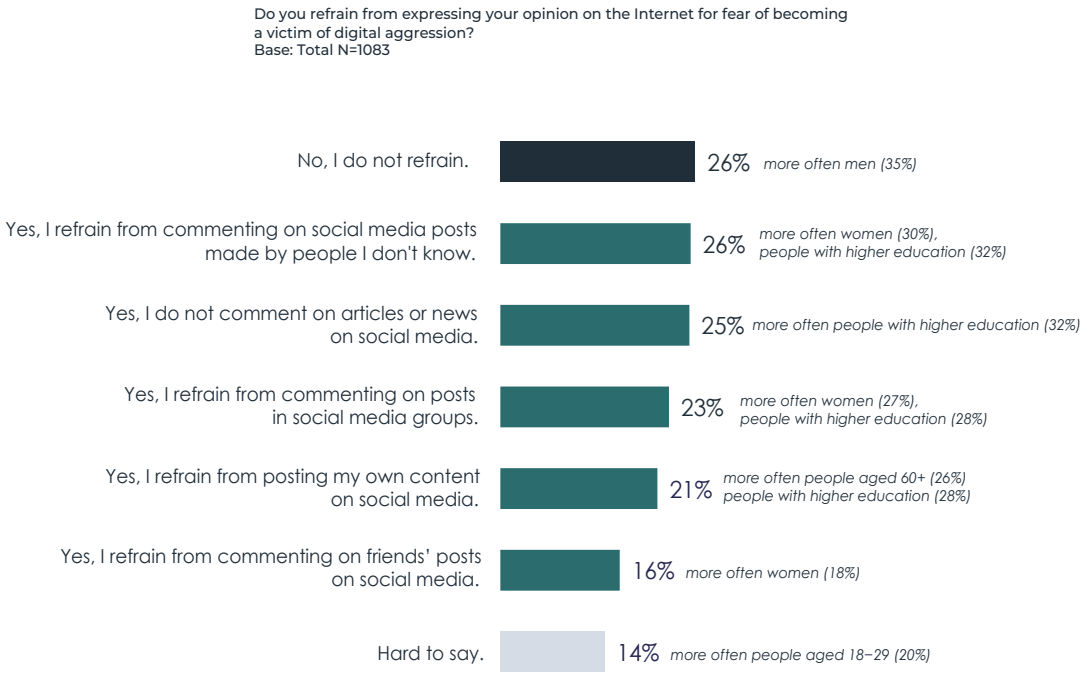
EXPRESSING OPINIONS AND FEAR OF AGGRESSION

Do you refrain from expressing your opinion on the Internet for fear of becoming a victim of digital aggression?
Sample size: N=1083

Only 26% of Poles do not limit their online activity due to fear of aggression. The same percentage avoids commenting on posts by strangers, especially women (30%) and individuals with higher education (32%). 25% refrain from commenting on articles or news on social media, particularly those with higher education (32%). 23% of Poles avoid commenting on posts in social media groups – more often women (27%) and people with higher education (28%). This indicates that public and group interactions are more often perceived as risky, leading to self-censorship. Older individuals and those with higher education are more likely to avoid posting their own content – 21% of Poles do not publish their own materials online. Interestingly, some users (16%) even refrain from commenting among friends, fearing negative reactions.

The experts we surveyed are also very reserved when it comes to commenting on posts online. Only 5 out of 16 do not refrain from writing comments due to fear of aggression.

Expressing opinions and fear of aggression



Only one in four Poles is not afraid to express their opinion online. Men are more likely to feel free of such concerns. The rest fear becoming victims of digital aggression, which leads them to refrain from posting comments under posts, articles, or in social media groups. They are relatively less likely to avoid commenting on posts shared by friends.

EXPERT COMMENT

PhD, Michał Chlebowski
Journalist, media expert
Department of Journalism
and Social Communication
SWPS University

The report clearly highlights the urgent need for action in two key areas: media education and the regulation of hate speech on the Internet. The data shows that the most commonly identified form of online aggression is hate speech – recognized by as many as 66% of respondents, with the percentage rising to 75% among those with higher education. It is also alarming that nearly half of the population has witnessed aggression against other Internet users, most often on social media platforms.

The problem is particularly severe among young people — they are the ones most frequently exposed to discrimination based on race, religion, or sexual orientation. At the same time, young users are the most active on the Internet, which makes them both potential victims and recipients of toxic content. This is why a robust media education program — covering topics such as recognizing hate speech, understanding the consequences of cyberbullying, and fostering a sense of responsibility for one's words — should be a priority starting at the primary school level.

The report also clearly indicates the insufficient effectiveness of current content moderation tools on social media platforms. Anonymity, the complexity of reporting systems, and the sheer volume of published content mean that many instances of hate go unaddressed. For this reason, more tailored legal regulations and greater accountability of digital platforms for user-generated content are necessary.

The fact that 10% of respondents say they have personally experienced online aggression, and 26% refrain from expressing their opinions online due to fear of verbal abuse, shows that this issue genuinely limits freedom of speech and impacts users' mental health. As a result, self-censorship emerges, and the public space on the Internet becomes increasingly closed and polarized.

What we need, therefore, is not only systemic reform but also grassroots educational efforts that will help rebuild a culture of dialogue online. Raising awareness about the consequences of hate speech remains essential. The data on suicide attempts and the types of aggression experienced by young people online is alarming. A collective societal effort is needed to make the Internet a safe space—free from violence and exclusion.

trolling
wyśmiewanie
race
osaczanie
stalking
dezinformacja
dręczenie
hate
dyskryminacja
doxxing
mocking
hate speech
szczucie
cyberbulling
dogpiling
mowa nienawiści
fake news
bullying
trole internetowe
discrimination
on-line outrage
religion
nękanie
disinformation

Knowledge of legal regulations and opinions about them

Is it easy to recognize what is illegal online?

EASE OF FINDING INFORMATION...
WHAT CONSTITUTES ILLEGAL CONTENT ON THE INTERNET

In your opinion, is it easy to find information about what constitutes illegal content on the Internet?
Sample size: N=1083

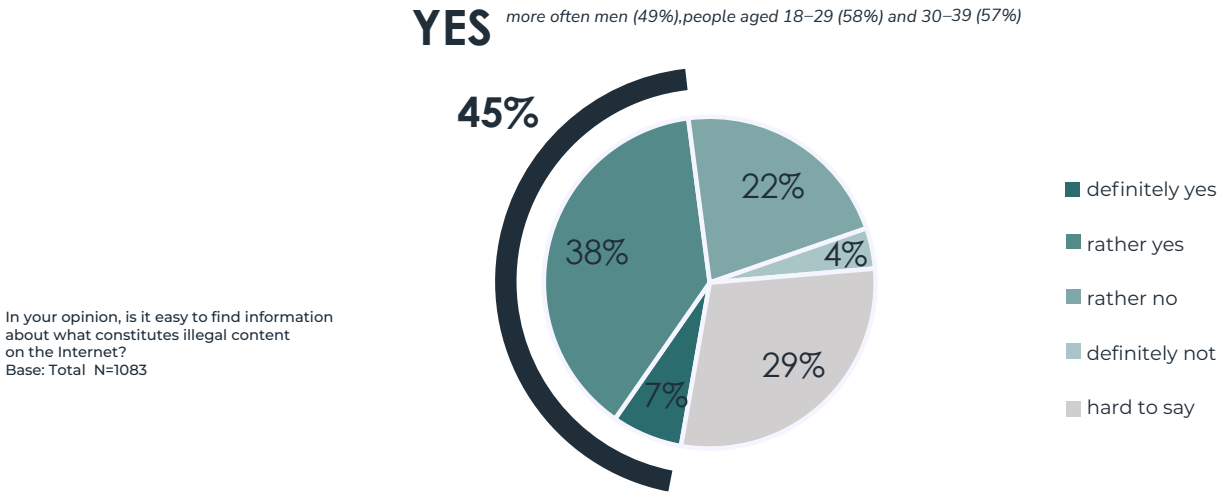
ASSESSMENT OF ACCESS TO KNOWLEDGE AND LEGAL REGULATIONS AND THEIR EFFECTIVENESS EASE OF FINDING INFORMATION...

In your opinion, is it easy to find information about legal regulations concerning illegal content on the Internet?
Sample size: N=1083

Almost half of the respondents (45%) believe that it is easy to find information about illegal content on the Internet (7% answered “definitely yes” and 38% chose “rather yes”). This opinion is more common among men (49%) and people aged 18–29 (58%) and 30–39 (57%). However, 26% believe it is not easy (4% “definitely not” and 22% “rather not”). This may suggest that legal regulations, moderation algorithms, and access restrictions influence the difficulty of finding such information. Interestingly, a significant proportion of respondents (29%) have difficulty expressing their opinion, which may indicate a lack of clear criteria for determining whether certain content is illegal. It may also stem from a lack of awareness of legal regulations regarding online content.

Experts rate access to information about what constitutes illegal content on the Internet more positively. Only 4 out of 16 assess this access poorly, and 2 had difficulty answering this question.

...What constitutes illegal content on the Internet

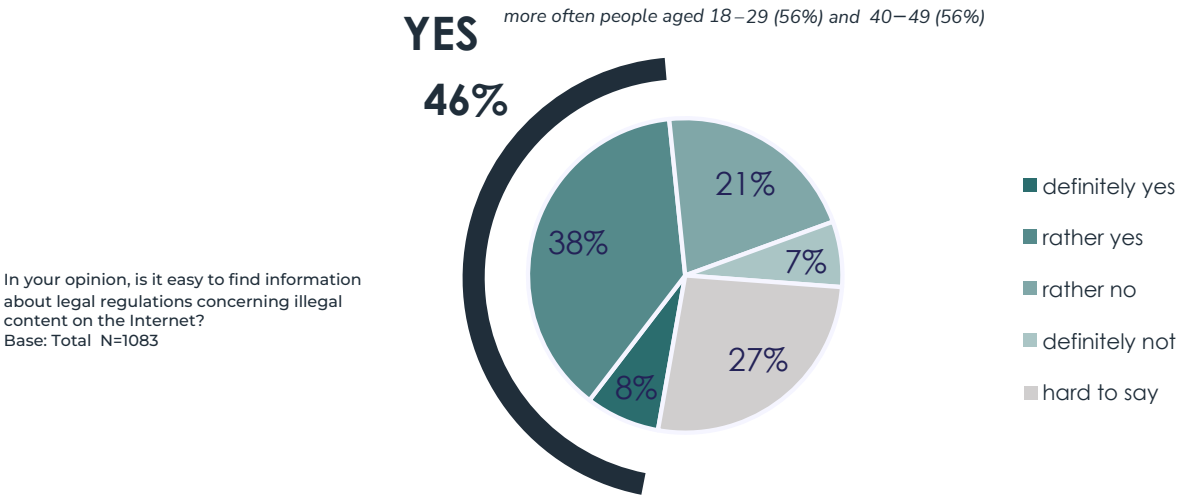


...ABOUT LEGAL REGULATIONS CONCERNING ILLEGAL CONTENT ON THE INTERNET

Nearly 46% of respondents believe that finding information about legal regulations is easy (8% answered "definitely yes," and 38% chose "rather yes"). This opinion is more common among people aged 18–29 (56%) and 40–49 (56%). However, 28% of respondents say that finding such information is difficult (7% answered "definitely no," and 21% selected "rather no"). This may result from the complex legal language, lack of understanding of the regulations, or information being scattered across various sources. Additionally, 27% of respondents find it difficult to express an opinion. This might be due to a lack of interest in the topic or unawareness of the existence of regulations concerning illegal content. These results suggest the need to create easily accessible guides written in clear, simple language to help users better understand internet law.

Experts have fewer difficulties finding information about legal regulations — 10 out of 16 consider access to such information easy, while 5 indicate challenges in this regard.

...Regarding legal regulations concerning illegal content on the Internet



EFFECTIVENESS OF LEGAL REGULATIONS IN COMBATING ILLEGAL CONTENT ON THE INTERNET

How do you assess the effectiveness of legal regulations in combating illegal content on the Internet?

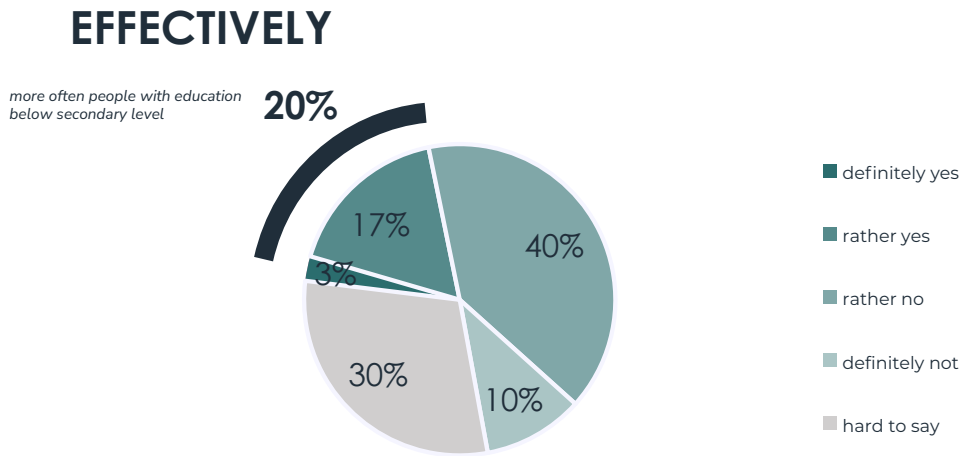
Sample size: N=1083

Only 20% of respondents consider the current legal regulations for combating illegal content on the Internet to be effective. This view is more commonly held by people with less than secondary education (24%), which may indicate less experience in analyzing law enforcement mechanisms online. As many as 50% of respondents believe that these regulations are rather or completely ineffective. The most skeptical are those with higher education, who may have a greater awareness of legal limitations. Additionally, 30% of respondents declare that they lack knowledge on this subject. The survey results indicate a need for better regulations, more effective content moderation, and efforts to raise public awareness about reporting violations.

Experts are even more critical in this area — none of the surveyed experts consider the current legal regulations to be fully effective. Three experts rated them as rather effective, while 11 out of 16 indicated that these regulations are ineffective. Two experts had difficulty providing an assessment.

EFFECTIVENESS OF LEGAL REGULATIONS IN COMBATING ILLEGAL CONTENT ON THE INTERNET

How do you assess the effectiveness of legal regulations in combating illegal content on the Internet?
Base: Total N=1083



EXPERT COMMENT

Krzysztof Żyto
Bącal Law Firm
Busiło Legal

The study results indicate a clear division of opinions – although nearly half of respondents (45%) believe it is easy to find information about illegal content online, experience shows that these assessments are often based on intuition rather than actual knowledge of the situation. It seems that for the average user, the primary and essential information about the legal status consists of descriptions of legal requirements (prohibitions and obligations). Only when such information raises doubts does the average user move on to the next stage of expanding their knowledge by searching for legal regulations.

The next question concerns precisely this issue—namely, the accessibility of information about legal regulations. When the laws are dispersed across various legal acts, it is important that searching for these acts allows for obtaining preliminary, general information in the form of a summary of legal acts and the topics they regulate, or accessible guides explaining basic concepts and issues. Specialized solutions of this kind are used in paid legal information systems, to which only a limited number of people have access.

The most worrying assessments concern the effectiveness of the regulations – only 20% of respondents consider them effective, while as many as 50% point to their ineffectiveness. This result clearly signals that the current regulations are not adapted to the rapidly changing online environment, and the law is failing to keep up with new challenges. Experts in particular, whose opinions carry significant weight, strongly condemn the existing approach, highlighting the urgent need to introduce modern and flexible legal solutions.

The above points, in my opinion, highlight the necessity to rethink the regulatory approach and amend the laws by simplifying them and supplementing with explanations, FAQs, and practical guides. Updating the law must take place in close cooperation with technical experts, sociologists, and social education specialists to create a legal framework that genuinely addresses the challenges of the 21st century. A positive step towards such an exchange of ideas is the NASK study and Report. Only through the collaboration of a broad group of specialists does the regulatory system have a chance to become more understandable, which will increase the likelihood of its effective application in practice and consequently contribute to better protection of the online space against illegal content.

Summary

AWARENESS VS. REALITY

Poles are fairly well aware of which types of content on the Internet are illegal. Out of 8 categories listed, on average they identify 6 as illegal. Child pornography is considered illegal by nearly every Pole (91%). The vast majority claim they do not encounter such content online (81%). The top 3 content types most frequently recognized as illegal also include personal data breaches (85%) and terrorist content (84%). However, these two are also among the least frequently encountered online. Three-quarters of Poles regard hate speech as a violation, and 55% encounter it online at least several times a month. Disinformation is less often associated with illegality (64% of respondents), yet over half (56%) encounter such information several times a month. Discrimination and unfair competition acts are also relatively less often recognized as illegal (below 70% of responses).

OPINIONS ABOUT ILLEGAL CONTENT

Less than half of Poles (42%) believe they have ever encountered illegal content on the Internet. This relatively low percentage likely results, among other reasons, from the fact that some people are unaware that areas such as discrimination or disinformation, which they come into contact with, also constitute prohibited acts. Those who report some experience with illegal content online most often encounter it on social media platforms (78% of respondents indicated this). Awareness of where to report illegal content is generally good — only 23% of respondents did not know where to report it. The most popular reporting bodies are the Police and platform administrators of social media/services, with the latter more frequently chosen. Other reporting options are indicated much less often. Importantly, although most Poles know where to report violations and are aware that illegal content negatively impacts society (90%), and believe that reporting can lead to content removal (71%), nearly half of those who encounter such content take no action (47%).

Opinions on the support provided by new technologies, such as artificial intelligence, in combating illegal content on the Internet are quite mixed. This is likely because this area is not yet sufficiently familiar to Poles to allow for definitive opinions. Nearly 40% of respondents believe that new technologies help in detecting and removing illegal content online. At the same time, a similar percentage are unable to assess this, probably due to a lack of sufficient knowledge. Men are more likely to be convinced of AI's support in this area.

Poles also do not have a clear stance regarding concerns about freedom of speech when it comes to the automatic removal of suspicious content — nearly half are not worried about this, but one in three sees it as a threat (more often men), and one in five have no opinion on the matter. Meanwhile, half of the respondents believe that controversial content, as long as it aligns with the principles of freedom of speech, should be legal (53%). This view is more commonly shared by men and better-educated individuals.

HATE ONLINE

Hate speech and mocking others are the most common forms of aggression appearing on the Internet, according to Poles. 10% of Poles declare that in the past 12 months they were personally exposed to aggression directly targeting them. More often, they witnessed aggression against others (43%). In both cases, these violations most frequently occurred on social media. Due to fear of digital aggression, Poles generally avoid commenting or expressing opinions online. They less often refrain from commenting on posts by their friends on social media, and only one in four people do not hold back from such activities. Men are more likely to lack such reservations.

KNOWLEDGE OF LEGAL REGULATIONS AND OPINIONS ABOUT THEM

Notably, Polish society is not convinced about the effectiveness of actions against illegal content on the Internet—only 20% believe that legal regulations in this area are effective, and slightly more (26%) think that social media platforms efficiently remove illegal content. Overall, the prevailing belief (44%) is that both removing illegal content and blocking the author's account are equally effective methods of combating illegal content online.

INDEX OF TERMS

Illegal content – means information that, by itself or through reference to an action, including the sale of products or the provision of services, is not compliant with the law of the European Union or the law of any Member State that is consistent with EU law, regardless of the specific subject matter or nature of that law **[Article 3(h) of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on the Digital Services Act and amending Directive 2000/31/EC (DSA), Official Journal of the EU L 277/1 of 27.10.2022].**

The concept of "illegal content" should be defined broadly to include information concerning illegal content, products, services, and activities. This term should be understood in particular as referring to information, regardless of its form, that under applicable law is either inherently illegal—such as illegal hate speech, terrorist content, or unlawful discriminatory content—or becomes illegal under current regulations because it relates to illegal activities. For example, this may include sharing images depicting the sexual abuse of children, unlawful sharing of private images without consent, cyberstalking, the sale of non-compliant or counterfeit products, selling goods or providing services in violation of consumer protection laws, unauthorized use of copyrighted materials, illegal offering of accommodation services, or illegal sale of live animals **[recital 12 of the DSA preamble]**.

It does not matter whether the illegal nature of the information or action arises from EU law or from national law that is consistent with EU law, nor what the exact nature or subject of that law is. The catalog of illegal content includes both behaviors legally classified as crimes and offenses, as well as behaviors violating administrative regulatory requirements—thus, some behaviors are subject to criminal sanctions while others are subject to administrative penalties. Despite this complex situation, it is necessary to provide an illustrative list of types of illegal content, starting from those that may facilitate the commission of terrorist offenses, crimes against life and health, such as disseminating pornography involving minors or animals, or violating personal rights. The example list should also include content for which the person posting it does not have intellectual property rights, industrial property rights, or trademark rights. This catalog should also cover content related to goods that do not meet safety requirements. Among illegal content, the law implementing the Digital Services Act should explicitly identify content prohibited under the Charter of Fundamental Rights, such as content inciting violence and hatred against a group of persons based on sex, age, race, skin color, ethnic or social origin, genetic features, language, religion or beliefs, political or any other opinions, nationality, membership of a national minority, property, birth, disability, age, and sexual orientation. To this group of illegal content should also be added content inciting hatred against a population group or individual because of their national origin, ethnic, racial, religious grounds, or due to lack of religious affiliation. The catalog of illegal content should also include content threatening public safety and order, as well as promoting actions contrary to the Polish national interest and attitudes and views inconsistent with morality and the public good. The catalog should also cover advertising of certain products and services such as alcohol, tobacco, drugs, gambling, prescription medicines, pharmacies, or tanning salons, misleading advertising, covert advertising, or unfair advertising. An exemplary catalog of illegal content should also indicate the illegality of content that may be shared by a digital service provider if certain conditions are not met. These include, for example: pornographic content distributed without effective safeguards preventing access by minors; advertising without

appropriate labeling; or advertisements for medical devices, medicinal products, and food for special dietary uses without the appropriate warnings required under separate regulations. **[K. Chałubińska-Jentkiewicz, Legal Protection of Digital Content, Warsaw 2022].**

Terrorist content – means materials of at least one of the following types; namely, materials that: a) incite the commission of one of the offenses referred to in Article 3(1)(a)–(i) of Directive (EU) 2017/541, where such materials, directly or indirectly, for example by glorifying terrorist acts, support the commission of terrorist offenses and thereby create a danger of committing one or more such offenses; b) urge a person or group of persons to commit or contribute to the commission of one of the offenses referred to in Article 3(1)(a)–(i) of Directive (EU) 2017/541; c) urge a person or group of persons to participate in the activities of a terrorist group, within the meaning of Article 4(b) of Directive (EU) 2017/541; d) provide instructions on the manufacture or use of explosives, firearms, or other types of weapons or toxic or dangerous substances, or on other specific methods or techniques for committing or contributing to the commission of one of the terrorist offenses referred to in Article 3(1)(a)–(i) of Directive (EU) 2017/541; e) create a risk of committing one of the offenses referred to in Article 3(1)(a)–(i) of Directive (EU) 2017/541. **[Article 2(7) of Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on preventing the dissemination of terrorist content online, OJ L 172/79 of 17.05.2021]**

Terrorist offenses include: a) attacks against human life that may cause death; b) attacks against the physical integrity of a person; c) kidnapping or taking hostages; d) causing extensive damage to government facilities or public utilities, transportation systems, infrastructure including information systems, fixed platforms located on the continental shelf, public places, or private property—if such damage may endanger human life or cause serious economic loss; e) seizure of an aircraft, watercraft, or other means of public or freight transport; f) manufacturing, possessing, acquiring, transporting, supplying, or using explosives or weapons, including chemical, biological, radiological, or nuclear weapons, as well as research on such weapons and development of chemical, biological, radiological, or nuclear weapons; g) releasing dangerous substances or causing fires, floods, or explosions resulting in danger to human life; h) disrupting or interrupting water supplies, electricity, or any other essential natural resources resulting in danger to human life; i) unlawful interference with systems referred to in Article 4 of Directive 2013/40/EU of the European Parliament and of the Council (1), in cases where Article 9(3) or Article 9(4)(b) or (c) of that Directive applies, and unlawful interference with data referred to in Article 5 of that Directive, in cases where Article 9(4)(c) of that Directive applies **[Article 3(1)(a)–(i) of Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism, repealing Council Framework Decision 2002/475/JHA, and amending Council Decision 2005/671/JHA, OJ L 88/6, 31.3.2017].**

Pornographic content – any material depicting a child participating in actual or simulated behaviors of an explicitly sexual nature, as well as any representation of a child's genital organs primarily for sexual purposes **[Article 20(2) of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, drawn up in Lanzarote on 25 October 2007, Official Journal of 2015, item 608].**

Pornographic content may depict an image of a minor that has been created or altered (participating in a sexual act). This refers to the protection of both real minors whose image has been manipulated,

as well as fictional minors (i.e. pornography featuring computer-generated images of children or pornographic animated films that depict scenes involving children, even though no real child was involved in the production of such material at any stage). Under Article 202 § 4 of the Polish Penal Code, the production, distribution, presentation, storage, or possession of such content is subject to criminal liability **[Supreme Court decision of January 18, 2021, case no. IV KK 251/20, LEX no. 3111703].**

Piracy-as-a-Service - a service facilitating illegal broadcasts. It involves providing a package of ready-made services that enable the creation, operation, and monetization of a pirated enterprise. These services violate the law by replicating legitimate streaming services. Operators providing unauthorized retransmissions have developed resilience strategies that allow them to circumvent law enforcement mechanisms. Therefore, it is important to closely monitor the development of new forms of piracy and resilience strategies, which may also affect other types of content and impact the ability of rights holders to effectively enforce their rights, taking into account in particular technological changes and new business models. **[Recital 4 of Commission Recommendation (EU) 2023/1018 of 4 May 2023 on combating online piracy of sports and other live events, OJ L 136/83].**

Personal data breach – means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.**[Article 4(12) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – GDPR), OJ L 119/1 of 4.5.2016].**

Hate speech – refers in particular to racist and xenophobic crimes. These are intentional acts that include: a) public incitement to violence or hatred directed against a group of persons defined by reference to race, skin color, religion, descent, or national or ethnic origin, or against a member of such a group, b) the commission of the act referred to in point (a); c) publicly approving of, denying, or grossly trivializing genocide, crimes against humanity, and war crimes as defined in Articles 6, 7, and 8 of the Statute of the International Criminal Court, committed against a group of persons defined by reference to race, colour, religion, descent, or national or ethnic origin, or against a member of such a group, where the conduct is likely to incite violence or hatred against that group or a member of it; d) publicly approving of, denying, or grossly trivializing the crimes referred to in Article 6 of the Charter of the International Military Tribunal annexed to the London Agreement of 8 August 1945, committed against a group of persons defined by race, colour, religion, descent, or national or ethnic origin, or against a member of such a group, where the conduct is likely to incite violence or hatred against that group or a member of it. The term „hatred" shall be understood as referring to hatred based on race, colour, religion, descent, or national or ethnic origin. **[Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, OJ L 328, 6.12.2008, p. 55–58.]**

Stalking – persistent harassment of another person or someone close to them, which causes that person to feel, due to the circumstances, a justified sense of threat, humiliation, or distress, or significantly infringes on their privacy **[Article 190a §1 of the Polish Penal Code].**

Disinformation – tan act involving the creation and sharing of false information in bad faith, or the manipulative presentation of true information intended to generate false beliefs. It refers to content produced either with the intent to cause harm or as a result of reckless repetition of unverified claims. Disinformation can be categorized using two criteria: its relation to truth and the intention behind its creation and dissemination. Thus, disinformation should be understood as verifiably false, misleading, or even true content (used to create a false impression on a given subject), which is created, presented, and distributed to gain economic advantage or to mislead public opinion, potentially causing public harm **[K. Chałubińska-Jentkiewicz, Legal Boundaries of Disinformation in Mass Media, Toruń 2023, p. 103].**

According to the EU Code of Practice on Disinformation (Luxembourg 2025), disinformation is defined as: „False, inaccurate, or misleading information created, presented, and disseminated for profit or with the deliberate intent to cause public harm." **[http://Code_of_Conduct_on_Disinformation_f9bhfVbrSm6IEbiMmtGRVsLHZKA_112678.pdf]**

Trolling – refers to deliberate, provocative, and antisocial behavior online aimed at inciting arguments or emotional reactions from other users. It typically involves posting controversial, inflammatory, or offensive content. Trolls often use tactics such as propaganda, manipulation, and distortion of facts to provoke responses and disrupt discussions. **[M. Nowikowska, "The Phenomenon of Trolling on the Internet," in: Media in the Digital Era, eds. K. Chałubińska-Jentkiewicz, M. Nowikowska, K. Wąsowski, Warsaw 2021, p. 194].**

REFERENCES

1. **Cert.pl**. https://cert.pl/o-nas/

2. **European Commission**. (2018). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018DC0236

3. **Jhaver, S., Ghoshal, S., Bruckman, A., Gilbert, E.** (2018). Online Harassment and Content Moderation: The Case of Blocklists. ACM Transactions on Computer-Human Interaction, 25(2): 1–33. https://doi.org/10.1145/3185593

4. **Just IDEA**. Piractwo – definicja. https://justidea.agency/pl/slownik/piractwo/?utm_source=chatgpt.com

5. **Kodeks karny** (Dz.U. j.t. z 2025 r. poz. 383).

6. **Kowalski, S., Tulli, M.** (2003). Zamiast procesu. Raport o mowie nienawiści. Warszawa: Wydawnictwo W.A.B. ISBN 83-89291-58-4

7. **NASK / Piechna, J.** (2019). Szkodliwe treści w Internecie. Nie akceptuję, reaguję! Poradnik dla rodziców. Warszawa. https://cyberprofilaktyka.pl/publikacje/Szkodliwe%20tre%C5%9Bci%20w%20Internecie_www.pdf

8. **Pundak, C., Steinhart, Y., Goldenberg, J.** (2021). Nonmaleficence in Shaming: The Ethical Dilemma Underlying Participation in Online Public Shaming. Journal of Consumer Psychology, 31: 478–500. https://doi.org/10.1002/jcpy.1227

9. **Rada Europy.** Rekomendacje R (97) 20 nt. mowy nienawiści. https://www.mowanienawisci.info/post/rekomendacja-r-97-20-komitetu-ministrow-rady-europy-nt-mowy-nienawisci/

10. **Rzecznik Praw Obywatelskich**. Czym jest dyskryminacja? https://bip.brpo.gov.pl/pl/content/czym-jest-dyskryminacja

11. **Serwis RP**. Doxing – nowe zjawisko i cyberzagrożenie. https://www.gov.pl/web/baza-wiedzy/doxing--nowe-zjawisko-i-cyberzagrozenie?utm_source=chatgpt.com

12. **TECHPEDIA**. Legalność dziecięcej pornografii na świecie. https://www.techpedia.pl/index.php?str=tp&no=32622

13. **Ustawa o świadczeniu usług drogą elektroniczną** (Dz.U. j.t. z 2024 r. poz. 1513).

14. **Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO)** – art. 4 pkt 12. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016R0679

15. **Rozporządzenie UE o usługach cyfrowych (Digital Services Act)** (2022). https://eur-lex.europa.eu/PL/legal-content/summary/digital-services-act.html

16. **Wallace, P.** (2003). Psychologia Internetu. Poznań: Rebis. ISBN 83-7301-075-0

17. **WHO (World Health Organization)**. (2024). A focus on adolescent peer violence and bullying in Europe, central Asia and Canada. HBSC international report from the 2021/2022 survey, vol. 2. ISBN: 978-92-890-6092-9. https://iris.who.int/bitstream/handle/10665/376323/9789289060929-eng.pdf?sequence=2&isAllowed=y

18. **Wydział Prewencji Zagrożeń CAT ABW.** Treści o charakterze terrorystycznym w Internecie. https://tpcoe.gov.pl/cpt/materialy/1839%2CTresci-o-charakterze-terrorystycznym-w-Internecie.html?utm_source=chatgpt.com

PART III

Infringement of intellectual property rights

Infringement of intellectual property rights in the context of illegal content and the trade in counterfeit goods on the Internet.

The illegal trade in counterfeit goods poses a significant and growing threat in the globalized economy. Its harmful impact on consumers, economic growth, innovation, the rule of law, the environment, and ultimately on trust in well-functioning global markets should not be underestimated.

Introduction

Online trade is constantly evolving, taking on new forms and expanding into new areas of exploitation. It is no longer limited to e-commerce stores or major online marketplaces, but also includes issues such as online streaming, paid broadcasts of sports and artistic events, as well as the trade in prohibited and counterfeit products on the so-called Deep Web and Dark Web.

E-commerce, more than other business models, often involves the sale of products and services based on intellectual property and its licensing. Music, images, photographs, software, design, training and educational modules, films, and systems, etc. can all be subjects of e-commerce, where intellectual property is the primary component of value in a transaction. Legal protection is crucial because valuable items traded online must be safeguarded by exclusive rights and supported by technological security systems. Otherwise, these assets may be stolen or counterfeited, and entire businesses can be destroyed as a result.

The total contribution made to the EU economy by sectors that heavily rely on intellectual property rights amounts to approximately 42% of GDP (€5.7 trillion) and accounts for 28% of employment (plus an additional 10% through indirect employment in sectors that do not rely intensively on intellectual property rights). Due to the high value associated with intellectual property rights, their infringement represents a lucrative criminal activity, resulting in significant costs for rights holders and the economy as a whole. According to a study conducted by the European Union Intellectual Property Office (EUIPO)[1], this issue is particularly significant in the context of the current crisis triggered by the pandemic.

1 EUIPO, *Status report on IPR infringement, 2020*, https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2020_Status_Report_on_IPR_infringement/2020_Status_Report_on_IPR_infringement_en.pdf (data dostępu: 15.05.2025).

According to estimates from a 2019 study conducted by the EUIPO and the OECD on intellectual property rights infringement in international trade, such infringements may have accounted for as much as 3.3% of global trade in 2016. Counterfeit goods represent as much as 6.8% of imports into the EU, amounting to €121 billion annually. These figures are significantly higher than those published in 2016, indicating that the problem has worsened in recent years and that counterfeiting has become increasingly attractive to criminal organizations.

As technology and distribution channels develop, alongside the growing range of counterfeit products, the way these organizations operate is becoming increasingly complex. To distribute their products and promote the distribution and consumption of illegal digital content, counterfeiters rely heavily on Internet-based business models. Websites offering counterfeit goods benefit from additional revenue through so-called high-risk advertisements (such as adult sites, gaming, and malware), and paradoxically, also from ads of legitimate brands. For these legitimate brands, advertising on such sites results in a double loss — damage to their own brand reputation and the unintended legitimization of the websites where their ads appear.

In addition to analyzing the supply of counterfeit goods and pirated content, a study was also conducted on the demand side—that is, the attitudes of EU citizens (consumers) towards intellectual property rights, specifically their willingness to use goods and services that infringe these rights. What motivates them to purchase counterfeit goods and gain illegal access to copyrighted content? The main factors are low prices, easy accessibility, and a low level of social stigma associated with such activities.

The latest data on the volume of international trade in counterfeit and pirated products shows that it has already reached €460 billion.

This accounts for approximately 3.3% of global trade and nearly 7% of EU imports. An important aspect of this is online trade and access to illegal content on the internet. The former—online trade—is associated with infringements of intellectual property rights such as trademarks (protecting brands), industrial designs (protecting shapes or designs), patents (protecting technology), and rights to new plant varieties. The latter—access to illegal content online—most often infringes intellectual property rights in the form of copyright.

Digital Piracy in the EU

At the end of 2024, data on digital piracy in the EU became available. According to this data[2], Europeans access illegal online content an average of 10 times per month. The latest report indicates that internet piracy among European internet users has remained steady compared to the previous year, with an average of 10 instances of illegal content access per internet user per month. Television content accounts for half of all cases of illegal access—an average of 5 accesses per internet user per month in the EU. Additionally, the number of illegal Internet Protocol Television (IPTV) sites has increased; in 2023, visits to pirate IPTV sites rose by 10%.

The report by the European Union Intellectual Property Office (EUIPO) showed that digital piracy across the entire EU remains at a high level.

2 EUIPO, *Online copyright infringement in the European Union – films, music, publications, software and TV (2017-2023), 2024*, https://www.euipo.europa.eu/en/publications/online-copyright-infringement-in-the-european-union-films-music--publications-software-and-tv-2017-2023 (data dostępu: 15.05.2025)

This trend is visible across all categories of online content, except for publications, where piracy levels have decreased, and music, where piracy has increased compared to early 2023. Regarding overall piracy, the EUIPO report showed that internet users in Austria (8.9), Spain (8.5), Poland (8.3), Romania (7.9), Germany (7.7), and Italy (7.3) access illegal content websites at rates below the EU average.

Streaming is the most common method of accessing pirated content. An alarming trend has been observed in illegal streaming—in 2023, visits to pirate IPTV websites increased by 10%. The study estimated that up to 1% of internet users in the EU may have subscribed to illegal IPTV sites within just two years, excluding existing users who subscribed before 2022. The EUIPO study also found that internet users are more likely to access pirated music and publications via mobile devices, whereas when it comes to watching illegal television content, users tend to prefer using their desktop computers.

It was found that economic and social factors contributing to piracy include income inequality, youth unemployment, and the proportion of young people in society. The study indicates that higher levels of income inequality and a larger share of young people in the population correlate with higher levels of piracy. Conversely, higher GDP per capita and greater awareness of legal content sources are associated with lower piracy rates.

Copyright piracy involves several methods of distributing unauthorized online content, such as illegal subscription services and open internet streams funded by advertising revenue. Providers of these services use sophisticated techniques to evade detection, often exploiting legitimate content distribution platforms.

The Importance of Sectors Heavily Relying on Intellectual Property Rights for Socio-Economic Development

Currently, the EU economy includes 357 sectors that heavily rely on intellectual property rights. Among these sectors, 229 (64%) make intensive use of intellectual property rights in relation to more than one type of intellectual property[3].

Sectors heavily reliant on intellectual property rights generated 29.7% of all jobs in the EU between 2017 and 2019, up from 28.9% in 2014–2016 (accounting for minor methodological differences between studies). On average, over 61 million people were employed in these sectors during this period across the EU. These sectors also created an additional 20 million jobs by supplying goods and services to the sectors heavily relying on intellectual property rights. Taking this indirect employment into account, the total number of jobs related to intellectual property rights amounted to as many as 82 million (39.4%).

During the same period, sectors heavily reliant on intellectual property rights generated over 47% of the EU's GDP, totaling €6.4 trillion.

3 EUIPO-EPO, *IPR-intensive industries and economic performance in the European Union. Industry-level analysis report, fourth edition, 2022*, https://www.euipo.europa.eu/en/publications/ipr-intensive-industries-and-economic-performance--in-the-european-union-industry-level-2022 (data dostępu: 15.05.2025).

They were also responsible for the majority of the EU's trade with the rest of the world and generated a trade surplus of €224 billion, contributing to maintaining the balance in the EU's external trade.

Sectors heavily reliant on intellectual property rights make a significant contribution to the functioning of the EU internal market. They account for over 75% of intra-EU trade. While countries such as Germany, France, Italy, and the Netherlands lead in creating new intellectual property rights, other countries—such as Hungary, Poland, and Estonia—also greatly benefit from the division of labor within sectors heavily reliant on intellectual property rights. In total, nearly 7 million jobs related to intellectual property rights in Member States are created by businesses from other Member States, with the share of such jobs in these sectors exceeding 30% in some countries.

Wages for employees in sectors heavily reliant on intellectual property rights are significantly higher—on average by 41%—compared to other sectors. It is also worth noting that the value added per employee is higher in these sectors than in other parts of the economy. A comparison of the results of this study with those from a 2019 study shows that the relative contribution of sectors heavily reliant on intellectual property rights to the EU economy increased between the periods 2014–2016 (2019 study) and 2017–2019 (2022 study), taking into account changes in the list of these sectors.

Among the sectors heavily reliant on intellectual property rights, the economic importance of those involved in developing technologies aimed at mitigating the effects of climate change, as well as sectors associated with green trademarks, has increased in recent years.

Sectors heavily reliant on patents related to technologies for mitigating the effects of climate change or green trademarks accounted for 9.3% of employment and 14.0% of GDP in the EU between 2017 and 2019, as well as a significant share of the EU's external trade. These are just basic figures from the analysis of EU countries—no studies have been conducted, and data directly concerning Poland are lacking.

The Importance of Younger Generations and the Scale of the Grey Market

Alarmingly, Generation Z currently shows greater tolerance for purchasing illegal goods, according to a report prepared by The Economist. The World Economic Forum estimates that economic losses resulting from illegal trade are equivalent to 3% of global GDP. According to the United Nations Conference on Trade and Development (UNCTAD), the global economy loses around 2 trillion dollars annually due to this..

Participants of the sixth World Summit Against Illegal Trade: Central and Eastern Europe, organized by The Economist, discussed the urgent need to combat the grey market, including regional cooperation between governments, law enforcement agencies, and businesses. The event was held in Poland for the first time in 2022. While the grey market remains a problem, Poland can set standards in many areas in the fight against this phenomenon. According to Eurostat data, Poland ranked first in Europe in 2021 for increasing VAT revenues between 2008 and 2021. This was the result of a series of implemented measures, including the introduction of the mandatory VAT control file and the split payment mechanism, commented Piotr Arak, then Director of the Polish Economic Institute.

At the summit, a report titled "Illegal Trade: Scale, Scope, Flows" prepared by The Economist was presented. It revealed that only 37% of Generation Z representatives (those born between 1997 and 2003) consider buying illegal goods unacceptable. Meanwhile, about 31% of Generation Z and 26% of millennials believe that consuming illegal goods is acceptable in cases of product shortages or unfavorable economic conditions.

Experts from the UN Global Compact Network Poland estimate that the total share of the grey economy in Poland during the pandemic was between 18% and 20%. Similar estimates are presented by the Institute for Economic Forecasts and Analysis, which predicts that the grey economy's contribution to Poland's GDP this year will amount to 18.9% (a total of 590 billion PLN). However, efforts to combat the grey economy have significantly accelerated since 2017, when the National Revenue Administration (Krajowa Administracja Skarbowa, KAS) was established.

Combating illegal trade in goods is crucial not only for fiscal reasons but also for protecting the security of Poland and the entire European Union. The Covid-19 pandemic caused a significant increase in e-commerce, while the war in Ukraine led to the introduction of various restrictions on the transport of goods to and from third countries. Customs and tax administrations must keep up with these changes and respond to new challenges. The pandemic and the war did not weaken the effectiveness of our actions because we quickly implemented appropriate mechanisms and procedures. This was also possible because the level of digitalization of the National Revenue Administration (KAS) has significantly increased in recent years — said Mariusz Gojny, then Deputy Minister of Finance and Deputy Head of KAS. The report prepared by The Economist also indicates that illegal trade on the Internet has become easier due to the development of online sales platforms. As many as 64% of respondents believe that illegal goods have become easier to obtain since the outbreak of the pandemic, and that consumers are now more willing to purchase them online. The findings are a cause for serious concern, as trade in counterfeit and pirated goods accounted for up 2.5% of global trade in 2019.

Considering imports to the EU alone, counterfeit goods accounted for up to 5.8% of total imports. These figures are higher than in previous years, and the illegal trade in counterfeits poses a serious threat to modern, open, and globalized economies.

The trade in counterfeit goods also poses a serious threat to the modern, efficient, and forward-looking global economy. It not only strikes at the very heart of the engine of sustainable economic growth but also presents significant risks to health (e.g., counterfeit car parts, fake batteries) and to the environment (e.g., counterfeit chemicals or pesticides).

To understand and combat the risks associated with the trade in counterfeit and pirated goods, governments need up-to-date information on its scale, scope, and trends. The Covid-19 pandemic has only intensified and deepened the impact of dangerous counterfeit trade, and in most cases, this crisis exacerbated already existing trends. This was particularly evident in the case of counterfeit medicines and other high-risk products such as alcoholic beverages, where disrupted supply chains and shifting demand created new areas of criminal activity. However, the widespread and rapid increase in counterfeit products was not limited to medicines and personal protective equipment—it also affected many other goods that may pose risks to health and safety, such as consumer goods and spare parts.

More Illegal Trade or More Dangerous Counterfeits?

The latest study, published in 2022 by the OECD and EUIPO[4], provides a quantitative assessment of the scope of trade in counterfeit products that pose risks to health, the environment, and safety, as well as the trends observed in this area. It is based on the analysis of a unique dataset compiled from customs seizures and enforcement records from various countries, combined with structured interviews conducted with enforcement experts.

In principle, all counterfeit goods carry some level of risk and can pose a threat to users. To account for varying degrees of danger, the study employed two approaches to define the scope of hazardous counterfeits. The broader approach includes products that are required to meet specific safety standards. These products fall under the jurisdiction of the U.S. Food and Drug Administration (FDA) or are covered by the proposed U.S. SHOP SAFE Act. Using this approach, the most frequently encountered dangerous counterfeits include clothing items, automotive parts, optical and medical devices, and pharmaceuticals.

Ult was found that the largest exporters of dangerous counterfeits are China and Hong Kong (China), accounting for more than three-quarters of all customs seizures. Due to the growing popularity of online trade, postal shipments have become the most common method for sending dangerous counterfeits. This significantly complicates inspection and detection procedures and reduces the risk of the crime being uncovered and penalized. The main destinations for small parcels containing hazardous items were the European Union and the United States. However, in terms of the value of customs seizures, maritime transport clearly dominates. The distribution of destinations for dangerous counterfeit goods shipped by sea was more varied, with Gulf countries topping the list.

A more targeted, narrower approach focuses only on food products, pharmaceuticals, cosmetics, and categories of goods most frequently subject to safety warnings and market withdrawals. Within this framework, the most commonly sold dangerous counterfeits include perfumes and cosmetics, clothing, toys, automotive spare parts, and pharmaceuticals. The majority of these goods originated from China (55% of all global customs seizures) and Hong Kong (China) (19%).

Sixty percent of the seized hazardous goods were shipped by mail, while maritime transport dominated in terms of the total value of seized items. Of all dangerous counterfeit products destined for the EU market, 60% were linked to online sales. However, their share in terms of value was relatively small. Among dangerous counterfeits ordered online, cosmetics were the most frequently purchased, followed by clothing, toys, and automotive spare parts. The majority of these goods (75%) were shipped from China.

The existing quantitative analysis of illegal trade in counterfeit and pirated goods indicates that the range of products targeted for counterfeiting is very broad and continuously expanding. Any product whose intellectual property increases the economic value for rights holders becomes a target for counterfeiters. Therefore, counterfeiting affects not only luxury goods but also intermediate products and a wide array of common consumer products. In all these cases, counterfeits cause economic damage by destroying jobs, stealing profits, and reducing incentives for innovation.

At the same time, for some products, counterfeits are often of low quality, which poses significant risks to consumers. These include health hazards (e.g., counterfeit pharmaceuticals, toys, or food products), safety risks (e.g., counterfeit automotive spare parts, counterfeit batteries), and environmental threats (e.g., counterfeit chemicals or pesticides).

4 OECD-EUIPO, *Illicit Trade. Dangerous Fakes. Trade in counterfeit goods that pose health, safety and environmental risks, 2022*, https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/03/dangerous-fakes_08dedd45/117e352b-en.pdf (data dostępu: 16.05.2025).

For all these products, legitimate suppliers must comply with health, safety, and environmental regulations to ensure that their products do not cause harm. Counterfeiters are not bound by these regulations, which means that the fake goods they offer can pose serious risks to health, safety, and the environment.

In addition to the harmful risks to health and safety, counterfeiting has far-reaching negative economic effects. OECD and EUIPO previously conducted a study on counterfeiting and piracy in the pharmaceutical sector, which documents the damaging impacts on economies. Further research has supplemented this work with additional analysis of the health, safety, and environmental risks posed by counterfeits across multiple sectors, including food products and personal protective equipment, where counterfeit items often fail to meet standards and are stored and transported under poor conditions, posing serious threats to consumer health. Toys and batteries are also examined, as counterfeit versions are frequently produced without any safety standards, thus potentially creating significant hazards. Chemicals and pesticides are counterfeited as well, and these fake products, which do not comply with environmental protection regulations, can cause substantial environmental damage.

Measuring the size and scope of counterfeiting is generally difficult due to the covert nature of the phenomenon. Although significant progress has been made through econometric work in estimating its prevalence in international trade, there is a lack of studies on the risks posed by counterfeit products, which mostly rely on unverified information.

Trade, moving online, carries with it a shadow of illegality.

As indicated by the aforementioned data, the scale of abuses in e-commerce to facilitate the trade of counterfeit goods is rapidly increasing. In recent years, e-commerce has grown quickly because consumers are becoming increasingly confident in ordering goods and services online and through social media.

The number of businesses engaged in business-to-consumer (B2C) e-commerce is steadily increasing. Between 2018 and 2020, online retail sales[5], which are part of total B2C sales, grew by 41% in the world's major economies, while total retail sales increased by less than 1%. This growth was driven by the Covid-19 pandemic, as consumers shopped online during lockdowns to avoid visiting physical stores. During the pandemic, the online environment also became a more popular target for illegal trade. Cybercrime enforcement agencies recorded an increase in various electronic crimes, including offers of illegal goods such as counterfeit or substandard medicines, tests, and other Covid-19 related products.

The growing popularity of e-commerce has not gone unnoticed by counterfeiters, who are increasingly using online trade to sell fake goods to consumers—some of whom believe they are purchasing authentic products, while others actively seek out counterfeit items because of their low prices.

5 OECD-EUIPO, *Misuse of e-commerce for trade in counterfeits, 2021*, https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/misuse-e-commerce-trade-in-counterfeits/EUIPO_OECD_misuse- -e-commerce-trade-in-counterfeits_study_en.pdf (data dostępu: 16.05.2025).

The links between e-commerce and the illegal trade in counterfeit goods are supported by a quantitative analysis examining the relationship between e-commerce and the number and value of counterfeit goods seizures by customs authorities from 2017 to 2019. The analysis found that this connection becomes stronger when indicators of illegal trade in counterfeit goods via small parcels are taken into account; this suggests that illegal goods purchased through e-commerce are often shipped in small packages, especially using postal services.

A case study of the European Union, which collected data on seizures of counterfeit goods related to e-commerce, provides further insight into the situation. The data show that 91% of counterfeit goods seizures connected to e-commerce involved postal services. In contrast, postal services accounted for only 45% of seizures of counterfeit goods not related to e-commerce.

In terms of value, the data show that 81.8% of seizures related to e-commerce involved postal services, while only 8.9% were linked to other methods of selling counterfeit goods. Regarding the origin of the goods, the sources of counterfeit products sold through e-commerce and other types of trade are similar. However, the share of China was higher for counterfeit goods sold via e-commerce (75.9%) compared to 45.9% of the total number of seizures.

Among counterfeit goods seized in the EU related to e-commerce, there is a wide range of products. At the top of the list are footwear (33.7% of all seizures), clothing (17.3%), perfumes and cosmetics (9.6%), leather goods (8.7%), electrical machinery and equipment (6.5%), toys (5.5%), and watches (5.2%).

The activities of bad-faith actors have flourished in e-commerce markets because it is relatively easy to create websites selling counterfeit items. Moreover, these actors continue to find new ways to place counterfeit products on trusted platforms. Law enforcement agencies are actively involved in identifying and shutting down fraudulent websites and cooperate with major platform operators and brand owners to detect the sale of counterfeit goods. However, the problem remains significant and continues to grow.

Difficulties in intercepting counterfeit goods are compounded by the methods used to ship products ordered through e-commerce. Counterfeiters try to exploit weaknesses in distribution channels to facilitate their illegal activities. In e-commerce, this largely happens through postal services. There is concern that postal and customs authorities are not adequately prepared to inspect small parcels and letter shipments for counterfeit detection. Their capacity to identify counterfeit goods on an international scale is limited because these shipments are mixed with billions of legally sold items.

Governments have taken a range of actions aimed at combating the sale of counterfeit goods online. These include reaching agreements with stakeholders to strengthen cooperation, as well as increased efforts to detect websites selling counterfeit goods and to take action against them. For example, in the European Union, the European Commission was responsible for developing and implementing a memorandum of understanding between platforms, brand owners, and other stakeholders to promote best practices in fighting the online sale of counterfeit goods. In the United States, the government proposed the creation of an e-commerce task force that brought together major online platforms to collaborate and coordinate efforts to combat counterfeit goods sold on their platforms.

In Australia, the government is developing a mechanism that enables consumers to identify legitimate product sellers by linking authorized sellers of specific brands with a public trademark registry. Additionally, the European Union and the United States are considering the introduction of regulations and directives which, once adopted, will establish new frameworks for combating crimes in electronic commerce, including the trade of illegal goods.

Operators of major platforms have developed multifaceted approaches to combat the sale of counterfeit goods on their platforms. Their actions include measures and mechanisms involving third-party sellers, consumers, brand owners, and law enforcement agencies, as well as the development and implementation of strategies for proactively detecting and removing counterfeit goods. However, the ability of online marketplaces to adequately vet third-party sellers has proven insufficient, and continuous efforts are being made to improve mechanisms for identifying and disciplining parties selling counterfeit goods. Analyses show that abuses by counterfeiters in online markets are very dynamic. Further research into the development of this dynamic is necessary, both at the industry level and through case studies.

Domestic Measures: National Revenue Administration of Poland

In our country, the National Revenue Administration plays an important role in the system combating counterfeiting and piracy. It is the authority responsible for tax and customs administration in Poland.

One of the tasks of the authority is the enforcement of intellectual property rights. The Customs and Tax Service, which is a law enforcement body, is part of the National Revenue Administration (KAS). It is worth emphasizing that the primary procedure followed by KAS is the destruction of counterfeit goods. Between 2018 and 2021, the most frequently counterfeited product categories were cosmetics, clothing, watches, jewelry and leather goods, games, sports equipment and toys, as well as cigarettes.

Seizing goods that infringe intellectual property rights at the moment they attempt to enter the EU market allows for effective combat against counterfeiting and piracy.

Here's the reminder of the objects protected by law in the activities of KAS:

- trademarks,
- industrial and utility designs,
- copyrights and related rights,
- patents,
- supplementary protection certificates,
- plant variety protections,
- designations of origin or geographical indications,
- topographies of integrated circuits,
- trade names.

The enforcement of intellectual property rights by customs authorities depends on cooperation with rights holders. One form of cooperation is the possibility of submitting a request for action to the customs authorities.

A request to initiate action by the customs authorities for the protection of intellectual property rights can be submitted to the Director of the Tax Administration Chamber in Warsaw. The request to initiate action is prepared using the form attached

to Commission Regulation (EU) No 1352/2013. The person authorized to submit the request is the rights holder or their representative, as well as a person authorized to use the intellectual property rights.

If the customs authorities, before the rights holder submits a request or before considering it, have sufficient grounds to suspect that goods infringe intellectual property rights, they may suspend the release of the goods or detain them for a period of 4 working days from the moment the rights holder receives the notification, to allow the rights holder to submit a request for action to the Director of the Tax Administration Chamber in Warsaw. If no request is submitted, the customs authority releases the detained goods.

There is also a third procedure, known as the „small shipments" procedure (3 items or 2 kg gross), which takes place without involving the rights holder. If, during a customs inspection, a customs officer identifies goods meeting these criteria, they suspend the release or detain the goods for a period of 10 working days without the need to consult the intellectual property rights holder.

The issue of detecting, prosecuting, and eliminating violations of industrial property rights is important for economic activity, strengthening jobs, and business development. Therefore, the Patent Office of the Republic of Poland cooperates with the National Revenue Administration by organizing joint conferences, webinars, and informational meetings.

Youth in Action

It is worth adding that data on the practices of young people in using intellectual property rights, as well as data on the characteristics of infringements—including online content violations in this important age group—are equally important. In this regard, EUIPO conducted a study on the behavior of individuals aged 15 to 24 in the European Union concerning intellectual property rights infringement. Both at the European and national levels, the study sheds light on the factors that lead young people to purchase counterfeit goods or access digital content from illegal sources, but it also highlights aspects that may encourage the younger generation to reduce infringements of intellectual property rights.

The 2022 study[6] further confirms the trends observed in its 2016 and 2019 editions and additionally provides better insight into the perceptions and attitudes of young people at a time when online commerce and digital consumption have significantly increased, influencing consumer behavior. The tendency to access digital content from legal sources has been clearly confirmed, as more and more young people declare a preference for legal alternatives over pirated content. However, 21% of respondents still admit to having knowingly accessed pirated content in the past 12 months, particularly movies, TV series, music, and live sports events, through specialized servers, apps, and social media. One-third of young consumers have difficulty distinguishing legal digital content from pirated content or increasingly do not pay attention to this distinction. On the other hand, the number of people intentionally purchasing counterfeit goods has increased. Thirty-seven percent of young people confirm that in the past 12 months they have bought at least one counterfeit product (14% in 2019).

6 EUIPO, *Intellectual Property and Youth Scoreboard 2022, 2022*, https://www.euipo.europa.eu/en/publications/intellectual-property-and-youth-scoreboard-2022-qualitative-analysis-additional-dimension-on-music (data dostępu: 16.05.2025).

This trend is concerning. A similar proportion of young people have accidentally purchased counterfeit goods and admit to having difficulty distinguishing original products from fakes. Although respondents still perceive price as the main significant factor driving the use of piracy or counterfeit goods, social influences—such as the behaviors of family, friends, and peers—are gaining increasing importancnce. Regarding the factors that could encourage young people to reflect and refrain from violating intellectual property rights, respondents most often mention personal risks related to cyber threats or online fraud, as well as a better understanding of the negative impact on the environment or society.

The EUIPO analysis should serve as a valuable tool to assist stakeholders, policymakers, as well as educators and civil society organizations in shaping awareness-raising initiatives to support informed choices among young citizens and consumers.

Young people still frequently use content from illegal sources and purchase counterfeit goods online. One third (33%) of respondents used content from illegal sources in the past 12 months, either by playing, downloading, or streaming it. Of this group, 21% did so intentionally, while 12% did so unintentionally. Although these results largely align with those from 2019, there was also a ten percentage point increase in the share of young people who say they do not access content from illegal sources (from 50% to 60%). This increase is consistent with findings reported in the broader recent literature on the subject. Regarding counterfeiting, just over half (52%) of young people surveyed bought at least one counterfeit product online in the past 12 months.

In total, 37% of respondents intentionally purchased a counterfeit product, and the same percentage did so unintentionally (respondents could have both intentionally and unintentionally purchased a specific type of counterfeit product at some point during the past 12 months). Although the results of this study are not directly comparable to those of previous editions, they indicate a significant increase in the number of people buying counterfeit goods since 2019, when 14% of respondents reported intentionally purchasing such goods, and 12% reported doing so unintentionally. This change likely reflects both the widely documented increase in online shopping during the Covid-19 pandemic and the improvements made to this question in the 2022 indicators report.

The types of counterfeit products respondents most frequently purchased in the past 12 months were clothing and accessories (17%) and footwear (14%). The main motivating factor for illegal access to digital content and the purchase of counterfeit goods remains cost, but other factors, especially social influences, are playing an increasingly important role. According to the 2019 findings, the primary reasons respondents intentionally accessed content from illegal sources were lower costs and a wider selection.

A new question added to the 2022 survey showed that for most types of content originating from illegal sources, the most popular access channels were dedicated websites, especially for movies (63%) and TV series (59%). For music, the most popular channel for accessing pirated content was apps (39%), and for images, social media (36%). The availability of more affordable, original products/content from legal sources, as well as the risk of penalties, remain the main factors encouraging young people to refrain from illegal alternatives.

At the same time, new response options added to the 2022 survey indicate other factors that could encourage young people to change their behavior. About half of those who admitted to accessing content from illegal sources stated that they might stop using such content if they experienced cyber threats (41%) or cyber fraud (40%), while 24% said they might stop if the content was of low quality.

Among those who purchased counterfeit products, about one third (31%) stated they would stop this practice if they encountered low-quality counterfeits, and about one quarter said they would do so if they experienced online fraud (23%) or a cyber threat (21%), or if they came into contact with a dangerous product (22%). A similar proportion of respondents indicated that a better understanding of the negative impact on the environment (19%) or society (17%) would deter them from buying counterfeit products.

The impact of artificial intelligence on the infringement and enforcement of intellectual property rights

Over the past 50 years, the world has witnessed groundbreaking innovations and revolutionary changes that have transformed the economy, jobs, and even society itself, fundamentally altering the way we live, work, and interact with one another. Artificial intelligence and related technologies are among the most important drivers of change and impact every area of intellectual property rights. They are also increasingly becoming tools for analyzing intellectual property rights infringements. A study by the European Union Intellectual Property Office (EUIPO)[7] sheds light on how these technologies are used both to protect industrial designs and copyrights, as well as to infringe upon them. It also explores various types of AI applications that have a significant impact on intellectual property.

Understanding the implications of these changes is crucial at a time when the Fourth Industrial Revolution (4IR) is transforming virtually every sector of the economy and society.

We are witnessing inventions and breakthroughs in the fields of autonomous transportation, biotechnology, the Internet of Things, smart devices, artificial intelligence, 3D printing, robotics, and quantum computing. These inventions impact, among others, healthcare, transportation, agriculture, and law enforcement, and the pace of global innovation has significantly accelerated over the past decade. According to some estimates, in 2023 there were around 29 billion connected devices worldwide utilizing artificial intelligence technologies, with the underlying algorithms becoming increasingly central.

According to reports from the European Cybercrime Centre (EC3) of Europol, the EU Agency for Cybersecurity (ENISA), and the United Nations, the number of intellectual property rights infringements through the malicious use of various new technologies, including artificial intelligence, is increasing. In May 2021, the EU Council recognized crime related to intellectual property rights violations as one of the top ten priorities in the fight against organized crime for the years 2022–2025. This issue will be addressed through the European multidisciplinary platform against criminal threats (EMPACT). The European Union Intellectual Property Office (EUIPO), through the European Observatory on Infringements of Intellectual Property Rights, will be actively involved in supporting the implementation of this priority within EMPACT.

In this new era, it is crucial that we adopt “smart” intellectual strategies. EUIPO, in cooperation with its network of partners and stakeholders in intellectual property, is developing tools and promoting best practices. This study represents a further step toward creating a center of excellence in intellectual property, where new technologies and artificial intelligence work to protect legitimate businesses and citizens, emphasize the EUIPO authorities, reflecting on the complex issues and conducting the very first study in this area.

7 EUIPO, *Study on the impact of artificial intelligence on the infringement and enforcement of copyright and design, 2022*, https://www.euipo.europa.eu/en/publications/study-on-the-impact-of-artificial-intelligence-on-the-infringement-and--enforcement-of-copyright-and-designs (data dostępu: 15.05.2025)

At the beginning of 2019, EUIPO established a Technology Expert Group (EG). The group consists of experts with knowledge and practical experience in monitoring the impact of new and emerging technologies on the infringement and enforcement of intellectual property rights.

In 2021, EUIPO commissioned the United Nations Interregional Crime and Justice Research Institute (UNICRI) to carry out the first in-depth research project in cooperation with the EUIPO expert group.

This provides a certain crime landscape — the annual strategic Internet Organised Crime Threat Assessment (IOCTA) report, prepared by Europol's European Cybercrime Centre (EC3), includes a review of emerging threats and changes in the cybercrime landscape. In 2020, the highest-priority threats were social engineering, ransomware software, and other forms of malware. When analysing criminal activity, it is important to consider the "cyber-" element in cybercrime, as it often affects nearly every aspect of such activity. In the recent IOCTA 2021 report, Europol listed ransomware affiliate programs exploiting supply chain attacks to break into networks of large corporations and public institutions, implementing new multi-layered extortion methods, multi-layered mobile malware attacks, and distributed denial-of-service (DDoS) attacks for ransom. Therefore, the EUIPO study also analyses and explains how these threats are relevant in the context of industrial designs and copyrights.

The development and evolution of cybercrime should also be considered in connection with the misuse of artificial intelligence, including AI-assisted crimes against intellectual property. The emerging malicious use of artificial intelligence significantly increases the impact of cybercrime because it can enhance large-scale social engineering attacks.

AI can be used, among other things, for:

- malware downloading documents to increase the effectiveness of attacks,
- avoiding image recognition and voice biometrics,
- creating ransomware attacks with intelligent targeting, evasion, and data poisoning by identifying blind spots in detection rules,
- enhancing blockchain capabilities in cybercrime.

The importance of addressing intellectual property-related crimes has also been recognized as a priority within the context of cybersecurity. In May 2021, the Council of the European Union placed intellectual property crime among the ten most important priorities in the fight against organized crime to be addressed during 2022–2025.

On May 26, 2021, the Council adopted conclusions setting out the EU priorities for 2022–2025 in combating serious and organized crime through the European multidisciplinary platform against criminal threats (EMPACT). Therefore, EUIPO decided to conduct a study assessing the impact of artificial intelligence technology both on the infringement and enforcement of rights related to the registration of industrial designs and copyrights.

Artificial intelligence offers several capabilities to improve the effectiveness of detecting intellectual property infringements and enforcing rights, as it can be used to perform many different functions: from sensing, reasoning, and acting, to evaluating and even predicting. Currently, the main areas of AI development include machine learning, natural language processing, computer vision, expert systems, and explainable artificial intelligence. Explainable AI is currently gaining increasing attention from experts and policymakers.

Other technologies supported by artificial intelligence, such as quantum computing, blockchain, 3D printing, generative design, cloud services, and robotics, also have enormous potential. Artificial intelligence can identify and prioritize threats, instantly detect malware in networks, guide incident response, and detect intrusions before they occur. For example, machine learning stands out as a key area of AI that can be used to develop law enforcement tools, such as analyzing large volumes of data to detect threats and identify social engineering bots, scanning images to detect fake websites containing illegal content, enhancing automatic content recognition (ACR) tools, and providing insights to uncover patterns of infringement.

Natural language processing can be used to analyze and block cyberattacks such as phishing, identify fraudulent behaviors, and create correlation analyses aimed at quickly detecting infringements. Computer speech and computer vision are also successfully utilized in this field. Some of their applications include pattern recognition to predict future infringements, detection of marketing for counterfeit goods, and detection and analysis of fake logos or other images. Quantum computing can be applied to enhance AI tools by enabling them to process larger amounts of data. For example, AI and quantum computing can be used by customs and law enforcement agencies to recognize patterns in large datasets and identify similarities. On the other hand, expert systems can be employed by law enforcement to decide which strategy is most appropriate to protect the system against specific vulnerabilities, including those related to infringements of industrial designs and copyrights.

When it comes to drivers, the capabilities of artificial intelligence make it attractive to malicious actors.

JArtificial intelligence can mimic many human activities and, in some cases, can surpass human capabilities in terms of performance and scalability. Moreover, some crimes—supported by AI technologies—can be committed on a much larger scale, simultaneously targeting thousands of victims. As the metaphor of a double-edged sword shows, the same technologies can be used both by malicious actors and for law enforcement purposes, including in the field of intellectual property rights.

Fraudsters and criminal groups use or may use the same AI techniques employed by law enforcement agencies to overcome cybersecurity measures and avoid detection. This is known as the “AI/cybersecurity paradox”: as AI matures and is increasingly used in cybersecurity, the potential drawbacks of this technological progress also grow.

In this regard, adversarial machine learning can help detect and overcome cybersecurity measures, including breaking protections and creating dynamic malware to evade detection. AI technologies can be leveraged to increase the effectiveness of such attacks, for example, AI-powered password guessing and CAPTCHA cracking.

Furthermore, natural language processing tools can be used to create deepfake videos, and generative design-based tools can be employed to produce copyright-infringing copies.

It is also important to remember that behind every artificial intelligence algorithm and its practical applications there is always a human. Explainable artificial intelligence, although it does not solve all possible problems, could be used by law enforcement agencies as part of an increased deployment of innovative tools—including AI—in analysis and forecasting, while better meeting the requirements of reliability, accountability, and transparency.

The use of artificial intelligence by law enforcement and the judiciary should always be subject to strong safeguards and human oversight through built-in human control.

Current limitations of artificial intelligence include, in particular, its dependence on large amounts of high-quality training data, inability to handle long-tail problems (i.e., data distribution issues), limited versatility, dependence on specific application scenarios, and the inherent biases of AI developers. More efficient machine learning algorithms can learn complex nonlinear relationships between input and output data, but doing so requires large amounts of high-quality data — here, resources from patent offices and customs data systems prove helpful.

Machines still need to better understand the world through perceptual and cognitive learning, enabling them to simulate real-world scenarios in order to perceive information and then transform that perceived information into abstract knowledge through attention, memory, and comprehension. This can be achieved by crossing, integrating, and optimizing algorithms as well as through continuous research improvement.

Furthermore, despite the broader use of innovative technologies in law enforcement, according to interviews conducted for the EUIPO study, the actual use of these technologies by public authorities to enforce infringements of industrial designs and copyrights remains underdeveloped.

Moreover, law enforcement and customs authorities will need to continuously monitor the landscape of new technologies to ensure they are adequately prepared and trained to face new technological challenges.

In summary, significant investments are flowing into research and development of artificial intelligence, along with machine learning technologies, and this trend is expected to continue in the coming years.

Consequently, an increase in the availability and use of these tools and technologies can be expected, both for legal and illegal purposes. A wide range of AI-related tools and technologies is currently or potentially being used for designing and infringing industrial designs, as well as for law enforcement (the EUIPO study presents many interesting cases in this area). Therefore, there is a clear need for better understanding, greater awareness, and enhanced capabilities among all stakeholders, including policymakers, intellectual property protection entities, businesses, and law enforcement authorities

Summary

Finally, it is worth adding and emphasizing that in the systems for prosecuting and combating infringements and piracy, it is not only necessary to strengthen cooperation and rely on modern technological tools—some of which have been developed by Polish inventors (such as digital watermarks for online content or nanotechnologies using quantum dots to mark legitimate physical goods)—but also to ensure coordination and collaboration with international organizations. Moreover, an important aspect is undertaking broad informational and communication activities targeted at relevant social groups, so they develop proper consumer awareness as well as awareness of related risks and threats.

An important group remains youth, and shaping in them an appropriate awareness of protected intellectual property. Certainly, this will also be supported by creating an attractive range of goods and services that are easily accessible but do not infringe exclusive rights.

Artificial intelligence, blockchain, and other advanced technologies present an opportunity for law enforcement agencies to more effectively detect intellectual property infringements. The problem of counterfeits has taken on a new dimension with the rise of online commerce. The issue of combating illegal trade in counterfeit goods on online stores is also being addressed in other forums, including the Organisation for Economic Co-operation and Development (OECD). OECD has established a task force to combat counterfeit trade and has initiated government-level discussions on this topic.

Finally, it is worth adding that in 2024, the Polish Patent Office (UPRP) began a series of meetings with representatives of the OECD, the Ministry of Finance, and the Ministry of Development and Technology. We are discussing counteracting illegal trade in counterfeit goods on online platforms and the possibilities for cooperation within the administration. Together, we can more effectively protect intellectual property and fair trade in online markets. The Polish Patent Office gladly joins this important project and will actively support its implementation.

Piotr Brylski
Legal Advisor
Polish Patent Office of the Republic of Poland

About the report publisher

NASK is a state research institute supervised by the Ministry of Digital Affairs. The Institute currently conducts multidimensional activities operating at the intersection of science, business, and public administration. One of the main tasks of NASK–PIB is to ensure a secure Internet and protect its users.

Under the Act on the National Cybersecurity System, the CSIRT NASK – Computer Security Incident Response Team – operates within the Institute as one of three national-level CSIRT teams. Its tasks include receiving, analyzing, and responding to incidents related to the security of Poland's civilian cyberspace, reported by operators of critical services, digital service providers, local governments, and private individuals. It also handles incidents involving illegal content published on the Internet that threatens children's safety. Additionally, it is responsible for monitoring internet threats and the state of cybersecurity at both sectoral and national levels. NASK–PIB also contributes to the analytical, research, and development support for the national cybersecurity system.

The Institute also conducts research and development activities focused on creating solutions that enhance the efficiency, reliability, and security of teleinformatics networks and other complex network systems. What distinguishes our research institute from strictly commercial enterprises is our approach to developing solutions for current and future client needs. At NASK–PIB, researchers frame commercial problems within the context of science, using its tools—which are often broader and more abstract—to achieve results that are not only satisfactory but also innovative. The main research focus is cybersecurity, understood as detection, warning, incident response, data acquisition, analysis, processing, and transfer, as well as complex network systems, including IoT systems and mobile ad hoc networks. Significant attention is also devoted to research on biometric identity verification methods in service security.

NASK–PIB also manages the .pl domain name registry and, as a telecommunications operator, offers innovative teleinformatics solutions for clients in the financial sector, business, administration, and academia. An important part of the Institute's activities is user education and the promotion of the information society concept, primarily aimed at protecting children and youth from risks associated with the use of new technologies. The Institute also implements projects crucial for the country's digital transformation—namely, the Nationwide Educational Network (Ogólnopolska Sieć Edukacyjna, OSE) and Electronic Document Management (Elektroniczne Zarządzanie Dokumentacją, EZD RP).

Editorial board

EDITORS-IN-CHIEF

Prof. dr hab. Katarzyna Chałubińska-Jentkiewicz
dr hab. Urszula Soler

EDITORIAL SECRETARIES

dr Monika Nowikowska
Krystyna Cieniewska

kontakt@journaldot.pl

REPORT EDITORIAL TEAM

Alina Wiśniewska-Skura

NASK