



WYDANIE SPECJALNE NR 2

dot.pl



NASK





dot.pl

RAPORT PODSUMOWUJĄCY 2024

WYDANIE SPECJALNE NR 2

WARSZAWA, MAJ 2025

ISSN 3071-673X

aid.pl mail.pl com.pl
agro.pl atm.pl edu.pl
gmina.pl info.pl mil.pl
targi.pl mil.pl gsm.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
nom.pl turystyka.pl

Spis treści

4	Wstęp
7	CZĘŚĆ I Rynek nazw domeny .pl
8	Fakty i liczby
9	Ranking europejskich rejestrów domen
10	Obsługa domen
18	Obsługa abonentów nazw domeny .pl
20	Wypowiedzi Partnerów Rejestru domeny .pl
26	Podział rynku nazw domeny .pl
29	CZĘŚĆ II Raport z badania na temat treści nielegalnych w Internecie
39	Osobiste doświadczenia z treściami nielegalnymi
51	Opinie na temat treści nielegalnych w Internecie
63	Nienawiść w sieci
73	Znajomość przepisów prawa i opinie na ich temat
85	CZĘŚĆ III Naruszanie praw własności intelektualnej w problematyce nielegalnych treści oraz handlu podrabianymi towarami w Internecie

Wstęp

Internet z natury ma charakter transgraniczny, a dotychczasowe rozwiązania prawne na szczeblu krajowym nie wystarczały w przypadku świadczenia usług cyfrowych na terytorium całej Unii Europejskiej. Dotyczy to także tych usług, które nie pochodzą od podmiotów działających na jednolitym rynku cyfrowym. Nieskuteczność dotychczasowych działań wpływała na zapewnienie bezpieczeństwa i jednakowego poziomu ochrony praw obywateli Unii i unijnych przedsiębiorców działających online.

W 2024 roku harmonizacja warunków rozwoju innowacyjnych transgranicznych usług cyfrowych z zachowaniem bezpiecznego środowiska internetowego stała się faktem na szczeblu unijnym. Nowe przepisy zrewolucjonizowały dotychczasowe zasady rządzące rynkiem usług cyfrowych.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych DSA) stanowi uzupełnienie obowiązujących przepisów sektorowych i zdaniem prawodawcy UE nie wpływa na stosowanie obowiązujących przepisów prawa Unii regulujących określone aspekty świadczenia usług społeczeństwa informacyjnego, które mają zastosowanie jako *lex specialis*. Rozporządzenie ma jednak zastosowanie do takich dostawców w stopniu, w jakim nie mają do nich zastosowania bardziej szczegółowe przepisy określone w dyrektywie o audiowizualnych usługach medialnych lub innych unijnych aktach prawnych, takich jak rozporządzenie w sprawie zapobiegania rozpowszechnianiu w Internecie treści o charakterze terrorystycznym. Ponadto bazuje ono na zaleceniu z 2018 r. dotyczącym nielegalnych treści (Zalecenie Komisji z dnia 1 marca 2018 r. w sprawie działań na rzecz skutecznego zwalczania nielegalnych treści w Internecie (C(2018) 1177 final)) oraz Forum UE ds. Internetu w odniesieniu do treści o charakterze terrorystycznym.

DSA wprowadza takie regulacje jak: (a) środki służące zwalczaniu nielegalnych towarów, usług lub treści w Internecie, np. mechanizm sygnalizowania takich treści przez użytkowników, a w przypadku platform – mechanizm współpracy z „zaufanymi podmiotami sygnalizującymi”, (b) nowe obowiązki dotyczące identyfikowalności użytkowników biznesowych na internetowych platformach handlowych, aby pomóc w identyfikowaniu sprzedawców nielegalnych towarów, (c) skuteczne zabezpieczenia dla użytkowników, w tym możliwość zakwestionowania decyzji platform w zakresie moderowania treści, (d) szeroko zakrojone środki na rzecz przejrzystości funkcjonowania platform internetowych, w tym w sprawie algorytmów stosowanych

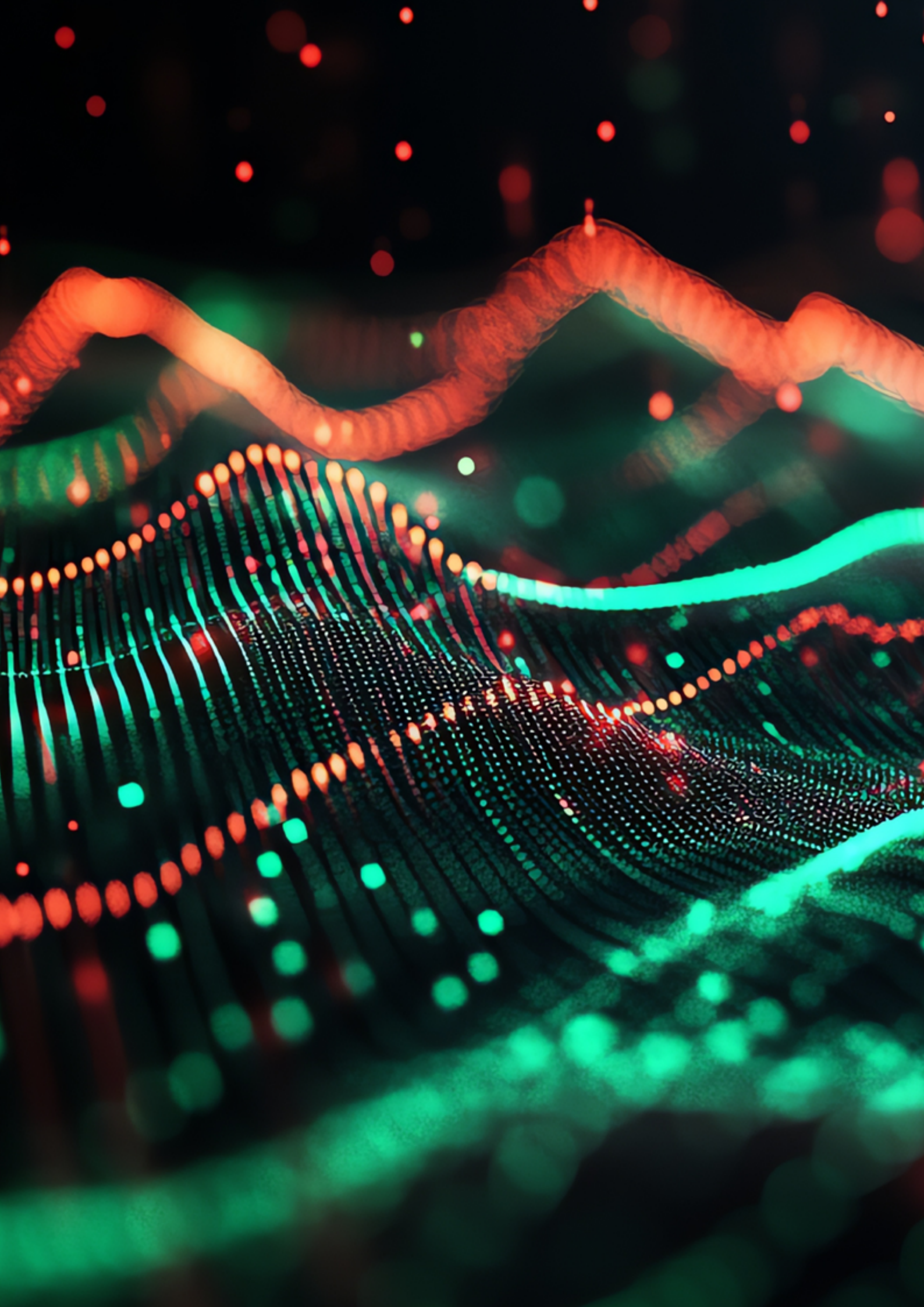
w podpowiedziach, (e) obowiązki bardzo dużych platform w zakresie zapobiegania niewłaściwemu wykorzystywaniu ich systemów poprzez podejmowanie działań opartych na ocenie ryzyka oraz poprzez przeprowadzanie niezależnych kontroli zarządzania ryzykiem związanym z tymi systemami, (f) udostępnianie naukowcom najważniejszych danych przez największe platformy, aby mogli oni badać, jak ewoluują zagrożenia w sieci, (g) strukturę nadzorczą odpowiadającą złożoności przestrzeni internetowej: kraje UE będą odgrywać główną rolę, przy wsparciu nowej Europejskiej Rady ds. Usług Cyfrowych, w przypadku bardzo dużych platform – wzmocniony nadzór i egzekwowanie przepisów przez Komisję.

W dużym stopniu nowe zasady dotyczą pośredników – dostawców usług cyfrowych. W regulacji zwrócono uwagę, że platformy zobowiązane to także te, które docierają do ponad 10% Europejczyków, czyli 45 mln użytkowników sieci i usług e-commerce. Nowe obowiązki związane są z działaniami mającymi na celu zwalczanie treści nielegalnych.

DSA posługuje się pojęciem treści nielegalnej. W akcie tym nie zdefiniowano szczegółowo, czym jest „treść nielegalna”. Zgodnie z art. 3 lit. h tego rozporządzenia „nielegalne treści” oznaczają informacje, które same w sobie lub przez odniesienie do działania, w tym sprzedaży produktów lub świadczenia usług, nie są zgodne z prawem Unii lub z prawem jakiegokolwiek państwa członkowskiego, które jest zgodne z prawem Unii, niezależnie od konkretnego przedmiotu lub charakteru tego prawa. To oznacza, że ustalenie, czy dana treść jest nielegalna, będzie determinowane przez przyjęty w danym państwie członkowskim system wartości (oczywiście poza wspólnymi zakresami takiego definiowania).

Ta nowa rzeczywistość regulacyjna w dużym stopniu zmienia sposób funkcjonowania jednolitego rynku usług cyfrowych, a ostatecznie wpłynie na funkcjonowanie całego środowiska cyfrowego, dlatego w raporcie pokazujemy nie tylko najnowsze wyniki i trendy związane z prowadzoną działalnością w Internecie. Bardzo ciekawe wyniki badań związane z tym, co dla internautów i dla ekspertów stanowią treści nielegalne, czy kwestie dotyczące istotnych wartości - co dla nas jest ważniejsze – wolność czy bezpieczeństwo – to główny wątek podjętej i dla nas najważniejszej tematyki - jak rozwija się świat Internetu.

Zapraszamy do dyskursu!



CZĘŚĆ I

Rynek nazw
domeny .pl

Fakty i liczby



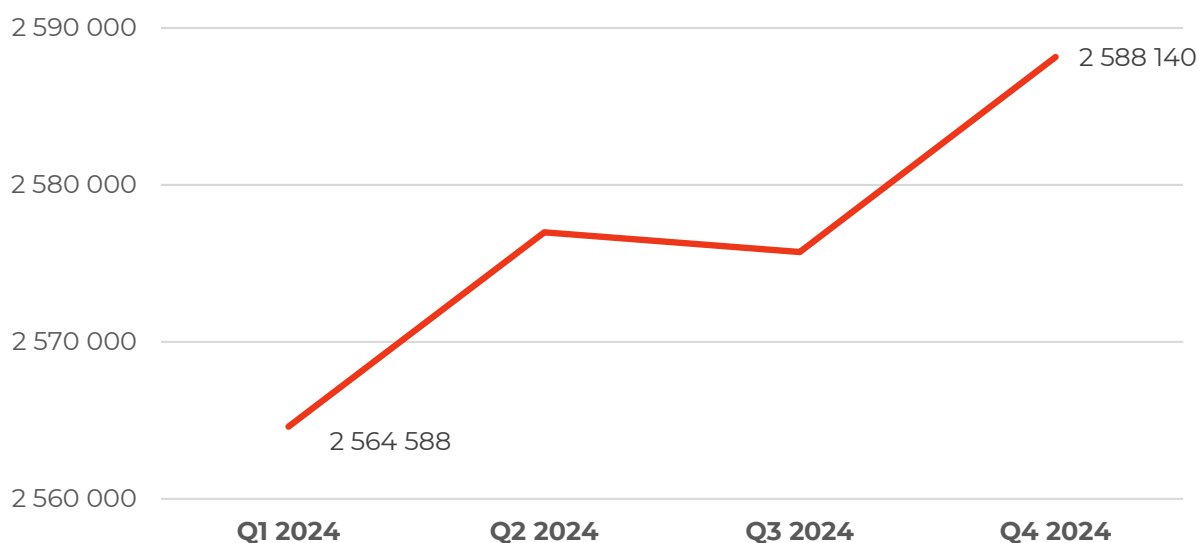
Ranking europejskich rejestrów domen

	.de	Niemcy	17 684 865
	.uk	Wielka Brytania	10 260 979
	.nl	Holandia	6 175 615
	.fr	Francja	4 216 306
	.it	Włochy	3 495 034
	.pl	Polska	2 588 140
	.es	Hiszpania	2 094 791
	.be	Belgia	1 718 090
	.cz	Czechy	1 485 493
	.se	Szwecja	1 456 166

Obsługa domen

Liczba nazw utrzymywanych w domenie .pl

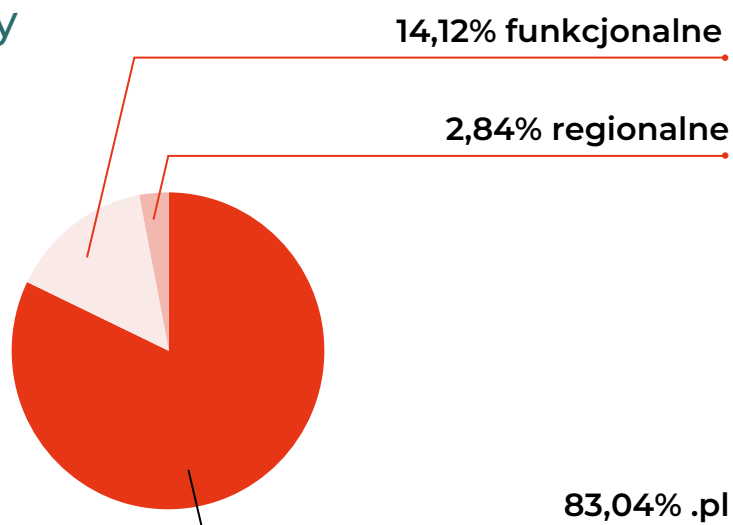
W 2024 roku o **41 733** zwiększyła się liczba aktywnych w DNS nazw domeny .pl, a dynamika roczna wyniosła **1,64%**.



Copyright by NASK

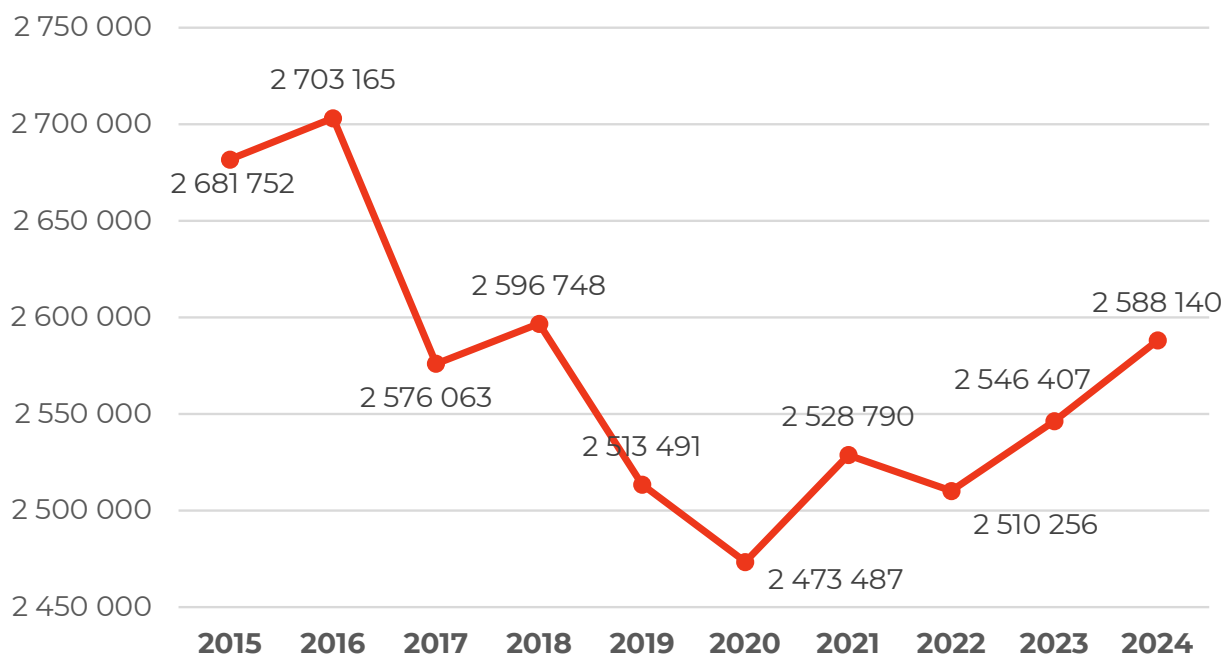
Aktywne w DNS nazwy domeny .pl z podziałem na typ strefy

Podział nazw na znajdujące się bezpośrednio w domenie .pl, w domenach funkcjonalnych, tj. com.pl, net.pl i innych, oraz w domenach regionalnych, np. waw.pl, slask.pl i innych.



Copyright by NASK

Liczba nazw domeny .pl w DNS, lata 2015–2024



Copyright by NASK

Liczba rejestracji nazw domeny .pl

2024 rok



liczba rejestracji
767 058



średnia dzienna liczba
rejestracji nazw
2 096



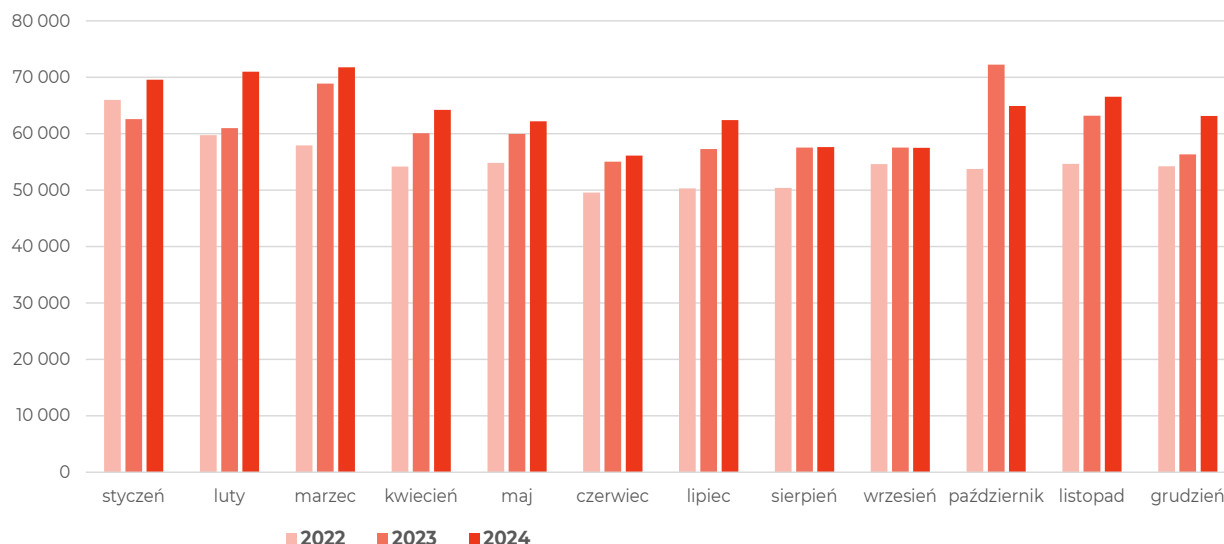
najwięcej domen
zarejestrowano
w marcu
71 758



najmniej domen
zarejestrowano
w czerwcu
56 117

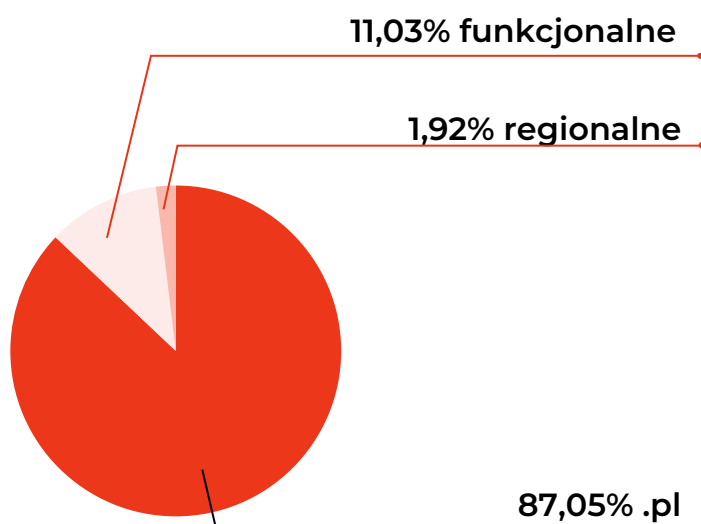
Copyright by NASK

Liczba rejestracji nazw domeny .pl



Copyright by NASK

Rejestracje nazw domeny .pl podzielone na typ strefy



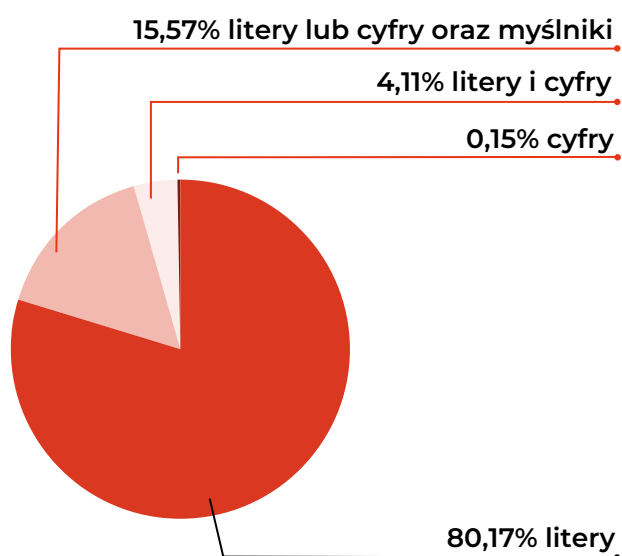
Podział nazw na znajdujące się bezpośrednio w domenie .pl, w domenach funkcjonalnych, tj. com.pl, net.pl i innych, oraz w domenach regionalnych. np. waw.pl, slask.pl i innych.

Copyright by NASK

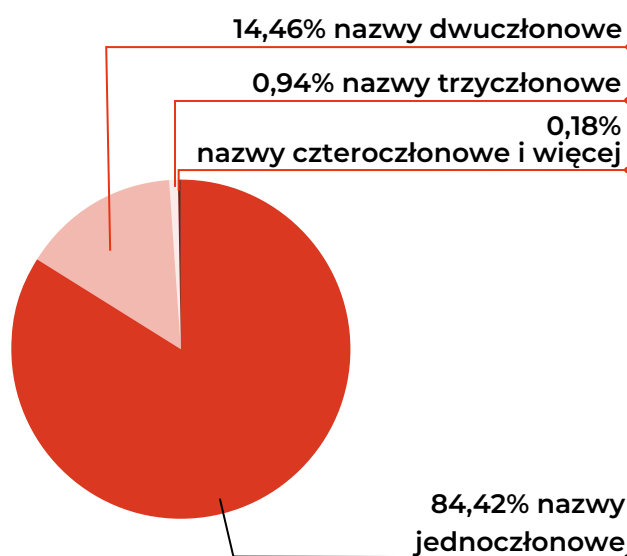
Struktura nazw domeny .pl

Średnia liczba znaków używanych w nazwach domeny .pl na koniec 2024 roku wyniosła **10,94**. Maksymalną liczbę **63** znaków miało **9** nazw domeny .pl.

Najbardziej powszechne były nazwy **dziwięcioznakowe**, w rejestrze było ich **233 099**. Maksymalna liczba członów występujących w jednej nazwie, odnotowana na koniec 2024 roku, wyniosła **11**.

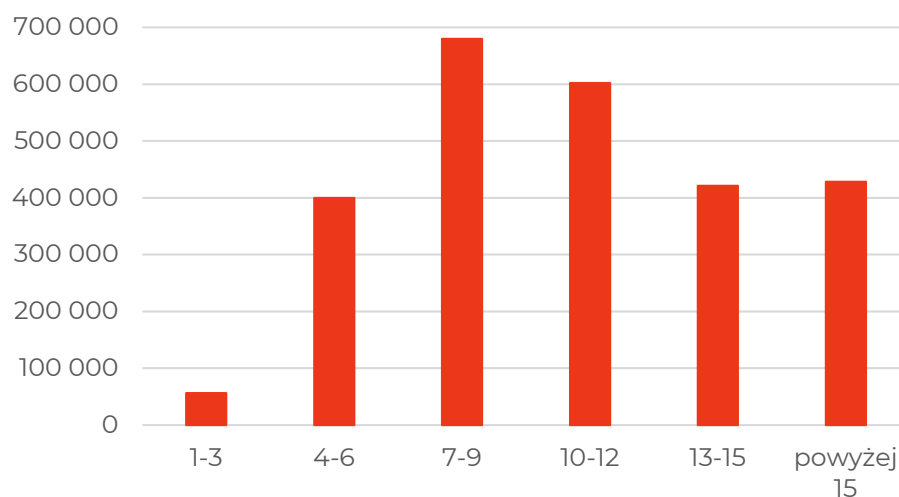


Znaki w nazwach domeny .pl, 2024



Liczba członów w nazwach domeny .pl, 2024

Copyright by NASK

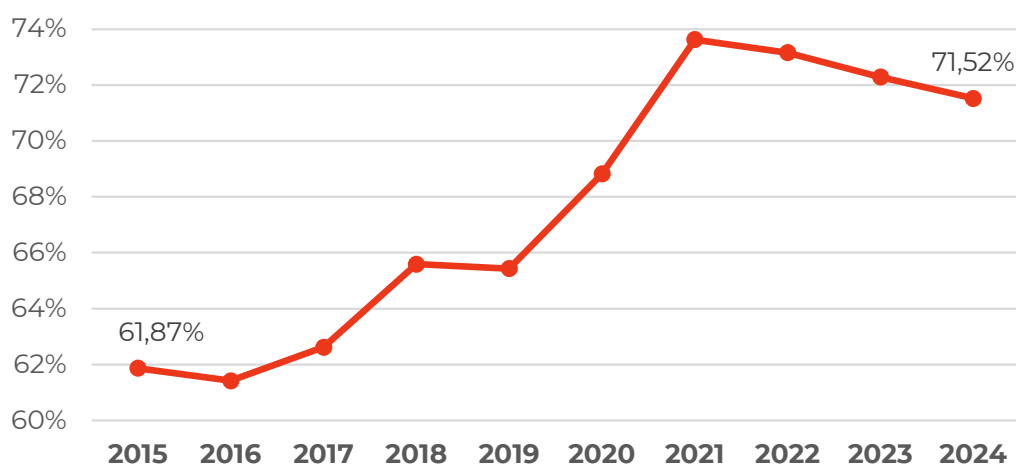


Liczba znaków w nazwach domeny .pl, 2024

Copyright by NASK

Odnowienia nazw domeny .pl na kolejny okres rozliczeniowy

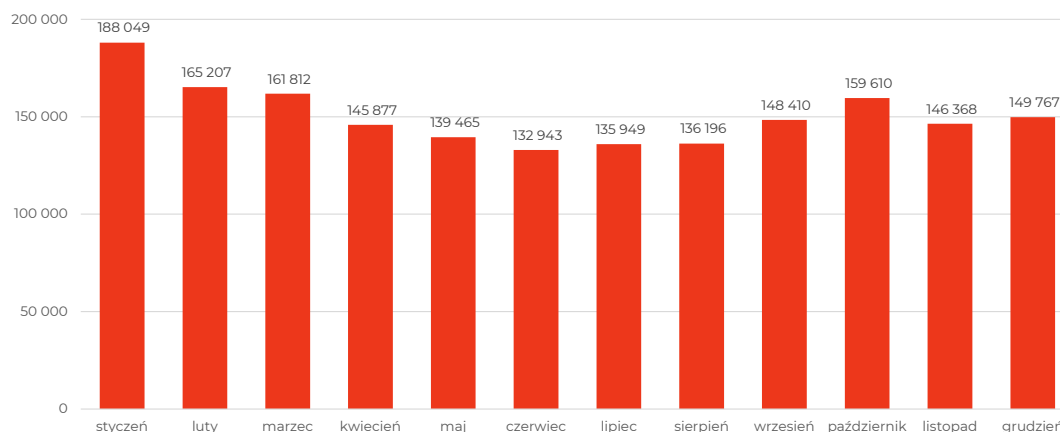
lata 2015–2024



Procent odnowień nazw domeny .pl, lata 2015–2024

Copyright by NASK

2024 rok

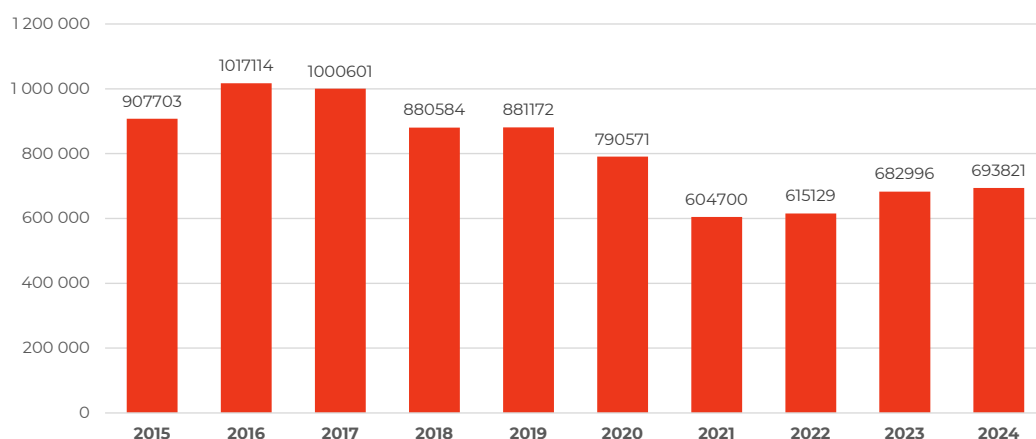


Liczba odnowionych nazw domeny .pl, 2024

Copyright by NASK

Liczba nieodnowionych nazw domeny .pl

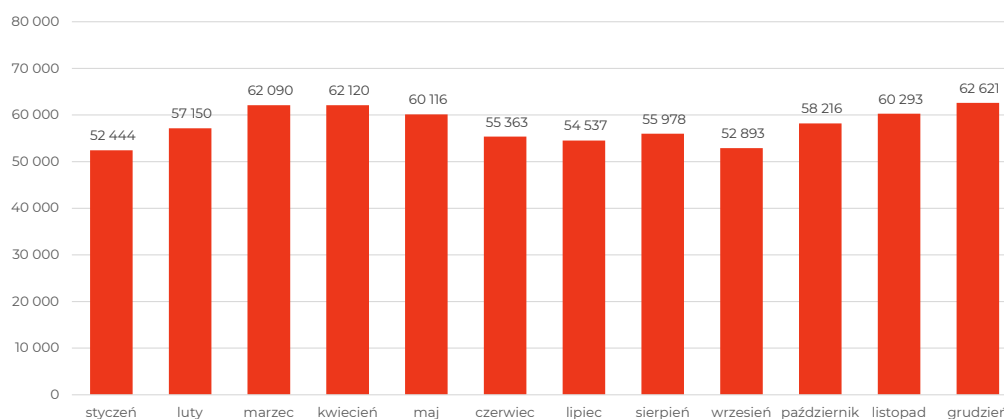
lata 2015–2024



Liczba nazw domeny .pl uwolnionych z powodu braku odnowienia, lata 2015–2024

Copyright by NASK

2024 rok

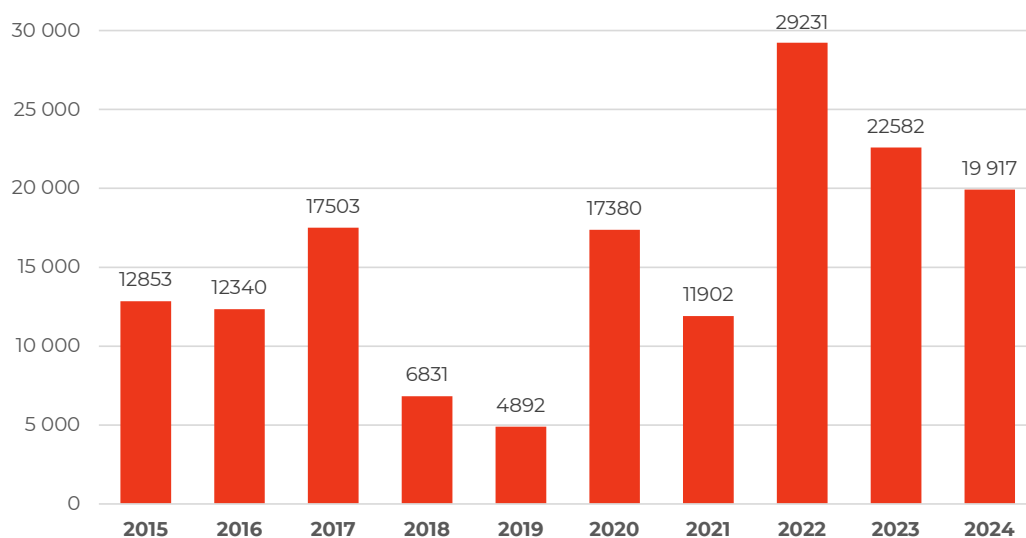


Liczba nazw domeny .pl uwolnionych z powodu braku odnowienia, 2024

Copyright by NASK

Liczba usuniętych nazw domeny .pl

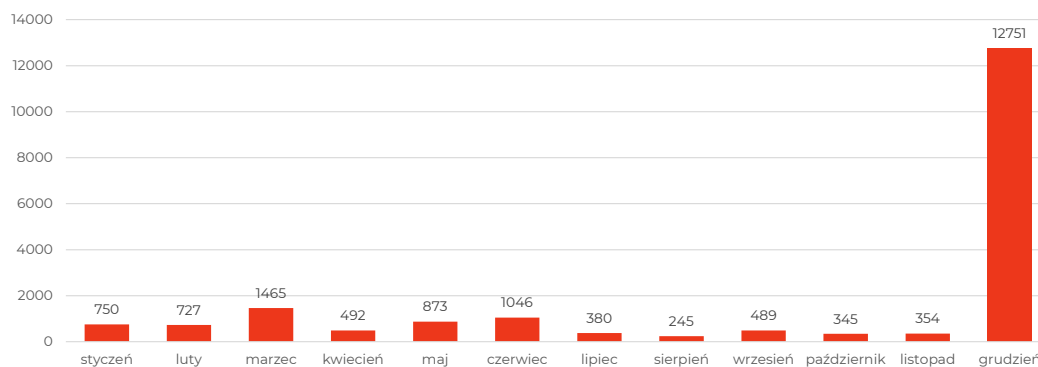
lata 2015–2024



Liczba nazw domeny .pl uwolnionych po wcześniejszym usunięciu, lata 2015–2024

Copyright by NASK

2024 rok

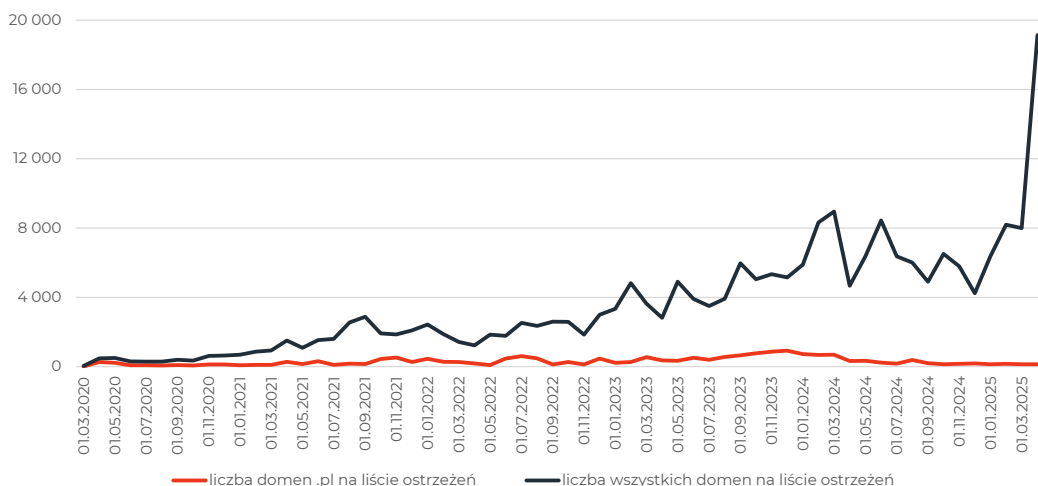


Liczba nazw domeny .pl uwolnionych po wcześniejszym usunięciu, 2024

Copyright by NASK

Liczba domen zablokowanych przez CERT Polska

lata 2020–2024



Liczba nazw domen zablokowanych przez CERT Polska, lata 2020–2024

Copyright by NASK

2024 rok

W 2024 roku domeny .pl stanowiły

5,51% wszystkich domen na liście ostrzeżeń przed niebezpiecznymi stronami. W porównaniu z rokiem 2023 to spadek o ponad połowę, do czego przyczyniło się m.in. usprawnienie procesu blokowania domen w strefie .pl, wprowadzone w lutym 2024 r.

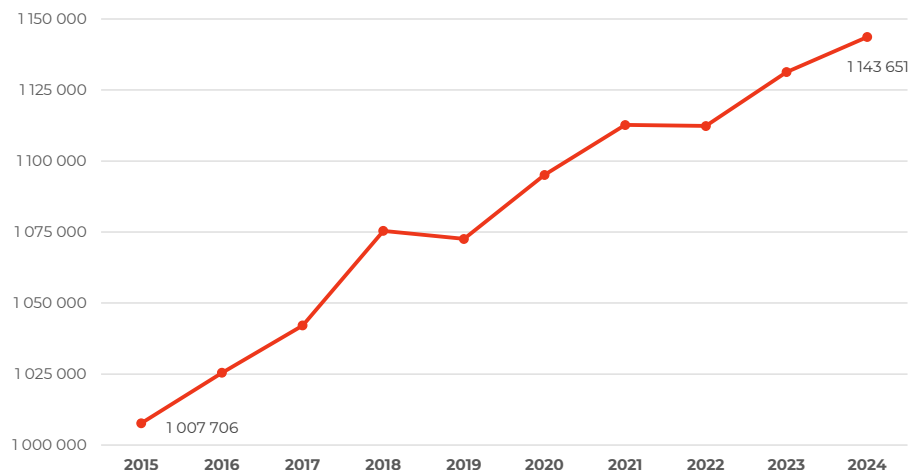
.com	35 312	.sbs	1 358
.xyz	4 724	.online	1 262
.pl	4 213	.info	1 165
.top	4 029	.lol	906
.shop	2 136	.pro	865
.site	1 977	.lat	677
.click	1 865	.pics	640
.cfd	1 666	.rest	549
.net	1 581	.eu	529
.org	1 503	.store	524

Top 20 rejestrów, których domeny trafiły na listę ostrzeżeń CERT Polska przed niebezpiecznymi stronami, 2024

Copyright by NASK

Obsługa abonentów nazw domeny .pl

Liczba abonentów nazw domeny .pl



Liczba Abonentów, lata 2015–2024

Copyright by NASK

12 319 liczba abonentów, którzy
dołączyli w 2024 roku

181 223 liczba zmian abonenta
nazw domeny .pl w 2024

2,26 nazw domeny .pl średnio
na jednego abonenta

64,42% abonentów to organizacje
35,58% abonentów to osoby fizyczne

Copyright by NASK

Lokalizacja abonentów domeny .pl

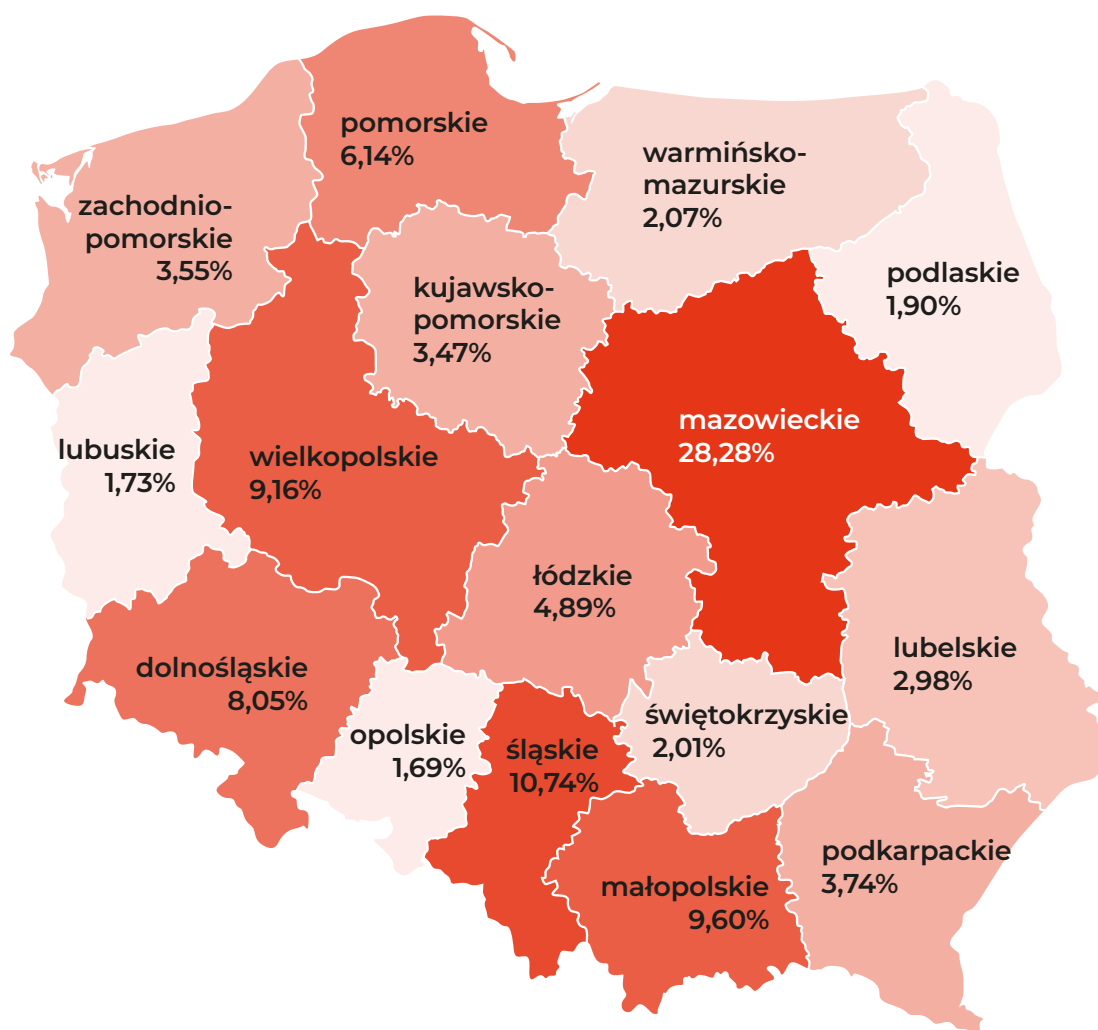
90,68% nazw domeny .pl istniejących
w DNS na koniec 2024 roku,
utrzymywanych na rzecz
abonentów z Polski

28,28% nazw było zarejestrowanych
na rzecz osób i organizacji
z województwa mazowieckiego,
z czego aż **20,69%** z Warszawy

Prawie połowę wszystkich abonentów z Polski
stanowili użytkownicy domen z województw:

28,28% mazowieckiego
10,74% śląskiego
9,60% małopolskiego

Copyright by NASK



Lokalizacja abonentów w Polsce, z podziałem na województwa, 2024

Copyright by NASK

Wypowiedzi Partnerów Rejestru domeny .pl

Aftermarket.pl Limited



Z unikalnej perspektywy rejestratora blisko związanego z wtórnym rynkiem domen możemy stwierdzić, że rok 2024 był dobrym rokiem dla domeny .pl. W porównaniu z rokiem 2023, liczba nowych domen z tym rozszerzeniem zarejestrowanych w naszym serwisie wzrosła o 10%, zaś liczba odnowień zwiększyła się o 7%. Świadczy to o stale rosnącym zainteresowaniu Polaków obecnością w Internecie. Domena .pl jest dla nich oczywistym pierwszym wyborem przy tworzeniu własnego adresu internetowego.

Z pewnością na wzrost liczby rejestracji i odnowień domen wpływ miały też akcje promocyjne rejestru domeny .pl, zachęcające rejestratorów do szukania nowych sposobów promocji tych domen. Choć część podmiotów swoje działania reklamowe ograniczyła do zwykłych obniżek cen, rok 2024 przyniósł także nieco ciekawych i kreatywnych akcji promocyjnych, co zaowocowało poprawą statystyk.

Także rynek wtórny domen zanotował podobny wzrost – łączna kwota sprzedaży domen na giełdzie Aftermarket.pl zwiększyła się o 6% w stosunku do poprzedniego roku. Pokazuje to, że rośnie świadomość faktu, iż dobry adres internetowy stanowi kluczowy element strategii marketingowej w Internecie, co sprawia że użytkownicy końcowi są skłonni dobrze zapłacić za wartościowy adres dla swojego serwisu.

Systematycznie tracą na znaczeniu domeny .pl trzeciego poziomu – funkcjonalne i regionalne. Kiedyś atrakcyjne ze względu na niższą cenę, po ujednoliceniu kosztów rejestracji z domenami .pl ich liczba stale spada. Ich udział w ogólnej liczbie rejestracji w naszym serwisie spadł aż o 15%, co wskazuje, iż mając do wyboru domeny drugiego i trzeciego poziomu w tej samej cenie, użytkownicy zdecydowanie wolą te pierwsze.

Marginalny pozostaje także udział domen IDN w ogólnej liczbie rejestracji. Widać, że idea rejestracji domen „z polskimi znakami” wciąż nie przebiła się do świadomości przeciętnego użytkownika Internetu. Wiele osób nadal nie wie, że takie domeny w ogóle istnieją oraz, że należy je rejestrować bądź zakupić osobno, co podwaja koszty.

Wyzwaniem pozostaje nadal zainteresowanie polskimi domenami podmiotów zagranicznych. Mimo, iż rozszerzenie .pl jest jednym z najpopularniejszych w Europie, jest ona rejestrowana niemal wyłącznie przez mieszkańców Polski. Udział podmiotów zagranicznych w rejestracjach domen .pl jest niewielki; proporcja ta jest jeszcze mniejsza w przypadku kupna domen na rynku wtórnym. Wydaje się, że dla osób z zagranicy rynek polski jest wciąż zbyt egzotyczny i mało znany.

OVH SAS

Polski rynek domen rozwija się dynamicznie, a użytkownicy coraz częściej wybierają rozwiązania, które zapewniają nie tylko konkurencyjne ceny, ale także wysoki poziom zabezpieczeń, automatyzację zarządzania oraz wsparcie techniczne na najwyższym poziomie. OVHcloud odpowiada na te potrzeby, oferując kompleksowe usługi rejestracji i zarządzania domenami, w tym zabezpieczenia DNSSEC, które m.in. chronią przed cyberatakami kryptologicznymi typu „man-in-the-middle” i podmianą danych w systemie DNS.

Ponadto cieszy nas fakt, że korzystanie z lokalnych, europejskich graczy rozwija rynek wewnętrzny. Rośnie zapotrzebowanie na stabilne usługi, zwłaszcza napędzane sztuczną inteligencją, co przekłada się na większe wykorzystanie zasobów chmurowych, np. naszej chmury publicznej czy gotowych rozwiązań wspierających wdrażanie sztucznej inteligencji w firmach i organizacjach, w tym do trenowania modeli LLM.

Jako jeden z kluczowych Partnerów NASK, niezmiennie pozostajemy największym operatorem z bogatą ofertą obejmującą szeroki zakres usług artificial intelligence, chmurowych, hostingowych oraz rejestracji domen, które spełniają oczekiwania zarówno małych firm, jak i dużych przedsiębiorstw – jak komentuje Robert Paszkiewicz, VP, Central and Eastern Europe, OVHcloud.

Home.pl S.A.

Początek roku 2025, w którym obchodzimy dwie ważne rocznice w historii domen – 40-lecie rejestracji pierwszej domeny .com, oraz 35-lecie utworzenia domeny .pl – to dobry moment na ocenę rynku.

Poczynając od wspomnianej już domeny .pl można zdecydowanie uznać, że miniony rok 2024 był dla niej kolejnym udanym okresem, umacniającym jej – niezakłóconą od dekad – pozycję jako ulubionej domeny polskich abonentów. Świadczy o tym również sytuacja na rynku odnowień domen .pl, który z roku na rok – i nie inaczej było w 2024 roku – jest coraz bardziej dojrzały i ustabilizowany. Wysoki wskaźnik odnowień potwierdza, że decyzja o wyborze domeny .pl jest z reguły długoterminową inwestycją, a abonenci cenią sobie stabilność.

Analiza rynku pokazuje również, że Klienci biznesowi coraz częściej zdają sobie sprawę z ważności posiadania własnej strony internetowej, która umożliwia im prezentację swoich usług i produktów w sieci. Mimo dynamicznego rozwoju i ekspansji social mediów, posiadanie własnej, niezależnej strony internetowej jest dla nich priorytetem. Co ważne, obserwujemy również zwiększoną świadomość Klientów w aspekcie bezpieczeństwa. Świadczy o tym fakt, że zakupowi domen często towarzyszą usługi komplementarne, w szczególności podnoszące bezpieczeństwo, takie jak certyfikaty SSL. Obserwujemy ten trend z dużym zadowoleniem i satysfakcją, ponieważ w home.pl sporo miejsca poświęcamy edukacji Klientów w obszarze cyberbezpieczeństwa.

Wspomniane już zainteresowanie Klientów własną stroną internetową wiąże się w oczywisty sposób z nazwą domeny. W tym aspekcie ważnym wyzwaniem jakie obserwujemy jest fakt, że większość „chwytliwych” i „prostych” nazw jest już zajęta. W takim przypadku istnieją co najmniej dwa rozwiązania: zakup domeny z rynku wtórnego lub nowoczesne narzędzia, takie jak wyszukiwarki z AI, które pomagają Klientom znaleźć idealną – czasem nieoczywistą – nazwę domeny. Obie te usługi znajdują się w portfolio home.pl.

Po udanym roku 2024 patrzymy z optymizmem w przyszłość, wierząc, że domena .pl pozostanie pierwszym wyborem Polaków, zarówno do użytku prywatnego, jak i komercyjnego.

nazwa.pl sp. z o.o.



Rok 2024 potwierdził wyraźny trend na rynku domen. Dziś liczy się realne wykorzystanie adresów internetowych, a nie nabywanie ich w celach inwestycyjnych. Firmy coraz częściej traktują domenę jako istotny element strategii biznesowej, zwłaszcza w kontekście rosnącego sektora e-commerce. W tym procesie kluczową rolę odgrywa nazwa.pl, która dostarcza nowoczesne usługi chmurowe i wspiera przedsiębiorstwa w ich obecności online.

Jako część NetArt Group patrzymy na rynek domen zarówno lokalnie, jak i globalnie. W Polsce rozszerzenie .pl niezmiennie pozostaje podstawowym wyborem firm i użytkowników prywatnych. Jego stabilność, prestiż i rozpoznawalność sprawiają, że przedsiębiorcy chętnie po nie sięgają. Jednocześnie na świecie obserwujemy wzrost znaczenia domen nTLD (new gTLDs), które zyskują popularność zwłaszcza wśród startupów i branż kreatywnych. Choć tradycyjne końcówki, takie jak .com, nadal dominują, to coraz więcej firm dostrzega potencjał w nowych typach domen dopasowanych do profilu działalności.

W ostatnich latach nastąpił wyraźny wzrost liczby firm posiadających strony internetowe i sklepy online, które opierają swoją działalność na zaawansowanych usługach chmurowych. Przedsiębiorstwa świadomie wybierają domeny, które są bezpośrednio wykorzystywane w biznesie, a nie jedynie parkowane czy przeznaczone do dalszej odsprzedaży. To zjawisko odzwierciedla nowoczesne podejście do budowania obecności w sieci – liczy się nie tylko rejestracja adresu, lecz także jego rzeczywiste zastosowanie w prowadzonej działalności gospodarczej.

Każdego dnia rośnie świadomość zagadnień związanych z zagrożeniami obecnymi w Internecie. Firmy chętnie inwestują w ochronę swoich marek poprzez rejestrację różnych wariantów domen oraz wybór rozwiązań technologicznych, takich jak DNSSEC. Klienci biznesowi poszukują skutecznej ochrony przed atakami phishingowymi i próbami przejęcia domen, zwracając szczególną uwagę na bezpieczeństwo w środowisku cyfrowym. W nazwa.pl aktywnie wspieramy te procesy, dlatego dostarczamy kompleksowe rozwiązania, które umożliwiają przedsiębiorstwom nie tylko skuteczne, lecz także bezpieczne funkcjonowanie w Internecie.

Polska utrzymuje silną pozycję na europejskim rynku domen krajowych, zajmując 6. miejsce pod względem liczby zarejestrowanych domen z rozszerzeniem .pl – około 2,6 miliona. Tym samym niezmiennie znajdujemy się w pierwszej dziesiątce państw europejskich, pozostając liderem w regionie Europy Środkowo-Wschodniej.

Analizując wskaźnik liczby domen przypadających na jedną firmę, który w Polsce wynosi około 1,04 domeny na firmę - można zauważyć umiarkowany poziom aktywności firm w przestrzeni online. Dla porównania: w Niemczech średnia ta wynosi 5,4 domeny na firmę, a w Holandii – 3,3, co wskazuje na istotny potencjał wzrostu w Polsce, szczególnie w sektorze MŚP. Z kolei wynik Polski jest wyższy niż np. we Francji (0,66), co świadczy o postępującej digitalizacji rodzimego biznesu.

W 2024 roku liczba zarejestrowanych domen .pl wzrosła o 2,3% rok do roku. Choć dynamika wzrostu nie była najwyższa w Europie, to stabilny przyrost rejestracji potwierdza zaufanie użytkowników do tej domeny, jako podstawowego narzędzia obecności online. Domena .pl pozostaje najczęściej wybieranym rozszerzeniem na polskim rynku, a jej pozycja umacniana jest dodatkowo przez wysoki wskaźnik odnowień i rosnącą jakość obsługi.

W mijającym roku zaobserwowaliśmy również rosnące zainteresowanie domenami dedykowanymi dla e-commerce. Dynamiczny rozwój handlu internetowego sprawił, że firmy coraz częściej szukają adresów, które nie tylko są łatwe do zapamiętania, ale także zoptymalizowane pod kątem SEO. To zjawisko idealnie wpisuje się w trend traktowania domeny jako integralnej części marki. Przedsiębiorcy coraz częściej wybierają nazwy, które nie tylko pasują do ich działalności, ale także komunikują wartości firmy.

Z większym zainteresowaniem domenami wiąże się również rosnąca świadomość konieczności ich ochrony. Według badań przeprowadzonych przez cyberFolks 16% podmiotów rejestrowało domeny w celu ochrony marki. Wartość domen sprawia, że coraz więcej firm zabezpiecza się przed cybersquattingiem i działaniami nieuczciwych podmiotów. Przedsiębiorcy decydują się na rejestrowanie różnych wariantów swoich domen w różnych rozszerzeniach, aby uniemożliwić ich przejęcie. Wzrost liczby ataków phishingowych i stron podszywających się pod znane marki tylko potwierdza, jak ważna staje się ochrona domen w strategii biznesowej. Coraz więcej firm traktuje swoją domenę na równi z nazwą, logo czy identyfikacją wizualną. Trendy wskazują, że w nadchodzących latach domeny będą odgrywać jeszcze większą rolę w budowaniu marek i zabezpieczaniu ich tożsamości w Internecie.

Podsumowując, Polska pozostaje ważnym graczem na europejskim rynku domen, z silną pozycją regionalną i stabilnym wzrostem. Jednocześnie nadal istnieje znaczny potencjał rozwoju, zwłaszcza w kontekście aktywizacji małych i średnich przedsiębiorstw oraz wykorzystania nowych możliwości, jakie daje dywersyfikacja rozszerzeń domenowych.

DD sp. z o.o.

W ubiegłym roku prawie 700 tysięcy domen .pl nie zostało odnowionych na kolejny okres. Z naszych statystyk wynika, że około 20% z tych domen zostało ponownie zarejestrowanych w chwilę po ich usunięciu. Mogą to być nazwy wartościowe ze względu na swoją historię, pozycję w wyszukiwarkach i przydatność w pozycjonowaniu stron. Mogą to być też domeny z ciekawymi nazwami, które były niedostępne, a po usunięciu znalazły nowe zastosowanie.

Nasz serwis, jako jeden z nielicznych w Polsce, obsługuje tzw. wtórny rynek domen internetowych. Przechwytyjemy domeny na zlecenie naszych klientów - rejestrujemy nazwy zaraz po ich usunięciu z rejestru. Naszymi klientami są głównie małe i średnie przedsiębiorstwa, agencje SEO oraz specjaliści z branży IT.

W roku 2024 nasz serwis odnotował 60% wzrost rejestracji domen w porównaniu do 2023 roku. Pierwsze miesiące bieżącego roku potwierdzają ten trend. Widzimy rosnące zainteresowanie specjalistycznymi usługami, takimi jak przechwytywanie czy obsługa dużych portfolio domen. Zapewniamy narzędzia, które pozwalają na łatwe zarządzanie i utrzymanie setek czy nawet tysięcy domen w ramach jednego portfolio. Nasze profesjonalne, ale jednocześnie indywidualne podejście, pozwala na dostosowanie się do indywidualnych potrzeb klientów.

W 2025 roku będziemy nadal aktywnie uczestniczyć w programach Rejestru domen .pl NASK, mających na celu promocję i rozwój rynku domen .pl. Rozszerzenie .pl to niekwestionowany lider i podstawowy wybór dla podmiotów prowadzących biznes w Polsce.

LH Sp. z o.o.

Rok 2024 w LH.PL oceniamy jako bardzo udany. Zwiększyliśmy liczbę zarejestrowanych nowych domen, spośród których domena .pl wciąż stanowi zdecydowaną większość rejestracji. Obserwujemy wciąż rosnące zainteresowanie widocznością firm w sferze online, co pozytywnie wpływa także na inne oferowane przez nas produkty. Niezmiennie realizujemy strategię, w której jakość obsługi klienta, bezpieczeństwo i stabilność usług cyfrowych są na pierwszym miejscu. W 2024 roku pozytywnie przeszliśmy audyt naszych systemów ISO 9001 oraz 27001, co stanowi potwierdzenie jakości oraz wysokiego poziomu bezpieczeństwa.

Podobnie jak w roku ubiegłym, nasz dział bezpieczeństwa zauważył zwiększoną liczbę ataków cybernetycznych, np. phishing – coraz więcej domen, w tym także domen .pl jest rejestrowanych w celu przeprowadzenia phishingu. Udoskonaliliśmy rozwiązania, które minimalizują ryzyka z tym związane.

Rok 2024 upłynął nam pod znakiem bezpieczeństwa, podobnie jak inni rejestratorzy oraz hostingodawcy, śledzimy losy Krajowego Systemu Cyberbezpieczeństwa i przygotowujemy się do wdrożenia NIS2.

Mimo wyzwań, zdecydowanie jesteśmy zadowoleni z wyników, jakie w roku 2024 osiągnęło LH.PL. Jesteśmy gotowi na dalszy rozwój i kolejne wyzwania w celu realizacji naszej misji zapewniania klientom ciągłości działania w sieci.

DOMENY.TV MSERWIS Sp. z o.o.



Rok 2024 był dla nas okresem stabilizacji. Nie zaobserwowaliśmy wzmożonego napływu rejestracji polskich domen. Odnotowaliśmy natomiast wzrost liczby przedłużeń o 4,77%. Wyraźnie pokazuje to rosnące przywiązanie użytkowników do posiadanych polskich adresów i chęć ich długoterminowego utrzymania. Nieustannie monitorujemy te zmiany i dostosowujemy swoje usługi, aby zapewnić jak najlepsze wsparcie naszym klientom w zarządzaniu ich adresami internetowymi.

.PL pozostaje niekwestionowanym liderem – stanowi u nas aż o 67,4% więcej rejestracji niż wszystkie pozostałe domeny łącznie. Jednocześnie zaznaczamy, że w naszym portfolio posiadamy największą w Polsce liczbę dostępnych do rejestracji rozszerzeń domenowych – obecnie oferujemy aż 1114 różnych rozszerzeń.

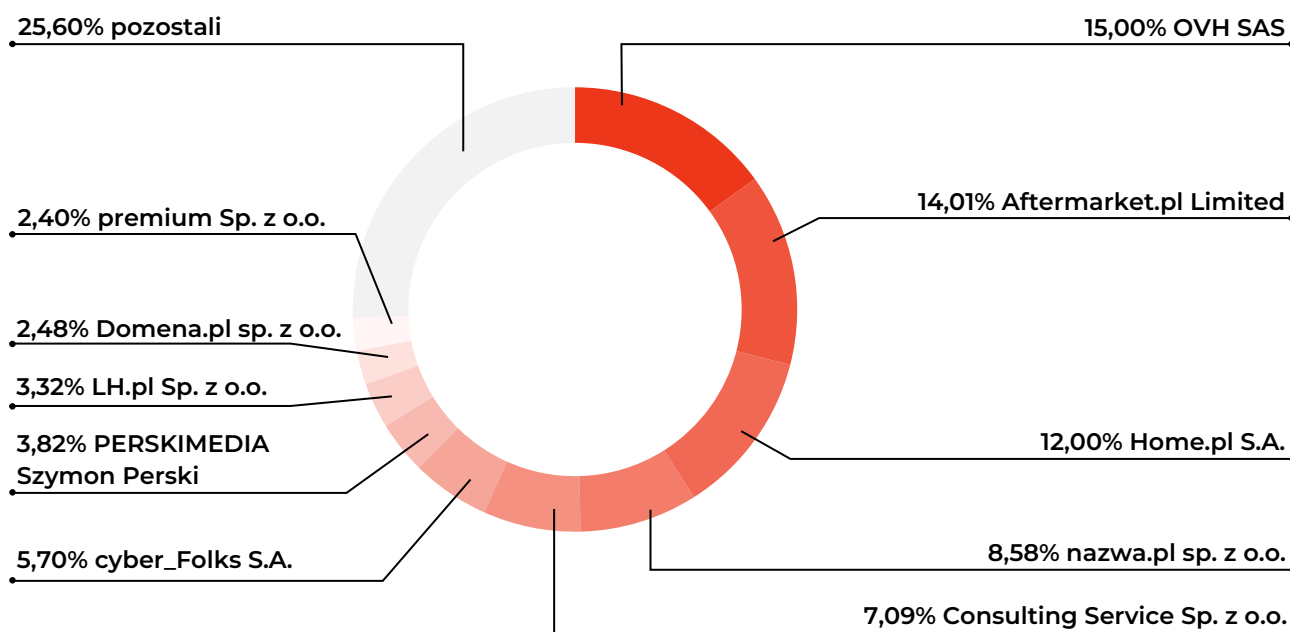
W 2024 roku, wychodząc naprzeciw potrzebom klientów w zakresie kreatywnego tworzenia nazw, rozbudowaliśmy nasz e-book o naming, który podpowiada, jak tworzyć atrakcyjne i skuteczne nazwy domen.

Zauważamy także coraz większe zainteresowanie kwestiami bezpieczeństwa, w tym DNSSEC oraz maksymalnym zabezpieczeniem zarówno samych domen, jak i panelu administracyjnego. W związku z tym nieustannie promujemy rozwiązania dwuskładnikowego uwierzytelniania (2FA) oraz inne narzędzia i mechanizmy, które pomagają naszym klientom zachować pełną kontrolę i bezpieczeństwo posiadanych adresów internetowych.

Wszystkie te działania i zmiany sprawiają, że stale podnosimy jakość naszych usług i odpowiadamy na zmieniające się potrzeby rynku. Doceniamy zaufanie naszych klientów i wspieramy ich w każdym aspekcie zarządzania domenami.

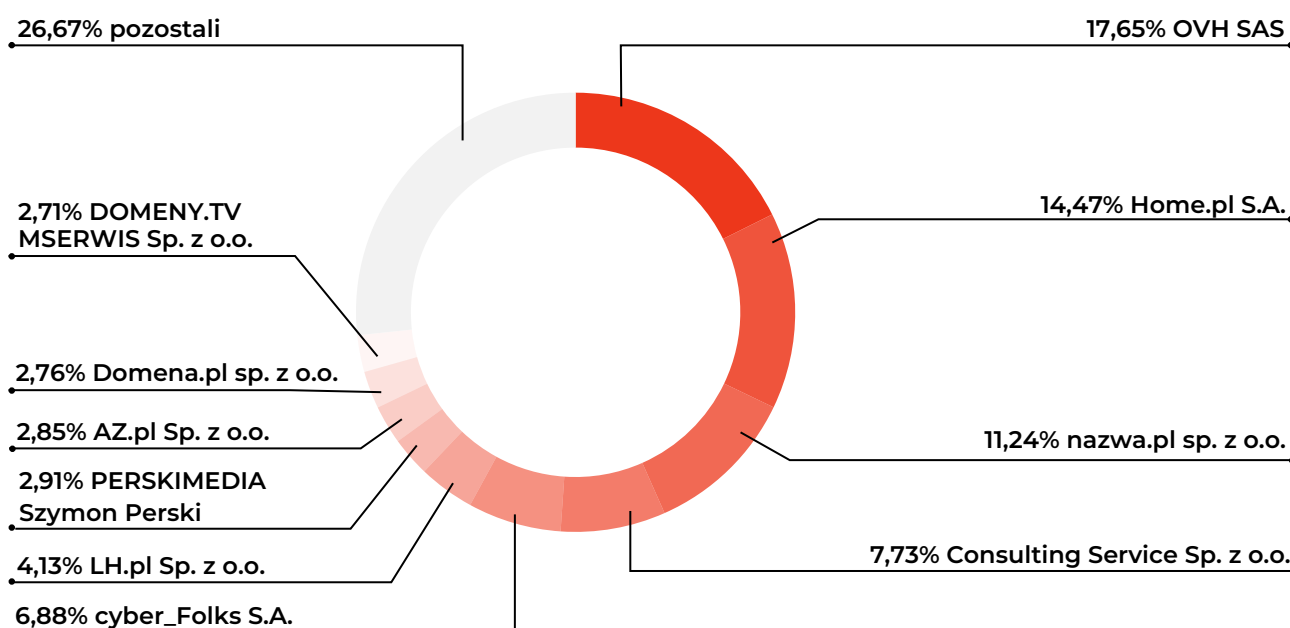
Podział rynku nazw domeny .pl

Procentowy udział Partnerów w obsłudze nazw domeny .pl, 2024



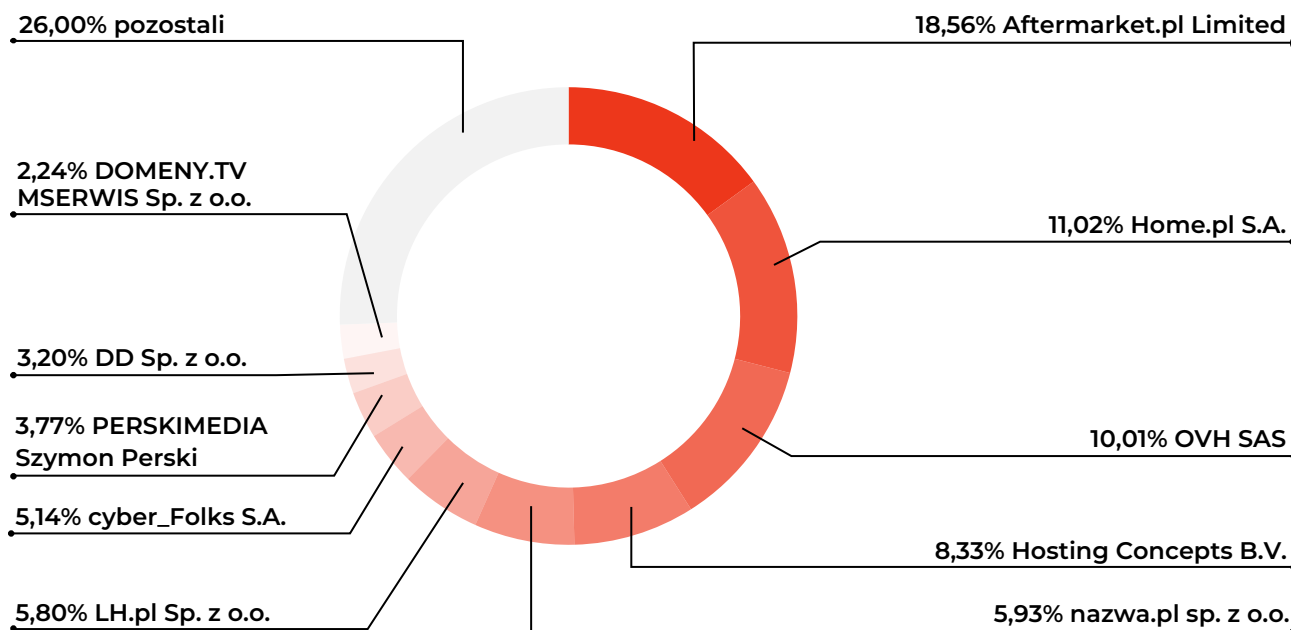
Copyright by NASK

Procentowy udział Partnerów w obsłudze Abonentów nazw domeny .pl, 2024



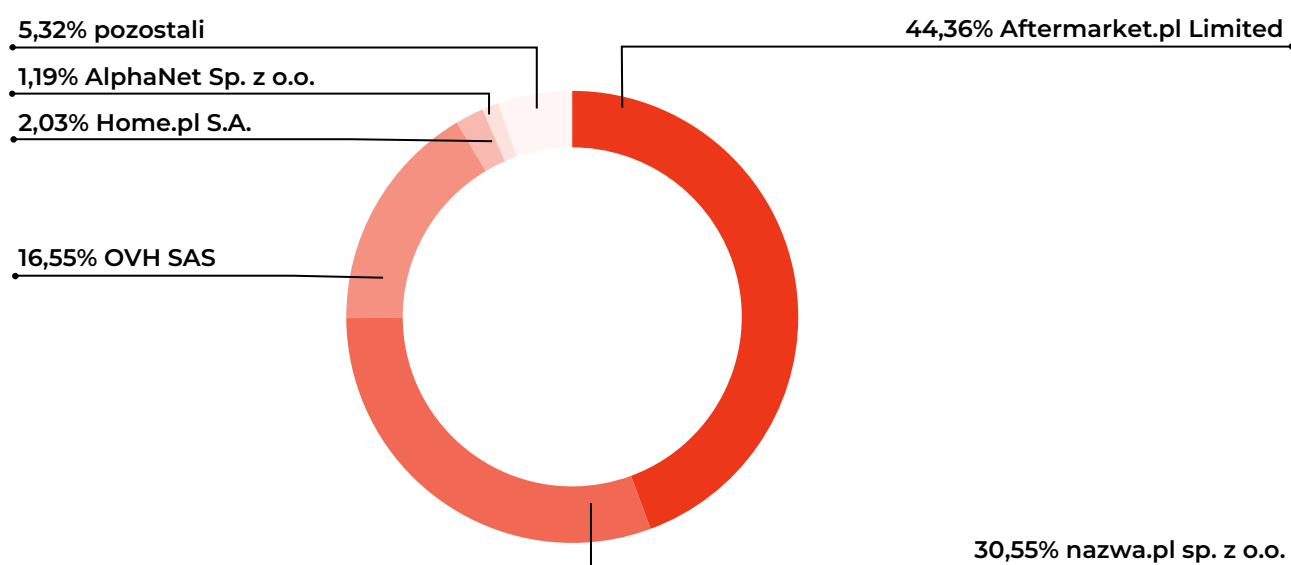
Copyright by NASK

Procentowy udział Partnerów w rejestracjach nazw domeny .pl, 2024



Copyright by NASK

Udział Partnerów w obsłudze nazw domeny .pl zabezpieczonych DNSSEC, 2024



Copyright by NASK



CZĘŚĆ II

Raport z badania na temat treści nielegalnych w Internecie

Informacje o badaniu

W tegorocznym raporcie Rejestru domeny .pl prezentujemy Państwu badania przeprowadzone wspólnie z Akademią Leona Koźmińskiego i Krajową Izbą Gospodarczą Elektroniki i Telekomunikacji (KIGEiT), poświęcone nielegalnym treściom w Internecie.

Tym razem o opinie poprosiliśmy dwie grupy respondentów. Pierwszą z nich była reprezentatywna grupa Polaków, a celem badania była ocena wiedzy Polaków na temat treści nielegalnych w Internecie, ich osobistych doświadczeń z nimi związanych, a także weryfikacja ich wiedzy na temat przepisów prawa, skuteczności zgłaszania nielegalnych treści oraz ochrony tożsamości cyfrowej. Wyniki przeprowadzonego ogólnopolskiego badania posłużą do opracowania rekomendacji dla instytucji publicznych oraz organizacji pozarządowych, które mogą przyczynić się do poprawy edukacji i ochrony użytkowników Internetu w Polsce.

Druga grupa respondentów obejmowała 16 rejestratorów - partnerów biznesowych, współpracujących z NASK-PIB w ramach Programu Partnerskiego NASK. Dobór przedstawicieli tej branży był celowy, z uwagi na ekspercki charakter badania. Ich opinie na temat nielegalnych treści w Internecie dodatkowo wzbogaciły ten raport. Wnioski uzyskane od rejestratorów pozwoliły na uzupełnienie raportu o perspektywę branżową, co umożliwia lepsze zrozumienie wyzwań stojących przed sektorem rejestracji domen oraz formułowanie skuteczniejszych rekomendacji dla polityki publicznej w obszarze cyberbezpieczeństwa i ochrony użytkowników Internetu.

PRÓBA BADAWCZA

- Reprezentatywna próba Polek i Polaków w wieku 18 lat+ (ze względu na płeć, wiek, województwo, wielkość miejsca zamieszkania i wykształcenie). Liczebność próby: N=1083
- Grupa 16 ekspertów - partnerów biznesowych, współpracujących z NASK-PIB w ramach Programu Partnerskiego

TERMIN REALIZACJI BADANIA

- listopad - grudzień 2024

METODOLOGIA BADANIA

- badanie online (CAWI) na reprezentatywnej grupie Polaków oraz partnerach biznesowych NASK-PIB
- badanie przeprowadzone na panelu badawczym ReaktorOpinii.pl należącym do grupy Accorp Sp. z o.o.

Pytania badawcze

1. Jakie treści w Internecie są według Pana(i) nielegalne?
2. Jak często spotyka się Pan(i) z następującymi treściami w Internecie?
3. Czy kiedykolwiek natknął/natknęła się Pan(i) na treści w Internecie, które są według Pana(i) nielegalne?
4. Gdzie w Internecie najczęściej natrafia Pan(i) na treści nielegalne?
5. Komu Pana(i) zdaniem można zgłosić fakt natrafienia na nielegalne treści w Internecie?
6. Jakie działania podejmuje Pan(i), kiedy natrafi na nielegalne treści w Internecie?
7. Czy uważa Pan(i), że zgłaszanie komuś treści nielegalnych może prowadzić do ich usunięcia?
8. Czy uważa Pan(i), że obecność treści nielegalnych w Internecie wpływa negatywnie na społeczeństwo?
9. W jaki sposób, Pana(i) zdaniem, obecność treści nielegalnych w Internecie wpływa negatywnie na społeczeństwo?
10. Czy Pana(i) zdaniem nowe technologie (takie jak sztuczna inteligencja) wspierają wykrywanie treści nielegalnych w Internecie?
11. Czy Pana(i) zdaniem nowe technologie (takie jak sztuczna inteligencja) wspierają usuwanie treści nielegalnych w Internecie?
12. Czy według Pan(i) platformy społecznościowe (np. Facebook, Instagram) skutecznie usuwają treści nielegalne?

- 13.** Co, Pana(i) zdaniem, jest bardziej skuteczne w walce z nielegalnymi treściami w Internecie – usuwanie treści nielegalnej, czy blokowanie dostępu do konta jej autorowi?
- 14.** Czy obawia się Pan(i) o wolność słowa w związku z automatycznym usuwaniem treści podejrzanych o to, że są nielegalne?
- 15.** Czy uważa Pan(i), że niektóre treści szkodliwe (np. kontrowersyjne opinie polityczne, religijne lub filozoficzne, kontrowersyjne dzieła artystyczne, których celem jest np. zwrócenie uwagi na jakiś ważny problem społeczny) powinny być legalne, jeśli są zgodne z zasadami wolności słowa?
- 16.** Czy ma Pan(i) obawy, że Pana(i) tożsamość cyfrowa (czyli informacje reprezentujące Pana/i osobę w Internecie) może zostać naruszona?
- 17.** Jakiego rodzaju agresja w Internecie jest Pana(i) zdaniem najczęstsza?
- 18.** Czy w ciągu ostatnich 12 miesięcy był(a) Pan(i) narażony(a) na agresję w Internecie – np. ktoś napisał w Internecie coś negatywnego lub obraźliwego na Pana(i) temat?
- 19.** Gdzie w Internecie był(a) Pan(i) narażony(a) na agresję?
- 20.** Czy w ciągu ostatnich 12 miesięcy był(a) Pan(i) świadkiem, że ktoś inny stał się ofiarą agresji w Internecie – np. że ktoś napisał w Internecie coś negatywnego lub obraźliwego na czyjś temat?
- 21.** Gdzie w Internecie zauważył(a) Pan(i), że ktoś inny stał się ofiarą agresji/naruszeń w Internecie?
- 22.** Czy powstrzymuje się Pan(i) od wyrażania swojej opinii w Internecie z obawy przed staniem się ofiarą agresji cyfrowej?
- 23.** Czy według Pana(i), łatwo jest znaleźć informacje na temat tego co stanowi treść nielegalną w Internecie?
- 24.** Czy według Pana(i) łatwo jest odnaleźć informacje na temat przepisów prawa dotyczących treści nielegalnych w Internecie?
- 25.** Jak ocenia Pan(i) skuteczność przepisów prawa w zakresie zwalczania treści nielegalnych w Internecie?

Najważniejsze wnioski z badania

1. Polacy dobrze rozpoznają nielegalne treści, jednak niektóre obszary, jak dezinformacja czy dyskryminacja, są rzadziej kojarzone z naruszeniem prawa.
2. Media społecznościowe są głównym miejscem styczności z nielegalnymi treściami, ale wielu Polaków nie wie, gdzie je zgłaszać.
3. Mimo tego, że Polacy mają świadomość zagrożeń, niemal połowa z nich nie podejmuje żadnych działań wobec treści nielegalnych.
4. Nowe technologie, w tym AI, są postrzegane jako potencjalnie pomocne, ale wiele osób nie ma zdania na ich temat.
5. Ponad połowa Polaków uważa, że kontrowersyjne treści powinny być legalne, jeśli mieszczą się w granicach wolności słowa.
6. Strach przed agresją w sieci powoduje ograniczenie swobody wypowiedzi, co negatywnie wpływa na debatę publiczną w Internecie.
7. Polacy są sceptyczni wobec skuteczności prawa i działań platform społecznościowych w zwalczaniu treści nielegalnych.
8. Mowa nienawiści i wyśmiewanie to najczęstsze formy agresji w sieci.
9. Strach przed agresją ogranicza aktywność Polaków w Internecie – wielu unika komentowania i wyrażania opinii.
10. Polacy wykazują wysoką świadomość zagrożeń, szczególnie w zakresie ochrony dzieci, danych osobowych i treści terrorystycznych.
11. Osoby starsze i lepiej wykształcone częściej identyfikują więcej rodzajów treści nielegalnych, co może świadczyć o większej wiedzy prawnej i doświadczeniu w ocenie ryzyka.

Nielegalne treści w Internecie

Wnioski z badań w liczbach



Płeć

KOBIETY:

- Częściej dostrzegają negatywny wpływ treści nielegalnych na społeczeństwo (92%).
- Częściej unikają wyrażania swojej opinii w Internecie (30%).
- Uważają, że oba sposoby (usuwanie treści nielegalnej lub blokowanie dostępu do konta jej autorowi) są równie skuteczne (49%).
- Najczęściej wybierają administratorów platform społecznościowych i serwisów internetowych jako miejsce zgłaszania treści nielegalnych (56%).
- Ich zdaniem drugą najczęściej wskazywaną formą agresji online jest wyśmiewanie innych – mocking (64%).
- Częściej dostrzegają cyberbullying (nękanie, poniżanie, zastraszanie), niż inne formy agresji (51%).

MĘŻCZYŹNI:

- Częściej spotykają się z nielegalnymi treściami w Internecie (47%).
- Częściej doświadczyli osobistego zetknięcia się z agresją w Internecie (13%).
- Często nie wykazują reakcji na treści nielegalne w Internecie (53%).
- Są bardziej przekonani o skuteczności nowych technologii w walce z nielegalnymi treściami w Internecie (51%).
- Uważają, że bardziej efektywne w walce z treściami nielegalnymi w Internecie jest blokowanie dostępu do konta ich autora (39%).
- Częściej wyrażają obawy przed automatycznym usuwaniem treści podejrzanych (40%).
- Są zdania, że kontrowersyjne treści powinny pozostać legalne, jeśli są zgodne z zasadami wolności słowa (57%).
- Uważają, że łatwo jest znaleźć informacje o treściach nielegalnych w Internecie (49%).



Wiek

- Osoby młode 18-29 lat najczęściej spotykały się z nielegalnymi treściami w Internecie (61%).
- Osoby w wieku 18-39 lat najczęściej wyrażają obawy przed automatycznym usuwaniem treści podejrzanych (43%).
- Osoby w wieku 18-29 lat najczęściej mają do czynienia w Internecie z dyskryminacją na tle rasowym, religijnym, seksualnym (56%).
- Głównie osoby młode 18-29 lat były świadkami agresji w Internecie (60%).
- Osoby w wieku 18-29 lat (58%) oraz 30-39 lat (57%) uważają, że łatwo jest znaleźć informacje o treściach nielegalnych w Internecie.
- Osoby w wieku 18-29 lat (56%) oraz 40-49 lat (56%) uważają, że znalezienie informacji na temat przepisów prawa dotyczących treści nielegalnych

w Internecie jest łatwe.

- Osoby w wieku 30-39 lat są szczególnie narażone na kontakt z treściami nielegalnymi poprzez platformy streamingowe (43%).
- Osoby w wieku 40-49 lat wskazały komunikatory jako główne źródło treści nielegalnych (35%).
- Osoby w wieku 40-49 lat najczęściej zauważają prowokowanie konfliktów i szerzenie dezinformacji (cybertrolling) (57%).
- Osoby w wieku 50-59 lat są silnie przekonane o zgłaszaniu treści nielegalnych do instytucji, które mogą prowadzić do ich usunięcia (80%).
- Osoby powyżej 70. roku życia uważają, że bardziej efektywne w walce z treściami nielegalnymi w Internecie jest blokowanie dostępu do konta ich autora (44%).



Wykształcenie

Osoby z wykształceniem wyższym:

- Częściej spotykają się z nielegalnymi treściami w Internecie (47%).
- Są częściej narażone na kontakt z nielegalnymi treściami poprzez platformy streamingowe (41%).
- Najczęściej wybierają administratorów platform społecznościowych i serwisów internetowych jako miejsce zgłaszania treści nielegalnych (59%).
- Częściej dostrzegają negatywny wpływ treści nielegalnych na społeczeństwo (94%).
- Są częściej przekonane o skuteczności nowych technologii w walce z treściami nielegalnymi w Internecie (51%).
- Najczęściej uważają, że oba sposoby (usuwanie treści nielegalnej lub blokowanie dostępu do konta jest autorowi) są równie skuteczne (52%).
- Są zdania, że kontrowersyjne treści powinny pozostać legalne, jeśli są zgodne z zasadami wolności słowa (59%).
- Najczęściej zgłaszają obawy o naruszenie tożsamości cyfrowej (67%).
- Najczęściej były świadkami agresji w Internecie (49%).
- Uważają, że najczęstszą formą agresji online jest mowa nienawiści (75%).
- Najczęściej zauważają prowokowanie konfliktów i szerzenie dezinformacji (cybertrolling) w Internecie (57%).
- Często unikają wyrażania swojej opinii w Internecie (32%).

Osoby z wykształceniem średnim i poniżej średniego:

- Osoby z wykształceniem średnim częściej osobiście zetknęły się z agresją w Internecie (13%).
- Uważają, że zetknięcie się z treściami nielegalnymi nie wpływa negatywnie na społeczeństwo (6%).
- Rzadziej obawiają się o naruszenie tożsamości cyfrowej w Internecie.
- Osoby z wykształceniem średnim i niższym rzadziej były świadkiem agresji w Internecie.
- Osoby z wykształceniem poniżej średniego uważają obowiązujące przepisy prawa w zakresie zwalczania treści nielegalnych w Internecie za skuteczne (24%).



dr hab. Monika Dorota Adamczyk
prof. KUL

Profesor KUL - Katedra Praw
Człowieka i Pracy Socjalnej
Instytut Nauk Socjologicznych
Wydział Nauk Społecznych
Katolicki Uniwersytet Lubelski
Jana Pawła II

KOMENTARZ EKSPERTA

Analizując wyniki raportu „Polacy wobec nielegalnych treści w Internecie”, nie sposób pominąć szerszy kontekst społeczny, w którym funkcjonujemy – kontekstu społeczeństwa 5.0. To koncepcja rzeczywistości silnie z informatyzowanej, w której technologia cyfrowa – od Internetu, przez sztuczną inteligencję, po Internet rzeczy – przenika wszystkie sfery życia, od pracy po relacje społeczne, edukację czy odpoczynek. W takim środowisku nie tylko dostęp do treści (zarówno legalnych, jak i nielegalnych) staje się powszechny, ale również niemożliwe staje się pełne odcięcie od świata cyfrowego. Internet nie jest już przestrzenią alternatywną – to integralna część naszej codzienności, która kształtuje tożsamość jednostek i wspólnot.

Najmocniej obecność tego cyfrowego wymiaru odczuwają przedstawiciele pokoleń Y (milenialsi), Z i Alfa – pokoleń „zanurzonych w ekranie”. Dane raportu jednoznacznie pokazują, że osoby w wieku 18–29 lat są najbardziej narażone na kontakt z nielegalnymi treściami – aż 61% z nich zetknęło się z nimi w Internecie. Co więcej, to ta grupa najczęściej doświadcza dyskryminacji na tle rasowym, religijnym czy seksualnym (56%), a także agresji (60%). To nie tylko świadectwo cyfrowej aktywności tej grupy, ale również ich szczególnej podatności na przemoc symboliczną oraz niestabilność norm społecznych w przestrzeni online.

Pokolenie X (obecnie osoby w wieku 40–59 lat) również coraz częściej dostrzega ciemną stronę cyfrowego świata. To właśnie ta grupa wiekowa najczęściej zauważa zjawiska takie jak trolling (57%) czy szerzenie dezinformacji, a osoby w wieku 40–49 lat wskazują komunikatory jako główne źródło nielegalnych treści (35%). Wskazuje to na potrzebę zwiększenia czujności i edukacji medialnej także wśród pokoleń, które weszły w świat cyfrowy później niż ich młodszy koledzy i koleżanki.

W przypadku najstarszych grup wiekowych (60+, a szczególnie 70+), dominuje przekonanie, że skuteczne działania powinny mieć charakter represyjny – np. blokowanie kont autorów nielegalnych treści (44%). To spojrzenie bliskie koncepcji społecznej kontroli, typowej dla pokolenia Baby Boomers, które wychowywało się w zupełnie innych warunkach komunikacyjnych, a obecnie mierzy się z koniecznością adaptacji do świata, którego reguły często są niejasne i zmienne.

Różnice w percepcji i reakcji na treści nielegalne dostrzegalne są również na poziomie wykształcenia. Osoby z wykształceniem wyższym wykazują większą świadomość zagrożeń i częściej dostrzegają

negatywny wpływ tych treści na społeczeństwo (94%), częściej także zgłaszają je administratorom (59%). Co istotne, są też bardziej przekonane o skuteczności nowych technologii w przeciwdziałaniu nielegalnym treściom (51%), choć jednocześnie obawiają się naruszeń tożsamości cyfrowej (67%) i często powstrzymują się od wyrażania opinii w sieci (32%). Mamy tu do czynienia z paradoksalnym zjawiskiem cyfrowej ambiwalencji – technologia daje poczucie bezpieczeństwa, ale jednocześnie budzi niepokój.

Szczególnie interesujące są różnice płciowe. Kobiety wykazują większą wrażliwość na przemoc symboliczną – częściej zauważają cyberbullying (51%) i mocking (64%), a także częściej unikają wypowiadania się w sieci (30%). Mężczyźni z kolei są bardziej przekonani o skuteczności technologii, jednocześnie częściej ignorują nielegalne treści (53%), co może wskazywać na postawy obojętności lub znormalizowanie agresji w przestrzeni cyfrowej.

W społeczeństwie 5.0, w którym granice między tym, co „realne”, a tym, co „wirtualne” stają się płynne, nielegalne treści w Internecie przestają być jedynie „problemem technicznym”. Są wyzwaniem społecznym, kulturowym i etycznym, wymagającym działań wielopoziomowych – od edukacji cyfrowej, przez regulacje prawne, po rozwój empatii i odpowiedzialności online. Ucieczka od Internetu nie jest możliwa – możliwe jest jedynie wypracowanie dojrzałych kompetencji cyfrowych, które pozwolą na świadome i odpowiedzialne korzystanie z jego zasobów.



Osobiste doświadczenia z treściami nielegalnymi

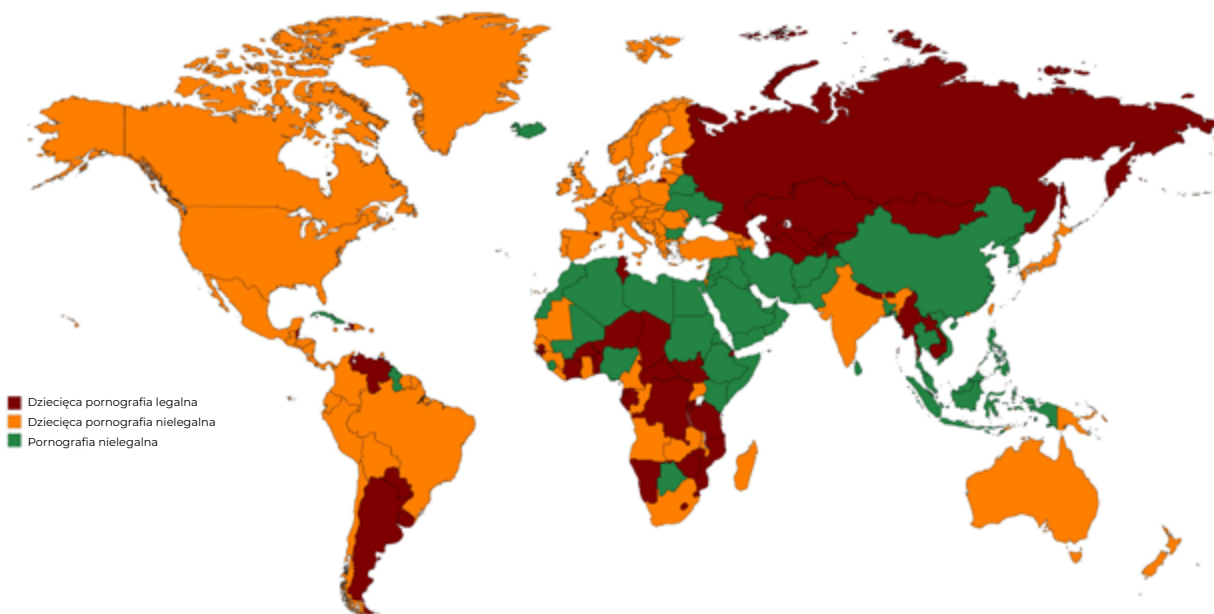
Czy rosnąca świadomość istnienia treści nielegalnych w Internecie sprawia, że czujemy się w sieci bezpieczniej?

Jakie treści w Internecie są według Pana(i) nielegalne?

Liczebność próby: N=1083

Najczęściej wskazywane treści nielegalne

Na pierwszym miejscu znajduje się pornografia dziecięca (93%). Powszechnie w Europie, w rozumieniu społecznym, a co za tym idzie, prawnym, wydaje się oczywiste, że pornografia dziecięca jest treścią nielegalną. Jednak jak widać na poniższym wykresie, tego typu treści nie są jednak jednoznacznie uznawane za nielegalne na całym świecie. Bardzo wysokie wskazania dotyczą także naruszenia danych osobowych (85%) i treści terrorystycznych (84%).



Legalność dziecięcej pornografii na świecie, Źródło: TECHPEDIA, <https://www.techpedia.pl/index.php?str=tp&no=32622>

Kwestie prawne i etyczne

Znaczny odsetek badanych (80%) uznaje naruszenie prawa własności intelektualnej za treść nielegalną. Świadczy to o rosnącej świadomości dotyczącej ochrony praw autorskich, jednak wciąż mogą występować różnice w interpretacji tego, co dokładnie jest nielegalne.

Treści związane z mową nienawiści i dyskryminacją

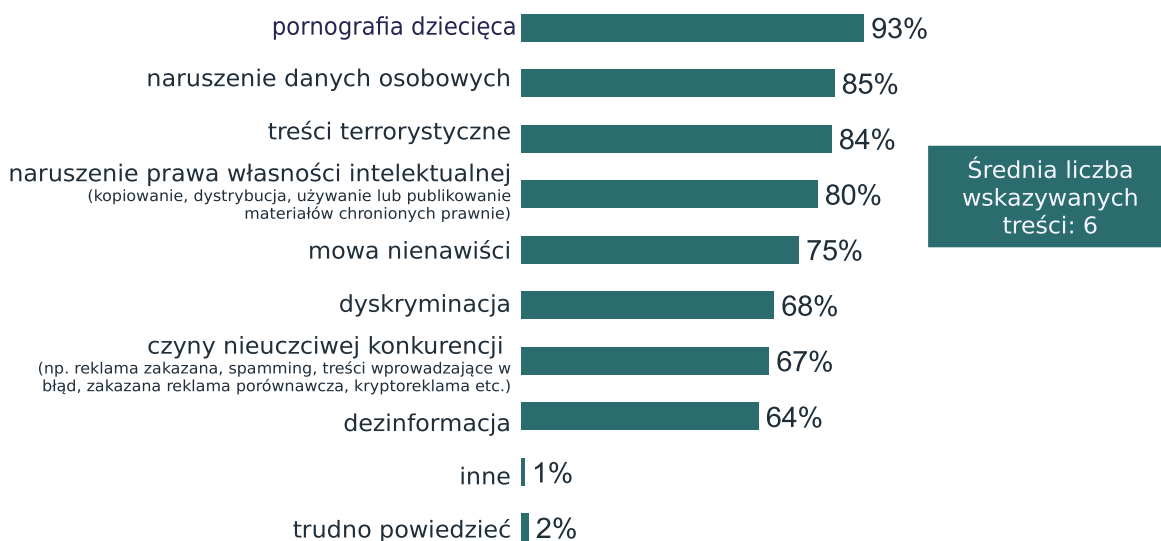
Mowa nienawiści (75%) oraz dyskryminacja (68%) są często uznawane za nielegalne, jednak nieco niższy poziom odpowiedzi w porównaniu z innymi kategoriami może wynikać z różnych regulacji prawnych oraz osobistych interpretacji wolności słowa.

Dezinformacja i nieuczciwa konkurencja

Dezinformacja została wskazana przez 64% respondentów, co sugeruje, że społeczeństwo coraz częściej postrzega ją jako zagrożenie, choć nie zawsze wiąże ją jednoznacznie z nielegalnością. Warto podkreślić, że według ubiegłorocznego raportu Fundacji Digital Poland „Dezinformacja oczami Polaków”, w Polsce utrzymuje się wysoki poziom dezinformacji – 91% Polaków zdecydowanie zgodziło się przynajmniej z jedną z badanych, fałszywych informacji (Fundacja Digital Poland, Dezinformacja oczami Polaków, Edycja 2024). Czyny nieuczciwej konkurencji (67%) również znalazły się wysoko, co może wynikać z rosnącej świadomości konsumenckiej i problemów związanych z fałszywymi reklamami czy kryptoreklamą.

Co ciekawe inną hierarchię wskazali badani przez nas eksperci. Na pierwszym miejscu, podobnie jak w badaniu ogólnopolskim, znalazła się pornografia dziecięca, jednak na drugim czyny nielegalnej konkurencji. Następnie wymienione zostały: naruszenie prawa własności intelektualnej, treści terrorystyczne, dezinformacja oraz dopiero na szóstej pozycji – naruszenie danych osobowych. Z dużym prawdopodobieństwem różnice te wynikają z charakteru branży, w której działają eksperci.

Treści nielegalne według badanych



Badanie wykazało, że Polacy mają wysoką świadomość dotyczącą treści nielegalnych w Internecie, jednak ich ocena różni się w zależności od kategorii. Najczęściej wskazywanymi treściami nielegalnymi są pornografia dziecięca, naruszenia danych osobowych i treści terrorystyczne. Kwestie prawne i etyczne, takie jak naruszenie prawa własności intelektualnej, również zostały wskazane przez większość badanych, co świadczy o rosnącej świadomości ochrony praw autorskich. Nieco większe rozbieżności pojawiły się w przypadku mowy nienawiści i dyskryminacji, co może wynikać z różnych interpretacji wolności słowa. Wśród dezinformacji i czynów nieuczciwej konkurencji zauważalny jest wzrost

społecznej świadomości zagrożeń, choć nie wszyscy jednoznacznie postrzegają je jako nielegalne. Wyniki te znajdują potwierdzenie w innych badaniach, np. w raporcie Fundacji Digital Poland, który wskazuje na wysoki poziom dezinformacji w Polsce. Co ciekawe, eksperci oceniają hierarchię zagrożeń nieco inaczej. Choć pornografia dziecięca pozostała na pierwszym miejscu, czyny nieuczciwej konkurencji znalazły się na drugim, wyprzedzając naruszenie praw własności intelektualnej i treści terrorystyczne. Naruszenie danych osobowych, które w badaniu ogólnym zajęły drugie miejsce, znalazły się dopiero na szóstej pozycji według ekspertów, co może wynikać ze specyfiki branż, w których działają.

CZĘSTOTLIWOŚĆ KONTAKTU Z NIELEGALNYMI TREŚCIAMI

Jak często spotyka się Pan(i) z następującymi treściami w Internecie?

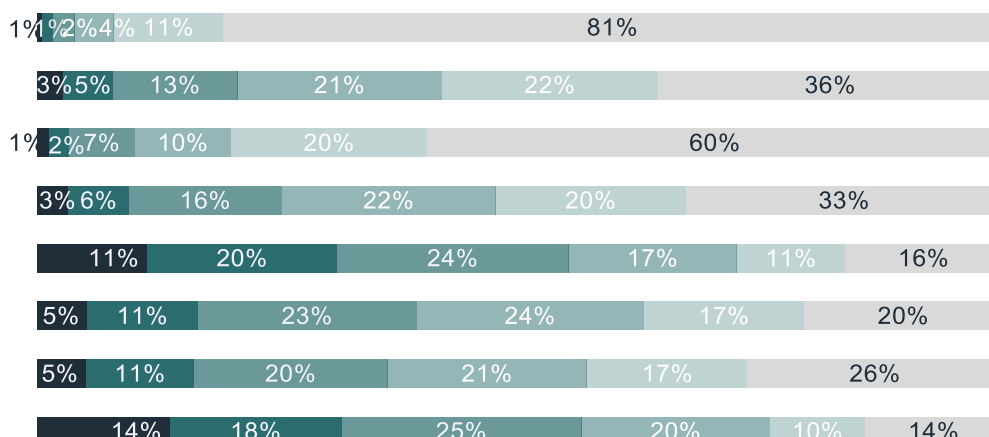
Liczebność próby: N=1083

Większość badanych deklaruje, że rzadko styka się z nielegalnymi treściami. W wielu kategoriach dominują odpowiedzi „wcale” lub „raz w roku lub rzadziej”, co sugeruje, że większość użytkowników rzadko natrafia na treści uznawane za nielegalne. Treści z najwyższą ekspozycją (co najmniej kilka razy w miesiącu) to dezinformacja oraz mowa nienawiści, które często pojawiają się w mediach społecznościowych i na forach internetowych. Najrzadziej napotymane wydają się treści najczęściej uznawane przez badanych za nielegalne, jak pornografia dziecięca – aż 81% badanych nigdy się z nią nie spotkało, a jedynie 4% zadeklarowało kontakt kilka razy w miesiącu.

Występują różnice w percepcji treści nielegalnych - niektóre osoby mogą nie być świadome tego, że pewne treści są nielegalne lub po prostu nie rozpoznają ich jako niezgodne z prawem, co może wpływać na wyniki badania.

Częstotliwość kontaktu z nielegalnymi treściami

■ codziennie ■ kilka razy w tygodniu ■ kilka razy w miesiącu ■ raz na kilka miesięcy ■ raz w roku lub rzadziej ■ wcale



Badanie pokazuje, że najczęściej spotykane są treści związane z dezinformacją, mową nienawiści i dyskryminacją, natomiast najbardziej oczywiste naruszenia prawa, jak pornografia dziecięca czy naruszenie danych osobowych, pozostają rzadko dostrzegane

przez przeciętnych użytkowników Internetu. Wysoka częstotliwość kontaktu z niektórymi kategoriami treści sugeruje konieczność zwiększenia świadomości użytkowników i wzmocnienia działań edukacyjnych oraz regulacyjnych.

DOŚWIADCZENIE Z NIELEGALNYMI TREŚCIAMI W INTERNECIE

Czy kiedykolwiek natknął/natknęła się Pan(i) na treści w Internecie, które są według Pana(i) nielegalne?

Liczebność próby: N=1083

Z badań wynika, że 42% respondentów przyznało, iż napotkało w sieci treści, które uznali za nielegalne. Jednocześnie 36% osób, mimo tego, że na początku badania przedstawiona została im definicja treści nielegalnych,

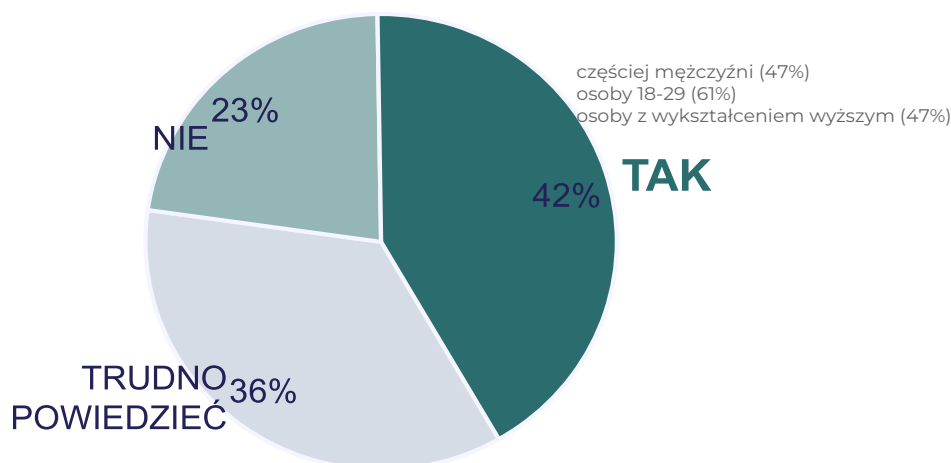
nie jest pewnych, czy miało do czynienia z takimi materiałami, co może świadczyć o niejednoznaczności definicji treści nielegalnych w percepcji badanych lub o braku wiedzy na ten temat. 23% respondentów stwierdziło, że nigdy nie zetknęło się z nielegalnymi treściami.

Wątpliwości natomiast nie mieli badani przez nas eksperci, niemalże jednomyślnie potwierdzając kontakt z treściami nielegalnymi w Internecie. Jedynie jedna osoba z szesnastu nie umiała jednoznacznie odpowiedzieć na to pytanie. Świadczy to o dużo większej wiedzy dotyczącej treści nielegalnych osób zajmujących się zawodowo Internetem.

Z analizy demograficznej dotyczącej całej populacji Polaków wynika natomiast, że częściej z nielegalnymi treściami spotykali się mężczyźni (47%), osoby młode w wieku 18–29 lat (61%) oraz osoby z wykształceniem wyższym (47%). Może to sugerować, że młodsze grupy Polaków oraz osoby bardziej wykształcone są bardziej aktywne w Internecie i częściej napotykają różne formy treści nielegalnych, np. w mediach społecznościowych, serwisach informacyjnych czy na forach dyskusyjnych.

Doświadczenie z nielegalnymi treściami w Internecie

Czy kiedykolwiek natknął/natknęła się Pan(i) na treści w Internecie, które są według Pana(i) nielegalne?
Podstawa: Total N=1083



Jednym z istotnych wniosków płynących z badania jest fakt, że znaczna część osób nie potrafi jednoznacznie określić, pomimo wstępnie deklarowanej wiedzy na ten temat,

czy spotkała się z nielegalnymi treściami, co może wskazywać na potrzebę większej edukacji użytkowników w zakresie rozpoznawania i zgłaszania takich materiałów.

MIEJSCA KONTAKTU Z NIELEGALNYMI TREŚCIAMI

Gdzie w Internecie najczęściej natrafia Pan(i) na treści nielegalne?

Liczebność próby: N=462 (Osoby, które kiedykolwiek natknęły się na nielegalne treści w Internecie)

Najwięcej badanych (78%) wskazało media społecznościowe (np. Facebook, Instagram) jako główne źródło takich materiałów. Może to wynikać z szerokiego zasięgu tych platform, łatwości na nich rozpowszechniania treści oraz trudności w ich moderowaniu.

Na drugim miejscu znalazły się fora internetowe (47%), gdzie częściej na nielegalne treści natrafiały osoby z wykształceniem wyższym (56%). Może to sugerować, że osoby bardziej wykształcone korzystają z forów jako źródła informacji i wymiany opinii, gdzie dezinformacja i treści nielegalne mogą być trudniejsze do wykrycia.

Platformy streamingowe (np. YouTube) zajmują trzecie miejsce (32%) – tutaj narażone na kontakt z nielegalnymi treściami są szczególnie osoby w wieku 30–39 lat (43%) oraz osoby z wykształceniem wyższym (41%). Może to wynikać z algorytmów rekomendujących treści oraz trudności w szybkim usuwaniu materiałów naruszających prawo.

Serwisy informacyjne (np. Onet, WP, Interia) zostały wskazane przez 28% badanych, przy czym częściej były to osoby z wykształceniem wyższym (36%). Może to sugerować obecność treści nielegalnych w sekcjach komentarzy lub artykułach opiniotwórczych.

Komunikatory (np. Messenger, WhatsApp) wskazało 25% respondentów, głównie osoby w wieku 40–49 lat (35%). Może to oznaczać, że prywatne grupy i czaty są również wykorzystywane do szerzenia treści nielegalnych, co utrudnia ich moderowanie.

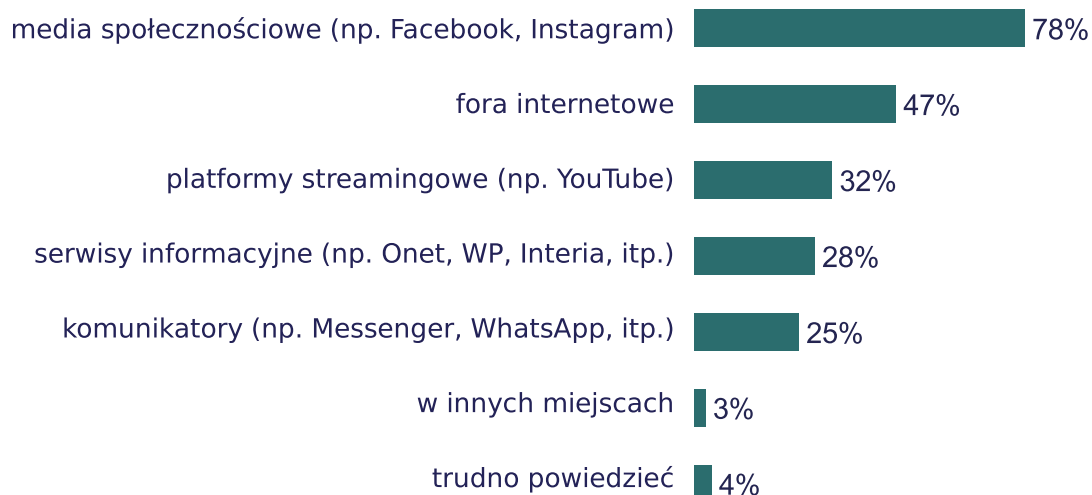
Zaledwie 3% użytkowników wskazało inne miejsca, a 4% miało trudności z jednoznacznym określeniem tego, gdzie spotkało nielegalne treści w Internecie.

Co ciekawe grupa kontrolna badanych przez nas ekspertów z branży związanej z Internetem stworzyła inną hierarchię miejsc kontaktu z nielegalnymi treściami w Internecie. Na pierwszym miejscu, podobnie jak ogół Polaków, wskazano media społecznościowe (15 wskazań), jednak na drugim znalazły się już platformy streamingowe (9), następnie fora internetowe (6), serwisy informacyjne (5). Komunikatory zostały wskazane na ostatniej pozycji. Prawdopodobnie wynika to z innej specyfiki korzystania z Internetu wśród osób na co dzień z nim pracujących.

Miejsca kontaktu z nielegalnymi treściami

Gdzie w Internecie najczęściej natrafia Pan(i) na treści nielegalne?

Podstawa: Osoby, które kiedykolwiek natknęły się na nielegalne treści w Internecie N= 462



Najważniejsze czynniki mające wpływ na najczęstszy dostęp do treści nielegalnych w poszczególnych źródłach:**Media społecznościowe:**

- Ogromna liczba użytkowników oraz łatwość publikacji treści.
- Łatwość rozprzestrzeniania dezinformacji i fake newsów.
- Złożoność mechanizmów moderacji.
- Anonimowość i trudność w egzekwowaniu prawa.

Platformy streamingowe:

- Długi czas reakcji na zgłoszenia.
- Łatwa dostępność i brak skutecznej moderacji na żywo.
- Obejście zabezpieczeń i algorytmów moderacyjnych.

Fora internetowe:

- Mniej restrykcyjna moderacja.
- Funkcjonowanie w „Dark Web”.
- Użytkownicy wymieniają się instrukcjami dotyczącymi obchodzenia prawa.

Serwisy informacyjne:

- Komentarze użytkowników.
- Publikacja kontrowersyjnych materiałów.
- Treści reklamowe i clickbaitowe.

Komunikatory:

- Mniejsza przypadkowa ekspozycja.
- Szyfrowanie wiadomości.
- Brak publicznej dostępności treści.



Media społecznościowe to najczęstsze źródło treści nielegalnych – niemal wszyscy respondenci wskazali Facebook, Instagram i podobne platformy jako miejsce, gdzie najczęściej napotykają treści niezgodne z prawem.

Wyniki te wskazują na konieczność lepszej regulacji treści internetowych, wzmocnienia narzędzi do zgłaszania naruszeń oraz zwiększenia świadomości użytkowników w zakresie odpowiedzialnego korzystania z przestrzeni cyfrowej.

Możliwe konsekwencje powszechnego kontaktu z treściami nielegalnymi**1. Zaburzenia rozwoju psychicznego i emocjonalnego**

- Ekspozycja na treści pornograficzne, zwłaszcza w młodym wieku, może prowadzić do:
 - nieprawidłowego rozwoju psychoseksualnego,
 - kształtowania niewłaściwych wzorców zachowań seksualnych,
 - fałszywych przekonań na temat własnego ciała,
- Negatywny wpływ na sferę seksualną życia.

2. Wzrost agresji i zachowań antyspołecznych

- Kontakt z treściami zawierającymi przemoc może:
 - skłaniać do agresywnych zachowań,
 - wzmacniać wrogość wobec rówieśników, osób starszych czy przedstawicieli, innych narodowości i wyznań.

3. Znieczulenie na przemoc i patologiczne zachowania

- Częsta styczność z materiałami przedstawiającymi przemoc może:
 - prowadzić do zubożenia na agresję i brutalność.
 - zwiększać tolerancję na przemoc w realnym życiu.

4. Lęk, niepokój i obniżenie poczucia bezpieczeństwa

- Dzieci i młodzież narażone na szkodliwe treści mogą:
 - doświadczać negatywnych emocji, takich jak lęk i niepokój,
 - odczuwać obniżenie poczucia bezpieczeństwa,
 - cierpieć z powodu pogorszenia nastroju i stanu psychicznego.

5. Ryzykowne zachowania i demoralizacja

- Ekspozycja na nielegalne treści może:
 - prowadzić do zachowań sprzecznych z normami społecznymi,
 - zwiększać skłonność do ryzykownych działań,
 - powodować demoralizację i utratę wartości etycznych.

6. Naruszenie prywatności i wyłudzenia

- Kontakty nawiązywane przez Internet mogą skutkować:
 - wyłudzeniem danych osobowych, loginów, haseł czy pieniędzy,
 - narażeniem na konsekwencje finansowe i wizerunkowe.

7. Problemy prawne

- Nawiązywanie kontaktów z oszustami lub udział w nielegalnej wymianie plików mogą prowadzić do:
 - oskarżeń o naruszenie prawa,
 - konsekwencji prawnych, takich jak kary grzywny, odpowiedzialność cywilna lub postępowanie karne.

8. Uzależnienie od Internetu

- Nadmierne korzystanie z Internetu, zwłaszcza w kontekście dostępu do treści nielegalnych, może prowadzić do:
 - uzależnienia od sieci i treści w niej zawartych,
 - negatywnego wpływu na życie osobiste, naukę i pracę,
 - zmniejszonej kontroli nad czasem spędzanym online, co może prowadzić do zaniedbywania obowiązków i relacji międzyludzkich.

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

ŚWIADOMOŚĆ TEGO, GDZIE MOŻNA ZGŁASZAĆ TREŚCI NIELEGALNE

Komu Pana(i) zdaniem można zgłosić fakt natrafienia na treści nielegalne w Internecie?

Liczebność próby: N=1083

Wyniki badania pokazują dużą różnorodność w podejmowanych działaniach w przypadku napotkania treści nielegalnych w Internecie. Najczęściej wybierane metody zgłaszania wskazują na preferowanie rozwiązań dostępnych na poziomie platform i krajowych instytucji. Jednocześnie część respondentów nie podejmuje żadnych działań, a narzędzia międzynarodowe, takie jak Europol czy INHOPE, nie są w ogóle wykorzystywane.

Polacy najczęściej wskazują Policję (54%) jako instytucję, do której można zgłaszać treści nielegalne. Może to sugerować, że większość osób utożsamia zgłaszanie takich treści z oficjalnymi organami ścigania. Administratorzy platform społecznościowych i serwisów internetowych zajęli drugie miejsce (53%), a częściej wskazywały ich kobiety (56%) oraz osoby z wyższym wykształceniem (59%). Jest to wynik rosnącej świadomości dotyczącej tego, że serwisy mają obowiązek moderować i usuwać nielegalne treści. Dostawcy usług internetowych zostali wskazani przez 21% badanych, co sugeruje, że ich rola w zwalczaniu treści nielegalnych nie jest powszechnie znana. Jeszcze niższą rozpoznawalność miały CERT Polska (16%), Europol (5%), strona Dyżurnet.pl (5%), organy nadzoru w innych krajach (4%) i Hotlines INHOPE (2%) - mimo tego, że są to instytucje zajmujące się cyberbezpieczeństwem i przeciwdziałaniem przestępczości internetowej.

Świadomość tego, gdzie można zgłaszać nielegalne treści



Wyniki badania wskazują, że większość respondentów ma świadomość istnienia różnych instytucji zajmujących się zwalczaniem treści nielegalnych w Internecie, jednak preferencje dotyczące zgłaszania są silnie skoncentrowane na krajowych podmiotach, takich jak CERT Polska, dostawcy usług internetowych i Policja. Instytucje międzynarodowe oraz specjalistyczne platformy zgłaszania, takie jak Europol, INHOPE czy Dyżurnet.pl, pozostają w dużej mierze pomijane, co może świadczyć o ich niskiej rozpoznawalności wśród użytkowników.

Dla porównania, badana przez nas grupa ekspertów – specjalistów ds. Internetu, to właśnie CERT Polska wskazała jako tę instytucję, do której należy zgłaszać treści nielegalne w Internecie, na drugim miejscu wskazując dostawców usług internetowych, dopiero na trzecim Policję ex equo z administratorami platform internetowych. Świadczy to o dużo większej, niż większości Polaków, ich wiedzy w tym zakresie.

Zespół CERT Polska działa w strukturach NASK – Państwowego Instytutu Badawczego, prowadzącego działalność naukową, Rejestr domeny .pl i dostarczającego zaawansowane usługi teleinformatyczne. Jako CSIRT NASK (Krajowy Zespół Reagowania na Incydynty Bezpieczeństwa Komputerowego,) odpowiada m.in. za:

- monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym;
- przekazywanie informacji dotyczących incydentów i ryzyk podmiotom krajowego systemu cyberbezpieczeństwa;
- wydawanie komunikatów o zidentyfikowanych zagrożeniach cyberbezpieczeństwa;
- reagowanie na zgłoszone incydynty;
- klasyfikowanie incydentów, w tym incydentów poważnych oraz incydentów istotnych, jako incydynty krytyczne oraz koordynowanie obsługi incydentów krytycznych;
- monitorowanie wskaźników zagrożeń cyberbezpieczeństwa;
- rozwijanie narzędzi i metod do wykrywania i zwalczania zagrożeń cyberbezpieczeństwa;
- prowadzenie działań z zakresu budowania świadomości w obszarze cyberbezpieczeństwa;

Źródło: Cert.pl, <https://cert.pl/o-nas/>

Zaskakujące jest to, że aż 23% badanych nie wie lub nie potrafi wskazać odpowiedniego miejsca do zgłoszenia treści nielegalnych, co świadczy o konieczności zwiększenia edukacji na temat dostępnych mechanizmów zgłaszania i odpowiednich organów zajmujących się zwalczaniem tego typu problemów w sieci. Średnia liczba wskazywanych miejsc wyniosła 2, co oznacza, że większość osób potrafiła wymienić jedynie jedno lub dwa źródła zgłaszania, co może sugerować ograniczoną wiedzę w tym zakresie.

CO MOŻNA ZROBIĆ?

- **Edukacja cyfrowa i kampanie społeczne** – konieczne jest zwiększenie świadomości na temat roli instytucji zajmujących się walką z nielegalnymi treściami w Internecie.
- **Promowanie Dyżurnet.pl i innych krajowych mechanizmów zgłaszania** – brak zgłoszeń może wynikać z niewiedzy o istnieniu takich narzędzi.
- **Zwiększenie zaufania do organów ścigania** – konieczne są działania zmierzające do przekonania użytkowników, że zgłaszanie Policji czy Europolowi może przynieść skuteczne efekty.
- **Zachęcanie do reagowania na nielegalne treści** – kampanie podkreślające, że każda interwencja ma znaczenie w walce z cyberprzestępczością.

DZIAŁANIA PO NATKNIĘCIU SIĘ NA NIELEGALNE TREŚCI

Jakie działania podejmuje Pan(i), kiedy natrafi na nielegalne treści w Internecie?

Liczebność próby: N=462 (Osoby, które kiedykolwiek natknęły się na nielegalne treści w Internecie)

Badanie dotyczące reakcji na nielegalne treści w Internecie ujawnia istotne tendencje w zachowaniu użytkowników oraz pokazuje, które metody zgłaszania są najczęściej stosowane. Wyniki wskazują, że użytkownicy preferują zgłaszanie treści nielegalnych bezpośrednio na platformach internetowych lub do krajowych instytucji zajmujących się cyberbezpieczeństwem, natomiast rzadko korzystają z instytucji międzynarodowych oraz organów ścigania. Istnieje także grupa osób, które nie podejmują żadnych działań, co budzi pewne obawy związane z pasywnością w obliczu naruszeń prawa w sieci.

Niemal połowa badanych (47%) nie podejmuje żadnych działań po zetknięciu się z treścią nielegalną w Internecie, co wskazuje na powszechną pasywność w reagowaniu na takie treści. Brak reakcji częściej dotyczy mężczyzn (53%).

Tylko 10% osób zgłasza napotkane nielegalne treści, co sugeruje, że mechanizmy zgłaszania mogą być niewystarczająco dostępne lub użytkownicy nie są świadomi tego, jak to zrobić. Natomiast 37% osób decyduje się na unikanie takich treści, co częściej dotyczy kobiet (46%). Może to wynikać z chęci ochrony siebie lub swoich bliskich przed nieprzyjemnymi lub niebezpiecznymi materiałami.

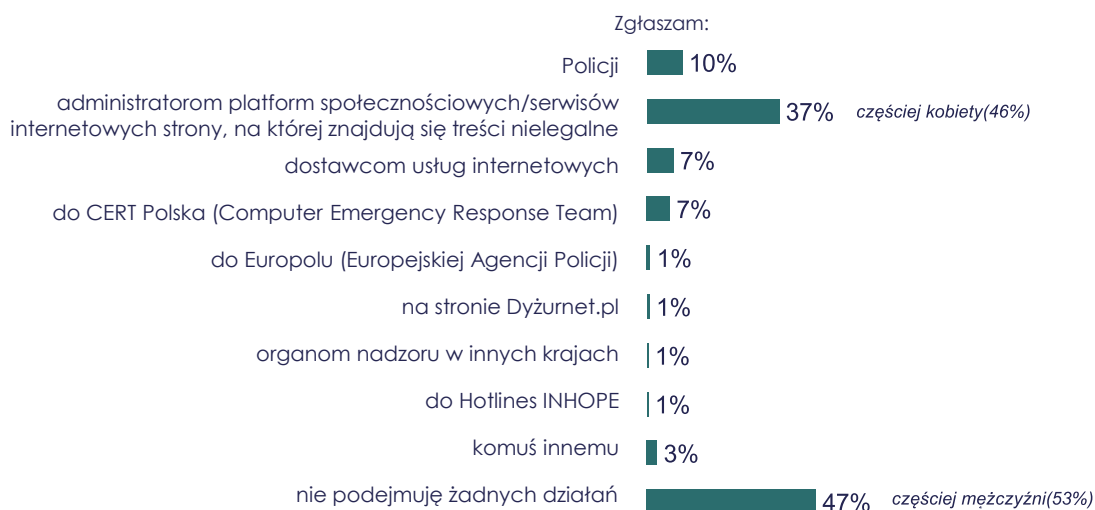
Pozostałe działania, takie jak ostrzeganie innych użytkowników czy podejmowanie kroków prawnych, są marginalne i mieszczą się w przedziale 1-7%. Może to wynikać z braku wiedzy na temat skutecznych metod przeciwdziałania nielegalnym treściom lub z obawy przed konsekwencjami.

Znacznie wyższą aktywność w tym zakresie wykazują eksperci Internetu. Jedynie trzech z szesnastu przebadanych przez nas ekspertów nie podejmuje żadnych działań związanych ze zgłaszaniem treści nielegalnych w Internecie.

Działania po natknięciu się na nielegalne treści

Jakie działania podejmuje Pan(i), kiedy natrafi na nielegalne treści w Internecie?

Podstawa: Osoby, które kiedykolwiek natknęły się na nielegalne treści w Internecie N=462



Wyniki wskazują na niski poziom aktywnej reakcji użytkowników na nielegalne treści w sieci. Konieczna jest większa edukacja i promocja narzędzi zgłaszania, aby zwiększyć skuteczność walki z tego typu treściami w Internecie.



prof. dr hab. Ryszard Szpyra

Kierownik Katedry
Bezpieczeństwa Informacyjnego
Instytutu Bezpieczeństwa
Międzynarodowy Wydział
Bezpieczeństwa Narodowego
Akademia Sztuki Wojennej

KOMENTARZ EKSPERTA

W klasycznym kapitalizmie skuteczność dominuje nad moralnością, bo system nagradza efektywność ekonomiczną i inną, a nie etyczność. Wielu badaczy, jak np. Zygmunt Bauman czy Naomi Klein, potwierdza, że kapitalizm sprzyja sytuacjom, w których wartość etyczna jest podporządkowana opłacalności i skuteczności. To jest jednym z głównych źródeł upadku cywilizacyjnego w zakresie dobrych manier i kultury osobistej i ogólnie etyczności. Brak powszechnego ostracyzmu oraz charakter współczesnych środków masowej komunikacji sprzyja szerzeniu się brutalizacji komunikacji społecznej. Co do tych ostatnich, to warto wymienić algorytmy i mechanizmy mediów społecznościowych, które promują negatywne treści wzbudzające emocje, co sprawia, że hejt „żyje” dłużej, szybciej się rozprzestrzenia i przyciąga uwagę. Potęgą wpływu właścicieli tzw. „big techów” sprawia, że politycy są sparaliżowani i nie są w stanie skutecznie regulować prawem ich działań. Czynią to skutecznie Chiny, jednak ich regulacje idą zbyt daleko, nadmiernie ograniczając ludzką wolność. I tu warto przywołać ważny dylemat między poziomem wolności a poziomem bezpieczeństwa, bowiem zwiększając jeden, zmniejszamy drugi. Ponadto charakter Internetu zapewnia większą anonimowość i brak bezpośrednich konsekwencji swojego działania. Do tego należy dodać nieustannie toczącą się walkę ideologiczną, cywilizacyjną i rosnącą polaryzację społeczną, co wywołuje efekt grupowego myślenia i traktowania innych z pogardą. Na skutek znacznego przyzwyczajania się społeczeństwa do takiego środowiska, przestaje to razić i wzbudzać powszechny sprzeciw. Ponadto elity intelektualne, a szczególnie polityczne, nie tworzą dobrego przykładu płynącego z góry. Politycy sami propagują kontrowersyjne treści, gdyż te wzbudzają emocje i przez to zwiększają zainteresowanie społeczne. Dlatego nie dziwi fakt wysokiej bierności społecznej na spotykane treści nielegalne w Internecie. Pasywność ta wynika także z małej wiary w skuteczność przeciwdziałania oraz rosnące przekonanie o niskiej szkodliwości społecznej, wynikające z przyzwyczajania się do istniejącego stanu rzeczy. Jeśli chodzi o przeciwdziałanie tym zjawiskom, to należałoby podejmować działania systemowe oraz doraźne. Działania systemowe wykraczają poza rozważane treści. Jeśli chodzi o działania doraźne, to są one prawidłowo wskazane. Wydaje się jedynie, że CERT jest powołany raczej do przeciwdziałania szkodliwym działaniom teleinformatycznym, niż do zwalczania nielegalnych treści zawartych w płynących strumieniach informacji cyfrowej.



Opinie na temat treści nielegalnych w Internecie

Nielegalne treści w sieci – widzisz i milczysz czy reagujesz?

CZY ZGŁASZANIE TREŚCI NIELEGALNYCH MOŻE PROWADZIĆ DO ICH USUNIĘCIA?

Czy uważa Pan(i), że zgłaszanie komuś treści nielegalnych może prowadzić do ich usunięcia?

Liczebność próby: N=1083

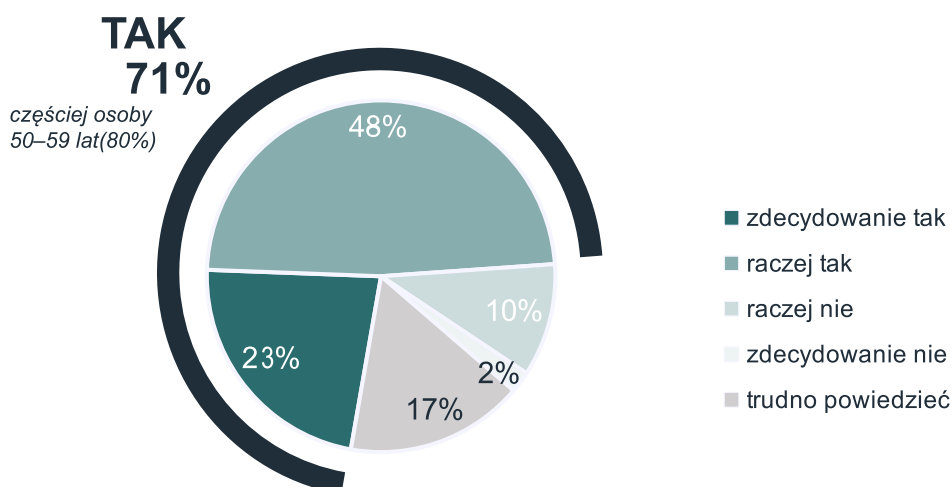
Zdecydowana większość badanych (71%) uważa, że zgłoszenia mogą prowadzić do usunięcia takich treści, w tym 48% jest tego całkowicie pewna, a 23% raczej tak sądzi. Przekonanie to jest szczególnie silne w grupie osób w wieku 50–59 lat (80%).

Jednak 17% respondentów nie potrafi jednoznacznie ocenić skuteczności zgłoszeń, a 12% jest sceptycznych, 10% uważa, że zgłoszenia raczej nie prowadzą do usunięcia, a 2% jest zdania, że zdecydowanie nie mają one wpływu.

Opinie badanych przez nas ekspertów nie odbiegają znacząco od opinii populacyjnej.

Czy zgłaszanie treści nielegalnych może prowadzić do ich usunięcia?

Czy uważa Pan(i), że zgłaszanie komuś treści nielegalnych może prowadzić do ich usunięcia?
Podstawa: Total N=1083



Wyniki sugerują, że świadomość respondentów dotycząca mechanizmów zgłaszania nielegalnych treści w sieci jest stosunkowo wysoka, choć część osób pozostaje niepewna co do ich skuteczności.

Może to wynikać z braku informacji na temat sposobu działania platform internetowych oraz różnic w egzekwowaniu zgłoszeń w różnych serwisach.

CZY NIELEGALNE TREŚCI WPŁYWAJĄ NEGATYWNIE NA SPOŁECZEŃSTWO?

Czy uważa Pan(i), że obecność treści nielegalnych w Internecie wpływa negatywnie na społeczeństwo?

Liczebność próby: N=1083

Zdecydowana większość respondentów (90%) uważa, że takie treści mają negatywny wpływ na społeczeństwo – w tym 50% jest tego całkowicie pewna, a 40% skłania się ku takiej opinii.

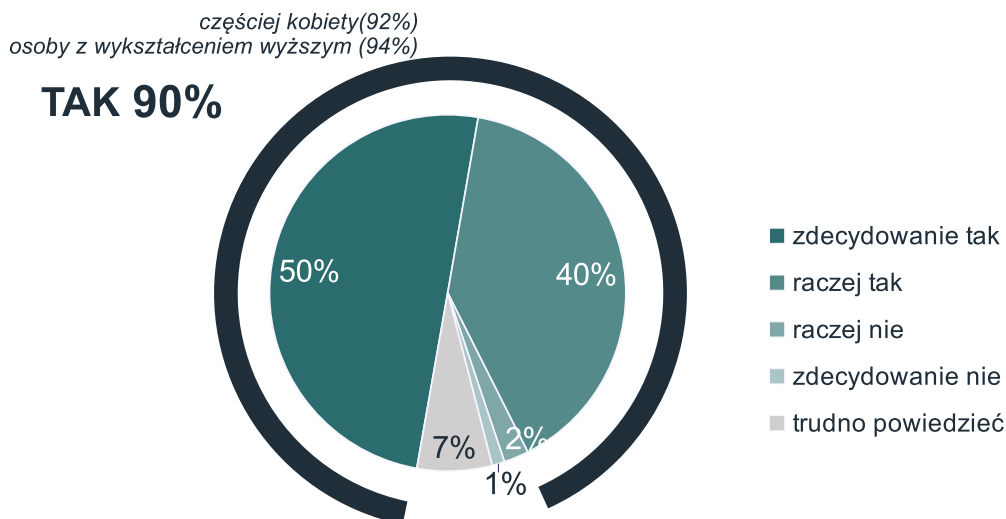
Jedynie 7% badanych ma wątpliwości, twierdząc, że raczej nie wpływają one negatywnie, a zaledwie 1% zdecydowanie nie dostrzega takiego wpływu. 2% respondentów nie potrafi określić swojego stanowiska.

Opinie ekspertów nie odbiegają tutaj od badania ogólnopolskiego.

Interesującym spostrzeżeniem wynikającym z wyników badania jest to, że częściej negatywny wpływ dostrzegają kobiety (92%) oraz osoby z wyższym wykształceniem (94%). Może to wynikać z większej świadomości zagrożeń związanych z nielegalnymi treściami lub częstszego kontaktu z rzetelnymi źródłami informacji na ten temat.

Czy nielegalne treści wpływają negatywnie na społeczeństwo?

Czy uważa Pan(i), że obecność treści nielegalnych w Internecie wpływa negatywnie na społeczeństwo?
Podstawa: Total N=1083



Z badania wynika, że społeczeństwo w dużej mierze dostrzega zagrożenia wynikające z obecności nielegalnych treści w Internecie, co wskazuje na potrzebę

skutecznych działań regulacyjnych i edukacyjnych w tym zakresie.

JAKI JEST NEGATYWNY WPŁYW TREŚCI NIELEGALNYCH NA SPOŁECZEŃSTWO?

W jaki sposób, Pana(i) zdaniem, obecność treści nielegalnych w Internecie wpływa negatywnie na społeczeństwo?

Liczebność próby: N=977 (osoby, które uważają, że treści nielegalne negatywnie wpływają na społeczeństwo)

Respondenci spontanicznie wskazali różne skutki, które ich zdaniem wynikają z obecności takich treści w sieci. Najczęściej wymienianym problemem jest szerzenie dezinformacji i wprowadzanie ludzi w błąd (25%). To podkreśla rosnące obawy związane z fake newsami, manipulacją informacyjną i propagandą, które mogą kształtować opinie publiczne oraz wpływać na decyzje społeczne i polityczne.

Kolejnymi negatywnymi skutkami wymienionymi przez badanych są:

- zachęcanie do złych zachowań i normalizacja patologicznych postaw (11%),
- budzenie agresji, nienawiści, wrogości i przemocy (10%),
- negatywny wpływ na zdrowie psychiczne, prowadzący do stresu, lęków, samookaleczeń i myśli samobójczych (10%).

Inne istotne zagrożenia to demoralizacja dzieci i młodzieży (8%), promowanie fałszywych przekonań poprzez manipulację informacjami (7%) oraz chaos informacyjny i zaburzenie postrzegania rzeczywistości (7%).

Jaki jest negatywny wpływ treści nielegalnych na społeczeństwo?

W jaki sposób, Pana(i) zdaniem, obecność treści nielegalnych w Internecie wpływa negatywnie na społeczeństwo?
Podstawa: osoby, które uważają, że treści nielegalne negatywnie wpływają na społeczeństwo, N=977





Wyniki badania wskazują, że społeczeństwo dostrzega wielowymiarowe zagrożenia związane z nielegalnymi treściami w Internecie – od dezinformacji i manipulacji, po negatywny wpływ na psychikę i wzrost agresji. Podkreśla

to potrzebę skuteczniejszych regulacji prawnych oraz większej edukacji medialnej, aby użytkownicy potrafili krytycznie oceniać treści, z którymi się stykają.

WSPARCIE NOWYCH TECHNOLOGII

WYKRYWANIE:

Czy Pana(i) zdaniem nowe technologie (takie jak sztuczna inteligencja) wspierają wykrywanie treści nielegalnych w Internecie?

Liczebność próby: N=1083

USUWANIE:

Czy Pana(i) zdaniem nowe technologie (takie jak sztuczna inteligencja) wspierają usuwanie treści nielegalnych w Internecie?

Liczebność próby: N=1083

1. Wykrywanie treści nielegalnych w Internecie

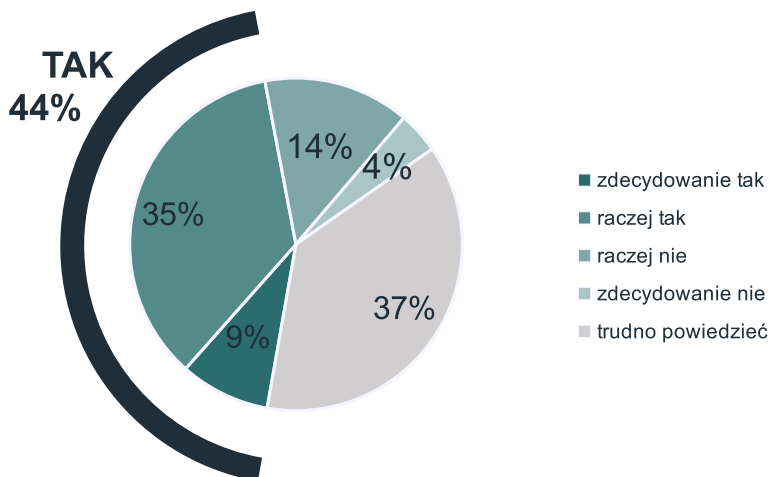
44% respondentów uważa, że nowe technologie pomagają w wykrywaniu treści nielegalnych (9% „zdecydowanie tak” i 35% „raczej tak”). Najczęściej przekonani o skuteczności technologii są mężczyźni (51%) i osoby z wykształceniem wyższym (51%). 18% badanych uważa, że nowe technologie nie są w tym obszarze wystarczająco skuteczne (14% „raczej nie” i 4% „zdecydowanie nie”). Może to sugerować, że użytkownicy zauważają błędy algorytmów i przypadki, w których sztuczna inteligencja nie rozpoznaje kontekstu. Dodatkowo aż 37% badanych nie ma zdania, co może oznaczać, że część użytkowników nie ma wiedzy na temat tego, jak działają algorytmy moderujące treści.

Wyniki te są zbieżne z opinią badanych przez nas ekspertów.

Wsparcie nowych technologii - wykrywanie

WYKRYWANIE

Czy Pana(i) zdaniem nowe technologie (takie jak sztuczna inteligencja) wspierają wykrywanie treści nielegalnych w Internecie?
Podstawa: Total N=1083



2. Usuwanie treści nielegalnych w Internecie

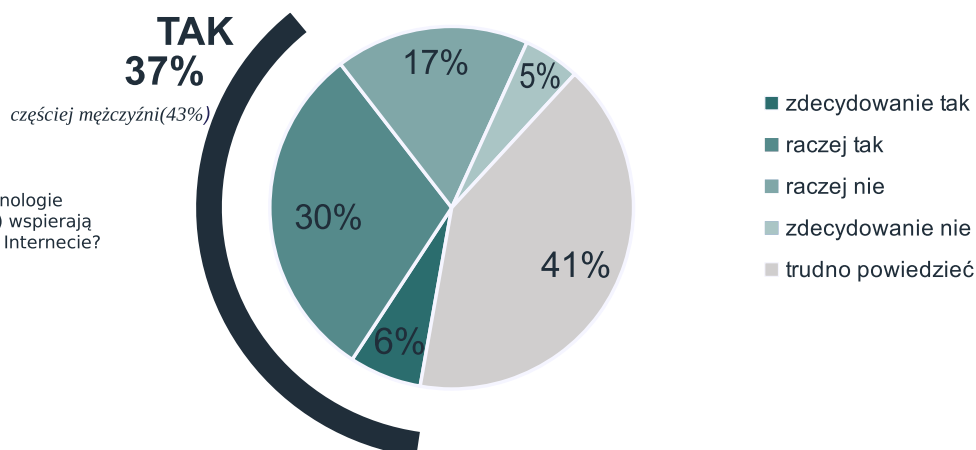
Jeszcze mniej badanych (37%) uważa, że technologie są skuteczne w usuwaniu treści nielegalnych (5% wybrało „zdecydowanie tak”, a 32% „raczej tak”). Oznacza to, że mniej osób wierzy w skuteczność usuwania niż wykrywania treści nielegalnych. 22% uważa, że technologie nie radzą sobie z usuwaniem treści (17% „raczej nie”, a 5% „zdecydowanie nie”). Może to wynikać z tego, że nawet jeśli algorytmy wykrywają nielegalne treści, ich usunięcie wymaga interwencji człowieka lub proces usuwania trwa zbyt długo, więc oceniany jest jako nieskuteczny. 41% respondentów zaznaczyło „trudno powiedzieć”, co może oznaczać, że użytkownicy nie wiedzą, jak dokładnie działa system moderacji treści w Internecie.

Także badani eksperci mieli w tych kwestiach wiele wątpliwości. Jedyne 7 na 16 ekspertów uważa, że nowoczesne technologie są skuteczne w usuwaniu treści nielegalnych w Internecie.

Wsparcie nowych technologii - usuwanie

USUWANIE

Czy Pana(i) zdaniem nowe technologie (takie jak sztuczna inteligencja) wspierają usuwanie treści nielegalnych w Internecie?
Podstawa: Total N=1083



44% badanych uważa, że nowe technologie, takie jak sztuczna inteligencja, skutecznie wspierają wykrywanie nielegalnych treści, ale tylko 37% twierdzi, że skutecznie je usuwają. Większość osób nie jest przekonana o skuteczności technologii, co oznacza,

że proces moderacji wciąż wymaga ulepszeń. Wskazuje to na konieczność tworzenia lepszych algorytmów, zwiększenia szybkości reakcji platform oraz przejrzystości w decyzji o usuwaniu treści.

SKUTECZNOŚĆ USUWANIA NIELEGALNYCH TREŚCI PRZEZ SOCIAL MEDIA

Czy według Pan(i) platformy społecznościowe (np. Facebook, Instagram) skutecznie usuwają treści nielegalne?

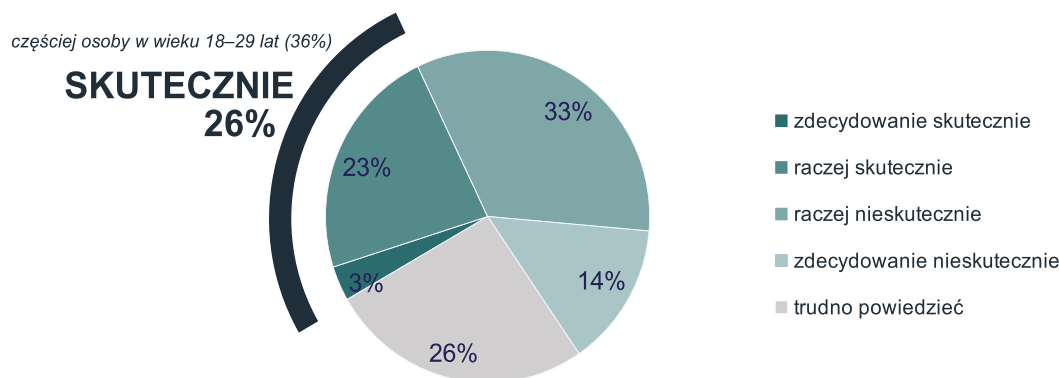
Liczebność próby: N=1083

Tylko 26% badanych uważa, że media społecznościowe skutecznie eliminują nielegalne treści – 3% określa ich działania jako „zdecydowanie skuteczne”, a 23% jako „raczej skuteczne”. Częściej takie poczucie mają osoby z najmłodszej grupy wiekowej (18–29 lat). Aż 47% respondentów uznaje działania platform za nieskuteczne – 33% ocenia je jako „raczej nieskuteczne”, a 14% jako „zdecydowanie nieskuteczne”. 26% badanych nie ma jednoznacznej opinii i zaznacza odpowiedź „trudno powiedzieć”.

Jeszcze bardziej krytyczna w tym zakresie jest badana przez nas grupa ekspertów. Większość z nich (12 na 16) negatywnie ocenia skuteczność usuwania treści nielegalnych przez platformy mediów społecznościowych.

Skuteczność usuwania treści nielegalnych przez Social Media

Czy według Pan(i) platformy społecznościowe (np. Facebook, Instagram) skutecznie usuwają treści nielegalne?
Podstawa: Total N=1083



Wyniki te wskazują, że większość Polaków nie ma zaufania do skuteczności platform społecznościowych w zwalczaniu nielegalnych treści. Może to wynikać z przypadków pozostawiania szkodliwych materiałów online, mimo zgłoszeń użytkowników lub zbyt wolnej reakcji administratorów. Znaczna

grupa badanych pozostaje niezdecydowana, co może sugerować niedostateczną wiedzę o działaniach platform w tym zakresie. Wyniki te wskazują na potrzebę większej transparentności i skuteczniejszych mechanizmów moderacji treści w mediach społecznościowych.

SKUTECZNOŚĆ METOD ZWALCZANIA TREŚCI NIELEGALNYCH

Co, Pana(i) zdaniem, jest bardziej skuteczne w walce z treściami nielegalnymi w Internecie – usuwanie treści nielegalnej, czy blokowanie dostępu do konta jej autorowi?

Liczebność próby: N=1083

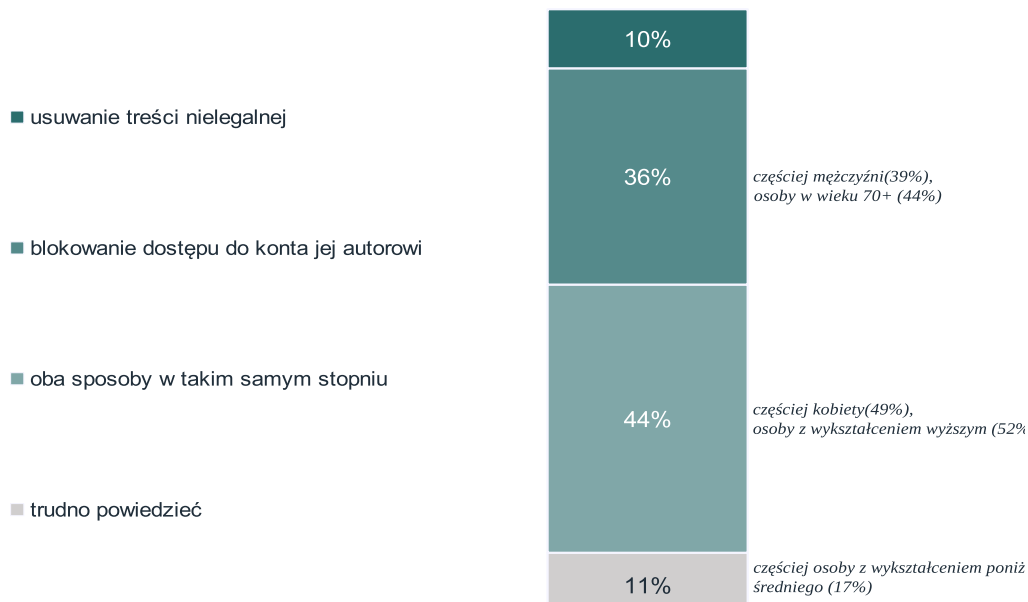
W kwestii skuteczności w walce z treściami nielegalnymi w Internecie zdania respondentów są podzielone. 44% z nich uważa, że oba sposoby (usuwanie treści nielegalnej lub blokowanie dostępu do konta jej autorowi) są równie skuteczne. Częściej tę opinię wyrażają kobiety (49%) oraz osoby z wyższym wykształceniem (52%). Zdaniem 36% badanych bardziej efektywne jest blokowanie dostępu do konta autora. Takie stanowisko częściej wyrażają mężczyźni (39%) oraz osoby powyżej 70. roku życia (44%). Tylko 10% badanych uważa, że usuwanie treści nielegalnych jest skuteczniejszym rozwiązaniem, natomiast 11% respondentów nie ma zdania na ten temat, częściej są to osoby z wykształceniem poniżej średniego (17%).

Co ciekawe, opinia ekspertów jest w tym zakresie inna. Badani specjaliści Internetu wskazywali usuwanie treści jako najskuteczniejszy sposób w walce z treściami nielegalnymi w Internecie lub ewentualnie oba sposoby. Blokowanie dostępu do konta wskazywali jako mało skuteczne.

Skuteczność metod zwalczania treści nielegalnych

Co, Pana(i) zdaniem, jest bardziej skuteczne w walce z nielegalnymi treściami w Internecie – usuwanie treści nielegalnej, czy blokowanie dostępu do konta jej autorowi?

Podstawa: Total N=1083



Większość badanych uważa, że skuteczna walka z nielegalnymi treściami powinna łączyć zarówno usuwanie nielegalnych materiałów, jak i blokowanie dostępu ich autorom. Mniej osób wierzy w samodzielną skuteczność jednej z tych metod, przy czym blokowanie dostępu do konta sprawców

jest postrzegane jako skuteczniejsze niż samo usuwanie treści. Wyniki te sugerują, że internauci oczekują bardziej zdecydowanych działań wobec osób publikujących nielegalne materiały, a nie tylko biernego usuwania ich skutków.

WOLNOŚĆ SŁOWA...

...A OBAWY PRZED AUTOMATYCZNYM USUWANIEM TREŚCI PODEJRZANYCH

Czy obawia się Pan(i) o wolność słowa w związku z automatycznym usuwaniem treści podejrzanych o to, że są nielegalne?

Liczebność próby: N=1083

34% respondentów badania ogólnopolskiego obawia się, że automatyczne usuwanie treści podejrzanych o bycie nielegalnymi może zagrozić wolności słowa. Najczęściej obawy takie wyrażają mężczyźni (40%) oraz osoby w wieku 18–39 lat (43%). Równocześnie 45% respondentów nie podziela tych obaw, a 21% nie ma na ten temat zdania. Wyniki sugerują, że choć spora część osób dostrzega ryzyko nadużyć w automatycznym moderowaniu treści, to jednak nie jest to dominująca obawa w społeczeństwie.

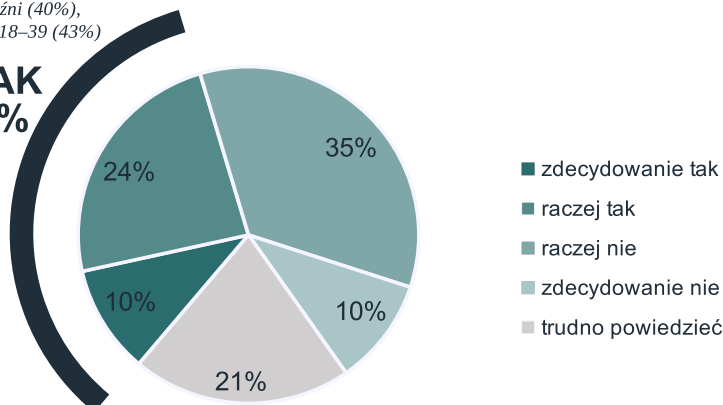
Podobne opinie wyrazili badani przez nas eksperci.

Wolność słowa... a obawy przed automatycznym usuwaniem treści podejrzanych

Czy obawia się Pan(i) o wolność słowa w związku z automatycznym usuwaniem treści podejrzanych o to, że są nielegalne?
Podstawa: Total N=1083

częściej mężczyźni (40%),
osoby w wieku 18–39 (43%)

TAK
34%



...A LEGALNOŚĆ TREŚCI KONTROWERSYJNYCH, ALE WAŻNYCH SPOŁECZNIE

Czy uważa Pan(i), że niektóre treści szkodliwe (np. kontrowersyjne opinie polityczne, religijne lub filozoficzne, kontrowersyjne dzieła artystyczne, których celem jest np. zwrócenie uwagi na jakiś ważny problem społeczny) powinny być legalne, jeśli są zgodne z zasadami wolności słowa?

Liczebność próby: N=1083

53% respondentów uważa, że kontrowersyjne treści (np. opinie polityczne, religijne, filozoficzne, sztuka krytyczna) powinny pozostać legalne, jeśli są zgodne z zasadami wolności słowa. Najczęściej pogląd ten podzielają mężczyźni (57%) oraz osoby z wyższym wykształceniem (59%). 17% badanych jest przeciwna takiej wolności słowa, podczas gdy 30% respondentów nie ma w tej kwestii zdania. Wyniki te pokazują, że większość badanych popiera prawo do publikowania treści kontrowersyjnych, ale nie wykraczających poza normy prawne.

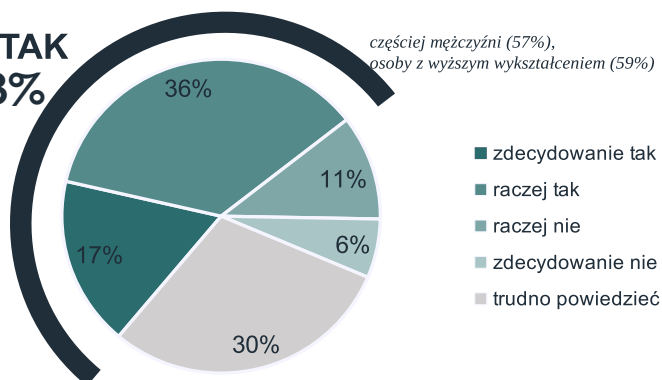
Jeszcze większymi zwolennikami legalności kontrowersyjnych treści, jeśli są zgodne z zasadami wolności słowa, są badani przez nas eksperci Internetu (11 głosów z 16).

Wolność słowa... a legalność treści kontrowersyjnych, ale ważnych społecznie

Czy uważa Pan(i), że niektóre treści szkodliwe (np. kontrowersyjne opinie polityczne, religijne lub filozoficzne, kontrowersyjne dzieła artystyczne, których celem jest np. zwrócenie uwagi na jakiś ważny problem społeczny) powinny być legalne, jeśli są zgodne z zasadami wolności słowa?
Podstawa: Total N=1083

TAK
53%

częściej mężczyźni (57%),
osoby z wyższym wykształceniem (59%)





Choć znaczna część społeczeństwa (34%) obawia się, że automatyczne usuwanie treści może zagrozić wolności słowa, to jednak większość nie postrzega tego jako kluczowego problemu. Ponad połowa respondentów (53%) uważa, że kontrowersyjne, ale ważne społecznie treści powinny być legalne, co wskazuje na duże przywiązanie do zasady wolności słowa, zwłaszcza wśród mężczyzn i osób z wyższym wykształceniem. Wyniki sugerują, że temat moderacji treści w Internecie budzi pewne obawy, ale większy nacisk kładziony jest na prawo do swobodnej wypowiedzi w sprawach istotnych społecznie.

Polacy nie mają jednoznacznej postawy w kwestii obaw o wolność słowa przy automatycznym usuwaniu podejrzanych treści – najczęściej nie mają takich obaw (blisko połowa), ale co trzeci widzi takie zagrożenie, a co piąty nie ma zdania na ten temat.

Częściej uważają, że treści kontrowersyjne, ale zgodne z zasadami wolności słowa, powinny być legalne – takiego zdania jest połowa społeczeństwa. Jedynie co szósty jest przeciwnego zdania, a pozostali nie mają określonej postawy.

OBAWY O NARUSZENIE TOŻSAMOŚCI CYFROWEJ

Czy ma Pan(i) obawy, że Pana(i) tożsamość cyfrowa (czyli informacje reprezentujące Pana/i osobę w Internecie) może zostać naruszona?

Liczebność próby: N=1083

62% respondentów wyraża obawy dotyczące potencjalnego naruszenia ich tożsamości cyfrowej. Najczęściej obawy takie zgłaszają osoby z wyższym wykształceniem (67%), co może wynikać z większej świadomości zagrożeń w cyberprzestrzeni. 42% badanych zdecydowanie obawia się naruszenia tożsamości cyfrowej, a kolejne 20% wyraziło umiarkowane obawy.

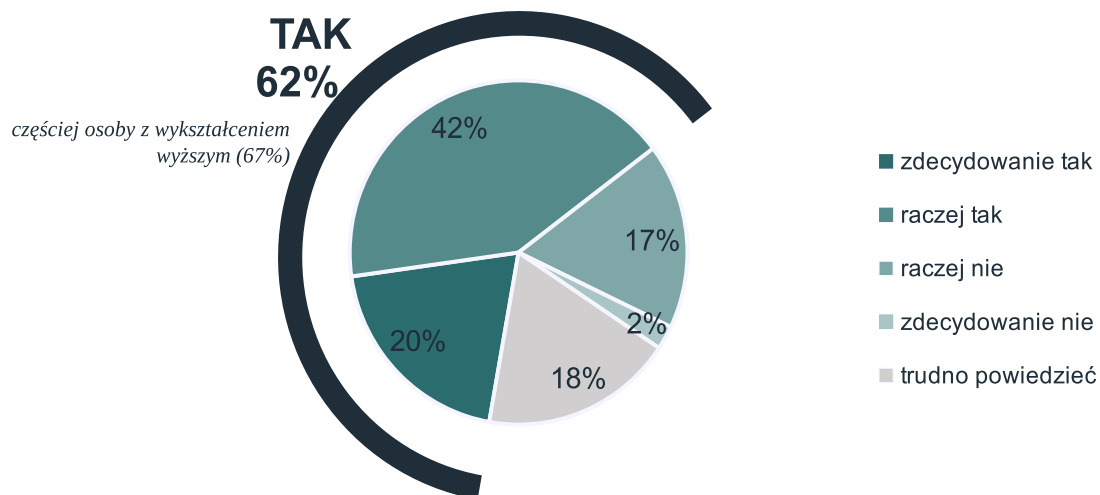
17% badanych raczej nie obawia się naruszenia swojej tożsamości cyfrowej, a zaledwie 2% zdecydowanie odrzuca taką możliwość. 18% respondentów nie ma zdania na ten temat, co może wskazywać na brak wiedzy lub świadomości zagrożeń związanych z ochroną danych osobowych w Internecie. Wyniki badania wskazują, że większość badanych jest świadoma ryzyka związanego z naruszeniem ich danych osobowych i cyfrowej tożsamości.

Jeszcze większą świadomość zagrożeń związanych z kradzieżą tożsamości w Internecie mają badani eksperci – aż 14 z nich (na 16) wyraża obawy z tym związane, a jedynie 1 nie czuje takiego zagrożenia.

Wysoki poziom obaw wśród osób z wyższym wykształceniem sugeruje, że osoby bardziej zaznajomione z technologiami cyfrowymi lepiej rozumieją też potencjalne zagrożenia, takie jak kradzież tożsamości, phishing czy naruszenia prywatności przez firmy technologiczne. Wciąż jednak prawie jedna piąta badanych wykazuje brak większych obaw, co może świadczyć o niskiej świadomości cyberzagrożeń lub przekonaniu o skuteczności stosowanych przez siebie zabezpieczeń.

Obawy o naruszenie tożsamości cyfrowej

Czy ma Pan(i) obawy, że Pana(i) tożsamość cyfrowa (czyli informacje reprezentujące Pana/i osobę w Internecie) może zostać naruszona?
Podstawa: Total N=1083



Badanie pokazuje, że obawy o bezpieczeństwo tożsamości cyfrowej są powszechne – większość użytkowników Internetu dostrzega ryzyko naruszenia swoich danych osobowych. Jednocześnie istnieje grupa osób, które nie są świadome zagrożeń lub nie postrzegają ich jako

istotnych. W kontekście rosnącej liczby ataków cybernetycznych, konieczna jest edukacja społeczeństwa na temat ochrony tożsamości cyfrowej oraz bezpiecznego korzystania z Internetu.



dr Agnieszka Jankowska

Członkini Zarządu
Fundacji Digital Poland,
Przewodnicząca
Rady ds. Cyfryzacji

KOMENTARZ EKSPERTA

Wyniki badań przeprowadzonych wśród Polek i Polaków, zawarte w raporcie „Polacy wobec nielegalnych treści w Internecie”, dostarczają cennych informacji o świadomości społecznej, postawach społecznych oraz oczekiwaniach społeczeństwa względem platform cyfrowych i państwa. Przede wszystkim należy wskazać na różnice w rozumieniu zagrożeń cyfrowych oraz poziomie wiedzy na ten temat – z jednej strony cieszy to, że 71% respondentów wierzy w sens zgłaszania treści nielegalnych w Internecie, gdyż dzięki temu treści te zostaną usunięte, z drugiej zaś co druga Polka i co drugi Polak (47%) uważają, że platformy internetowe nie są wystarczająco skuteczne w usuwaniu treści nielegalnych, 26% z nas nie ma w tym temacie zdania (a więc wiedzy), a 29% uważa, że zgłoszenie treści nielegalnej nie prowadzi do jej usunięcia.

Uznajemy, że zgłaszanie treści nielegalnych jest kluczowym narzędziem w walce z dezinformacją, mową nienawiści, czy innymi patologicznymi zjawiskami w sieci. Respondenci dostrzegają negatywne konsekwencje obecności nielegalnych treści w Internecie, wskazując m.in. właśnie na szerzenie dezinformacji i fałszywych informacji (25%), normalizowanie patologicznych postaw i zachęcanie do złych zachowań (11%) oraz pobudzanie agresji, nienawiści i przemocy, jak i negatywny wpływ na zdrowie psychiczne (10%). Dane te podkreślają konieczność reagowania na treści szkodliwe, co wymaga zaangażowania zarówno użytkowników, platform cyfrowych, jak i państwa. Ponadto, niezbędne są skuteczniejsze regulacje prawne w tym zakresie, ale także systemowa prewencja, a więc szeroka edukacja społeczeństwa w zakresie cyberbezpieczeństwa i cyberhigieny oraz edukacja medialna. Państwo powinno odegrać bardziej aktywną rolę w edukacji społeczeństwa w zakresie umiejętności korzystania z mediów, wyposażenia obywateli w umiejętność krytycznego myślenia, analizowania informacji dostępnych w sieci oraz odróżniania opinii od faktów, i szerzej – bezpiecznego poruszania się w sieci, w tym wiedzę, jakiego rodzaju, jak oraz gdzie zgłaszać nielegalne treści.

Interesującym zagadnieniem zbadanym w przedmiotowym raporcie jest również kwestia wolności słowa. 34% badanych obawia się, że automatyczne usuwanie treści nielegalnych może naruszać wolność słowa, podczas gdy 45% nie dostrzega takich zagrożeń. Warto zauważyć, że ta różnica może wynikać z braku pełnej świadomości na temat potencjalnych nadużyć, jak również z różnic w interpretacjach samego pojęcia wolności słowa w kontekście ograniczeń technologicznych. Z drugiej strony, 62% badanych wyraża obawy dotyczące naruszenia ich tożsamości cyfrowej, co wskazuje na rosnącą świadomość zagrożeń związanych z prywatnością i bezpieczeństwem danych w Internecie. Wyższy poziom obaw wśród osób z wyższym wykształceniem sugeruje, że lepsza znajomość technologii cyfrowych wiąże się z większą świadomością ryzyka. Niemniej jednak fakt, że około 20% badanych nie ma zdania na ten temat, świadczy o potrzebie intensywniejszych działań edukacyjnych.



Nienawiść w sieci

Czym skutkuje obawa przed agresją w sieci?

RODZAJE AGRESJI W INTERNECIE

Jakiego rodzaju agresja w Internecie jest Pana(i) zdaniem najczęstsza?

Liczebność próby: N=1083

Najczęstsze formy agresji online

Według badanych najczęstszą formą agresji online jest mowa nienawiści (*hate speech*) – 66%. Jest to najczęściej wskazywana forma agresji w Internecie, polegająca na słownej przemocy wobec osób lub grup społecznych. Najczęściej dostrzegana jest przez osoby z wyższym wykształceniem (75%).

Wyśmiewanie innych (*mocking*) – 61% to druga najczęściej wskazywana forma agresji, szczególnie dostrzegana przez kobiety (64%).

Prowokowanie konfliktów i szerzenie dezinformacji (*cybertrolling*) – 50%; najczęściej zauważana jest przez osoby w wieku 40–49 lat (57%) i osoby z wyższym wykształceniem (57%).

Dyskryminacja na tle rasowym, religijnym, seksualnym także jest zdaniem badanych często obecna w Internecie (48%). Najczęściej mają z nią do czynienia osoby młodsze w wieku 18–29 lat (56%).

Cyberbullying (nękanie, poniżanie, zastraszanie), pomimo licznych kampanii społecznych, to wciąż bardzo obecna w Internecie forma agresji. Dostrzega ją aż 46%, najczęściej kobiety (51%).

Badani wymieniają także *doxxing* (publikowanie prywatnych danych w celu zastraszania lub ośmieszenia) – 43%, *dogpiling* (grupowa agresja) – 32% oraz zjawisko oburzenia w sieci (*online outrage*) – 19%.

Jedynie co dziesiąty Polak deklaruje, że miał do czynienia w Internecie z bezpośrednio go dotyczącą agresją. Najczęściej takie naruszenie miało miejsce w mediach społecznościowych.

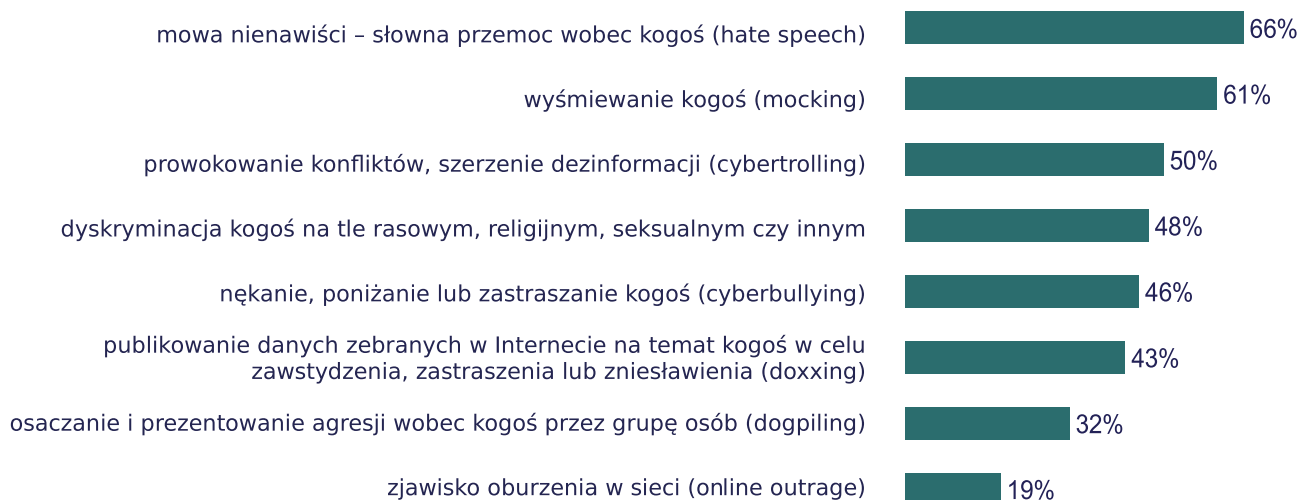
Niecała połowa społeczeństwa (43%) twierdzi, że była świadkiem agresji w Internecie, która dotyczyła innej osoby. Najczęściej miała ona miejsce w mediach społecznościowych.

Badani przez nas eksperci jako formę agresji najczęściej występującą w Internecie wskazywali trolling (prowokowanie konfliktów i szerzenie dezinformacji) (13 wskazań), na drugim miejscu mowę nienawiści (11), a następnie wyśmiewanie (10). Na kolejnych miejscach znalazły się dyskryminacja i osaczanie (7) oraz zjawisko oburzenia w sieci (5).

Rodzaje agresji w Internecie

Jakiego rodzaju agresja w Internecie jest Pana(i) zdaniem najczęstsza?
Podstawa: Total N=1083

Średnia liczba wskazywanych form agresji: 4



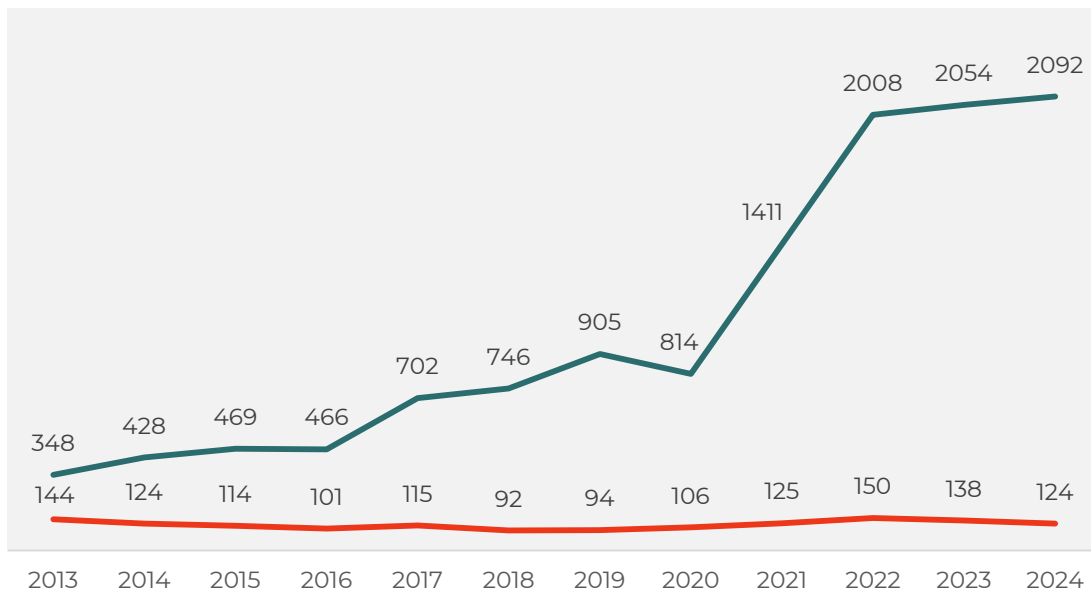
Najczęściej była to agresja związana z mową nienawiści (hate speech) – 13 wskazań, z trollingiem (provokowanie konfliktów, dezinformacja) – 10 i wyśmiewaniem (mocking) – 6. Nieco mniej osób zaobserwowało zjawisko wściekłości internetowej (online outrage) – 4, dyskryminację (na tle rasowym, religijnym, seksualnym czy innym) – 3, nękanie (bullying) i osaczanie (dogpiling) – 2 oraz wykraczanie poza prywatność (doxxing) – 1



Powyższe wyniki badania wskazują na dużą potrzebę regulacji i moderacji treści – wysoka obecność mowy nienawiści i trolling wskazuje na konieczność skuteczniejszych działań platform internetowych. Konieczna jest także edukacja cyfrowa, gdyż to także sami użytkownicy sieci powinni być świadomi

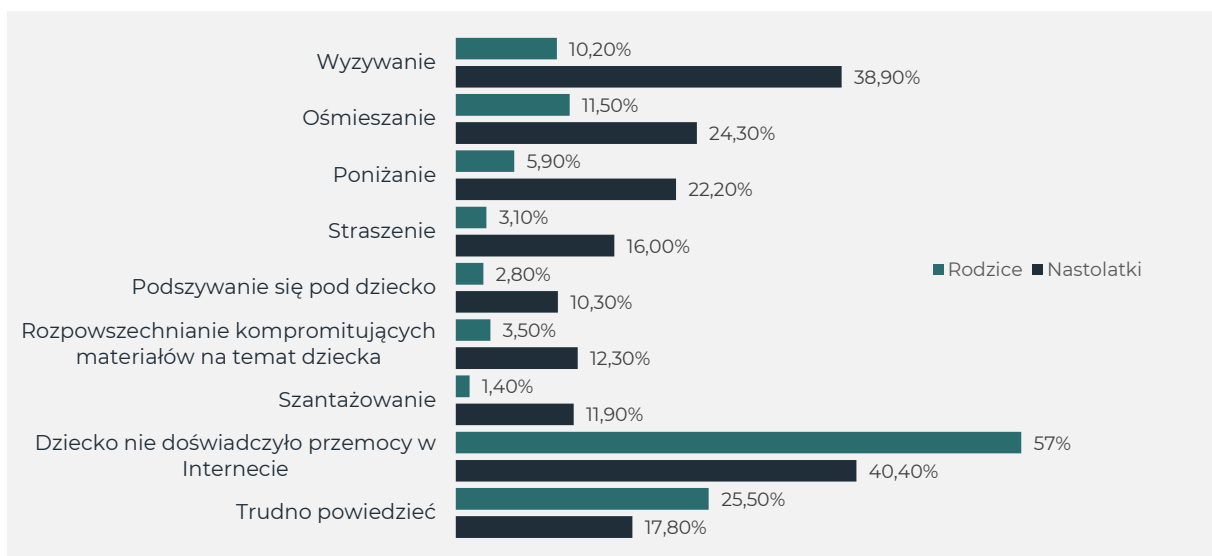
konsekwencji cyberprzemocy i naruszeń prywatności. Zauważalny wzrost agresji w Internecie wymaga interwencji społecznej i prawnej, aby przeciwdziałać narastającym problemom związanym z nękanem i dezinformacją.

Liczba prób samobójczych i prób samobójczych zakończonych zgonem w grupie wiekowej 13-18



Źródło: Zestawienie portal ciekaweliczby.pl na podstawie danych Policji

Porównanie deklaracji dotyczących doświadczenia przemocy w Internecie przez nastolatki z wiedzą rodziców na ten temat



Źródło: NASK, Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów i rodziców,
<https://www.nask.pl/magazyn/nastolatki-3-0-raport-z-ogolnopolskiego-badania-uczniow-i-rodzicow>

OSOBISTE ZETKNIĘCIE Z AGRESJĄ W INTERNECIE

Czy w ciągu ostatnich 12 miesięcy był(a) Pan(i) narażony(a) na agresję w Internecie – np. ktoś napisał w Internecie coś negatywnego lub obraźliwego na Pana(i) temat?

Liczebność próby: N=1083

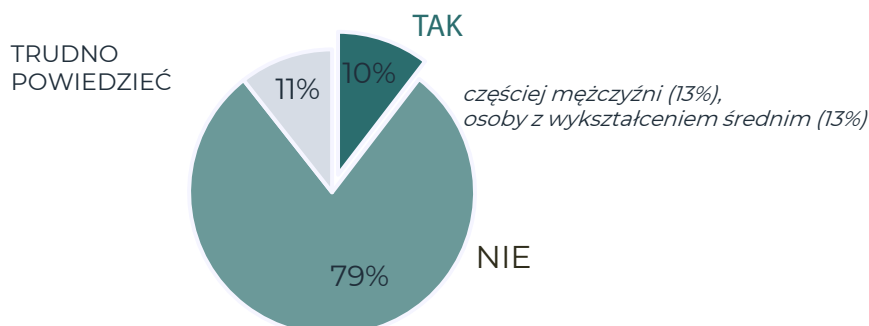
- 10% badanych doświadczyło agresji w Internecie - częściej byli to mężczyźni (13%) oraz osoby z wykształceniem średnim (13%).
- 79% odpowiedziało „nie”, co oznacza, że zdecydowana większość respondentów nie doświadczyła agresji w sieci, albo nie była świadoma tego, że taka sytuacja była jej udziałem.
- 11% nie było pewnych, czy doświadczyło agresji, co sugeruje, że niektóre przypadki mogą być trudne do jednoznacznej oceny.
- Nieco częściej z agresją w Internecie mieli do czynienia badani przez nas eksperci (4 z 16). Żaden z nich nie miał problemu z identyfikacją działań agresywnych z Internetu.

Niski odsetek osób doświadczających agresji (10%) może sugerować, że problem nie jest powszechny lub że użytkownicy unikają sytuacji, które mogłyby prowadzić do ataków w sieci. Na tak niewielki wynik może wpływać także to, że badanie było przeprowadzone wśród dorosłych użytkowników Internetu, a przecież to właśnie dzieci i młodzież najczęściej i najaktywniej z niego korzystają. W tej grupie wiekowej odsetek doświadczających agresji byłby z dużym prawdopodobieństwem dużo wyższy. Potwierdzają to przeprowadzane co cztery lata badania Światowej Organizacji Zdrowia.

79% respondentów nie miało styczności z agresją online, co może oznaczać skuteczne filtrowanie treści przez platformy lub świadome unikanie kontrowersyjnych dyskusji. 11% respondentów nie była w stanie odpowiedzieć na to pytanie, co może wskazywać na brak jednoznacznych definicji agresji internetowej lub niski poziom świadomości na temat cyberprzemocy.

Osobiste zetknięcie z agresją w Internecie

Czy w ciągu ostatnich 12 miesięcy był(a) Pan(i) narażony(a) na agresję / naruszenia w Internecie – np. ktoś napisał w Internecie coś negatywnego lub obraźliwego na Pana(i) temat?
Podstawa: Total N=1083



Nie ulega wątpliwości, że problem agresji internetowej istnieje, chociaż według powyższych wyników badania dotyka stosunkowo niewielką grupę użytkowników. Doświadczenia z agresją w sieci częściej zgłaszają mężczyźni i osoby z wykształceniem średnim – może to wynikać z ich większej

aktywności w określonych przestrzeniach internetowych. Warto edukować użytkowników o różnych formach agresji online oraz o metodach reagowania na nie, zwłaszcza, że część osób nie potrafi jednoznacznie ocenić, czy padła ofiarą agresji.

ZETKNIĘCIE SIĘ Z TAKĄ AGRESJĄ

Gdzie w Internecie zauważył(a) Pan(i), że ktoś inny stał się ofiarą agresji/naruszeń w Internecie?

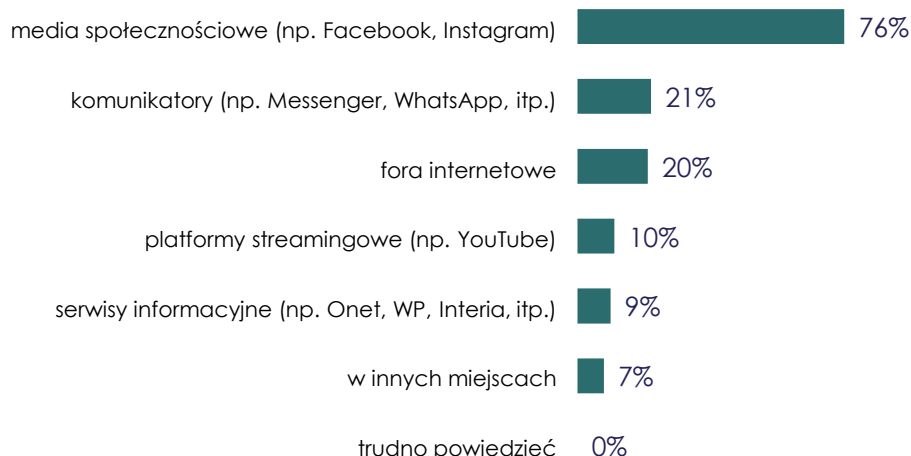
Podstawa: Osoby, które były świadkiem agresji w Internecie, Liczebność próby: N=478

Media społecznościowe są zdecydowanie najczęstszym miejscem zetknięcia się z agresją online - wskazało je aż 76% badanych. To zdecydowanie najwyższy wynik, co wskazuje, że przestrzeń publiczna w mediach społecznościowych są szczególnie podatne na negatywne interakcje. W nieco mniejszym stopniu jest ona także obecna na komunikatorach i forach internetowych (21% doświadczyło agresji na komunikatorach np. Messenger, WhatsApp, a 20% zetknęło się z nią na forach internetowych).

Na te same miejsca wskazali eksperci.

Miejsce zetknięcia się z taką agresją

Gdzie w Internecie był(a) Pan(i) narażony(a) na agresję?
Podstawa: Osoby, które w ciągu ost.12 miesięcy były narażone na naruszenia w Internecie, N=115



Te wyniki sugerują, że agresja występuje także w bardziej zamkniętych przestrzeniach online, ale na mniejszą skalę niż w mediach społecznościowych.

Dużo mniejsza liczba przypadków agresji występuje na platformach streamingowych i serwisach informacyjnych (10% wskazało na platformy streamingowe (np. YouTube), a 9% doświadczyło agresji w serwisach informacyjnych (np. Onet, WP, Interia)). Oznacza to, że w miejscach nastawionych

głównie na konsumowanie treści (wideo, wiadomości) agresja jest rzadsza niż w interaktywnych przestrzeniach.

Co ciekawe nikt z badanych nie miał problemu ze wskazaniem przestrzeni w Internecie, w której można zetknąć się z agresją. Respondenci mają świadomość tego, gdzie doświadczyli agresji, co sugeruje, że problem jest dla nich realny i dobrze zidentyfikowany.

Media społecznościowe – dominujące źródło nielegalnych treści (np. Facebook, Instagram, Twitter, TikTok) – dlaczego?

- Ogromna liczba użytkowników i łatwość publikacji treści – media społecznościowe to dynamiczne środowisko, w którym użytkownicy publikują ogromne ilości materiałów w czasie rzeczywistym. Nie wszystkie z nich podlegają skutecznej moderacji.
- Rozprzestrzenianie dezinformacji i fake newsów – platformy społecznościowe są jednym z głównych kanałów rozpowszechniania fałszywych informacji.

- Złożoność mechanizmów moderacji – choć platformy posiadają narzędzia do wykrywania i usuwania nielegalnych treści, ich skuteczność jest ograniczona. Automatyczne algorytmy wykrywające naruszenia często są niewystarczające, a ręczna moderacja nie nadąża za skalą problemu.
- Anonimowość i trudność w egzekwowaniu prawa – użytkownicy mogą tworzyć fałszywe konta, udostępniać materiały, a następnie je usuwać, zanim zostaną wykryte przez administratorów.

BYCIE ŚWIADKIEM AGRESJI W INTERNECIE

Czy w ciągu ostatnich 12 miesięcy był(a) Pan(i) świadkiem, że ktoś inny stał się ofiarą agresji w Internecie – np. że ktoś napisał w Internecie coś negatywnego lub obraźliwego na czyjś temat?

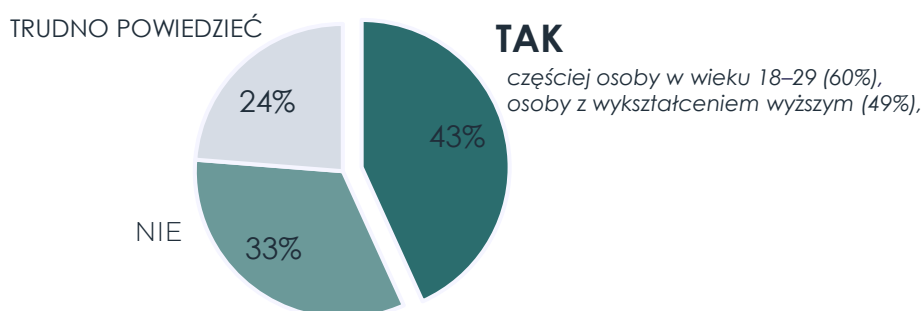
Liczebność próby: N=108

Prawie połowa (43%) badanych była świadkami agresji w Internecie, dotyczy to szczególnie osób młodszych (18–29 lat) – 60% oraz osób z wykształceniem wyższym (49%). Jednak aż 33% nie zauważyło takich przypadków, a 24% miało trudności z określeniem, czy coś było agresją, czy też nie. Może to wynikać z mniejszej aktywności w mediach społecznościowych osób starszych, unikania toksycznych treści lub innej definicji agresji online. 24% badanych zaznaczyło opcję „Trudno powiedzieć”, co sugeruje, że nie zawsze łatwo jest jednoznacznie rozpoznać agresję w Internecie. Może to wynikać z niejasnych granic między żartem a obraźliwą treścią lub braku świadomości na temat mowy nienawiści.

Dużo częściej z agresją spotykali się eksperci (lub potrafili ją jasno zdefiniować) – 13 wskazań na 16 odpowiedzi. Jedynie jedna osoba zadeklarowała, że w ciągu ostatnich 12 miesięcy nie zaobserwowała agresji w Internecie i 2 miały problem z udzieleniem odpowiedzi na to pytanie.

Bycie świadkiem agresji w Internecie

Czy w ciągu ostatnich 12 miesięcy był(a) Pan(i) świadkiem, że ktoś inny stał się ofiarą agresji w Internecie – np. że ktoś napisał w Internecie coś negatywnego lub obraźliwego na czyjś temat?
Podstawa: Total N=1083



Wskazuje to na konieczność działań edukacyjnych i systemowych, aby zwiększyć świadomość i skuteczność reagowania na agresję online.

WYRAŻANIE OPINII A OBAWY PRZED AGRESJĄ

Czy powstrzymuje się Pan(i) od wyrażania swojej opinii w Internecie z obawy przed staniem się ofiarą agresji cyfrowej?

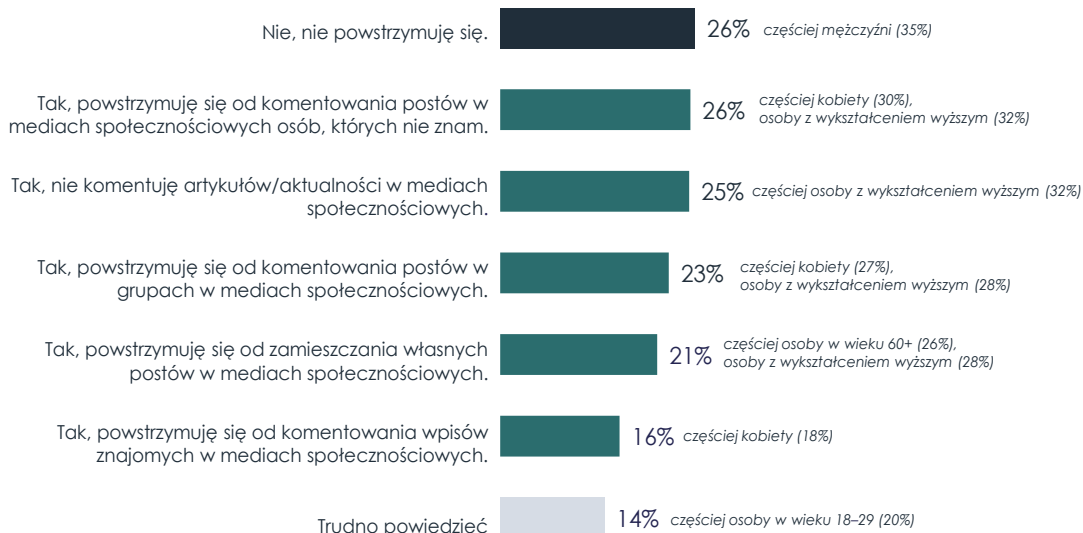
Liczebność próby: N=1083

Jedynie 26% Polaków nie ogranicza swojej aktywności online z obawy przed agresją, tyle samo unika komentowania postów nieznajomych, dotyczy to częściej kobiet (30%) i osób z wykształceniem wyższym (32%). 25% nie komentuje artykułów/aktualności w mediach społecznościowych, zwłaszcza osoby z wyższym wykształceniem (32%). 23% Polaków powstrzymuje się od komentowania postów w grupach w mediach społecznościowych – częściej kobiety (27%) i osoby z wykształceniem wyższym (28%). Oznacza to, że publiczne i grupowe interakcje są częściej postrzegane jako ryzykowne, co prowadzi do autocenzury. Osoby starsze i z wyższym wykształceniem są bardziej skłonne do unikania publikowania własnych treści – nie zamieszcza ich w Internecie 21% Polaków. Co ciekawe część użytkowników sieci (16%) wstrzymuje się od komentowania nawet wśród znajomych, obawiając się negatywnych reakcji.

Bardzo powściągliwi w komentowaniu postów w Internecie są także zbadani przez nas eksperci. Jedynie 5 z nich (na 16) nie powstrzymuje się od pisania komentarzy z obawy przed agresją.

Wyrażanie opinii a obawy przed agresją

Czy powstrzymuje się Pan(i) od wyrażania swojej opinii w Internecie z obawy przed staniem się ofiarą agresji cyfrowej?
Podstawa: Total N=1083



Jedynie co czwarty Polak nie obawia się wyrażania swojej opinii w Internecie. Częściej takich oporów nie mają mężczyźni. Pozostali mają obawy, że staną się ofiarami agresji cyfrowej, więc powstrzymują się przed

umieszczaniem komentarzy w postach, artykułach, czy na grupach w mediach społecznościowych. Relatywnie rzadziej rezygnują z komentowania wpisów znajomych.



dr Michał Chlebowski
dziennikarz, medioznawca,
Katedra Dziennikarstwa
i Komunikacji Społecznej
Uniwersytet SWPS

KOMENTARZ EKSPERTA

Z raportu wyraźnie widać, że potrzebą podjęcia pilnych działań w dwóch kluczowych obszarach: edukacji medialnej oraz regulacji związanych z mową nienawiści w Internecie. Dane wskazują, że najczęściej wskazywaną formą agresji online jest właśnie mowa nienawiści – zauważyło ją aż 66% badanych, a wśród osób z wyższym wykształceniem odsetek ten wzrasta do 75%. Niepokojący jest również fakt, że niemal połowa społeczeństwa była świadkiem agresji wobec innych użytkowników sieci, najczęściej w mediach społecznościowych.

Problem jest szczególnie dotkliwy wśród młodzieży – to właśnie te osoby najczęściej doświadczają dyskryminacji na tle rasowym, religijnym czy seksualnym. Jednocześnie młodzi użytkownicy są najbardziej aktywni w Internecie, co czyni ich zarówno potencjalnymi ofiarami, jak i odbiorcami toksycznych treści. Dlatego właśnie solidny program edukacji medialnej – obejmujący takie zagadnienia jak rozpoznawanie mowy nienawiści, zrozumienie konsekwencji cyberprzemocy i budowanie postaw odpowiedzialności za słowo – powinny być priorytetem już na poziomie szkół podstawowych.

Raport jednoznacznie wskazuje również na niedostateczną skuteczność obecnych narzędzi moderacji treści w mediach społecznościowych. Anonimowość, złożoność systemów zgłaszania i skala publikowanych treści sprawiają, że wiele przejawów nienawiści pozostaje bez reakcji. Z tego względu konieczne są lepiej dopasowane regulacje prawne i większa odpowiedzialność platform cyfrowych za treści publikowane przez użytkowników.

Fakt, że 10% badanych deklaruje, że osobiście doświadczyło agresji online, a 26% powstrzymuje się od wyrażania opinii w sieci z obawy przed przemocą słowną, pokazuje, że problem ten realnie ogranicza wolność słowa i wpływa na zdrowie psychiczne użytkowników. W efekcie pojawia się autocenzura, a przestrzeń publiczna w Internecie staje się coraz bardziej zamknięta i spolaryzowana.

Potrzebujemy zatem nie tylko reform systemowych, ale i oddolnych działań edukacyjnych, które pomogą odbudować kulturę dialogu w sieci. Kluczowe pozostaje budowanie świadomości na temat konsekwencji mowy nienawiści. Dane dotyczące prób samobójczych oraz rodzajów agresji doświadczanej przez młodzież w sieci – biją na alarm. Potrzeba wspólnego społecznego wysiłku, by uczynić Internet przestrzenią bezpieczną, wolną od przemocy i wykluczenia.

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



Znajomość przepisów prawa i opinie na ich temat

Czy łatwo rozpoznać co jest nielegalne w sieci?

ŁATWOŚĆ ZNALEZIENIA INFORMACJI...

CO STANOWI TREŚĆ NIELEGALNĄ W INTERNECIE

Czy według Pana(i), łatwo jest znaleźć informacje na temat tego co stanowi treść nielegalną w Internecie?

Liczebność próby: N=1083

OCENA DOSTĘPU DO WIEDZY I PRZEPISÓW PRAWA ORAZ ICH SKUTECZNOŚCI

ŁATWOŚĆ ZNALEZIENIA INFORMACJI...

Czy według Pana(i) łatwo jest odnaleźć informacje na temat przepisów prawa dotyczących treści nielegalnych w Internecie?

Liczebność próby: N=1083

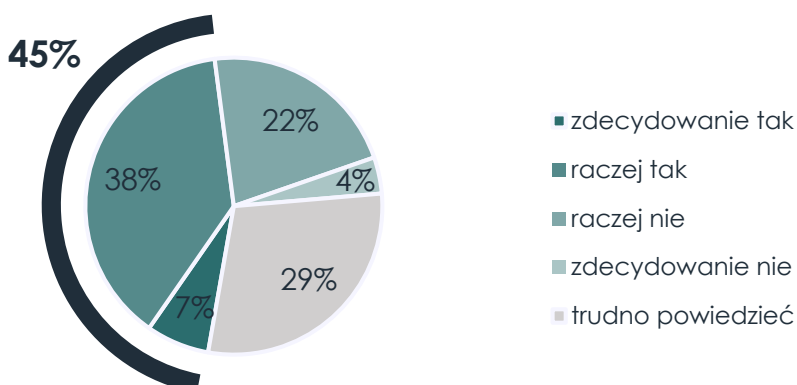
Prawie połowa badanych (45%) uważa, że łatwo jest znaleźć informacje o treści nielegalnychach w Internecie (7% respondentów odpowiedziało „zdecydowanie tak”, a 38% zaznaczyło opcję „raczej tak”). Tego zdania częściej są mężczyźni (49%) oraz osoby w wieku 18–29 lat (58%) i 30–39 lat (57%). Jednak 26% uważa, że nie jest to łatwe (4% „zdecydowanie nie”, a 22% „raczej nie”). Może to sugerować, że regulacje prawne, algorytmy moderujące oraz ograniczenia dostępu do treści wpływają na trudność w znalezieniu takich informacji. Co ciekawe znaczny odsetek badanych ma trudności z określeniem swojej opinii (29%), co może wskazywać na brak jednoznacznych kryteriów, według których określają, czy dane treści są nielegalne. Może to również wynikać z nieświadomości prawnych regulacji dotyczących treści internetowych.

Lepiej dostęp do informacji dotyczącej tego, co stanowi treść nielegalną w Internecie oceniają eksperci. Jedynie 4 z 16 źle ocenia ten dostęp, a 2 miało trudność w odpowiedzi na to pytanie.

..Co stanowi treść nielegalną w Internecie

TAK częściej mężczyźni (49%), osoby w wieku 18–29 (58%) i w wieku 30–39 (57%)

Czy według Pana(i), łatwo jest znaleźć informacje na temat tego co stanowi treść nielegalną w Internecie?
Podstawa: Total N=1083

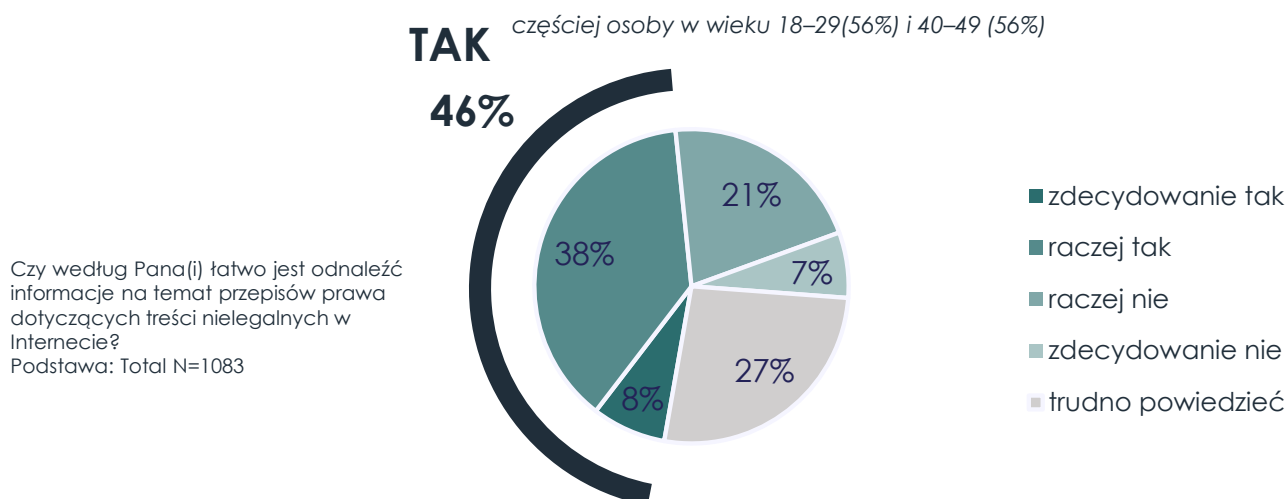


...NA TEMAT PRZEPISÓW PRAWA DOTYCZĄCYCH TREŚCI NIELEGALNYCH W INTERECIE

Blisko 46% badanych uważa, że znalezienie informacji na temat przepisów prawa jest łatwe (8% odpowiedziało „zdecydowanie tak”, a 38% wybrało opcję „raczej tak”). Częściej taką opinię wyrażają osoby w wieku 18–29 lat (56%) oraz 40–49 lat (56%). Jednak 28% badanych, twierdzi, że znalezienie takich informacji jest trudne (7% odpowiedziało „zdecydowanie nie”, a 21% zaznaczyło „raczej nie”). Może to wynikać z trudnego języka prawniczego, braku zrozumienia przepisów lub rozproszenia informacji w różnych źródłach. 27% badanych ma trudności z określeniem swojej opinii. Być może wynika to z braku zainteresowania tym tematem lub nieświadomości istnienia przepisów dotyczących treści nielegalnych. Wyniki te mogą wskazywać na potrzebę stworzenia napisanych przystępnym językiem i łatwo dostępnych przewodników, które ułatwią użytkownikom zrozumienie prawa internetowego.

Mniejszy problem ze znalezieniem informacji na temat przepisów prawa mają eksperci – 10 na 16 uważa, że dostęp do nich jest łatwy, a 5 wskazuje na trudności z tym związane.

...Na temat przepisów prawa dotyczących treści nielegalnych w Internecie



SKUTECZNOŚĆ PRZEPISÓW PRAWA W ZAKRESIE ZWALCZANIA TREŚCI NIELEGALNYCH W INTERNECIE

Jak ocenia Pan(i) skuteczność przepisów prawa w zakresie zwalczania treści nielegalnych w Internecie?

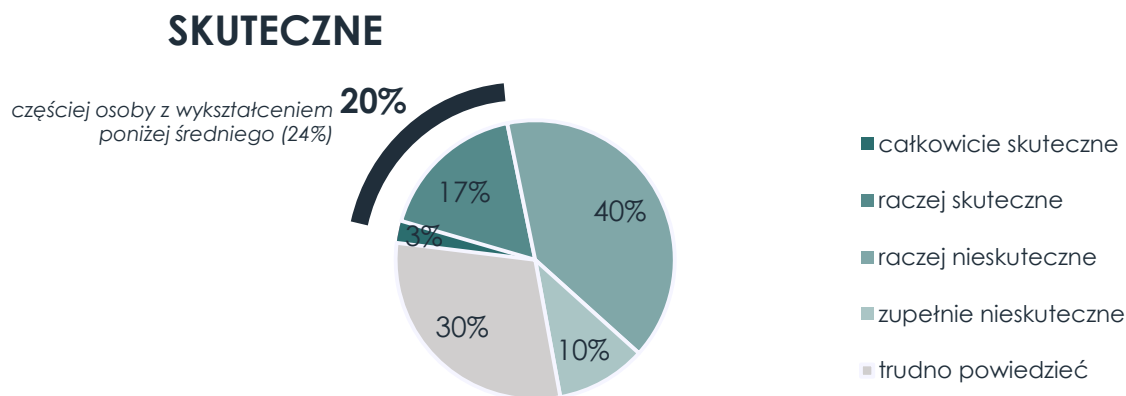
Liczebność próby: N=1083

Tylko 20% badanych uważa obowiązujące przepisy prawa w zakresie zwalczania treści nielegalnych w Internecie za skuteczne. Częściej tę opinię wyrażają osoby z wykształceniem poniżej średniego (24%), co może oznaczać mniejsze doświadczenie w analizowaniu mechanizmów egzekwowania prawa w Internecie. Aż 50% badanych twierdzi, że przepisy te są raczej lub całkowicie nieskuteczne. Najczęściej sceptyczne są osoby z wyższym wykształceniem, które mogą mieć większą świadomość ograniczeń prawnych. Aż 30% badanych deklaruje, że nie ma wiedzy na ten temat. Wyniki badania wskazują, że potrzebne są lepsze regulacje, skuteczniejsza moderacja treści i praca nad zwiększeniem świadomości społecznej dotyczącej zgłaszania naruszeń.

Jeszcze bardziej krytyczni w tym obszarze są eksperci – żaden z badanych nie uważa, by te przepisy prawa były całkowicie skuteczne, 3 wskazuje na odpowiedź raczej skuteczne, a 11 ekspertów na 16 wskazuje na nieskuteczność tych przepisów. Dwóch ekspertów miało problem z oceną.

Skuteczność przepisów prawa w zakresie zwalczania treści nielegalnych w Internecie

Jak ocenia Pan(i) skuteczność przepisów prawa w zakresie zwalczania treści nielegalnych w Internecie?
Podstawa: Total N=1083





Krzysztof Żyto
Kancelaria Prawna Bącal
Busiło Legal

KOMENTARZ EKSPERTA

Wyniki badania wskazują na wyraźny podział opinii – mimo, że blisko połowa respondentów (45%) uważa, że łatwo znaleźć informacje o nielegalnych treściach w sieci, to doświadczenie wskazuje, że oceny te często opierają się na intuicji, a nie na rzeczywistej znajomości stanu rzeczy. Wydaje się, iż dla przeciętnego użytkownika to właśnie informacje opisujące wymagania prawne (zakazy i nakazy) stanowią pierwszą i zasadniczą informację o stanie prawnym. Dopiero wówczas, gdy taka informacja wywołuje wątpliwości, przeciętny użytkownik przechodzi do następnego etapu poszerzenia swojej wiedzy, poprzez poszukiwania przepisów prawa.

Kolejne pytanie dotyczy właśnie tej kwestii, a mianowicie dostępności informacji o przepisach prawa. W przypadku, gdy przepisy są rozproszone (znajdują się w różnych aktach prawnych) to istotne jest, by wyszukując takich aktów prawnych możliwe było uzyskanie wstępnej, ogólnej informacji w postaci zestawienia aktów prawnych i zagadnień w nich regulowanych czy też przystępnych przewodników wyjaśniających podstawowe pojęcia i zagadnienia. Rozwiązania o specjalistycznym charakterze stosowane są w płatnych systemach dostępu do informacji prawnej, do których niewiele osób posiada dostęp.

Najbardziej niepokojące są oceny dotyczące skuteczności przepisów – jedynie 20% respondentów uważa je za efektywne, natomiast aż 50% wskazuje na ich nieskuteczność. Taki wynik jednoznacznie sygnalizuje, że obowiązujące regulacje są niedostosowane do dynamicznie zmieniającej się przestrzeni internetowej, a prawo nie nadąża za nowymi wyzwaniami. Szczególnie eksperci, których opinie mają kluczowe znaczenie, zdecydowanie potępią dotychczasowe podejście, wskazując na pilną potrzebę wprowadzenia nowoczesnych i elastycznych rozwiązań prawnych.

Powyższe wskazuje, w mojej opinii, na konieczność przemyślenia podejścia do regulacji i zmiany przepisów poprzez ich uproszczenie i uzupełnienie o wyjaśnienia, FAQ's czy praktyczne poradniki. Aktualizacja prawa musi odbywać się przy ścisłej współpracy z ekspertami technicznymi, socjologami, specjalistami od edukacji społecznej, aby stworzyć ramy prawne realnie odpowiadające wyzwaniom XXI wieku. Dobrym krokiem do takiej wymiany myśli jest badanie NASK i Raport. Tylko przy współpracy szerokiego grona specjalistów system regulacji ma szansę być bardziej zrozumiały, co zwiększy szansę na jego efektywne stosowanie w praktyce i w konsekwencji przyczyni się do lepszego zabezpieczenia przestrzeni internetowej przed nielegalnymi treściami.

Podsumowanie

ŚWIADOMOŚĆ VS. RZECZYWISTOŚĆ

Polacy są dość dobrze zorientowani, które treści w Internecie są nielegalne. Spośród 8 podanych na liście, średnio wskazują na 6 z nich. Pornografia dziecięca to obszar nieprawny dla niemal każdego Polaka (91%). Zdecydowana większość twierdzi, że nie napotyka w sieci na takie treści (81%). W top 3 treści najczęściej uznawanych za nielegalne znalazły się też naruszenia danych osobowych (85%) oraz treści terrorystyczne (84%). Jednak z żadną z tych dwóch najczęściej nie spotykamy się w Internecie. 3/4 Polaków uważa mowę nienawiści za naruszenie, a 55% styka się z nią w Internecie przynajmniej kilka razy w miesiącu. Dezinformacja, to obszar, który relatywnie słabiej jest łączony z czynem zabronionym (64% wskazań), ale ponad połowa (56%) przynajmniej kilka razy w miesiącu spotyka się z tego typu informacjami. Dyskryminacja i czyny nieuczciwej konkurencji to również obszary stosunkowo rzadziej uznawane za nielegalne (poniżej 70% wskazań).

OPINIE NA TEMAT TREŚCI NIELEGALNYCH

Mniej niż połowa Polaków (42%) uważa, że natknęła się kiedykolwiek na nielegalne treści w Internecie. Dość niewielki odsetek takich deklaracji zapewne wynika m.in. z tego, że część osób nie jest świadoma tego, że takie obszary, jak właśnie dyskryminacja czy dezinformacja, z którymi mają kontakt, to również czyny zabronione. Osoby, które deklarują pewne doświadczenie z nielegalnymi treściami w Internecie, najczęściej natrafiły na nie w mediach społecznościowych (miejsce to wskazywane jest przez 78% respondentów). Świadomość tego, gdzie można zgłaszać nielegalne treści, jest wśród ogółu poprawna – jedynie 23% ankietowanych nie wiedziało, które miejsce wskazać. Najbardziej popularne to Policja i administratorzy platform społecznościowych/serwisów. Ci drudzy są częściej wybierani do zgłoszeń. Pozostałe miejsca wskazywane są znacznie rzadziej. Co jednak ważne, choć większość Polaków wie, gdzie można zgłaszać naruszenie, mają też świadomość tego, że nielegalne treści negatywnie wpływają na społeczeństwo (90%) oraz uważają, że zgłoszenie może prowadzić do ich usunięcia (71%), to jednak blisko połowa z tych, którzy na nie natrafiają, nie podejmuje żadnych działań (47%).

Opinie na temat wsparcia nowych technologii, takich jak sztuczna inteligencja, w zwalczaniu treści nielegalnych w Internecie są dość niejednoznaczne, co prawdopodobnie wynika z tego, że nie jest to jeszcze obszar wystarczająco znany Polakom, by móc się konkretnie na ten temat wypowiadać. Blisko 40% ogółu uważa, że nowe technologie pomagają w wykrywaniu czy w usuwaniu treści nielegalnych w Internecie. Jednocześnie podobny procent nie jest w stanie tego ocenić (zapewne przez brak wystarczającej wiedzy). Częściej przekonanie o wsparciu sztucznej inteligencji w tym zakresie mają mężczyźni.

Polacy też nie mają jednoznacznej postawy w kwestii obaw o wolność słowa przy automatycznym usuwaniu podejrzanych treści – najczęściej się tego nie obawiają (blisko połowa), ale co trzeci widzi takie zagrożenie (częściej mężczyźni), a co piąty nie ma zdania na ten temat. Co drugi zaś uważa, że treści kontrowersyjne, ale zgodne z zasadami wolności słowa, powinny być legalne (53%). Taką opinię częściej podzielają mężczyźni i osoby lepiej wykształcone.

NIENAWIŚĆ W SIECI

Mowa nienawiści i wyśmiewanie kogoś to najczęściej występujące (zdaniem Polaków) formy agresji pojawiające się w Internecie. 10% Polaków deklaruje, że w ciągu ostatnich 12 miesięcy było narażonych na agresję, która bezpośrednio dotyczyła ich osoby. Częściej byli świadkami agresji wobec innej osoby (43%). W obu przypadkach te naruszenia najczęściej miały miejsce w mediach społecznościowych. Z obawy przed agresją cyfrową, zazwyczaj Polacy stronią od komentowania/wyrażania swoich opinii w Internecie. Stosunkowo rzadziej rezygnują z komentowania wpisów swoich znajomych w social media, a jedynie co czwarta osoba nie powstrzymuje się przed tego typu aktywnościami. Częściej takich oporów nie mają mężczyźni.

ZNAJOMOŚĆ PRZEPISÓW PRAWA I OPINIE NA ICH TEMAT

Co warto uwagi – polskie społeczeństwo nie jest też przekonane o skuteczności działań przeciwko nielegalnym treściom w Internecie – jedynie 20% uważa, że przepisy prawa w tym zakresie są skuteczne, a niewiele więcej (26%) uważa, że platformy społecznościowe sprawnie usuwają nielegalne treści. Ogólnie dominuje przekonanie (44%), że usuwanie treści nielegalnych, jak i blokowanie dostępu do konta jej autorowi, to równie skuteczne metody zwalczania treści nielegalnych w Internecie.

INDEKS POJĘĆ

Treści nielegalne – oznaczają informacje, które same w sobie lub przez odniesienie do działania, w tym sprzedaży produktów lub świadczenia usług, nie są zgodne z prawem Unii lub z prawem jakiegokolwiek państwa członkowskiego, które jest zgodne z prawem Unii, niezależnie od konkretnego przedmiotu lub charakteru tego prawa [art. 3 lit. h) **Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych DSA)** Dz.Urz. UE L 277/1 z 27.10.2022].

Pojęcie „nielegalnych treści” należy zdefiniować szeroko, tak by obejmowało informacje dotyczące nielegalnych treści, produktów, usług i działań. Pojęcie to należy rozumieć w szczególności jako odnoszące się do informacji, niezależnie od ich formy, które zgodnie z obowiązującym prawem są albo same w sobie nielegalne, takie jak nielegalne nawoływanie do nienawiści lub treści o charakterze terrorystycznym i niezgodne z prawem treści dyskryminujące, albo które stają się nielegalne na mocy obowiązujących przepisów ze względu na fakt, iż odnoszą się one do nielegalnych działań. Na przykład może to być udostępnianie obrazów przedstawiających niegodziwe traktowanie dzieci w celach seksualnych, bezprawne udostępnianie prywatnych obrazów bez zgody, cyberstalking, sprzedaż produktów niespełniających wymogów lub podrobionych, sprzedaż towarów lub świadczenie usług z naruszeniem prawa ochrony konsumentów, nieuprawnione wykorzystanie materiałów chronionych prawem autorskim, nielegalne oferowanie usług zakwaterowania lub nielegalna sprzedaż żywych zwierząt [motyw 12 preambuły DSA].

Nie ma znaczenia, czy nielegalny charakter informacji lub działanie wynika z prawa Unii czy z prawa krajowego, które jest zgodne z prawem Unii, oraz jaki jest dokładny charakter lub przedmiot danego prawa. Na katalog nielegalnych treści składają się zarówno zachowania klasyfikowane prawnie jako przestępstwa i wykroczenia, jak i zachowania naruszające administracyjne wymagania regulacyjne – zatem niektóre zachowania zagrożone są sankcjami karnymi, a inne sankcjami administracyjnymi. Mimo tak skomplikowanej sytuacji, konieczne jest przykładowe wyliczenie typów nielegalnych treści poczynwszy od takich, które mogą ułatwić popełnienie przestępstwa o charakterze terrorystycznym, popełnienie przestępstwa przeciwko życiu i zdrowiu, polegające na upowszechnianiu pornografii z udziałem małoletniego lub zwierząt, naruszające dobra osobiste. W przykładowym wyliczeniu powinny się również znaleźć treści, w odniesieniu do których umieszczający je odbiorca usługi nie posiada praw własności intelektualnej, przemysłowej lub prawa do znaku towarowego. W tym katalogu powinny się także znaleźć treści związane z towarami niespełniającymi wymogów bezpieczeństwa. Wśród treści nielegalnych, w ustawie wdrażającej akt o usługach cyfrowych, należy wprost wskazać treści zakazane w związku z Kartą Praw Podstawowych, takie jak: zawierające nawoływanie do przemocy i nienawiści wobec grupy osób ze względu na płeć, wiek, rasę, kolor skóry, pochodzenie etniczne lub społeczne, cechy genetyczne, język, religię lub przekonania, poglądy polityczne lub wszelkie inne poglądy, przynależność państwową, przynależność do mniejszości narodowej, majątek, urodzenie, niepełnosprawność, wiek i orientację seksualną. Do tej grupy treści nielegalnych należy dodać także te nawołujące do znieważania grupy ludności lub poszczególniej osoby z powodu jej przynależności narodowej,

etnicznej, rasowej, wyznaniowej albo z powodu jej bezwyznaniowości. W katalogu treści nielegalnych powinny się również znaleźć treści zagrażające bezpieczeństwu i porządkowi publicznemu, a także propagujące działania sprzeczne z polską racją stanu oraz postawy i poglądy sprzeczne z moralnością i dobrem społecznym. Katalog powinien również obejmować reklamę niektórych produktów i usług takich jak np.: alkohol, tytoń, narkotyki, gry hazardowe, leki na receptę, apteki czy solaria, reklama wprowadzająca w błąd, kryptoreklama czy nieuczciwa reklama. Przykładowy katalog treści nielegalnych powinien również wskazywać na nielegalność treści, które mogą zostać udostępnione przez dostawcę usługi cyfrowej, o ile nie spełnią odpowiednich warunków. Będą to np.: treści pornograficzne rozpowszechniane bez zastosowania skutecznych zabezpieczeń przed dostępem osób małoletnich, reklama bez stosownego oznaczenia, czy reklamy wyrobów medycznych i produktów leczniczych oraz żywności specjalnego przeznaczenia bez odpowiednich ostrzeżeń, wymaganych zgodnie z odrębnymi przepisami [K. Chałubińska-Jentkiewicz, *Prawna ochrona treści cyfrowych*, Warszawa 2022].

Treści o charakterze terrorystycznym – oznaczają materiały co najmniej jednego z poniższych rodzajów; a mianowicie materiały, które: a) podlegają do popełnienia jednego z przestępstw, o których mowa w art. 3 ust. 1 lit. a)–i) dyrektywy (UE) 2017/541, w przypadku gdy takie materiały, bezpośrednio lub pośrednio, na przykład poprzez pochwalanie aktów terrorystycznych, popierają popełnianie przestępstw terrorystycznych i tym samym stwarzają niebezpieczeństwo popełnienia jednego lub większej liczby takich przestępstw; b) nakłaniają osobę lub grupę osób do popełnienia lub przyczynienia się do popełnienia jednego z przestępstw, o których mowa w art. 3 ust. 1 lit. a)–i) dyrektywy (UE) 2017/541; c) nakłaniają osobę lub grupę osób do uczestniczenia w działaniach grupy terrorystycznej, w rozumieniu art. 4 lit. b) dyrektywy (UE) 2017/541; d) udzielają instruktażu w zakresie wytwarzania lub stosowania materiałów wybuchowych, broni palnej lub innych rodzajów broni lub trujących lub niebezpiecznych substancji, lub w zakresie innych szczególnych metod lub technik w celu popełnienia lub przyczynienia się do popełnienia jednego z przestępstw terrorystycznych, o których mowa w art. 3 ust. 1 lit. a)–i) dyrektywy (UE) 2017/541; e) stwarzają zagrożenie popełnienia jednego z przestępstw, o których mowa w art. 3 ust. 1 lit. a)–i) dyrektywy (UE) 2017/541 [art. 2 pkt 7 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie przeciwdziałania rozpowszechnianiu w Internecie treści o charakterze terrorystycznym Dz.Urz UE L 172/79 z 17.05.2021].

Przestępstwa terrorystyczne obejmują: a) ataki na życie ludzkie, które mogą powodować śmierć; b) ataki na integralność fizyczną osoby; c) porwania lub branie zakładników; d) spowodowanie rozległych zniszczeń obiektów rządowych lub obiektów użyteczności publicznej, systemu transportowego, infrastruktury, w tym systemu informacyjnego, stałych platform umieszczonych na szelfie kontynentalnym, miejsca publicznego lub mienia prywatnego – jeżeli zniszczenia te mogą zagrozić życiu ludzkiemu lub spowodować poważne straty gospodarcze; e) zajęcie statku powietrznego, statku wodnego lub innego środka transportu publicznego lub towarowego; f) wytwarzanie, posiadanie, nabywanie, przewożenie, dostarczanie lub używanie materiałów wybuchowych lub broni, w tym broni chemicznej, biologicznej, radiologicznej lub jądrowej, jak również badania nad taką bronią i rozwój broni chemicznej, biologicznej, radiologicznej lub jądrowej; g) uwalnianie substancji niebezpiecznych lub powodowanie pożarów, powodzi lub wybuchów, czego rezultatem jest zagrożenie życia ludzkiego; h) zakłócanie lub przerywanie dostaw wody, energii elektrycznej lub wszelkich innych podstawowych zasobów naturalnych, czego rezultatem jest zagrożenie życia ludzkiego; i) niezgodna z prawem ingerencja

w systemy, o której mowa w art. 4 dyrektywy Parlamentu Europejskiego i Rady 2013/40/UE (1), w przypadkach gdy zastosowanie ma art. 9 ust. 3 lub art. 9 ust. 4 lit. b) lub c) tej dyrektywy, oraz niezgodna z prawem ingerencja w dane, o której mowa w art. 5 tej dyrektywy, w przypadkach gdy zastosowanie ma art. 9 ust. 4 lit. c) tej dyrektywy **[art. 3 ust. 1 lit a) – i) Dyrektywy Parlamentu Europejskiego i Rady (UE) 2017/541 z dnia 15 marca 2017 r. w sprawie zwalczania terroryzmu i zastępująca decyzję ramową Rady 2002/475/WSiSW oraz zmieniająca decyzję Rady 2005/671/WSiSW Dz. Urz. UE L 88/6 z 31.03.2017]**.

Treści pornograficzne – wszelkie materiały ukazujące dziecko uczestniczące w rzeczywistych lub symulowanych zachowaniach o wyraźnie seksualnym charakterze, a także wszelkie przedstawianie organów płciowych dziecka w celach głównie seksualnych **[art. 20 ust. 2 Konwencji Rady Europy o ochronie dzieci przed seksualnym wykorzystywaniem i niegodziwym traktowaniem w celach seksualnych, sporządzona w Lanzarote dnia 25 października 2007 r. Dz.U. z 2015, poz. 608]**.

Treści pornograficzne mogą przedstawiać wytworzony albo przetworzony wizerunek małoletniego (uczestniczącego w czynności seksualnej). Chodzi tu zatem zarówno o ochronę małoletnich realnie istniejących, których wizerunek został zmieniony, jak i obrazy nieistniejącego małoletniego (pornografia, która pokazuje wizerunki dzieci wygenerowane komputerowo czy też pornograficzne filmy animowane, które ukazują sceny z udziałem dzieci, jednakże żadne rzeczywiście istniejące dziecko nie brało udziału w produkcji takiego filmu na jakimkolwiek jego etapie). W tym zakresie penalizacją art. 202 § 4 kodeksu karnego objęto produkowanie, rozpowszechnianie, prezentowanie, przechowywanie lub posiadanie takich treści **[postanowienie Sądu Najwyższego 18.01.2021 r., IV KK 251/20, LEX nr 3111703]**.

Piractwo jako usługa „Piracy-as-a-Service” – usługa ułatwiająca nielegalne transmisje. Polega ona na zapewnieniu pakietu gotowych usług ułatwiających stworzenie, obsługę i monetyzację pirackiego przedsięwzięcia. Usługi te, naruszają prawo, poprzez powielanie legalnej usługi transmisji strumieniowej. Operatorzy udostępniający nieuprawnione retransmisje opracowali strategie odporności, które pozwalają im obejść mechanizmy służące egzekwowaniu prawa. Należy zatem uważnie monitorować rozwój nowych form piractwa i strategii odporności, które mogą mieć wpływ również na inne rodzaje treści i wpływać na zdolność uprawnionych podmiotów do skutecznego egzekwowania ich praw, uwzględniając w szczególności zmiany technologiczne i nowe modele biznesowe **[motyw 4 Zalecenia Komisji (UE) 2023/1018 z dnia 4 maja 2023 r. w sprawie zwalczania piractwa internetowego wydarzeń sportowych i innych wydarzeń na żywo Dz.Urz. UE L 136/83]**.

Naruszenie ochrony danych osobowych – oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych **[art. 4 pkt 12 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych Dz.Urz. UE L. 119/1 z 4.05.2016 r.)]**.

Mowa nienawiści – to w szczególności przestępstwa na tle rasistowskim i ksenofobicznym. Są to czyny popełniane umyślnie obejmujące: a) publiczne nawoływanie do przemocy lub nienawiści skierowanej przeciwko grupie osób, którą definiuje się według rasy, koloru

skóry, wyznawanej religii, pochodzenia albo przynależności narodowej lub etnicznej, lub przeciwko członkowi takiej grupy; b) popełnienie czynu, o którym mowa w lit. a), przez publiczne rozpowszechnianie lub rozprowadzanie tekstów, obrazów lub innych materiałów; c) publiczne aprobowanie, negowanie lub rażące pomniejszanie zbrodni ludobójstwa, zbrodni przeciwko ludzkości oraz zbrodni wojennych w rozumieniu art. 6, 7 i 8 statutu Międzynarodowego Trybunału Karnego skierowanych przeciwko grupie osób, którą definiuje się według rasy, koloru skóry, wyznawanej religii, pochodzenia albo przynależności narodowej lub etnicznej, lub przeciwko członkowi takiej grupy, jeśli czyny takie mogą podburzać do przemocy lub wzbudzać nienawiść skierowaną przeciwko tej grupie lub jej członkowi; d) publiczne aprobowanie, negowanie lub rażące pomniejszanie zbrodni określonych w art. 6 Karty Międzynarodowego Trybunału Wojskowego załączonej do porozumienia londyńskiego z dnia 8 sierpnia 1945 r., a skierowanych przeciwko grupie osób, którą definiuje się według rasy, koloru skóry, wyznawanej religii, pochodzenia albo przynależności narodowej lub etnicznej, lub przeciwko członkowi takiej grupy, jeśli czyny takie mogą podburzać do przemocy lub wzbudzać nienawiść skierowaną przeciwko tej grupie lub jej członkowi. Termin „nienawiść” należy rozumieć jako odnoszący się do nienawiści okazywanej ze względu na rasę, kolor skóry, religię, pochodzenie lub przynależność narodową lub etniczną **[Decyzja ramowa Rady 2008/913/WSiSW z dnia 28 listopada 2008 r. w sprawie zwalczania pewnych form i przejawów rasizmu i ksenofobii za pomocą środków prawnokarnych Dz.U. L 328 z 6.12.2008, s. 55–58]**.

Stalking – uporczywe nękanie innej osoby lub osoby dla niej najbliższej, wzbudzające u niej uzasadnione okolicznościami poczucie zagrożenia, poniżenia lub udręczenia lub istotnie naruszające jej prywatność **[art. 190a § 1 Kodeksu karnego]**.

Dezinformacja – to akt, w ramach którego fałszywe informacje są tworzone i udostępniane w złej wierze lub prawdziwe informacje przekazywane są w taki sposób by wywołać fałszywe opinie. Informacja tworzona z intencją generalnej szkody bądź także bezmyślne powtarzanie niesprawdzonych informacji. Przekazy te można podzielić korzystając z dwóch kryteriów łącznie: stosunku do prawdy oraz intencji tworzenia i rozpowszechniania. Zatem dezinformację należy rozumieć jako możliwe do zweryfikowania nieprawdziwe, wprowadzające w błąd lub także prawdziwe informacje (mające na celu wywołanie fałszywej opinii na dany temat), tworzone, przedstawiane i rozpowszechniane w celu uzyskania korzyści gospodarczych lub wprowadzenia w błąd opinii publicznej, które mogą wyrządzić szkodę publiczną **[K. Chałubińska-Jentkiewicz, *Prawne granice dezinformacji w środkach społecznego przekazu*, Toruń 2023, s. 103]**.

Dezinformacja to fałszywa, niedokładna lub wprowadzająca w błąd informacja stworzona, zaprezentowana i rozpowszechniana dla zysku lub rozmyślnego spowodowania szkody publicznej **[Kodeks postępowania UE w zakresie zwalczania dezinformacji, Luxemburg 2025, http://Code_of_Conduct_on_Disinformation_f9bhfVbrSm6IEbiMmtGRVsLHZKA_112678.pdf]**.

Trolling – to celowe, prowokujące, antyspołeczne zachowanie w Internecie, które ma na celu wywołanie dyskusji z innymi użytkownikami, polegające na zamieszczaniu kontrowersyjnych, prowokacyjnych lub obraźliwych treści. Do narzędzi trollingu zalicza się propagandę, manipulację, przeinaczanie faktów **[M. Nowikowska, *Zjawisko „trollingu” w Internecie [w:] Media w erze cyfrowej*, red. K. Chałubińska-Jentkiewicz, M. Nowikowska, K. Wąsowski, Warszawa 2021, s. 194]**.

Źródła

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/sownik/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%2CTreści-o-charakterze-terrorystycznym-w-Internecie.html?utm_source=chatgpt.com



CZĘŚĆ III

Naruszanie praw własności intelektualnej

Naruszanie praw własności intelektualnej w problematyce nielegalnych treści oraz handlu podrabianymi towarami w Internecie

Nielegalny handel podrabianymi towarami stanowi znaczące i rosnące zagrożenie w zglobalizowanej gospodarce. Nie należy lekceważyć jego szkodliwego wpływu na konsumentów, wzrost gospodarczy, innowacyjność, praworządność, wreszcie na środowisko i ostatecznie na zaufanie do dobrze funkcjonujących rynków światowych.



Wprowadzenie

Handel w Internecie przybiera obecnie coraz to nowe formy i obejmuje nowe obszary eksploatacji. To już nie tylko handel w sklepach internetowych czy na dużych platformach e-handlu, ale także kwestie streamingu online, płatnych transmisji wydarzeń sportowych czy artystycznych, a także handel zakazanymi i podrobionymi produktami w tzw. Deepwebie i Darkwebie.

E-commerce, bardziej niż inne systemy biznesowe, często obejmuje sprzedaż produktów i usług opartych na własności intelektualnej i jej licencjonowaniu. Muzyka, obrazy, zdjęcia, oprogramowanie, design, moduły szkoleniowe i edukacyjne, filmy, systemy,

itp. mogą być przedmiotem e-handlu, gdzie własność intelektualna jest głównym składnikiem wartości w transakcji. Ochrona prawna jest ważna, ponieważ rzeczy wartościowe, którymi handluje się w Internecie, muszą być chronione przez prawa wyłączne i przy użyciu technologicznych systemów bezpieczeństwa. W przeciwnym razie rzeczy te mogą zostać skradzione lub podrobione, zaś całe przedsiębiorstwa – zniszczone.

Łączny wkład wnoszony do gospodarki UE przez sektory intensywnie korzystające z praw własności intelektualnej sięga w przybliżeniu 42% PKB (5,7 biliona euro) i obejmuje 28% zatrudnienia (plus dodatkowe 10% w wyniku zatrudnienia pośredniego w sektorach niekorzystających intensywnie z praw własności intelektualnej). Ze względu na wysoką wartość powiązaną z prawami własności intelektualnej naruszanie tych praw stanowi dochodową działalność przestępczą, przez co właściciele praw i gospodarka ponoszą znaczne koszty. Jak wynika z badania przeprowadzonego przez Urząd UE ds. Własności Intelektualnej (EUIPO)¹, ma to szczególne znaczenie w okresie obecnego kryzysu wywołanego pandemią.

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).

Według szacunkowych danych uzyskanych w wyniku badania przeprowadzonego w 2019 r. przez EUIPO i OECD dotyczących naruszenia praw własności intelektualnej w handlu międzynarodowym, w 2016 r. mogły one obejmować aż 3,3% światowego handlu. Podrabiane towary stanowią aż 6,8% przywozu do UE, czyli 121 mld euro rocznie. Te zestawienia liczbowe są znacznie wyższe niż opublikowane w 2016 r. Wynika z tego, że w ostatnich latach problem nasilił się jeszcze bardziej, a podrabianie stało się atrakcyjne dla organizacji przestępczych.

W miarę rozwoju technologii i kanałów dystrybucyjnych, równoległe ze wzrostem asortymentu podrabianych produktów, sposób funkcjonowania takich organizacji staje się coraz bardziej złożony. Do celów dystrybucji ich produktów oraz promowania dystrybucji i konsumpcji nielegalnych treści cyfrowych, fałszerze stosują modele działalności gospodarczej oparte w głównej mierze na Internecie. Strony internetowe, na których oferowana jest sprzedaż towarów podrobionych, odnoszą korzyści w postaci dodatkowych przychodów z reklam tzw. wysokiego ryzyka (strony dla dorosłych, gry i złośliwe oprogramowanie), a także, paradoksalnie, z reklam legalnych marek, którym to markom reklama na takich stronach przynosi dwójakiego rodzaju straty - szkodę dla własnej marki i uwiarygodnienie strony internetowej, na której marka się pojawia.

Poza analizą dostaw towarów podrobionych i pirackich treści, przeprowadzono również badanie po stronie popytu, tj. postaw obywateli UE (konsumentów) względem praw własności intelektualnej, czyli ich gotowości do korzystania z towarów i usług naruszających prawa własności intelektualnej. Co ich motywuje do nabywania towarów podrobionych i do uzyskiwania nielegalnego dostępu do treści chronionych prawem autorskim? Są to niskie ceny, łatwy dostęp i niski stopień stygmatyzacji społecznej powiązanej z takimi działaniami.

Najnowsze dane wielkości międzynarodowego handlu podrobionymi i pirackimi produktami pokazują, że wynosi on już 460 miliardów euro.

Stanowi to ok. 3,3% światowego handlu i blisko 7% importu UE. Jego ważnym aspektem jest handel internetowy oraz dostęp do nielegalnych treści w sieci. Ten pierwszy, czyli handel internetowy, związany jest z naruszeniami praw własności intelektualnej, takimi jak znaki towarowe (chroniące markę), wzory przemysłowe (chroniące kształty lub design), patenty na wynalazki (chroniące technologię) czy naruszenia praw do nowych odmian roślin. Ten drugi, czyli dostęp do nielegalnych treści w sieci, najczęściej narusza prawa własności intelektualnej w postaci praw autorskich.



Cyfrowe piractwo w UE

Pod koniec 2024 r. poznaliśmy dane o cyfrowym piractwie w UE. Wynika z nich², że Europejczycy korzystają średnio aż 10 razy w miesiącu z nielegalnych treści online. Według najnowszego raportu w tym zakresie piractwo internetowe wśród europejskich internautów utrzymuje się na stałym poziomie w porównaniu z ubiegłym rokiem i wynosi 10 dostępow do nielegalnych treści miesięcznie na użytkownika Internetu. Z kolei treści telewizyjne stanowią połowę wszystkich przypadków nielegalnego dostępu – średnio 5 dostępow miesięcznie na użytkownika Internetu w UE. Wzrosła także liczba nielegalnych stron telewizji internetowej (IPTV) – w 2023 r. liczba odwiedzin pirackich stron IPTV wzrosła o 10%.

Raport Urzędu UE ds. Własności Intelektualnej (EUIPO) wykazał, że piractwo cyfrowe w całej UE utrzymuje się na wysokim poziomie. Tendencja ta

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)

jest widoczna we wszystkich kategoriach treści internetowych, z wyjątkiem publikacji, w których poziom piractwa spadł, oraz muzyki, gdzie poziom piractwa wzrósł w porównaniu z początkiem 2023 r. Jeśli chodzi o ogólne piractwo, raport EUIPO wykazał, że użytkownicy Internetu w UE wchodzi na strony z nielegalnymi treściami na poziomie niższym niż średnia unijna w Austrii (8,9), Hiszpanii (8,5), Polsce (8,3), Rumunii (7,9), Niemczech (7,7) i we Włoszech (7,3).

Transmisja strumieniowa jest najczęstszą metodą dostępu do treści pirackich. Zaobserwowano alarmującą tendencję w zakresie nielegalnego streamingu – w 2023 r. odnotowano 10% wzrost liczby odwiedzin stron pirackiej telewizji IPTV. W badaniu oszacowano, że nawet 1% użytkowników Internetu w UE mógł dokonać subskrypcji na nielegalnych stronach IPTV w ciągu zaledwie dwóch lat, nie licząc istniejących użytkowników, którzy takiej subskrypcji dokonali przed 2022 r. Badanie EUIPO wykazało również, że użytkownicy Internetu chętniej wybierają dostęp do pirackiej muzyki i publikacji za pośrednictwem urządzeń mobilnych, jednak jeśli chodzi o oglądanie nielegalnych treści telewizyjnych, użytkownicy wolą raczej korzystać ze swoich komputerów stacjonarnych.

Stwierdzono, że czynnikami ekonomicznymi i społecznymi odpowiadającymi za piractwo są między innymi nierówności dochodowe, bezrobocie młodzieży i odsetek młodych osób w społeczeństwie. Badanie wskazuje, że wyższy poziom nierówności dochodowych i większy odsetek młodych osób w społeczeństwie korelują z wyższym poziomem piractwa. Z kolei wyższe PKB na mieszkańca i większa znajomość źródeł legalnych treści wiążą się z niższymi wskaźnikami piractwa.

Piractwo praw autorskich obejmuje kilka metod rozpowszechniania nieautoryzowanych treści online, np. nielegalne usługi subskrypcyjne i otwarte internetowe transmisje strumieniowe finansowane przychodami z reklam. Dostawcy takich usług wykorzystują wyrafinowane techniki w celu

utrudnienia wykrycia, często korzystając z legalnych usług dystrybucji treści.



Znaczenie sektorów gospodarki intensywnie korzystających z praw własności intelektualnej dla rozwoju społeczno-gospodarczego

Obecnie gospodarka UE obejmuje 357 sektorów intensywnie korzystających z praw własności intelektualnej. Spośród tych sektorów 229 (64%) intensywnie korzysta z praw własności intelektualnej w odniesieniu do więcej niż jednego prawa własności intelektualnej³.

Sektory intensywnie korzystające z praw własności intelektualnej wygenerowały 29,7% wszystkich miejsc pracy w UE w latach 2017–2019, co oznacza wzrost z 28,9% w latach 2014–2016 (z uwzględnieniem niewielkich różnic metodologicznych między poszczególnymi badaniami). Średnio w tym okresie zatrudnienie znalazło w tych sektorach ponad 61 mln osób w UE. Sektory te zapewniły kolejne 20 mln miejsc pracy dostarczając towary i usługi na rzecz sektorów intensywnie korzystających z praw własności intelektualnej. Biorąc pod uwagę wskazane zatrudnienie pośrednie, całkowita liczba miejsc pracy związanych z prawami własności intelektualnej wyniosła aż 82 mln (39,4%).

W tym samym okresie sektory intensywnie korzystające z praw własności intelektualnej wygenerowały ponad 47% unijnego PKB o łącznej wartości 6,4 bln EUR. Odpowiadały one również za

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).

większość wymiany handlowej UE z resztą świata i wygenerowały nadwyżkę handlową w wysokości 224 mld EUR, przyczyniając się do utrzymania równowagi w handlu zewnętrznym UE.

Sektory intensywnie korzystające z praw własności intelektualnej wnoszą istotny wkład w funkcjonowanie rynku wewnętrznego UE. Odpowiadają one za ponad 75% handlu wewnątrz UE. Podczas gdy państwa takie jak Niemcy, Francja, Włochy i Holandia przodują w tworzeniu nowych praw własności intelektualnej, inne państwa, choćby Węgry, Polska i Estonia, również w dużym stopniu korzystają z podziału pracy w sektorach intensywnie korzystających z praw własności intelektualnej. W sumie niemal 7 milionów miejsc pracy związanych z prawami własności intelektualnej w państwach członkowskich jest tworzonych przez przedsiębiorstwa z innych państw członkowskich, przy czym udział takich miejsc pracy w sektorach intensywnie korzystających z praw własności intelektualnej przekracza w niektórych państwach 30%.

Także płace pracowników w sektorach intensywnie korzystających z praw własności intelektualnej są znacznie, bo średnio o 41%, wyższe w porównaniu z innymi sektorami. Należy przy tym zaznaczyć, że wartość dodana na pracownika również jest w tych sektorach wyższa niż w innych sektorach gospodarki. Z porównania wyników tego badania z wynikami badania przeprowadzonego w 2019 r. wynika, że względny wkład sektorów intensywnie korzystających z praw własności intelektualnej w gospodarkę UE odnotował wzrost między okresem 2014–2016 (badanie z 2019 r.) a 2017–2019 (badanie z 2022 r.), przy uwzględnieniu zmiany w wykazie tych sektorów.

Wśród sektorów intensywnie korzystających z praw własności intelektualnej w ostatnich latach wzrosło znaczenie gospodarcze tych zaangażowanych w rozwój technologii służących łagodzeniu skutków zmiany klimatu i sektorów związanych z zielonymi znakami towarowymi. Sektory intensywnie korzystające z patentów w zakresie technologii służących łagodzeniu skutków zmiany klimatu lub

zielonych znaków towarowych odpowiadały za 9,3% zatrudnienia i 14,0% PKB w UE w latach 2017–2019 oraz za znaczną część handlu zewnętrznego UE. To tylko podstawowe dane płynące z analizy krajów unijnych – nie przeprowadzono badań i brakuje danych dot. bezpośrednio Polski.



Znaczenie młodszych pokoleń i skala szarej strefy

Co niepokojące, obecnie pokolenie Z wykazuje większą tolerancję dla kupowania nielegalnych towarów - tak wynika z raportu przygotowanego przez „The Economist”. Światowe Forum Ekonomiczne szacuje, że straty gospodarcze wynikające z nielegalnego handlu są równoważne 3% światowego PKB. Według Konferencji Narodów Zjednoczonych ds. Handlu i Rozwoju gospodarka światowa traci na tym rocznie 2 tryliony dolarów.

O konieczności walki ze zjawiskiem szarej strefy, w tym o regionalnej współpracy między rządami, organami ścigania i biznesem, rozmawiali uczestnicy szóstego Światowego Szczytu Przeciwko Nielegalnemu Handlowi: Europa Środkowo-Wschodnia organizowanego przez „The Economist”. Po raz pierwszy wydarzenie odbyło się w Polsce w 2022 r. *Szara strefa wciąż jest problemem, ale Polska może w wielu obszarach wyznaczać standardy walki z tym zjawiskiem. Według danych Eurostatu w 2021 r. zajęliśmy 1. miejsce w Europie pod względem zwiększania dochodów z VAT w latach 2008-2021. Był to efekt szeregu wprowadzonych rozwiązań, m.in. jednolitego pliku kontrolnego czy mechanizmu split payment* - komentował Piotr Arak, ówczesny Dyrektor Polskiego Instytutu Ekonomicznego.

Podczas szczytu zaprezentowano raport „Nielegalny handel: skala, zakres, przepływy” przygotowany przez „The Economist”. Wynika z niego, że jedynie 37% przedstawicieli pokolenia Z (osoby urodzone w latach 1997-2003) uważa za nieakceptowalne kupowanie nielegalnych towarów. Z kolei ok. 31% przedstawicieli pokolenia Z i 26% tzw. millenialsów uznaje, że konsumpcja nielegalnych towarów jest dopuszczalna w przypadku niedoboru produktów lub niekorzystnych warunków ekonomicznych.

Eksperci UN Global Compact Network Poland szacują, że całkowity udział szarej strefy w Polsce w trakcie pandemii wyniósł 18-20%. Podobne szacunki przedstawia Instytut Prognoz i Analiz Gospodarczych, według którego udział szarej strefy w tworzeniu tegorocznego PKB Polski ma wynieść 18,9% (łącznie 590 mld zł). Jednak jej zwalczanie nabrało wyraźnego przyspieszenia od 2017 r., kiedy utworzono Krajową Administrację Skarbową (KAS).

Zwalczanie nielegalnego obrotu towarami ma kluczowe znaczenie nie tylko ze względu na kwestie fiskalne, ale również dla ochrony bezpieczeństwa obszaru Polski i całej Unii Europejskiej. Pandemia Covid-19 spowodowała duży wzrost handlu e-commerce, a wojna w Ukrainie - wprowadzanie różnych obostrzeń na przewóz towarów z i do państw trzecich. Administracje celne i podatkowe muszą nadążyć za tymi zmianami i odpowiadać na nowe wyzwania. Pandemia i wojna nie osłabiły skuteczności naszego działania, ponieważ szybko wdrożyliśmy odpowiednie mechanizmy i procedury. Było to możliwe również dlatego, że w ostatnich latach znacznie wzrósł poziom informatyzacji KAS - mówił Mariusz Gojny, ówczesny wiceminister finansów i zastępca szefa KAS.

Z raportu przygotowanego przez „The Economist” wynika również, że nielegalny handel w Internecie jest łatwiejszy wskutek rozwoju platform sprzedażowych. Aż 64% respondentów uważa, że nielegalne towary stały się łatwiejsze do nabycia od czasu wybuchu pandemii i konsumenci są teraz bardziej skłonni do ich nabywania w sieci.

Wyniki budzą poważne obawy, ponieważ handel towarami podrabianymi i pirackimi stanowił do 2,5% światowego handlu w 2019 r.. Biorąc pod uwagę

tylko przywóz do UE, podrabiane towary stanowiły do 5,8% przywozu. Kwoty te są wyższe od tych z poprzednich lat, a nielegalny handel podróbkami stanowi poważne zagrożenie dla nowoczesnych, otwartych i zglobalizowanych gospodarek.

Handel podrabianymi towarami stanowi także poważne zagrożenie dla współczesnej, wydajnej i przyszłościowej gospodarki światowej. Nie tylko uderza w samo serce silnika zrównoważonego wzrostu gospodarczego, ale także stwarza poważne zagrożenie dla zdrowia (np. podrabiane samochodowe części zamienne, podrabiane akumulatory) oraz zagrożenia dla środowiska (np. podrabiane chemikalia lub pestycydy).

Aby zrozumieć i zwalczać ryzyko związane z handlem towarami podrobionymi i pirackimi, rządy potrzebują aktualnych informacji na temat skali, zakresu i tendencji w tym zakresie. Pandemia Covid-19 tylko pogłębiła i wywarła mocniejszy wpływ na handel niebezpiecznymi podróbkami, a w większości przypadków kryzys ten doprowadził do zaostrzenia się istniejących już trendów. Dotyczyło to w szczególności podrabianych leków oraz pozostałych wyrobów wysokiego ryzyka, takich jak napoje alkoholowe, gdzie przerwane łańcuchy dostaw i zmiana popytu doprowadziły do powstania nowych obszarów aktywności przestępczej. Powszechny, gwałtowny wzrost liczby sfalszowanych produktów dotyczył jednak nie tylko leków i środków ochrony indywidualnej, ale także wielu innych towarów, które również mogą stanowić zagrożenie dla zdrowia i bezpieczeństwa, takich jak artykuły konsumpcyjne i części zamienne.



Bardziej nielegalny handel czy groźne podróbki

Najnowsze, pochodzące z 2022 r., badanie OECD i EUIPO⁴, przedstawia ocenę ilościową zakresu handlu podrabianymi produktami, które stanowią zagrożenie dla zdrowia, środowiska naturalnego i bezpieczeństwa, a także obserwowanych w nim trendów. Jest ono wynikiem analizy unikatowego, pochodzącego z różnych krajów zbioru danych dotyczących zajęć dokonanych przez służby celne oraz danych związanych z egzekwowaniem przepisów, w połączeniu z ustrukturyzowanymi wywiadami przeprowadzonymi z ekspertami ds. egzekwowania przepisów.

Co do zasady wszystkie podrabiane towary wiążą się z ryzykiem i mogą stanowić zagrożenie dla użytkowników. Aby uwzględnić różne stopnie ryzyka, w badaniu zastosowano dwa podejścia do określenia zakresu niebezpiecznych podróbek. W szerszym podejściu uwzględniono towary, które muszą spełniać określone normy bezpieczeństwa produktu. Są one objęte zakresem działania amerykańskiej Agencji Żywności i Leków lub są przedmiotem projektu amerykańskiej ustawy SHOP SAFE ACT. Przy zastosowaniu takiego podejścia można stwierdzić, że najczęściej występującymi niebezpiecznymi podróbkami są artykuły odzieżowe, części samochodowe, aparatura optyczna i medyczna oraz farmaceutyki.

Ustalono, że największymi eksporterami niebezpiecznych podróbek są Chiny i Hongkong (Chiny), których dotyczy ponad trzy czwarte dokonanych zajęć celnych. W związku z rosnącą popularnością handlu przez Internet najczęstszą metodą wysyłki niebezpiecznych podróbek są przesyłki pocztowe, co znacznie komplikuje procedury sprawdzania i wykrywania oraz zmniejsza ryzyko wykrycia przestępstwa i nałożenia kar. Głównymi miejscami przeznaczenia małych przesyłek zawierających artykuły niebezpieczne były Unia Europejska i Stany Zjednoczone. Jednak pod względem wartości zajęć celnych wyraźnie dominuje transport drogą morską. Rozkład miejsc odbioru niebezpiecznych podróbek wysyłanych drogą morską był zróżnicowany, a na szczycie listy znalazły się państwa Zatoki Perskiej.

Bardziej ukierunkowane, węższe podejście uwzględnia tylko artykuły spożywcze, produkty farmaceutyczne, kosmetyki i kategorie towarów, wobec których najczęściej wydawano ostrzeżenia dotyczące bezpieczeństwa i wycofywano je z rynku. W tym ujęciu do najczęściej sprzedawanych niebezpiecznych podróbek należą perfumy i kosmetyki, odzież, zabawki, części zamienne do samochodów oraz produkty farmaceutyczne. Większość tych towarów pochodziła z Chin (55% wszystkich zajęć celnych na świecie) i Hongkongu (Chiny) (19%). 60% zajętych towarów niebezpiecznych wysłano pocztą, natomiast pod względem wartości zajętych towarów dominującym środkiem transportu był transport morski. 60% wszystkich zajęć produktów niebezpiecznych przeznaczonych na rynek UE miało związek ze sprzedażą przez Internet. Udział tych produktów pod względem wartości był jednak nieznaczny. Wśród niebezpiecznych podróbek zamawianych w Internecie najczęściej kupowano kosmetyki, a w dalszej kolejności – odzież, zabawki i części zamienne do samochodów. Większość tych towarów (75%) wysłano z Chin.

Istniejąca analiza ilościowa nielegalnego handlu podrabianymi i pirackimi towarami wskazuje, że asortyment produktów będących przedmiotem podrabiania jest bardzo szeroki i stale się poszerza. Każdy produkt, którego własność intelektualna zwiększa wartość ekonomiczną posiadaczy praw, staje się celem fałszerzy. Podrabianie dotyczy zatem nie tylko towarów luksusowych, ale także produktów pośrednich i szerokiej gamy powszechnych produktów konsumpcyjnych. W przypadku wszystkich tych towarów podróbki powodują szkody gospodarcze, niszcząc miejsca pracy, kradnąc zyski i zmniejszając zachęty do innowacji.

Jednocześnie w przypadku niektórych produktów podróbki są często niskiej jakości, co stwarza znaczne ryzyko dla konsumentów. Należą do nich zagrożenia dla zdrowia (np. podrobione farmaceutyki, zabawki lub produkty spożywcze), zagrożenia dla bezpieczeństwa (np. podrobione samochodowe części zamienne, podrobione baterie) oraz zagrożenia dla środowiska (np.

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).

podrabiane chemikalia lub pestycydy). W przypadku wszystkich tych produktów legalni dostawcy muszą przestrzegać przepisów dotyczących zdrowia, bezpieczeństwa i ochrony środowiska, aby mieć pewność, że ich produkty nie spowodują szkód. Fałszerze nie są związani tymi przepisami, w związku z czym oferowane przez nich fałszywe towary mogą stanowić poważne zagrożenie dla zdrowia, bezpieczeństwa i środowiska.

Oprócz szkodliwych zagrożeń dla zdrowia i bezpieczeństwa podrabianie ma daleko idące szkodliwe skutki gospodarcze. OECD i EUIPO już wcześniej przeprowadziły badanie dotyczące podrabiania i piractwa w sektorze farmaceutycznym, które dokumentuje szkodliwe skutki dla gospodarek. Kolejne badania uzupełniają wykonaną pracę o dalszą analizę dotyczącą zagrożeń dla zdrowia, bezpieczeństwa i środowiska stwarzanych przez podróbki w wielu sektorach, w tym produktów spożywczych i środków ochrony indywidualnej, w których podróbki często nie spełniają norm oraz są przechowywane i transportowane w złych warunkach, co może stanowić poważne zagrożenie dla zdrowia konsumentów. Badane są także zabawki i baterie, w przypadku których często produkowane są podróbki bez zachowania jakichkolwiek norm bezpieczeństwa, a co za tym idzie mogą stwarzać znaczne zagrożenia. Podrabiane są także chemikalia i pestycydy, w przypadku których fałszywe produkty, które nie są zgodne z przepisami dotyczącymi ochrony środowiska, mogą prowadzić do znacznych szkód w środowisku.

Pomiar wielkości i zakresu fałszerstw jest na ogół trudny ze względu na potajemny charakter tego zjawiska. Chociaż w wyniku prac ekonometrycznych poczyniono znaczne postępy w mierzeniu jego rozpowszechnienia w handlu międzynarodowym, brakuje prac dotyczących zagrożeń stwarzanych przez podrabiane produkty, które opierają się głównie na niepotwierdzonych informacjach.



Handel, przenosząc się do Internetu, ciągnie swój cień nielegalności

Jak wynika z wyżej wspomnianych danych, gwałtownie rośnie skala nadużyć w handlu elektronicznym w celu ułatwienia handlu towarami podrobionymi. W ostatnich latach handel elektroniczny szybko się rozwija, ponieważ konsumenci są coraz bardziej przekonani do zamawiania towarów i usług przez Internet i poprzez media społecznościowe.

Liczba przedsiębiorstw prowadzących handel elektroniczny między przedsiębiorcami i konsumentami (B2C) stale rośnie. W latach 2018-2020 sprzedaż detaliczna online⁵, stanowiąca część łącznej sprzedaży B2C, wzrosła o 41% w głównych gospodarkach świata, przy czym całkowita sprzedaż detaliczna wzrosła o mniej niż 1%. Wzrost ten spowodowała pandemia Covid-19, ponieważ konsumenci dokonywali zakupów online w trakcie lockdownu, aby uniknąć odwiedzania sklepów stacjonarnych. W czasie pandemii środowisko internetowe stało się również bardziej popularnym celem nielegalnego handlu. Organy egzekwowania prawa w dziedzinie cyberprzestępczości odnotowały wzrost liczby różnych przestępstw elektronicznych, w tym ofert nielegalnych towarów, m.in. sfalszowanych lub substandardowych leków, testów i innych towarów związanych z Covid-19.

Rosnąca popularność handlu elektronicznego nie umknęła uwadze fałszerzy, którzy coraz intensywniej wykorzystują handel elektroniczny do sprzedaży

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).

podrobionych towarów konsumentom - niektórzy z nich sądzą, że kupują autentyczne towary, a inni aktywnie poszukują podrabianych towarów po niskich cenach. Powiązania handlu elektronicznego z nielegalnym handlem towarami podrobionymi są poparte analizą ilościową, w której bada się związek między handlem elektronicznym a liczbą i wartością konfiskat towarów podrobionych przez organy celne w latach 2017-2019. W analizie stwierdzono, że powiązanie staje się silniejsze, gdy uwzględnione zostaną wskaźniki nielegalnego handlu podrobionymi towarami przy użyciu małych paczek; sugeruje to, że nielegalne towary zakupione drogą handlu elektronicznego są często wysyłane za pośrednictwem małych paczek, zwłaszcza z wykorzystaniem usług pocztowych.

Studium przypadku Unii Europejskiej, w którym zgromadzono dane dotyczące zatrzymań towarów podrobionych powiązanych z handlem elektronicznym, dostarcza więcej informacji na temat tej sytuacji. Z danych wynika, że 91% zatrzymań towarów podrobionych związanych z handlem elektronicznym dotyczyło usług pocztowych. Z kolei na usługi pocztowe przypadło jedynie 45% zatrzymań podrobionych towarów niezwiązanych z handlem elektronicznym.

Pod względem wartości z danych wynika, że 81,8% zatrzymań związanych z handlem elektronicznym dotyczyło usług pocztowych, natomiast zaledwie 8,9% przypadło na inne sposoby sprzedaży towarów podrobionych. Jeżeli chodzi o pochodzenie, źródła towarów podrobionych sprzedawanych za pośrednictwem handlu elektronicznego i innych rodzajów handlu są podobne. Udział Chin był jednak wyższy w przypadku podrobionych towarów sprzedawanych za pośrednictwem handlu elektronicznego (75,9% w porównaniu do 45,9% całkowitej liczby zatrzymań).

Do zatrzymanych w UE towarów podrobionych związanych z handlem elektronicznym zalicza się szeroki wachlarz produktów. Na najwyższym miejscu plasują się obuwie (33,7% wszystkich zatrzymań), odzież (17,3%), perfumy i kosmetyki (9,6%), wyroby skórzanе (8,7%), maszyny elektryczne i sprzęt elektryczny (6,5%), zabawki (5,5%) i zegarki (5,2%). Działalność podmiotów działających w złej

wierze rozkwitła na rynkach handlu elektronicznego, gdyż stosunkowo łatwo jest utworzyć strony internetowe sprzedające przedmioty podrobione. Ponadto podmioty te nadal znajdują nowe sposoby umieszczania produktów podrabianych na zaufanych platformach. Organy ścigania aktywnie angażują się w identyfikowanie i zamykanie oszukańczych stron oraz współpracują z operatorami dużych platform i właścicielami marek w celu wychwytywania sprzedaży towarów podrobionych, lecz problem ten jest nadal znaczny i wciąż rośnie.

Trudności związane z przechwytywaniem podrobionych towarów potęgują środki, za pomocą których produkty zamówione w handlu elektronicznym są wysyłane. Fałszerze próbują wykorzystywać słabości kanałów dystrybucji w celu ułatwienia swojej nielegalnej działalności. W przypadku handlu elektronicznego odbywa się to w dużej mierze za pośrednictwem poczty. Istnieje obawa, że organy pocztowe i celne nie są dobrze przygotowane do kontroli przesyłek małych paczek i paczek listowych, służących wykrywaniu podróbek. Mają one ograniczone możliwości wykrywania towarów podrobionych na skalę międzynarodową, ponieważ wysyłki tych produktów przemieszane są z miliardami przedmiotów sprzedawanych zgodnie z prawem.

Rządy podjęły szereg działań mających na celu zwalczanie sprzedaży towarów podrobionych przez Internet, do których należą zawarcie porozumień z zainteresowanymi stronami, które służą zacieśnieniu współpracy, oraz wzmożone wysiłki na rzecz wykrywania stron internetowych sprzedających towary podrobione i podejmowania działań przeciwko nim. Na przykład w Unii Europejskiej Komisja Europejska była odpowiedzialna za opracowanie i wdrożenie protokołu ustaleń między platformami, właścicielami marek i innymi zainteresowanymi stronami w celu propagowania dobrych praktyk w walce z internetową sprzedażą podrobionych towarów. W Stanach Zjednoczonych rząd zaproponował utworzenie grupy roboczej ds. handlu elektronicznego, która skupiła główne platformy internetowe w celu współpracy i współdziałania w zakresie sposobów zwalczania towarów podrobionych sprzedawanych na ich platformach.

W Australii rząd opracowuje mechanizm umożliwiający konsumentom identyfikację sprzedawców legalnych produktów poprzez powiązanie autoryzowanych sprzedawców określonych marek z publicznym rejestrem znaków towarowych. Oprócz tego w Unii Europejskiej i Stanach Zjednoczonych rozważa się wprowadzenie przepisów i dyrektyw, które po przyjęciu ustanowią nowe ramy walki z przestępstwami w handlu elektronicznym, w tym handlem nielegalnymi towarami.

Operatorzy dużych platform opracowali wieloaspektowe podejścia do zwalczania sprzedaży towarów podrzobionych na swoich platformach. Ich działania obejmują środki i mechanizmy z udziałem sprzedawców będących osobami trzecimi, konsumentów, właścicieli marek i organów ścigania, a także opracowanie i wdrożenie strategii proaktywnego wykrywania i usuwania towarów podrzobionych. Zdolność platform handlowych do odpowiedniego sprawdzania sprzedawców będących osobami trzecimi okazała się jednak niewystarczająca i nieustannie czynione są starania na rzecz poprawy mechanizmów identyfikacji i dyscyplinowania stron sprzedających towary podrzobione. Analizy pokazują, że nadużycia na rynkach internetowych przez fałszerzy są bardzo dynamiczne. Konieczne jest dalsze badanie rozwoju tej dynamiki, zarówno na poziomie przemysłu, jak i za pomocą studiów przypadku.



Działania na gruncie polskim: Krajowa Administracja Skarbowa

W naszym kraju w systemie zwalczania podróbek i piractwa istotne miejsce zajmuje Krajowa Administracja Skarbowa, która jest organem

administracji skarbowej i celnej w Polsce. Jednym z zadań organu jest egzekwowanie praw własności intelektualnej. W struktury KAS wchodzi Służba Celno-Skarbowa, która jest organem ścigania. Warto podkreślić, że podstawowym trybem prowadzenia postępowania dla KAS jest dążenie do zniszczenia podrzobionych towarów. W latach 2018-2021 najczęściej podrabianymi kategoriami towarowymi były: kosmetyki, odzież, zegarki, biżuteria i galanteria, gry, sprzęt sportowy i zabawki oraz papierosy.

Zatrzymywanie towarów naruszających prawa własności intelektualnej w momencie próby wprowadzenia ich na rynek UE pozwala skutecznie walczyć z fałszerstwem i piractwem.

Przypomnijmy, że przedmiotami ochrony prawa w działalności KAS są:

- znaki towarowe,
- wzory przemysłowe i użytkowe,
- prawa autorskie i pokrewne,
- patenty,
- dodatkowe świadectwa ochronne,
- ochrony odmian roślin,
- nazwy pochodzenia lub oznaczenia geograficzne,
- topografie układów scalonych,
- nazwy handlowe.

Zapewnienie przez organy celne ochrony praw własności intelektualnej zależy od współpracy z właścicielami praw. Jedną z form współpracy jest możliwość złożenia wniosku o podjęcie działania przez organy celne.

Do Dyrektora Izby Administracji Skarbowej w Warszawie można złożyć wniosek o podjęcie działań przez organy celne w celu ochrony praw własności intelektualnej. Wniosek o podjęcie działań sporządza się na formularzu będącym

załącznikiem do Rozporządzenia Komisji (UE) nr 1352/2013. Osobą uprawnioną do wniesienia wniosku jest właściciel prawa lub jej pełnomocnik, a także osoba uprawniona do używania praw własności intelektualnej.

Jeśli organy celne, przed złożeniem wniosku przez posiadacza prawa lub przed jego uwzględnieniem, mają wystarczające powody, by podejrzewać, iż towary naruszają prawo własności intelektualnej, mogą one zawiesić dopuszczenie towarów lub zatrzymać je na okres 4 dni roboczych od chwili otrzymania zawiadomienia przez posiadacza prawa, aby umożliwić posiadaczowi prawa złożenie wniosku o podjęcie działań do Dyrektora Izby Administracji Skarbowej w Warszawie. Jeśli wniosek nie zostanie złożony, organ celny zwalnia zatrzymane towary.

Istnieje jeszcze trzecia procedura, tzw. „małych przesyłek” (3 szt. lub 2 kg brutto), która odbywa się bez angażowania posiadacza praw. Jeśli w trakcie kontroli celnej funkcjonariusz celny zidentyfikuje towary spełniające kryteria, to bez konieczności konsultacji z posiadaczem praw własności intelektualnej, zawiesza zwolnienie towaru / zatrzymuje towar na okres 10 dni roboczych.

Problematyka wykrywania, ścigania i likwidowania naruszeń praw własności przemysłowej jest istotna dla obrotu gospodarczego, wzmacniania miejsc pracy i rozwoju przedsiębiorstw. Dlatego Urząd Patentowy RP współpracuje z Krajową Administracją Skarbową, organizując wspólne konferencje, webinary i spotkania informacyjne.



Młodzież w działaniu

Warto dodać, że niemniej ważne są dane o procederach w korzystaniu z praw własności intelektualnej przez ludzi młodych i dane o charakterystyce naruszeń, w tym naruszeń treści online w tej istotnej grupie wiekowej. W tym zakresie EUIPO przeprowadziło badanie na temat zachowania osób w wieku od 15 do 24 lat w Unii Europejskiej w odniesieniu do naruszania praw własności intelektualnej. Zarówno na szczeblu europejskim, jak i krajowym badanie rzuca światło na czynniki skłaniające młodych ludzi do kupowania podrabianych towarów lub uzyskiwania dostępu do treści cyfrowych z nielegalnych źródeł, ale także podkreśla aspekty, które mogą skłonić młodsze pokolenie do ograniczenia naruszeń praw własności intelektualnej.

Badanie⁶ z 2022 r. w większym stopniu potwierdza tendencje zauważone w jego edycjach z 2016 i 2019 r., a dodatkowo umożliwia lepszy wgląd w percepcję i postawy młodych ludzi w czasach, gdy handel internetowy i konsumpcja cyfrowa znacznie wzrosły, wpływając na zachowania konsumentów. Tendencja do uzyskiwania dostępu do treści cyfrowych z legalnych źródeł została wyraźnie potwierdzona, gdyż coraz więcej młodych ludzi deklaruje, że od treści pirackich woli legalne alternatywy. Jednak 21% respondentów nadal przyznaje, że w ciągu ostatnich 12 miesięcy świadomie uzyskało dostęp do pirackich treści, w szczególności filmów, seriali telewizyjnych, muzyki i wydarzeń sportowych na żywo, ze specjalnych serwerów, aplikacji i mediów społecznościowych. Jedna trzecia młodych konsumentów ma trudności z odróżnieniem legalnych treści cyfrowych od treści pirackich lub coraz częściej nie zwraca na to uwagi. Z drugiej strony wzrosła liczba osób celowo kupujących podróbione towary. 37% młodych ludzi potwierdza, że w ciągu ostatnich 12 miesięcy kupiło przynajmniej jeden podróbiony produkt (14% w 2019 r.).

Tendencja ta jest niepokojąca. Podobny odsetek młodych ludzi nabył podróbki przypadkiem i przyznaje, że ma trudności z odróżnieniem towarów oryginalnych od podróbionych. Choć respondenci nadal postrzegają cenę jako główny istotny

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).

czynnik skłaniający do korzystania z piractwa lub podrabianych towarów, coraz większe znaczenie zyskują wpływy społeczne, takie jak zachowania rodziny, przyjaciół i osób z otoczenia.

Jeśli chodzi o czynniki, które mogłyby skłonić młodych do refleksji i powstrzymania się przed naruszaniem praw własności intelektualnej, badani najczęściej wymieniają ryzyko osobiste związane z cyberzagrożeniami lub oszustwami internetowymi, a także lepsze zrozumienie negatywnego wpływu na środowisko lub społeczeństwo.

Analiza EUIPO powinna stanowić cenne narzędzie, które pomoże zainteresowanym stronom, decydentom, a także pedagogom i organizacjom społeczeństwa obywatelskiego w kształtowaniu inicjatyw podnoszących świadomość, aby wspierać świadome wybory młodych obywateli i konsumentów.

Młodzież nadal często korzysta z treści pochodzących z nielegalnych źródeł i kupuje w Internecie podrobione towary. Jedna trzecia (33%) respondentów korzystała w ciągu ostatnich 12 miesięcy z treści pochodzących z nielegalnych źródeł, odtwarzała je, pobierała lub przysyłała strumieniowo. Spośród tego odsetka 21% osób zrobiło to celowo, a 12% nieumyślnie. Chociaż wyniki te są w dużym stopniu zbieżne z wynikami z 2019 r., odnotowano również, że o dziesięć punktów procentowych wzrósł odsetek młodych ludzi, którzy twierdzą, że nie uzyskują dostępu do treści z nielegalnych źródeł (z 50% do 60%). Wzrost ten jest zgodny z wynikami badań przedstawionymi w szerzej pojmowanej najnowszej literaturze przedmiotu. Jeśli chodzi o podrabianie, nieco ponad połowa (52%) młodych ludzi objętych badaniem kupiła w ciągu ostatnich 12 miesięcy co najmniej jeden podrobiony produkt w Internecie.

Łącznie 37% respondentów kupiło podrobiony produkt umyślnie i taki sam odsetek zrobił to nieumyślnie (respondenci mogli zarówno umyślnie, jak i nieumyślnie kupić określony rodzaj podrobionego produktu w pewnym momencie w ciągu ostatnich 12 miesięcy). Choć wyniki tego badania nie są bezpośrednio porównywalne z wynikami jego poprzednich edycji, wskazują one jednak na

znaczny wzrost liczby osób kupujących podrobione towary od 2019 r., kiedy to 14% respondentów zgłosiło, że kupiło takie towary celowo, a 12% poinformowało, że zrobiło to nieumyślnie. Zmiana ta prawdopodobnie odzwierciedla zarówno szeroko udokumentowany wzrost liczby zakupów przez Internet w czasie pandemii Covid-19, jak i udoskonalenia wprowadzone do tego pytania w zestawieniu wskaźników z 2022 r.

Rodzaje podrobionych produktów, które respondenci najczęściej kupowali w ciągu ostatnich 12 miesięcy, to odzież i akcesoria (17%) oraz obuwanie (14%). Najważniejszym czynnikiem motywującym do nielegalnego dostępu do treści cyfrowych i zakupu podrobionych towarów pozostaje koszt, ale coraz większą rolę odgrywają też inne czynniki, zwłaszcza wpływy społeczne. Zgodnie z ustaleniami z 2019 r. głównymi powodami, dla których respondenci umyślnie uzyskiwali dostęp do treści z nielegalnych źródeł, pozostawały niższe koszty i większy wybór.

Nowe pytanie dodane do badania w roku 2022 wykazało, że w przypadku większości rodzajów treści pochodzących z nielegalnych źródeł najpopularniejszym kanałem dostępu do nich były specjalne strony internetowe, zwłaszcza w przypadku filmów (63%) i seriali telewizyjnych (59%). W przypadku muzyki najpopularniejszym kanałem dostępu do pirackich treści były aplikacje (39%), a w przypadku zdjęć – media społecznościowe (36%). Dostępność bardziej przystępnych cenowo, oryginalnych produktów/treści pochodzących z legalnych źródeł oraz ryzyko poniesienia kary pozostają głównymi czynnikami, które skłaniają młodych ludzi do rezygnacji z nielegalnych alternatyw.

Jednocześnie nowe opcje odpowiedzi dodane do badania z 2022 r. wskazują na inne czynniki, które mogą skłonić młodych ludzi do zmiany zachowania. Około połowa osób, które przyznały, że uzyskały dostęp do treści z nielegalnych źródeł stwierdziła, że mogłaby zaprzestać korzystania z nich, gdyby doświadczyła cyberzagrożeń (41%) lub cyberoszustw (40%), natomiast 24% osób stwierdziło, że mogłaby to zrobić, gdyby treści były niskiej jakości. Spośród osób, które nabyły podrobione produkty, około jedna trzecia (31%) stwierdziła, że zaprzestałaby tej

praktyki, gdyby zetknęła się z podróbką niskiej jakości, a około jedna czwarta stwierdziła, że zrobiłaby to, gdyby doświadczyła oszustwa internetowego (23%) lub cyberzagrożenia (21%), albo gdyby zetknęła się z niebezpiecznym produktem (22%). Podobny odsetek respondentów stwierdził, że lepsze zrozumienie negatywnego wpływu na środowisko (19%) lub społeczeństwo (17%) powstrzymałoby ich przed nabywaniem produktów podrobionych.



Wpływ sztucznej inteligencji na naruszenie i egzekwowanie praw własności intelektualnej

W ciągu ostatnich 50 lat świat był świadkiem przełomowych innowacji i rewolucyjnych zmian, które zmieniły gospodarkę, miejsca pracy, a nawet samo społeczeństwo, fundamentalnie zmieniając sposób, w jaki żyjemy, pracujemy i odnosimy się do siebie nawzajem. Sztuczna inteligencja i powiązane technologie należą do najważniejszych motorów zmian i mają wpływ na każdy obszar praw własności intelektualnej. Mogą być także, i stają się coraz częściej, narzędziem do analizowania naruszeń praw własności intelektualnej. Badanie Urzędu UE ds. Własności Intelektualnej (EUIPO)⁷ rzuca światło na to, w jaki sposób te technologie są wykorzystywane zarówno do ochrony wzorów przemysłowych i praw autorskich, jak i do ich naruszania. Jest też podróżą po różnych typach aplikacji SI, które wywierają istotny wpływ na własność intelektualną.

Zrozumienie implikacji tych przemian jest kluczowe w czasach, gdy Czwarta Rewolucja Przemysłowa (4IR) przekształca praktycznie każdą dziedzinę gospodarki i społeczeństwa. Obserwujemy

wynalazki i przełomy w dziedzinie transportu autonomicznego, biotechnologii, Internetu Rzeczy, inteligentnych urządzeń, sztucznej inteligencji, druku 3D, robotyki i obliczeń kwantowych. Wynalazki te wpływają między innymi na opiekę zdrowotną, transport, rolnictwo i organy ścigania, a tempo globalnych innowacji znacznie przyspieszyło w ciągu ostatniej dekady. Według niektórych szacunków w 2023 roku na świecie było około 29 miliardów połączonych urządzeń wykorzystujących technologie sztucznej inteligencji, a leżące u ich podstaw algorytmy stają się coraz bardziej centralne.

Z kolei, jak donoszą Europejskie Centrum ds. Cyberprzestępczości (EC3) Europolu, Agencja UE ds. Cyberbezpieczeństwa (ENISA) oraz Organizacja Narodów Zjednoczonych, rośnie liczba naruszeń praw własności intelektualnej poprzez złośliwe wykorzystanie różnych nowych technologii, w tym sztucznej inteligencji. W maju 2021 r. Rada UE uznała przestępczość związaną z naruszeniami własności intelektualnej za jeden z dziesięciu najważniejszych priorytetów w walce z przestępczością zorganizowaną na lata 2022-2025. Kwestia ta zostanie rozwiązana za pośrednictwem europejskiej, multidyscyplinarnej platformy przeciwko zagrożeniom przestępczym (EMPACT). Urząd Unii Europejskiej ds. Własności Intelektualnej, za pośrednictwem Europejskiego Obserwatorium Naruszeń Praw Własności Intelektualnej, będzie aktywnie zaangażowany we wspieranie realizacji tego priorytetu w ramach EMPACT. *W tej nowej erze bardzo ważne jest, abyśmy przyjęli „inteligentne” strategie intelektualne, zaś EUIPO, we współpracy ze swoją siecią partnerów i interesariuszy w zakresie własności intelektualnej, opracowuje narzędzia i promuje najlepsze praktyki. To badanie stanowi kolejny krok na drodze do stworzenia centrum doskonałości własności intelektualnej, w którym nowe technologie i sztuczna inteligencja działają w celu ochrony legalnych firm i obywateli, podkreślają władze EUIPO, pochylając się nad złożoną problematyką i wykonując właśnie pierwsze badanie w tym zakresie.*

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).

Na początku 2019 r. EUIPO powołało grupę ekspertów ds. wpływu technologii (Technology Expert Group, EG). W skład grupy wchodzi eksperci posiadający wiedzę i praktyczne doświadczenie w monitorowaniu wpływu nowych i powstających technologii na naruszanie i egzekwowanie praw własności intelektualnej.

W 2021 r. EUIPO zleciło Międzyregionalnemu Instytutowi Badań nad Przestępczością i Sprawiedliwością Organizacji Narodów Zjednoczonych (UNICRI) przeprowadzenie pierwszego dogłębnego projektu badawczego we współpracy z grupą ekspertów EUIPO.

Daje to pewien krajobraz przestępczości - coroczne strategiczne sprawozdanie z oceny zagrożenia przestępczością internetową (IOCTA), opracowywane przez Europejskie Centrum ds. Cyberprzestępczości (EC3) Europolu, zawiera przegląd pojawiających się zagrożeń i zmian w krajobrazie cyberprzestępczości. W 2020 r. zagrożeniami o najwyższym priorytecie były inżynieria społeczna, oprogramowanie ransomware i inne formy złośliwego oprogramowania. Analizując działalność przestępczą, należy wziąć pod uwagę wpływ elementu „cyber-” w cyberprzestępczości, ponieważ często ma on wpływ na prawie każdy aspekt tej działalności. W niedawnym raporcie IOCTA 2021 Europol wymienił programy partnerskie ransomware wykorzystujące ataki w łańcuchu dostaw w celu włamania się do sieci dużych korporacji i instytucji publicznych oraz wdrażania nowych wielowarstwowych metod wymuszeń, wielowarstwowych ataków mobilnego szkodliwego oprogramowania i blokady usługi (DDoS) dla okupu. Dlatego badanie EUIPO także analizuje i wyjaśnia, w jaki sposób te zagrożenia są również istotne w kontekście wzorów przemysłowych i praw autorskich.

Rozwój i ewolucję cyberprzestępczości należy również rozpatrywać w powiązaniu z niewłaściwym wykorzystywaniem sztucznej inteligencji, w tym z przestępstwami przeciwko własności intelektualnej wspomaganymi przez sztuczną inteligencję. Pojawiające się złośliwe wykorzystanie sztucznej inteligencji zdecydowanie zwiększa wpływ cyberprzestępczości, ponieważ jest w stanie udoskonalić ataki socjotechniczne na dużą skalę.

AI między innymi może być wykorzystywana:

- dla złośliwego oprogramowania pobierającego dokumenty w celu zwiększenia skuteczności ataków,
- aby uniknąć rozpoznawania obrazu i biometrii głosu,
- do tworzenia ataków ransomware z inteligentnym ukierunkowaniem, unikaniem i zanieczyszczeniem danych poprzez identyfikowanie martwych punktów w regułach wykrywania,
- ulepszenie możliwości blockchain w przestępczości internetowej.

Znaczenie uwzględnienia przestępstw związanych z własnością intelektualną również zostało uznane za priorytet w kontekście cyberbezpieczeństwa. W maju 2021 r. Rada Ministrów UE umieściła przestępczość w obszarze własności intelektualnej wśród dziesięciu najważniejszych priorytetów w walce z przestępczością zorganizowaną, które należy uwzględnić w latach 2022-2025. 26 maja 2021 r. Rada przyjęła konkluzje określające priorytety UE na lata 2022-2025 w walce z poważną i zorganizowaną przestępczością za pośrednictwem europejskiej, multidyscyplinarnej platformy przeciwko zagrożeniom przestępczym (EMPACT). Dlatego EUIPO postanowiło wykonać badanie oceny wpływu technologii sztucznej inteligencji zarówno na naruszanie, jak i egzekwowanie praw z rejestracji wzorów przemysłowych i praw autorskich.

Sztuczna inteligencja ma kilka możliwości poprawy skuteczności wykrywania naruszeń praw własności intelektualnej oraz ich egzekwowania, ponieważ może być wykorzystywana do wykonywania wielu różnych funkcji: od wyczuwania, rozumowania i działania, po ocenę, a nawet przewidywanie. Obecnie głównymi obszarami rozwoju sztucznej inteligencji są uczenie maszynowe, przetwarzanie języka naturalnego, wizja komputerowa, systemy eksperckie i wyjaśnialna sztuczna inteligencja. Wyjaśnialna sztuczna inteligencja cieszy się obecnie coraz większym zainteresowaniem ekspertów

i decydentów. Inne technologie wspierane przez sztuczną inteligencję, takie jak obliczenia kwantowe, blockchain, drukowanie 3D, projektowanie generatywne, usługi w chmurze i robotyka, również mają ogromny potencjał. Sztuczna inteligencja może identyfikować i ustalać priorytety zagrożeń, natychmiast wykrywać złośliwe oprogramowanie wsieci, kierować reagowaniem na incydenty wykrywać włamania, zanim one wystąpią. Na przykład uczenie maszynowe wyróżnia się jako kluczowa dziedzina sztucznej inteligencji, którą można wykorzystać do opracowania narzędzi organów ścigania, takich jak analiza dużych ilości informacji w celu wykrywania zagrożeń i identyfikowania botów socjotechnicznych, skanowanie obrazów w celu wykrywania fałszywych stron zawierających nielegalne treści, ulepszanie narzędzi do automatycznego rozpoznawania treści (ACR) i zapewnianie wglądu w celu znalezienia wzorców naruszeń.

Przetwarzanie języka naturalnego może służyć do analizowania i blokowania cyberataków, takich jak phishing, identyfikowania zachowań oszustów oraz tworzenia analizy korelacji mającej na celu szybką identyfikację naruszeń. Mowa komputerowa i widzenie komputerowe są również z powodzeniem wykorzystywane w tej dziedzinie. Niektóre z ich zastosowań obejmują rozpoznawanie wzorców w celu przewidywania przyszłych naruszeń, wykrywanie marketingu towarów naruszających prawa oraz wykrywanie i analizę fałszywych logo lub innych obrazów. Obliczenia kwantowe można zastosować w celu ulepszenia narzędzi sztucznej inteligencji, umożliwiając im przetwarzanie większych ilości danych. Na przykład sztuczna inteligencja i obliczenia kwantowe mogą być wykorzystywane przez organy celne i organy ścigania do rozpoznawania wzorców w dużych zbiorach danych i identyfikowania podobieństw. Z drugiej strony systemy eksperckie mogą być wykorzystywane przez organy ścigania do decydowania, która strategia jest bardziej odpowiednia do ochrony systemu przed określonymi słabymi punktami, w tym tymi związanymi z naruszeniem wzorów przemysłowych i praw autorskich.

Jeśli chodzi o sterowniki, możliwości sztucznej inteligencji sprawiają, że jest ona atrakcyjna dla

złośliwych aktorów. Sztuczna inteligencja może naśladować wiele czynności wykonywanych przez ludzi, a w niektórych przypadkach może przewyższać ludzkie możliwości pod względem wydajności i skalowalności. Co więcej, niektóre przestępstwa – przy wsparciu technologii AI – mogą być popełniane na znacznie większą skalę, atakując jednocześnie tysiące ofiar. Jak pokazuje metafora miecza obosiecznego, te same technologie mogą być wykorzystywane zarówno przez złośliwe podmioty, jak i do celów egzekwowania prawa, w tym w dziedzinie praw własności intelektualnej. Oszuści i grupy przestępcze wykorzystują lub mogą wykorzystywać te same techniki sztucznej inteligencji, których używają organy ścigania, aby przewyżczyć środki bezpieczeństwa cybernetycznego i uniknąć wykrycia. Jest to znane jako „zagadka sztucznej inteligencji / cyberbezpieczeństwa”: w miarę jak sztuczna inteligencja dojrzewa i jest coraz częściej wykorzystywana w dziedzinie cyberbezpieczeństwa, zwiększają się również potencjalne wady tego postępu technologicznego. Pod tym względem przeciwstawne uczenie maszynowe może pomóc wykryć i przewyżczyć środki bezpieczeństwa cybernetycznego, w tym przełamywanie zabezpieczeń i tworzenie dynamicznego złośliwego oprogramowania w celu uniknięcia wykrycia. Technologie sztucznej inteligencji mogą być wykorzystywane do zwiększania skuteczności takich ataków, jak w przypadku wspieranego przez sztuczną inteligencję odgadywania haseł i łamania CAPTCHA. Ponadto można zastosować narzędzia do przetwarzania języka naturalnego do tworzenia teledysków typu deepfake, a narzędzia oparte na projektowaniu generatywnym mogą być wykorzystywane do tworzenia kopii naruszających prawa autorskie.

Warto także pamiętać, że za każdym algorytmem sztucznej inteligencji i jego praktycznymi wektorami zastosowań zawsze stoi człowiek. Wyjaśnialna sztuczna inteligencja, choć nie rozwiązuje wszystkich możliwych problemów, mogłaby być wykorzystywana przez organy ścigania w ramach zwiększonego nasycenia innowacyjnych narzędzi – w tym AI – w analizie i prognozowaniu, przy jednoczesnym lepszym spełnieniu przesłanek rzetelności,

rozliczalności i przejrzystości. Wykorzystywanie sztucznej inteligencji przez organy ścigania i sądownictwo powinno zawsze podlegać silnym zabezpieczeniom i nadzorowi ze strony człowieka poprzez wbudowaną, ludzką kontrolę.

Obecne ograniczenia sztucznej inteligencji obejmują w szczególności jej zależność od dużej ilości wysokiej jakości danych treningowych, niemożność radzenia sobie z problemami długiego ogona (tj. dystrybucji danych), jej ograniczoną wszechstronność, zależności od konkretnych scenariuszy aplikacji oraz nieodłączne uprzedzenia twórcy sztucznej inteligencji. Bardziej wydajne algorytmy uczenia maszynowego mogą uczyć się złożonych nieliniowych relacji między danymi wejściowymi i wyjściowymi, ale zrobienie tego wymaga dużej ilości wysokiej jakości danych – tutaj pomocne stają się zasoby urzędów patentowych oraz systemy danych służb celnych.

Maszyny nadal muszą dokładniej rozumieć świat poprzez uczenie się percepcyjne i kognitywne, umożliwiając symulowanie rzeczywistych scenariuszy, aby postrzegać informacje, a następnie przekształcać te postrzegane informacje w abstrakcyjną wiedzę poprzez uwagę, pamięć i rozumienie. Można to osiągnąć poprzez skrzyżowanie, integrację i optymalizację algorytmu oraz ciągłe doskonalenie badań. Ponadto, pomimo szerszego wykorzystania innowacyjnych technologii w egzekwowaniu prawa, zgodnie z wywiadami przeprowadzonymi na potrzeby badania EUIPO, faktyczne wykorzystanie tych technologii przez władze publiczne do egzekwowania naruszeń wzorów przemysłowych i praw autorskich jest nadal niezaawansowane. Ponadto organy ścigania i organy celne będą musiały stale monitorować krajobraz nowych technologii, aby upewnić się, że są odpowiednio przygotowane i przeszkolone, by stanąć w szranki z nowymi możliwościami technologicznymi.

Podsumowując, w badania i rozwój sztucznej inteligencji, wraz z technologiami uczenia maszynowego, napływają ogromne inwestycje i przewiduje się, że trend ten utrzyma się

w ciągu najbliższych lat. W związku z tym można spodziewać się wzrostu dostępności i wykorzystania tych narzędzi i technologii, zarówno do celów legalnych, jak i nielegalnych. Szeroka gama narzędzi i technologii związanych ze sztuczną inteligencją jest obecnie lub potencjalnie wykorzystywana do projektowania i naruszania wzorów przemysłowych oraz egzekwowania prawa (badanie EUIPO przedstawia wiele interesujących casusów w tym zakresie). Istnieje zatem wyraźna potrzeba lepszego zrozumienia, większej świadomości i zwiększonych zdolności ze strony wszystkich zainteresowanych stron, w tym decydentów, podmiotów zajmujących się ochroną własności intelektualnej, przedsiębiorstw i organów ścigania.



Podsumowanie

Na koniec warto dodać i podkreślić, że w systemach ścigania i zwalczania naruszeń oraz piractwa, nie tylko konieczne jest zacieśnianie współpracy oraz postawienie na nowoczesne instrumenty technologiczne, których autorami są również polscy wynalazcy (jak cyfrowe znaki wodne dla treści online czy nanotechnologie, wykorzystujące kropki kwantowe do oznaczania legalnych towarów fizycznych), ale także koordynacja i współpraca z organizacjami międzynarodowymi. Niemniej, ważnym aspektem jest podjęcie szerokich działań informacyjnych i komunikacyjnych, adresowanych do adekwatnych grup społecznych, aby zyskały właściwą świadomość konsumencką i świadomość powiązanych ryzyk oraz zagrożeń. Ważną

grupą pozostaje młodzież i kształtowanie w niej odpowiedniej świadomości chronionej własności intelektualnej. Z pewnością przyczyni się do tego także tworzenie atrakcyjnej oferty towarów i usług, łatwo dostępnych, ale nienaruszających praw wyłącznych.

Sztuczna inteligencja, *blockchain* czy inne zaawansowane technologie są szansą dla organów ścigania, aby skuteczniej dostrzegać naruszenia własności intelektualnej. Problem podróbek zyskał nowy wymiar wraz z popularyzacją handlu internetowego. Temat zwalczania nielegalnego handlu podróbkami w sklepach online jest także poruszany na innych forach, w tym na forum Organizacji Współpracy Gospodarczej i Rozwoju (OECD). OECD utworzyła grupę zadaniową ds. zwalczania handlu podróbkami, a także rozpoczęła dyskusje na szczeblach rządowych w tym temacie.

Na koniec warto dodać, że w 2024 r. Urząd Patentowy RP rozpoczął serię spotkań z przedstawicielami OECD, Ministerstwa Finansów oraz Ministerstwa Rozwoju i Technologii. Dyskutujemy o przeciwdziałaniu nielegalnemu handlowi podróbkami na platformach internetowych i możliwościach współpracy w ramach administracji. Wspólnie możemy skuteczniej chronić własność intelektualną i uczciwy handel na rynkach internetowych. UPRP z chęcią przyłącza się do tego ważnego projektu i będzie aktywnie wspierać jego realizację.

Piotr Brylski
radca

Urząd Patentowy Rzeczypospolitej Polskiej

O wydawcy raportu

NASK jest państwowym instytutem badawczym, nadzorowanym przez Ministerstwo Cyfryzacji. Instytut prowadzi obecnie wielowymiarową działalność, operując na styku nauki, biznesu i administracji publicznej. Do głównych aktywności NASK-PIB należy zapewnienie bezpiecznego Internetu i ochrona jego użytkowników.

Na mocy ustawy o Krajowym Systemie Cyberbezpieczeństwa w strukturach Instytutu działa CSIRT NASK – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego – jeden z trzech zespołów CSIRT poziomu krajowego. W ramach swoich zadań przyjmuje, analizuje i podejmuje działania oraz koordynuje reakcje na incydenty dotyczące bezpieczeństwa cywilnej cyberprzestrzeni Polski zgłaszane przez operatorów usług kluczowych, dostawców usług cyfrowych, samorząd terytorialny i osoby prywatne oraz na incydenty związane z nielegalnymi treściami publikowanymi w Internecie i zagrażającymi bezpieczeństwu dzieci. Odpowiada także za monitorowanie zagrożeń internetowych i stanu cyberbezpieczeństwa na poziomie sektorowym i krajowym. NASK-PIB współtworzy ponadto zaplecze analityczne oraz badawczo-rozwojowe dla krajowego systemu cyberbezpieczeństwa.

Instytut prowadzi również działalność badawczo-rozwojową w zakresie opracowywania rozwiązań zwiększających efektywność, niezawodność i bezpieczeństwo sieci teleinformatycznych oraz innych złożonych systemów sieciowych. Tym, co wyróżnia nasz instytut badawczy od ściśle komercyjnych przedsiębiorstw jest podejście do tworzenia rozwiązań dla obecnych i przyszłych potrzeb klientów. W NASK-PIB badacze problem komercyjny ujmują w ramy nauki, by za pomocą jej narzędzi, nierzadko szerszych i bardziej abstrakcyjnych, dojść do wyników nie tylko satysfakcjonujących, ale również innowacyjnych. Główny nurt badań wyznacza cyberbezpieczeństwo, rozumiane jako wykrywanie, ostrzeganie, reagowanie na incydenty, pozyskiwanie, analiza, przetwarzanie i transfer danych, a także złożone systemy sieciowe, w tym systemy IoT oraz mobilne sieci ad hoc. Istotne miejsce zajmują badania dotyczące biometrycznych metod weryfikacji tożsamości w bezpieczeństwie usług.

NASK-PIB prowadzi także Rejestr nazw domeny .pl, a jako operator telekomunikacyjny oferuje innowacyjne rozwiązania teleinformatyczne dla klientów finansowych, biznesowych, administracji i nauki. Ważnym elementem działalności Instytutu jest też edukacja użytkowników oraz promowanie koncepcji społeczeństwa informacyjnego, głównie w celu ochrony dzieci i młodzieży przed zagrożeniami, związanymi z użytkowaniem nowych technologii. Instytut realizuje również projekty kluczowe dla cyfrowej transformacji kraju – Ogólnopolska Sieć Edukacyjna (OSE) oraz Elektroniczne Zarządzanie Dokumentacją (EZD RP).



Redakcja czasopisma

REDAKTORZY NACZELNI

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

SEKRETARZE REDAKCJI

dr Monika Nowikowska
Krystyna Cieniewska

kontakt@journaldot.pl

REDAKCJA RAPORTU

Alina Wiśniewska-Skura



NASK

NASK