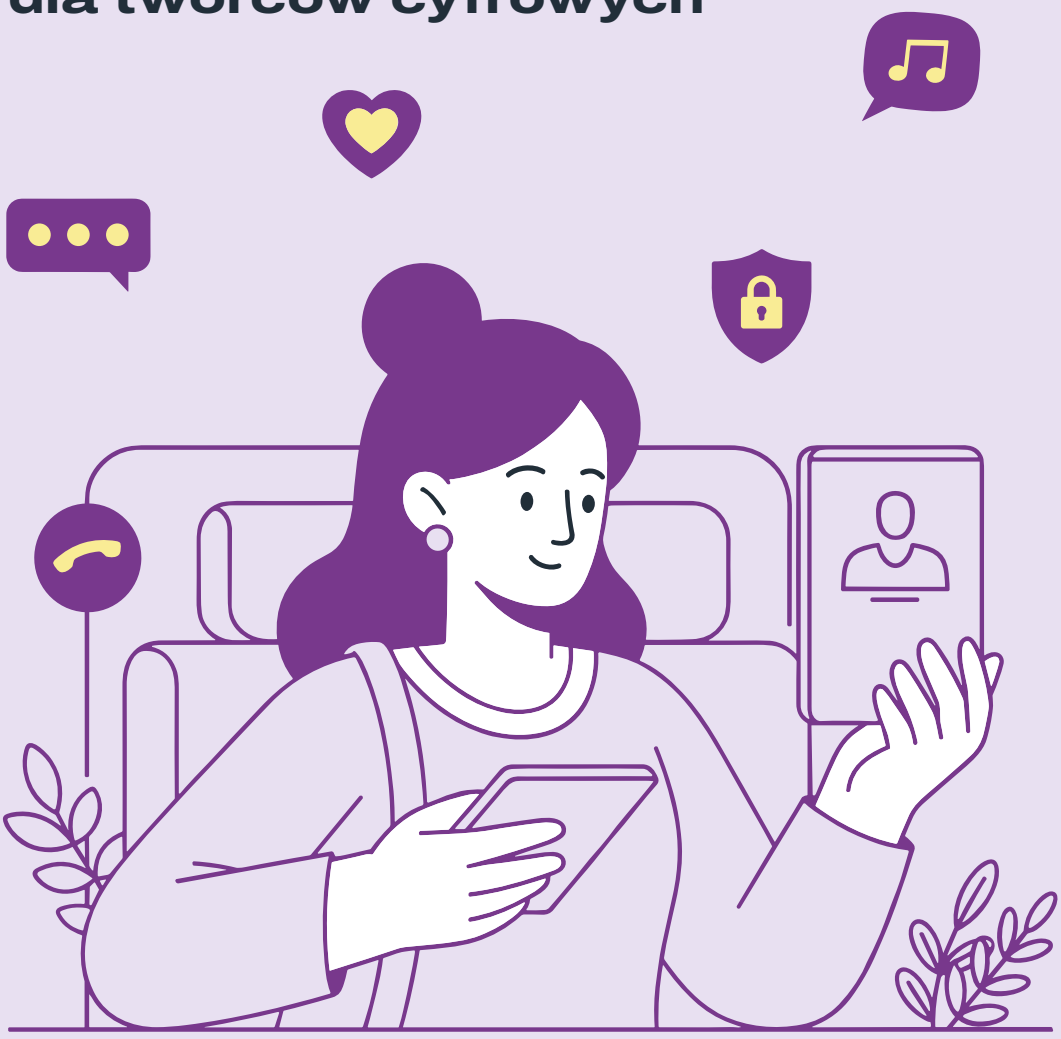
MASZ WPŁYW

Przewodnik po cyberbezpieczeństwie dla twórców cyfrowych



NASK

MASZ WPŁYW

Przewodnik po cyberbezpieczeństwie dla twórców cyfrowych

Autorzy
Sylwia Adamczyk
Ewelina Bartuzi-Trokielewicz
Oliwia Chojnacka
Monika Ciślak
Adrian Kordas
Anna Kwaśnik
Alicja Martinek
Anna Pudłowska
Agnieszka Wrońska
Paweł Zegarow
Olga Zabolewicz

NASK
Ministerstwo Cyfryzacji
PROJEKT FINANSOWANY ZE ŚRODKÓW MINISTERSTWA CYFRYZACJI

Tytuł
Masz wpływ. Przewodnik po cyberbezpieczeństwie dla twórców cyfrowych

Autorzy
Sylwia Adamczyk, Ewelina Bartuzi-Trokielewicz, Oliwia Chojnacka, Monika Ciślak, Adrian Kordas, Anna Kwaśnik, Alicja Martinek, Anna Pudłowska, Agnieszka Wrońska, Paweł Zegarow, Olga Zabolewicz

Redakcja
Anna Kwaśnik

Wsparcie merytoryczne
Karol Bojke, Iwona Prószyńska, Ewelina Włodarczyk

Poradnik uzupełniono o głosy twórców cyfrowych i influencerów
Janina Bąk, Karolina Czak, Wojciech Kardyś, Małgorzata Rozenek-Majdan

Opracowanie graficzne
Marcin Ślusarczyk

Redakcja językowa i korekta
Katarzyna Nakonieczna, Łukasz Szczęsny

ISBN: 978-83-68356-58-8

2026

NASK – Państwowy Instytut Badawczy
ul. Kolska 12, 01-045 Warszawa
www.nask.pl

SPIS TREŚCI

WSTĘP

Współczesny twórca czy twórczyni cyfrowa nie tylko tworzy treści, ale także aktywnie uczestniczy i współtworzy środowisko informacyjne, w którym codziennie funkcjonują tysiące odbiorczyń i odbiorców. Media społecznościowe stały się przestrzenią wpływu, inspiracji i dialogu, ale również miejscem, w którym szczególnego znaczenia nabiera odpowiedzialność za bezpieczeństwo własne oraz innych. Cyberbezpieczeństwo nie jest dziś wyłącznie zagadnieniem technicznym. To kompetencja społeczna, element etyki komunikacji i świadomego budowania zaufania w sieci.

Influencerzy i influencerki odgrywają wyjątkową rolę w kształtowaniu postaw swoich społeczności. Mogą wzmacniać dobre praktyki, reagować na dezinformację, chronić swoją i cudzą prywatność oraz promować odpowiedzialne korzystanie z nowych technologii, w tym narzędzi opartych na sztucznej inteligencji. Ich działania mają realny wpływ na to, jak użytkownicy i użytkowniczki rozumieją zagrożenia cyfrowe i jak sobie z nimi radzą.

Ten poradnik powstał jako wsparcie w świadomym i bezpiecznym funkcjonowaniu w środowisku online. Publikację rozpoczyna omówienie roli i odpowiedzialności twórców i twórczyń w mediach społecznościowych. Następnie przedstawione są zagadnienie równowagi między prywatnością a wizerunkiem, wskazujące, jak świadomie decydować o tym, co i w jakim zakresie udostępniać publicznie, aby chronić siebie i swoich bliskich. Kolejna część, poświęcona dezinformacji i manipulacjom, pokazuje, jak można wzmacniać swoją odporność na fałszywe treści, unikać

nieświadomego ich rozpowszechniania oraz budować wiarygodność w oczach odbiorców. Istotnym elementem poradnika są również zagadnienia dotyczące bezpieczeństwa kont i danych, obejmujące praktyczne wskazówki związane z ochroną tożsamości cyfrowej, zarządzaniem dostępami i reagowaniem na incydenty bezpieczeństwa. Szczególne miejsce zajmuje temat wizerunku dziecka w sieci (zjawiska sharentingu), który dotyczy publikowania treści z udziałem najmłodszych, z uwzględnieniem ich prawa do prywatności i bezpieczeństwa. Rozwinięciem zagadnień związanych z ochroną tożsamości jest rozdział poświęcony deepfake'om i kradzieży wizerunku, wyjaśniający mechanizmy tych zjawisk oraz sposoby ograniczania związanego z nimi ryzyka. W poradniku nie mogło zabraknąć także części dotyczącej wykorzystania sztucznej inteligencji w działalności twórczej – omówiony został zarówno potencjał wsparcia dla influencerów i influencerek, jak i potencjalne zagrożenia prawne, etyczne i wizerunkowe wynikające z używania narzędzi AI. Całość uzupełnia praktyczna mapka wskazująca instytucje, organizacje i miejsca, w których można zgłaszać incydenty oraz uzyskać wsparcie w obliczu zagrożeń bezpieczeństwa cyfrowego.

Mamy nadzieję, że publikacja ta stanie się nie tylko źródłem wiedzy, lecz także inspiracją dla cyfrowych autorów i autorek do budowania bezpieczniejszej, bardziej świadomej i odpowiedzialnej przestrzeni online. Wspólnie z odbiorcami i odbiorczyniami i dla nich,

bo, Ty Cyfrowy Twórco / Cyfrowa Twórczyni, „Masz wpływ"...

ROLA I ODPOWIEDZIALNOŚĆ TWÓRCÓW W MEDIACH SPOŁECZNOŚCIOWYCH

Monika Ciślak

RELACJA TWÓRCA–ODBIORCA JAKO RELACJA ASYMETRYCZNA

Ilu ludzi na świecie korzysta z internetu i mediów społecznościowych? Na czym polega zasada 90–9–1? Ilu polskich twórców i twórczyń funkcjonuje w internecie? Dlaczego influencerzy i influencerki powinni działać odpowiedzialnie?

O tym przeczytasz w tym rozdziale.

Według danych z *Digital 2026 Global Overview Report*[1], opublikowanego przez We Are Social i Meltwater, w październiku 2025 roku globalna społeczność internetu przekroczyła już rozmiar 6,04 miliarda osób (co oznacza wzrost o 294 mln względem poprzedniego roku). To znaczy, że 73,2% ludzi na świecie ma dostęp do sieci.

Co ciekawe, dla znacznej większości internautek i internautów obecność w sieci oznacza także aktywność na platformach społecznościowych: aż 68,7% globalnej populacji z nich korzysta, co przekłada się na 5,66 miliarda użytkowników i użytkowniczek. Globalnie największym zainteresowaniem cieszą się: YouTube, WhatsApp, Instagram i Facebook.

Ponad 73% ludności świata ma dostep do internetu, a prawie 69% korzysta z SoMe

Jak na tym tle wygląda Polska?

Na koniec 2025 roku aż **34,1 miliona Polaków i Polek miało dostęp do sieci – to aż 89,8% populacji naszego kraju**[2].

Popularność mediów społecznościowych w Polsce przewyższa średni globalny poziom – w naszym kraju mieszka 27,1 mln użytkowników i użytkowniczek (71,3% populacji). Najpopularniejsze platformy to YouTube, Facebook oraz TikTok, który w 2025 roku wyprzedził Instagrama, choć obie aplikacje wciąż cieszą zbliżonym zainteresowaniem[3]. Warto jednak pamiętać, że wyjęta

1 We Are Social, Meltwater. (2025). *Digital 2026 Global Overview*. https://datareportal.com/reports/digital-2026-global-overview-report [dostęp: 30.03.2026 r.]

2 Tamże.

3 Tamże.

z kontekstu liczba użytkowników i użytkowniczek nie zawsze odzwierciedla rzeczywiste preferencje korzystania z platform.

Według raportu *Polacy w social mediach 2026* IAB Polska osoby ankietowane poproszone o oznaczenia platformy, z której najchętniej korzystają, wskazywały portale YouTube, Facebook i Instagram[4].

TABELA 1. **Popularność platform społecznościowych w różnych grupach wiekowych**

Oznacz platformy społecznościowe, z których lubisz korzystać. Udział odpowiedzi dla poszczególnych platform, udzielonych przez respondentów z grup wiekowych 18-24 lata, 35-44 lata oraz 60+.

	18-24 lata		35-44 lata		60+ lat	
	Liczba odpowiedzi (n)	%	Liczba odpowiedzi (n)	%	Liczba odpowiedzi (n)	%
Facebook	16,8%	3,25	3,21	3,29	2,97	3,32
Instagram	42,7%	3,15	3,09	3,23	2,80	3,25
LinkedIn	17,7%	3,10	3,08	3,19	2,71	3,20
Pinterest	9,1%	3,10	3,04	3,08	2,96	3,12
Snapchat	46,4%	3,07	3,00	3,15	2,71	3,16
Threads	12,6%	3,07	3,05	3,07	2,85	3,08
TikTok	67,0%	3,06	2,98	3,15	2,67	3,16
Twitter/X	67,6%	3,05	2,96	3,16	2,66	3,15
YouTube	49,1%	3,03	2,90	3,17	2,63	3,15
Żadna z powyższych	9,1%	3,03	2,96	3,14	2,63	3,11

Źródło: Grupa Robocza Social Media IAB Polska. 2026. *Polacy w social mediach.*

To, jak korzystamy z social mediów, zależy od wielu czynników, m.in. wieku, płci czy technicznych aspektów samej platformy. Jedno jest jednak pewne: social media są napędzane przez stosunkowo niewielką grupę aktywnych twórców i twórczyń, podczas gdy ogromna większość użytkowników i użytkowniczek funkcjonuje jako konsumenci treści.

4 Grupa Robocza Social Media IAB Polska. (2026). *Polacy w social mediach*. https://www.iab.org.pl/baza-wiedzy/typ-dokumentu/raport/raport-polacy-w-social-mediach/ [dostęp 30.03. 2026 r.]

Na początku lat 90. powstała zasada 90–9–1[5], która pokazuje nierówność zaangażowania internautów i internautek:

- **90%** – bierni odbiorcy i odbiorczynie, którzy jedynie przeglądają treści,
- **9%** – użytkownicy i użytkowniczki sporadycznie reagujący (np. zostawiają lajki i komentarze),
- **1%** – aktywni twórcy i twórczynie regularnie publikujący treści.

Obserwacja ta pozostaje aktualna – tylko niewielka część użytkowników i użytkowniczek realnie tworzy internet. Na początku 2026 roku Krajowa Rada Radiofonii i Telewizji oszacowała[6], że w Polsce działa około **800 000** influencerów i influencerek **≈ 2,35%** wszystkich użytkowników i użytkowniczek internetu.
Oznacza to, że relatywnie mała grupa twórców i twórczyń ma realny wpływ na opinie, gusta i decyzje milionów odbiorców i odbiorczyń.

WPŁYW NA DECYZJE ZAKUPOWE I SPOŁECZNE

Aby lepiej zrozumieć, dlaczego działalność twórców i twórczyń cyfrowych ma tak duże znaczenie, trzeba przyjrzeć się bliżej temu, dlaczego Polki i Polacy sięgają po social media.

Dlaczego Polki i Polacy korzystają z social mediów?

Polacy i Polki korzystają z mediów społecznościowych głównie dla rozrywki, w celu zdobywania informacji, kontaktu z innymi oraz dla zabicia czasu. Jak wynika z przytaczanego badania IAB Polska[7], ponad połowa użytkowniczek i użytkowników trafia tam również na rekomendacje produktów i usług. Działalność twórców i twórczyń cyfrowych odpowiada na większość z tych potrzeb – influencerzy i influencerki dostarczają rozrywki i wiedzy, a także budują u swojej publiczności poczucie bliskości i pozwalają jej oderwać się od codzienności.

---

5 Nielsen, J. (2006). *The 90-9-1 Rule for Participation Inequality in Social Media and Online Communities*. https://www.nngroup.com/articles/participation-inequality/ [dostęp: 03.04.2026 r.]

6 Krajowa Rada Radiofonii i Telewizji. (2026). I*nfluencerzy – odpowiedzialność w blasku zasięgów*. https://www.gov.pl/web/krrit/odpowiedzialnosc-transparentnosc-wiarygodnosc--nowy-informator-krrit-dla-influencerow [dostęp: 30.03.2026 r.]

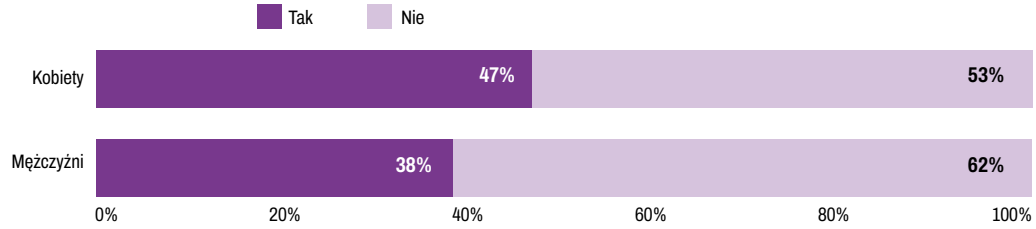
7 Grupa Robocza Social Media IAB Polska. (2026). *Polacy w social mediach.*

JAK POLKI I POLACY KONSUMUJĄ TREŚCI?

Blisko 42% internautów i internautek przyznaje, że śledzi działalność influencerów i infuencerek, przy czym kobiety taką deklaracje składały znacznie częściej.

WYKRES 1.

Czy śledzisz influencerów w mediach społecznościowych?
Próba: osoby korzystające z mediów społecznościowych w celach prywatnych i/lub zawodowych (*n* = 987 osób).

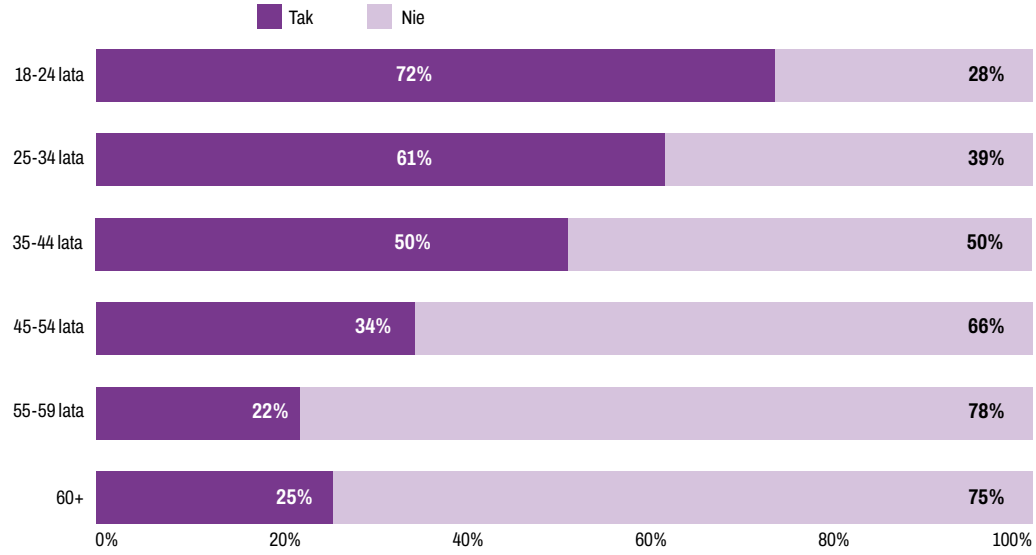


Grupa Robocza Social Media IAB Polska. (2026). *Polacy w social mediach.*

Różnica w podejściu do twórców i twórczyń cyfrowych jest skorelowana nie tylko z płcią, ale także z wiekiem.

WYKRES 2.

Czy śledzisz influencerów w mediach społecznościowych?
Próba: osoby korzystające z mediów społecznościowych w celach prywatnych i/lub zawodowych (*n* = 987 osób).



Grupa Robocza Social Media IAB Polska. (2026). *Polacy w social mediach.*

Działaniami internetowych twórców i twórczyń najbardziej zainteresowani są młodzi użytkownicy i użytkowniczki sieci: aż 72% osób w wieku 18–24 lata deklaruje, że śledzi influencerów i influencerki w mediach społecznościowych.

Choć *influencer marketing* dynamicznie się rozwija i przynosi wymierne korzyści zarówno markom, jak i twórcom oraz twórczyniom, deklarowane zaufanie do influencerów i infuencerek spada. Zgodnie z 5. edycją badania *Ranking prestiżu zawodów i specjalności SW Research*[8], influencerzy i YouTuberzy znaleźli się wśród najmniej szanowanych zawodów w Polsce. Jako główne przyczyny wskazywane są m.in. nadmierna autopromocja, tworzenie kontrowersyjnych lub dezinformujących treści, brak autentyczności oraz oderwanie od problemów codziennego życia odbiorców i odbiorczyń.

TABELA 2. **10 najgorzej ocenianych zawodów.**
(CAWI, 22–23.04.2025, *n* = 1000)

Zawód / funkcja	% odpowiedzi	Pozycja w rankingu 2025	Pozycja w rankingu 2024	Zmiana względem 2024
Influencer	13,6	1	1	0
Youtuber	13,8	2	2	0
Poseł na Sejm RP	21,7	3	4	-1 ↓
Europoseł*	22,2	4	–	–
Radny gminny	24,9	5	7	-3 ↓
Rekruter / HR-owiec	25,5	6	5	0
Pracownik infolinii / call-center	26,4	7	8	-2 ↓
Trener biznesu / coach	26,5	8	6	1 ↑
Senator RP**	26,7	9	–	–
Minister	27,6	10	10	-2 ↓

* Suma odpowiedzi „dużym" i „bardzo dużym" w odpowiedzi na pytanie: „Jakim poważaniem darzysz osoby o poniższym zawodzie / funkcji?"
** Po raz pierwszy w zestawieniu.

Źródło: SW Reseach. (2025). Ranking prestiżu zawodów i specjalności.

Wpływ twórców i twórczyń na decyzje internautek i internautów jest złożony – choć Polki i Polacy deklarują ograniczone zaufanie do influencerów i influencerek jako grupy, aż 40% konsumentów przyznaje, że dokonało zakupu pod wpływem ich rekomendacji[9].

8 SW Reseach. (2025). Ranking prestiżu zawodów i specjalności. https://swresearch.pl/ranking-zawodow [dostęp: 30.03.2026 r.]

9 Tamże.

Skuteczność influencerów i influencerek można wyjaśnić m.in. poprzez model AIDA (*attention* – uwaga, *interest* – zainteresowanie, *desire* – pragnienie, *action* – działanie), który opisuje kolejne etapy procesu zakupowego. Twórcy i twórczynie działający online przyciągają uwagę odbiorców i odbiorczyń, budują zainteresowanie produktem, wzmacniają jego atrakcyjność, a ostatecznie mogą skłaniać do podjęcia decyzji zakupowej.

Z perspektywy psychologii decyzji konsumenckich ich wpływ rośnie szczególnie tam, gdzie kluczową rolę odgrywają emocje, a nie wyłącznie racjonalne argumenty.

ODPOWIEDZIALNOŚĆ ZA REKOMENDACJE

Można wskazać 5 kluczowych obszarów odpowiedzialnego działania w mediach społecznościowych:

TABELA 3. **Pięć kluczowych obszarów odpowiedzialnego działania w social mediach.**

1. Transparentne oznaczanie współpracy **Należy oznaczać wszystkie formy współpracy (płatne, barterowe, prezenty, linki afiliacyjne, autopromocję) w sposób jednoznaczny i widoczny (np. #reklama, #współpraca).**	**2. Odpowiedzialność za treści i opinie** **Publikowane materiały powinny być rzetelne i nie mogą wprowadzać w błąd.** **Szczególną ostrożność należy zachować przy promowaniu produktów regulowanych (np. alkohol, leki, hazard).**
3. Legalność działalności **Działalność o charakterze zarobkowym wiąże się z obowiązkiem jej formalizacji oraz rozliczania podatków.**	**4. Ochrona małoletnich i etyka** **Treści kierowane do dzieci wymagają szczególnej odpowiedzialności.** **Nie należy bezpośrednio nakłaniać do zakupu ani stosować ukrytych form reklamy.**
5. Ochrona wizerunku i danych (RODO) **Należy respektować prawa autorskie, dobra osobiste oraz wizerunek innych osób.** **Działania związane z przetwarzaniem danych (np. do newsletteru) powinny być zgodne z obowiązującymi przepisami.**	

Źródło: Opracowanie własne.

Korzyści z odpowiedzialnego działania

Przestrzeganie powyższych zasad niesie ze sobą konkretne korzyści:

- zwiększa wiarygodność u potencjalnych reklamodawców,
- buduje zaufanie odbiorców i odbiorczyń,
- zapewnia dodatkową ochronę prawną (np. możliwość zgłoszenia sprawy do KRRiT lub UKE).

Warto wiedzieć

W relacjach z odbiorcami i odbiorczyniami często pojawiają się prośby o pomoc w sprawach osobistych. W takich sytuacjach należy zachować szczególną ostrożność i nie udzielać porad wykraczających poza własne kompetencje, zwłaszcza w obszarze zdrowia fizycznego i psychicznego.

W razie wątpliwości najlepiej skierować odbiorcę/odbiorczynię do odpowiednich specjalistów lub instytucji pomocowych.

Lista kontaktów i numerów wsparcia znajduje się na końcu poradnika.

W pigułce

- Media społecznościowe są dziś podstawowym środowiskiem komunikacji – korzysta z nich ponad **2/3 populacji świata**.
- Większość użytkowników i użytkowniczek internetu **nie tworzy treści**, lecz je tylko konsumuje – aktywni twórcy i twórczynie stanowią bardzo niewielki procent.
- Grupą najbardziej zainteresowaną influencerami i influencerkami są osoby **w wieku 18–24 lata (72%)**.
- Mimo dużego wpływu na odbiorców i odbiorczynie, **prestiż zawodu influencera w Polsce jest niski**.
- Odpowiedzialne działania twórców i twórczyń zwiększają **wiarygodność, bezpieczeństwo i zaufanie odbiorców i odbiorczyń**.

MIĘDZY PRYWATNOŚCIĄ A WIZERUNKIEM – JAK ŚWIADOMIE BUDOWAĆ OBECNOŚĆ W SIECI

Paweł Zegarow

Ile swojego życia warto pokazywać w social mediach i czy autentyczność w sieci pomaga?
Gdzie kończy się „bycie sobą", a zaczyna oversharing?
Jakie ryzyka wizerunkowe, prawne i biznesowe niesie nieprzemyślana publikacja?
Jak reagować na krytykę w internecie?
Prawo do bycia zapomnianym to gwarancja czy obietnica?

O tym przeczytasz w tym rozdziale.

Współczesna komunikacja w mediach społecznościowych opiera się na paradoksie. To, co zawodowe, coraz częściej wymaga elementów prywatności, by budować zaufanie, a to, co prywatne, musi być zarządzane w sposób profesjonalny, by nie zaszkodzić reputacji.

Profesjonalizm nie oznacza już dystansu, lecz autentyczność opartą na wartościach, doświadczeniach i osobowości. Platformy zawodowe, takie jak LinkedIn, przestały pełnić wyłącznie funkcję cyfrowych wizytówek, a konta prywatne (np. na Instagramie) coraz częściej wspierają działalność zawodową i budowanie wizerunku.

W praktyce granica między sferą prywatną a zawodową uległa zatarciu. Dzielenie się wybranymi elementami życia może wzmacniać wiarygodność, jednak istnieje cienka granica między autentycznością a działaniem na szkodę własnego wizerunku. Nadmierne ujawnianie prywatności (*oversharing*) może okazać się nieprofesjonalne oraz prowadzić do chaosu komunikacyjnego.

Udostępnianie fragmentów życia prywatnego w celu budowania wizerunku zawodowego wiąże się także z dodatkowym ryzykiem. Pojęcie relacji parasocjalnej, opisane przez D. Hortona i R. Wohla[10], odnosi się do jednostronnych więzi, jakie widownia tworzy z postaciami medialnymi. Zjawisko to jest widoczne również w mediach społecznościowych – dzielenie się prywatnością może tworzyć iluzję bliskości, przez co odbiorcy i odbiorczynie zaczynają postrzegać twórcę/twórczynię jak kogoś znajomego lub bliskiego.

10 Horton, D., Wohl, R. (1956). Mass Communication and Para-Social Interaction: Observations on Intimacy at a Distance. *Psychiatry, 19*(3), 215–229.

Prywatność jako proces

Prywatność w sieci nie jest stanem stałym, lecz procesem wymagającym świadomego zarządzania. Ograniczona widoczność treści nie gwarantuje ich poufności – mogą one zostać upublicznione i trafić do szerokiego grona odbiorców. W konsekwencji każda publikacja powinna być tworzona z założeniem, że może stać się publiczna.

Ryzyko techniczne (metadane i kontekst)

Odpowiedzialność obejmuje również kwestie techniczne. Pliki graficzne zawierają metadane, które mogą ujawniać m.in. lokalizację, dlatego nawet pozornie neutralne zdjęcie może zdradzić szczegóły życia prywatnego. Choć część platform usuwa wybrane metadane automatycznie, nie jest to standard ani gwarancja bezpieczeństwa. Dlatego warto samodzielnie dbać o ich usuwanie oraz kontrolować elementy widoczne w tle publikowanych materiałów.

W praktyce oznacza to świadomy wybór publikowanych treści – **nie wszystkie elementy życia prywatnego powinny trafiać do przestrzeni publicznej.**

PAMIĘĆ INTERNETU I MIT ZNIKAJĄCYCH TREŚCI

Media społecznościowe mogą sprawiać wrażenie ulotnej przestrzeni, jednak publikowane treści mają charakter trwały. Usunięcie wpisu nie oznacza jego zniknięcia – może on nadal funkcjonować w archiwach, pamięci podręcznej wyszukiwarek czy w formie zrzutów ekranu wykonanych przez osoby trzecie. Treści mogą być kopiowane, udostępniane i reinterpretowane, często bez pierwotnego kontekstu. W praktyce oznacza to, że nawet usunięta publikacja może nadal funkcjonować w obiegu i wpływać na czyjś wizerunek.

Dostępność narzędzi analitycznych sprawia, że śledzenie aktywności w internecie nie jest zarezerwowana wyłącznie dla specjalistów i specjalistek. Nawet podstawowa znajomość metod takich jak OSINT, czyli tzw. biały wywiad, pozwala na odtworzenie historii działań danej osoby w sieci.

OSINT (*open-source intelligence*) to zbieranie informacji z ogólnodostępnych źródeł. Publikowane w internecie treści tworzą cyfrowy ślad, który z czasem zaczyna układać się w spójny obraz. Nie chodzi o pojedynczy post czy zdjęcie. Znaczenie ma to, co powstaje z wielu drobnych elementów zestawionych razem.

Treści archiwalne mogą być także oceniane według zmieniających się norm społecznych, co stanowi dodatkowe ryzyko w długiej perspektywie.

Prawo do bycia zapomnianym

Warto pamiętać, że mechanizmy usuwania treści mają ograniczoną skuteczność. Nawet skorzystanie z prawa do bycia zapomnianym nie gwarantuje całkowitego usunięcia informacji z internetu – pozwala jedynie ograniczyć ich widoczność, np. w wynikach wyszukiwania.

W tym celu można skorzystać z formularza Google:

https://support.google.com/websearch/contact/content_removal_form?hl=pl

KONSEKWENCJE WIZERUNKOWE, PRAWNE I BIZNESOWE PUBLIKACJI

W dobie szybkiego przepływu informacji błędy w obszarze autoprezentacji mogą realnie zagrozić nie tylko reputacji, ale też stabilności zawodowej. Skutki kryzysu wizerunkowego mogą wykraczać poza falę negatywnych komentarzy i mieć długofalowy wpływ na wizerunek i sytuację zawodową oraz wiązać się z odpowiedzialnością prawną.

Konsekwencje wizerunkowe

- trwała zmiana postrzegania twórcy/twórczyni przez odbiorców i odbiorczynie, media i partnerów biznesowych,
- ocenianie przede wszystkim przez pryzmat kryzysu, a nie kompetencji,
- utrata zaufania odbiorców i odbiorczyń oraz osłabienie relacji ze społecznością,
- wytworzenie długotrwałych skojarzeń z konkretnym zdarzeniem lub skandalem.

Konsekwencje biznesowe

- spadek atrakcyjności dla reklamodawców i partnerów biznesowych,
- wycofywanie się marek z dotychczasowych form współpracy i realizowanych kampanii,
- zrywanie umów oraz utrata źródeł dochodu,
- ograniczenie możliwości nawiązywania nowych współprac
- konieczność przebudowy lub redefinicji marki osobistej.

Konsekwencje prawne

- sprawy o naruszenie dóbr osobistych (np. publikacja nieprawdziwych treści o innych osobach),
- odpowiedzialność za zniesławienie lub znieważenie,
- następstwa naruszenia praw autorskich,
- reperkusje wynikające z niewywiązywania się z umów,
- możliwość uznania aktywności w sieci za naruszenie obowiązków służbowych,
- konieczność usunięcia treści, publikacji przeprosin, a także zapłaty odszkodowania lub zadośćuczynienia.

Konsekwencje te mogą mieć charakter długotrwały i wykraczać poza moment publikacji, wpływając na sytuację zawodową, finansową i reputację.

Budowanie marki osobistej w internecie wymaga konsekwencji i długoterminowego podejścia. Wizerunek online jest sumą wszystkich działań, a nie pojedynczych publikacji. Kluczowe znaczenie mają spójność komunikacji, autentyczność oraz zgodność treści z deklarowanymi wartościami.

Zasady świadomej obecności w sieci zostały zebrane w praktycznej checkliście na końcu tej części.

JANINA BĄK

Oversharing i brak granic

NASK: **Obecność w sieci i pokazywanie w niej swojego życia to bycie pod ciągłą presją i poddawanie się ocenie innych. Jaką jedną radę dałabyś początkującym influencerom/influencerkom i twórcom/twórczyniom cyfrowym, która pomogłaby im w zachowaniu dobrostanu psychicznego?**

J. Bąk: Zanim zaczniesz publikować, świadomie zdecyduj, ile swojego życia chcesz pokazać – i ile życia swoich bliskich. Osobiście rekomenduję nie ujawniać zbyt wielu szczegółów o miejscu zamieszkania, dzieciach czy codziennych miejscach pobytu. Nie wszyscy ludzie w sieci będą Ci życzliwi, a raz ujawniona informacja zostaje w sieci na zawsze.

Na co dzień pamiętaj, że Twoje profile to Twoja przestrzeń i masz prawo czuć się tam bezpiecznie – gdy ktoś Cię hejtuje, notorycznie pisze przykre komentarze lub po prostu narusza Twoje granice, to masz prawo takie komentarze skasować, a taką osobę zablokować. I warto to robić, bo najważniejsze to dbać o siebie, nie o samopoczucie kogoś, kto Ci źle życzy.

A jeśli bycie online zacznie Cię przytłaczać, pozwól sobie na dłuższą przerwę offline – tydzień, dwa, miesiąc. Wiem z doświadczenia, że ludzie o Tobie nie zapomną, a taka przerwa może pomóc Ci wrócić do równowagi, a następnie do swoich zajęć z nową energią.

Media społecznościowe promują treści silnie nacechowane emocjonalnie, co może prowadzić do przekraczania granic prywatności. Oversharing pojawia się wtedy, gdy publikowane treści są zbyt osobiste lub nieadekwatne do kontekstu.

Treści prywatne często generują duże zaangażowanie, co może prowadzić do presji ujawniania coraz większej części swojego życia. W efekcie osoba publikująca może być postrzegana przede wszystkim przez pryzmat życia prywatnego, a nie kompetencji.

Świadome zarządzanie prywatnością polega na selekcji treści i utrzymaniu kontroli nad tym, co trafia do przestrzeni publicznej.

Ryzykowne sytuacje

- publikowanie zbyt prywatnych informacji,
- dzielenie się szczegółami z życia innych osób,
- stopniowe zwiększanie zakresu ujawnianych treści pod wpływem reakcji odbiorców.

Konsekwencje

- szczegóły życia prywatnego zaczynają dominować w publicznym wizerunku nad kompetencjami,
- zmienia się sposób postrzegania twórcy/twórczyni pojawia się presja na dalsze ujawnianie życia prywatnego.

Jak reagować

- świadomie selekcjonować publikowane treści,
- wyznaczyć jasne granice prywatności i konsekwentnie ich przestrzegać,
- oddzielać elementy życia prywatnego od komunikacji zawodowej.

Zasada

Nie pokazuj wszystkiego – publikuj tylko te treści, za pomocą których chcesz świadomie wzmacniać swój wizerunek.

Wybieraj → Ograniczaj → Kontroluj

REAGOWANIE NA KRYTYKĘ I EMOCJE W SIECI

Media społecznościowe działają szybko, a emocje jeszcze szybciej. W takich warunkach impulsywne reakcje mogą prowadzić do błędów, które zostają utrwalone i wielokrotnie powielane.

Największe kryzysy wizerunkowe często wynikają nie z samej zaistniałej początkowo sytuacji, lecz z nietrafionej reakcji na nią. Pojedyncza emocjonalna odpowiedź może zostać rozpowszechniona szerzej niż wcześniejsza działalność i zdominować sposób postrzegania całego zajścia.

Odpowiedzialna komunikacja w sieci wymaga umiejętności kontrolowania emocji i świadomego odraczania reakcji. W praktyce to właśnie sposób odpowiedzi decyduje o tym, czy sytuacja stanie się kryzysem, czy elementem budowania wiarygodności.

Ryzykowne sytuacje

- odpowiadanie na krytykę „na gorąco”,
- wchodzenie w konflikty i polaryzujące dyskusje,
- impulsywne reagowanie na wiadomości lub zaczepki.

Konsekwencje

- emocjonalne treści mają największy potencjał rozpowszechniania,
- pojedyncza reakcja może diametralnie zmienić odbiór twórcy/twórczyni,
- nawet usunięte treści mogą nadal funkcjonować w obiegu.

Jak reagować

- odraczać reakcję i dać sobie czas na ocenę sytuacji,
- świadomie decydować, na które dyskusje warto odpowiadać,
- zachować spokojny i rzeczowy ton komunikacji.

Zasada

Nie reaguj impulsywnie – daj sobie czas i odpowiadaj dopiero wtedy, gdy masz kontrolę nad emocjami.

Zatrzymaj się → Przemyśl → Odpowiedz

Między intencją a konsekwencjami

W mediach społecznościowych łatwo założyć, że treść zostanie odebrana zgodnie z intencją autora lub autorki. W praktyce komunikaty są interpretowane przez odbiorców i odbiorczynie przez pryzmat ich emocji, doświadczeń i przekonań. To, co miało być żartem lub neutralnym komentarzem, może zostać odebrane jako nieodpowiednie lub kontrowersyjne.

Po publikacji kończy się kontrola nad przekazem – treść zaczyna funkcjonować samodzielnie, bywa wyrywana z kontekstu i reinterpretowana. Internauci i internautki, którzy konsumują dużą liczbę komunikatów, nie analizują intencji twórcy/twórczyni, lecz reagują na uproszczony, często emocjonalny obraz rzeczywistości. W efekcie znaczenie intencji maleje, a kluczowy staje się społeczny odbiór publikacji oraz jej konsekwencje.

Ryzykowne sytuacje

- przekonanie, że odbiorcy i odbiorczynie właściwie odczytają intencję,
- stosowanie ironii lub żartów bez jednoznacznego kontekstu,
- publikowanie treści na tematy wrażliwe lub polaryzujące.

Konsekwencje

- treści mogą funkcjonować poza pierwotnym kontekstem,
- odbiór zależy od emocji i doświadczeń odbiorców i odbiorczyń,
- znaczenie intencji ustępuje interpretacji i reakcji społecznej.

Jak reagować

- analizować komunikaty z perspektywy różnych odbiorców i odbiorczyń,
- unikać niejednoznacznych i łatwych do błędnej interpretacji treści,
- uwzględniać możliwe konsekwencje publikacji.

Zasada

Nie zakładaj, że Twoja intencja zostanie zrozumiana – zawsze bierz pod uwagę możliwy nieżyczliwy odbiór Twojej wypowiedzi.

Przemyśl → Uwzględnij → Odpowiadaj

Twórcy i twórczynie internetowe pełnią istotną rolę w kształtowaniu opinii, postaw oraz zachowań społecznych. Wielu użytkowników i użytkowniczek social mediów postrzega ich jako autorytety i wzory do naśladowania. Z tego powodu działalność influencerów i influencerek wykracza poza funkcję rozrywkową i wiąże się z realną odpowiedzialnością.

Warto podkreślić, że odpowiedzialność obejmuje także sposób zakończenia działalności w internecie. Twórca lub twórczyni powinni w transparentny sposób poinformować swoją społeczność o planowanym zaprzestaniu aktywności oraz z wyprzedzeniem komunikować sytuacje, które mogą wywołać dezorientację odbiorców i osłabić relację opartą na zaufaniu.

CHECKLISTA DOBRYCH PRAKTYK W KOMUNIKACJI CYFROWEJ

Jeśli zależy Ci na budowaniu spójnego, wiarygodnego i bezpiecznego wizerunku w sieci, potraktuj poniższą checklistę jako narzędzie do szybkiego sprawdzenia, czy Twoje działania są przemyślane i zgodne z Twoimi celami. Przed publikacją możesz sprawdzić z poszczególnymi punktami treść przekazu i upewnić się, że niczego nie pomijasz.

Emocje i komunikacja

- Nie publikujesz pod wpływem emocji.
- Świadomie decydujesz, na które komentarze i dyskusje reagujesz.
- Zachowujesz rzeczowy i spokojny ton komunikacji.
- Unikasz impulsywnych odpowiedzi i eskalowania konfliktów.

Bezpieczeństwo i prywatność

- Nie ujawniasz wrażliwych informacji (np. adres, dane prywatne).
- Kontrolujesz, co znajduje się w tle publikowanych materiałów.
- Dbasz o bezpieczeństwo cyfrowe i ustawienia prywatności.
- Świadomie zarządzasz granicą między życiem prywatnym a zawodowym.

Relacje i współprace

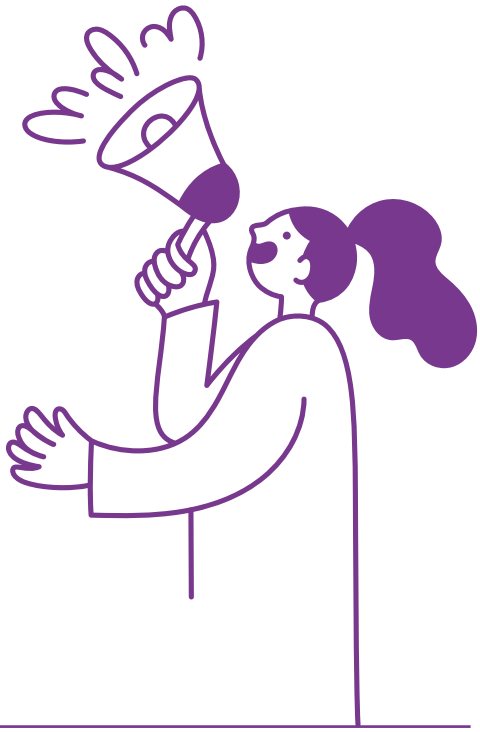
- Szanujesz prywatność innych osób.
- Uwzględniasz różnorodność odbiorców i odbiorczyń oraz możliwe interpretacje treści.
- Podejmujesz współprace zgodne z profilem i wartościami.
- Dbasz o transparentność działań i komunikacji.

Kontrola i refleksja

- Regularnie przeglądasz wcześniejsze publikacje.
- Oceniasz, czy starsze treści nadal są spójne z Twoim wizerunkiem.
- Wyciągasz wnioski z wcześniejszych działań i reakcji odbiorców.

Pytanie do refleksji

Zanim opublikujesz treść, zadaj sobie jedno kluczowe pytanie:
Czy ta publikacja wspiera mój wizerunek, czy może mu zaszkodzić?



W pigułce

- **Media społecznościowe rządzą się paradoksem**: profesjonalny wizerunek wymaga autentyczności, ale jednocześnie zmusza do coraz większej kontroli nad tym, ile prywatności pokazujemy światu.
- **Internet nie zapomina**, a raz opublikowane treści mogą mieć długofalowe konsekwencje prawne, biznesowe i emocjonalne. OSINT nie jest zarezerwowany wyłącznie dla specjalistów i specjalistek!
- Stosowanie prostych zasad: **wybieraj**, **ograniczaj i kontroluj publikowane treści**, pozwala budować spójny i bezpieczny wizerunek cyfrowy.
- **Oversharing może zwiększać widoczność i zaangażowanie odbiorców**, ale jednocześnie **prowadzi do utraty kontroli nad obecnością w sieci** i zwiększa ryzyko konsekwencji wizerunkowych, prawnych i osobistych.
- **Świadoma obecność w sieci wymaga stawiania granic**, kontroli emocji, refleksji przed publikacją oraz dbania o własne bezpieczeństwo i dobrostan psychiczny.
- **Twórczynie i twórcy cyfrowi często stają się dla odbiorców i odbiorczyń autorytetami i wzorami do naśladowania** oraz wpływają na ich opinie i postawy, dlatego powinni odpowiedzialnie prowadzić swoją działalność, także jasno informując o jej zakończeniu, aby nie naruszyć zaufania społeczności.

TWÓRCA CYFROWY W OBLICZU DEZINFORMACJI: ODPORNOŚĆ I ODPOWIEDZIALNOŚĆ

Sylwia Adamczyk

Dlaczego fałszywe informacje rozchodzą się szybciej niż fakty? Czym różni się dezinformacja od misinformacji? Co to jest cherry picking? Jaką rolę odgrywają boty, trolle i algorytmy? Jak influencerki i influencerzy są wykorzystywani w kampaniach wpływu? Czy umiesz rozpoznać dezinformację w praktyce?

O tym przeczytasz w tym rozdziale.

Współczesne platformy internetowe generują niekończące się strumienie treści – wpisy tekstowe, wideo, zdjęcia, podcasty czy artykuły – w tempie przekraczającym możliwości przyswojenia ich wszystkich naraz. W warunkach przeciążenia informacyjnego rośnie ryzyko kontaktu z treściami fałszywymi, a ich krytyczna analiza staje się coraz trudniejsza. Już w 2018 roku badania przeprowadzone na Massachusetts Institute of Technology[11] wykazały, że fałszywe wiadomości w mediach społecznościowych rozprzestrzeniają się szybciej niż prawdziwe. Fałsz potrzebował sześć razy mniej czasu na dotarcie do użytkowników i miał średnio 70% więcej szans na udostępnienie na ówczesnym Twitterze (dziś X), niż informacja prawdziwa. Tymczasem według *Reuters Institute Digital News Report 2025*[12], media społecznościowe są wykorzystywane do pozyskiwania wiadomości przez ponad połowę Polek i Polaków (54%). W tak dynamicznym środowisku informacyjnym influencerzy i influencerki, dysponując znacznym zasięgiem w internecie i wpływem na swoich odbiorców i odbiorczynie, powinni w szczególny sposób dbać o weryfikację publikowanych treści oraz własną odporność informacyjną.

Fałszywe informacje w mediach społecznościowych rozchodzą się nawet sześć razy szybciej i mają o dużo większe szanse na udostępnienie niż prawdziwe

11 Vosoughi, S., Roy, D., Aral, S. (2018). The spread of true and false news online. *Science, 359*(6380), 1146–1151. https://doi.org/10.1126/science.aap9559 [dostęp: 26.03.2026r.]

12 Reuters Institute. (2025). *Digital News Report 2025*. https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2025 [dostęp: 26.03.2026 r.]

JANINA BĄK

NASK: **Zajmujesz się nauką. W sieci nie brakuje dezinformacji, rozsiewanych mitów, teorii spiskowych. Czy social media, a zwłaszcza influencerzy/influencerki napędzają dezinformację?**

J. Bąk: Tak, social media mogą napędzać dezinformację, ale problem nie dotyczy wyłącznie influencerów/influencerek. W ostatnim czasie widzieliśmy fałszywe informacje rozpowszechniane także przez lekarzy, osoby z tytułami naukowymi czy ekspertów z pozoru godnych zaufania. To ważna lekcja: autorem dezinformacji może być właściwie każdy. Dlatego dziś nie wystarczy sprawdzać, kto mówi, ale również: na jakich źródłach opiera swoje tezy. Każdą sensacyjną wypowiedź warto weryfikować, sięgać do rzetelnych badań i nie wierzyć nikomu wyłącznie na słowo.

KLUCZOWE POJĘCIA I MECHANIZMY

Zanim jednak powiemy więcej o weryfikacji treści, warto najpierw uporządkować podstawowe definicje. Pozwoli to na lepsze zrozumienie złożoność zaburzeń w przestrzeni informacyjnej.

Dezinformacja to fałszywa bądź wprowadzająca w błąd treść, która jest tworzona lub rozpowszechniana celowo, z zamiarem oszukania odbiorców i odbiorczyń bądź pozyskania określonych korzyści: np. ekonomicznych czy politycznych. Choć to pojęcie spotykane jest w przestrzeni publicznej najczęściej, pełne zrozumienie zjawiska wymaga uwzględnienia także dwóch pozostałych kategorii zaburzeń, czyli misinformacji i malinformacji.

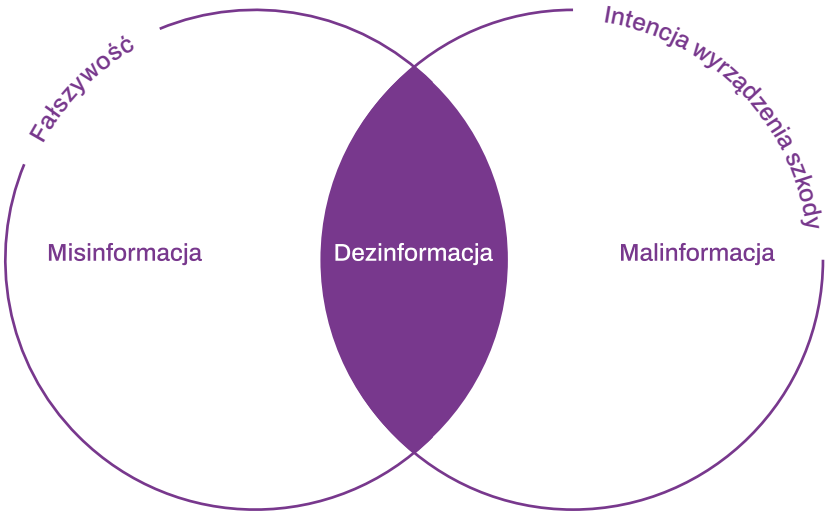
Misinformacja to fałszywa bądź wprowadzająca w błąd treść, która jest tworzona bądź rozpowszechniana bez złych zamiarów oraz bez świadomości jej nieprawdziwości – w wyniku pomyłki lub

błędnego przekonania na dany temat. Kluczową różnicą między dezinformacją i misinformacją jest intencja.

Malinformacja to z kolei rodzaj zakłócenia w sferze informacyjnej, w ramach którego wykorzystywane są prawdziwe treści, ale w złej intencji – z zamiarem wyrządzenia szkody. Może to być ujawnienie poufnych informacji czy publikowanie bądź rozpowszechnianie treści prywatnych i intymnych bez zgody osoby lub grupy, których dotyczą.

GRAFIKA

Schemat zaburzeń informacyjnych



Źródło: NASK na podst. C. Wardle, H. Derakhshan. (2017). *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making.*

Zjawiska te nie ograniczają się do polityki – obejmują także tematy zdrowia, klimatu, technologii, bezpieczeństwa i wiele innych obszarów. Mogą wywierać negatywny wpływ zarówno na całe społeczeństwa (np. w kontekście zdrowia publicznego czy procesów demokratycznych), jak i na jednostki podejmujące decyzje na podstawie fałszywych przesłanek.

Dezinformacja może pochodzić z różnych źródeł – od aktorów państwowych, przez grupy interesu, po zwykłych użytkowników internetu, a jej przekaz bywa dodatkowo wzmacniany przez boty i trolle.

Boty to zautomatyzowane konta naśladujące ludzkie zachowanie, wykorzystywane do masowego rozpowszechniania treści. Często działają w dużych grupach (w ramach tzw. farm botów), co umożliwia manipulowanie przekazem na szeroką skalę. Trolle to z kolei realni użytkownicy, którzy prowokują konflikty i zaburzają dyskusję – również mogą działać w zorganizowanych grupach.

Istotną rolę odgrywają także algorytmy platform, promujące treści angażujące i generujące reakcje. Materiały wywołujące silne emocje są częściej wzmacniane przez systemy rekomendacji, co sprzyja rozprzestrzenianiu się treści nieprawdziwych lub zmanipulowanych. Personalizacja przekazu prowadzi ponadto do powstawania baniek informacyjnych, ograniczających kontakt z odmiennymi perspektywami i zniekształcających obraz rzeczywistości.

INFLUENCERZY W KAMPANII WYBORCZEJ

Jednym z głośniejszych przykładów zaangażowania influencerów i influencerek w promowanie określonych narracji była kampania przed wyborami prezydenckimi w Rumunii. Pierwsza tura wyborów przyniosła niespodziewany sukces, znanego z prorosyjskich wypowiedzi, nacjonalistycznego kandydata Călina Georgescu, który zdobył 23% głosów. Jego popularność napędzana była głównie viralową kampanią na dużych platformach[13]. Na dwa tygodnie przed wyborami na TikToku uaktywniła się sieć 25 000 kont bezpośrednio powiązana z kampanią Georgescu[14].

Dużą rolę w całej operacji odegrała platforma Telegram. Zespół analityczny firmy Open Minds wykazał ścisłe powiązanie niemal jednej czwartej rumuńskojęzycznych kanałów na Telegramie z rosyjskimi mediami prokremlowskimi[15]. Choć Telegram nie jest

13 EDMO. (2025). *Electoral Disinformation Ecosystems in Romania and its Diaspora: Cross-Platform Dynamics and Strategic Narratives during the 2024–2025 Electoral Cycle.* https://edmo.eu/publications/electoral-disinformation-ecosystems-in-romania-and-its-diaspora-cross-platform-dynamics-and-strategic-narratives-during-the-2024-2025-electoral-cycle/ [dostęp: 30.03.2026 r.]

14 Președintele României. (4 grudnia 2024). https://www.presidency.ro/ro/media/comunicat-de-presa1733327193 [dostęp: 30.03.2026 r.]

15 Open Minds. (2025). *End of Democracy: How Pro-Russian Telegram Channels Influence Romanian Elections.* https://www.openminds.ltd/reports/end-of-democracy-how-pro-russian-telegram-channels-influence-romanian-elections [dostęp: 31.03.2026 r.]

najpopularniejszym komunikatorem w Rumunii, odegrał istotną rolę w mobilizowaniu wyborców i wyborczyń o radykalnych poglądach i stanowił punkt wyjścia dla kampanii prowadzonych na innych platformach. Rumuńskie służby wywiadowcze informowały, że kampania Georgescu na TikToku była koordynowana właśnie poprzez grupę na Telegramie[16].

Opłacani influencerzy i influencerki odegrali w kampanii Călina Georgescu rolę multiplikatorów przekazu, nadając jej pozór spontaniczności i organicznego poparcia. Treści polityczne były klasyfikowane przez TikToka jako rozrywkowe, co umożliwiało ich szeroką dystrybucję bez ograniczeń typowych dla przekazów politycznych. Część materiałów nie była oznaczana jako sponsorowana, co pozwalało ukrywać finansowanie. W efekcie influencerzy i influencerki stali się jednym z kluczowych narzędzi budowania widoczności kandydata wśród młodych odbiorców.

6 grudnia 2024 roku pierwsza tura wyborów została unieważniona przez rumuński Sąd Konstytucyjny. Sędziowie uznali, że Georgescu złamał zasadę równości szans, wykorzystując nieprzejrzyste technologie cyfrowe i sztuczną inteligencję. Sąd Konstytucyjny uznał ponadto, że kampanię Georgescu w internecie wspierał zewnętrzny aktor państwowy[17].

Angażowanie twórców i twórczyń internetowych w operacje dezinformacyjne nie ogranicza się do jednego kraju. Pod koniec 2024 roku dziennik Le Monde, powołując się na źródła wywiadowcze, ujawnił, że Rosja kontaktowała się z ponad dwoma tysiącami europejskich twórców i twórczyń, oferując udział w kampaniach wpływu. Propozycje zaakceptowało 20 influencerek i/lub influencerów. Nie wiadomo jednak, na ile świadomie[18].

16 Euronews.com. (2025). *Dezinformacja zagraża wyborom w Rumunii.* https://pl.euronews.com/europa/2025/05/15/rumunia-zmaga-sie-z-dezinformacja-przed-wyborami-prezydenckimi [dostęp: 31.03.2026 r.]

17 Całus, K. (2025). Rumunia: nowe wybory prezydenckie bez Georgescu. *Ośrodek Studiów Wschodnich*. https://www.osw.waw.pl/pl/publikacje/analizy/2025-03-18/rumunia-nowe-wybory-prezydenckie-bez-georgescu

18 Fundacja Instytut Cyberbezpieczeństwa. (2025). *Rosjanie werbują influencerów w USA, Francji i Rumunii. Czas na Polskę?* https://instytutcyber.pl/aktualnosci/rosjanie-werbuja-influencerow-w-usa-francji-i-rumunii-czas-na-polske/ [dostęp: 01.04.2026 r.]

Twórcy i twórczynie internetowe powinni zachować szczególną ostrożność wobec propozycji współpracy pochodzących od nieznanych podmiotów, zwłaszcza gdy dotyczą one tematów politycznych lub społecznych. Warto dokładnie weryfikować, kto stoi za ofertą, sprawdzać historię firmy lub osoby oraz zachować czujność wobec nietypowych propozycji.

ROZPOZNAWANIE DEZINFORMACJI WŚRÓD INFLUENCERÓW I INFLUENCEREK

Według badania przeprowadzonego wśród influencerów i influencerek przez UNESCO[19], sprawdzanie faktów nie jest normą w ramach ich cyfrowej aktywności. 62% respondentów w ogóle nie przeprowadzało weryfikacji informacji przed ich publikacją. Inni mieli trudności z określeniem właściwych kryteriów oceny wiarygodności treści znalezionych w internecie. Największy odsetek badanych – blisko 42% – wskazywał, że głównym wskaźnikiem wiarygodności jest dla nich „liczba polubień i udostępnień", jakie zdobył dany post. To nie jest dobre kryterium weryfikacji informacji.

POPULARNOŚĆ
lajki
udostępnienia
komentarze

≠

~~WIARYGODNOŚĆ~~
~~rzetelne źródło~~
~~fakty~~
~~weryfikacja~~

Warto zwrócić uwagę na psychologiczny **mechanizm społecznego dowodu słuszności, za sprawą którego** odbiorcy i odbiorczynie uznają treść za wiarygodną, jeśli widzą, że inni ją popierają lub masowo udostępniają. W operacjach dezinformacyjnych efekt ten bywa wzmacniany, np. poprzez wykorzystanie botów.

Weryfikując informacje, nie należy opierać się na liczbie reakcji. Kluczowe jest sprawdzenie autora/autorki, aktualności treści oraz potwierdzenie informacji w różnych, wiarygodnych źródłach. Istotna jest również znajomość metod manipulacji stosowanych w dezinformacji.

19 UNESCO. (2024). *Behind The Screens Behind The Screens Insights from Digital Content Creators Understanding their Intentions, Practices and Challenges.* https://unesdoc.unesco.org/ark:/48223/pf0000392006 [dostęp: 31.03.2026 r.]

Wybrane metody manipulacji

- **Podszywanie się,** czyli używanie logotypu lub wizerunku osoby czy organizacji w celu wykorzystania ich wiarygodności do szerzenia szkodliwych informacji.
- **Cherry picking,** czyli wybiórcze wykorzystywanie danych jako dowodów na potwierdzenie określonej tezy, przy jednoczesnym ignorowaniu pozostałych faktów, które przeczyłyby temu twierdzeniu.
- **Manipulowanie danymi,** czyli wyciąganie z nich fałszywych wniosków, ich niepoprawna interpretacja lub pozbawianie kontekstu w celu wprowadzenia w błąd.
- **Fałszywe powiązanie,** czyli sugerowanie pozornych zależności między informacjami w rzeczywistości niezwiązanymi ze sobą w celu wprowadzenia odbiorcy/odbiorczyni w błąd poprzez wywołanie wrażenia, że dwa zjawiska są od siebie zależne.
- **Dowód anegdotyczny,** czyli argument opierający się na osobistych doświadczeniach lub pojedynczych przykładach, niepoparty badaniami lub danymi statystycznymi. Prowadzi do błędnych wniosków, zakładając przeniesienie indywidualnego doświadczenia na ogólny trend.
- **Teoria spiskowa,** czyli alternatywne wyjaśnienie jakiegoś zdarzenia, zakładające istotny udział spiskującej grupy próbującej zataić prawdę przed opinią publiczną.

W przekazach dezinformacyjnych często wykorzystywane są materiały generowane lub zmanipulowane przy użyciu sztucznej inteligencji – tzw. deepfake **(zob. str. 60).** Ze względu na dynamiczny rozwój technologii, mogą być one coraz trudniejsze do rozpoznania gołym okiem.

Dlatego każdy przekaz warto oceniać krytycznie – zastanowić się, czy przedstawione wydarzenia są wiarygodne, spójne i możliwe w rzeczywistości.

W 2026 roku dezinformacja i misinformacja znalazły się po raz kolejny w czołówce globalnych zagrożeń w perspektywie krótkoterminowej w rankingu czynników ryzyka Światowego Forum

Ekonomicznego *Global Risks Report 2026*[20]. Zjawiska te stanowią zagrożenie, którego nie należy ignorować. Zachowanie przejrzystości i budowanie własnej odporności informacyjnej powinny być dla twórców i twórczyń cyfrowych kluczowymi elementami funkcjonowania w infosferze.

Treści o charakterze dezinformacyjnym można zgłaszać do Ośrodka Analizy Dezinformacji NASK przez formularz dostępny pod adresem **www.zglos-dezinformacje.nask.pl**.

JAK ROZPOZNAĆ DEZINFORMACJĘ? PRAKTYCZNE PORADY

5 zasad

1. **Myśl krytycznie**
   Zastanów się, czy dana informacja jest spójna i logiczna i czy sytuacja, której dotyczy, jest możliwa w rzeczywistości.

2. **Nie ufaj popularności**
   Liczba polubień, komentarzy i udostępnień nie świadczy o prawdziwości treści.

3. **Sprawdzaj źródło**
   Zwróć uwagę na autora/autorkę i oceń jego/jej wiarygodność oraz kompetencje w danym obszarze.

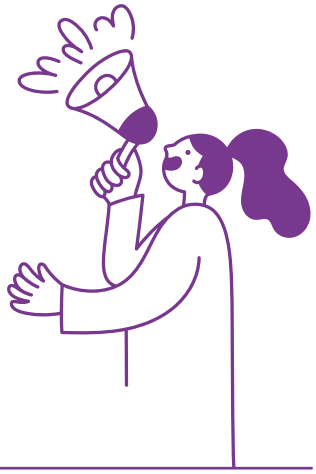
4. **Weryfikuj informacje**
   Potwierdzaj treści w kilku niezależnych i rzetelnych źródłach, w tym w oficjalnych komunikatach i raportach.

5. **Zwracaj uwagę na emocje**
   Jeśli treść wywołuje silne emocje, zastanów się, czy nie jest zaprojektowana tak, aby wpłynąć na Twoją reakcję.

20 World Economic Forum. (2026). *Global Risks Report 2026*. https://www.weforum.org/publications/global-risks-report-2026/ [dostęp: 01.04.2026 r.]

Pytanie do refleksji

Co zrobisz następnym razem, zanim udostępnisz treść, która wywołuje silne emocje?



W pigułce

- Fałszywe treści mogą być rozpowszechniane celowo (**dezinformacja**), lub nieświadomie (misinformacja). Możliwe jest też użycie prawdziwych informacji w szkodliwym kontekście (**malinformacja**).
- Dezinformację może tworzyć każdy, dlatego warto sprawdzać źródła, a nie tylko autora/autorkę wpisu.
- Dezinformacja wykorzystuje **różne techniki manipulacji**, np. wybieranie tylko wygodnych faktów (cherry picking), podszywanie się pod wiarygodne źródła czy fałszywe powiązania. Coraz większym wyzwaniem są też materiały tworzone przez sztuczną inteligencję, np. deepfake.
- **Algorytmy, boty i trolle zwiększają zasięg manipulacyjnych treści, a liczba lajków i udostępnień nie świadczy o ich wiarygodności.**
- Influencerzy i influencerki, ze względu na swój wpływ, powinni szczególnie uważnie weryfikować publikowane materiały.
- Budowanie odporności informacyjnej polega na **krytycznym myśleniu, sprawdzaniu faktów i świadomym reagowaniu na treści w sieci**.

BEZPIECZEŃSTWO KONT I DANYCH – SPOKOJNA GŁOWA W CYFROWYM ŚWIECIE

Anna Kwaśnik

Dlaczego konto twórcy jest atrakcyjne dla cyberprzestępców? Jak zabezpieczyć swoje konto? Silne hasło – czyli jakie? W jaki sposób przejmowane są konta? Na czym polega socjotechnika? Czy odzyskanie przejętego konta jest możliwe. Jak można to zrobić? Co zawiera codzienna checklista bezpieczeństwa?

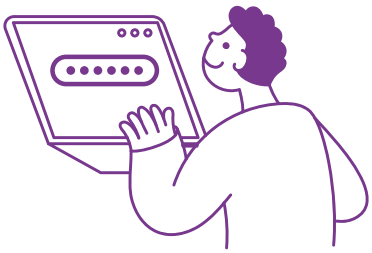
O tym przeczytasz w tym rozdziale.

DLACZEGO OCHRONA KONT JEST TAK WAŻNA

Konto w mediach społecznościowych to dla twórców i twórczyń nie tylko przestrzeń ekspresji, ale i narzędzie pracy oraz realna wartość biznesowa. Utrata dostępu oznacza przerwane kampanie, zerwanie kontaktu z odbiorcami i odbiorczyniami, spadek wiarygodności i często straty finansowe. To nie jest teoretyczne ryzyko.

Z podobnymi incydentami mierzyli się zarówno twórcy w Polsce, jak i na świecie – m.in. MrBeast, którego konto zostało przejęte i wykorzystane do publikowania nieautoryzowanych treści oraz promowania oszustw kryptowalutowych[21].

Co ważne – odzyskanie konta bywa trudne, czasochłonne, a czasem wręcz niemożliwe. Zdarzają się sytuacje, w których nawet platforma nie jest w stanie przywrócić dostępu (np. po dłuższym czasie od usunięcia konta). Dlatego bezpieczeństwo nie jest dodatkiem, lecz podstawowym elementem pracy w mediach społecznościowych.



21 BBC News. (2023). *MrBeast's X account hacked to promote crypto scam.* https://www.bbc.com/news/technology-66850821 [dostęp: 01.04.2026 r.]

SKALA PROBLEMU – DANE, KTÓRE WARTO ZNAĆ

W 2025 roku przejęto ponad 429 mln kont w mediach społecznościowych, a co trzeci użytkownik doświadczył incydentu bezpieczeństwa

Naruszenia bezpieczeństwa kont nie są już niszowym problemem – ich skala jest realna i rośnie wraz z popularnością twórców i twórczyń internetowych. Według badań wykorzystanie skradzionych danych logowania lub ich małej siły jest jednym z najczęstszych wektorów naruszeń bezpieczeństwa[22].

Skala problemu pokazuje, że przejęcia kont nie stanowią pojedynczych incydentów, ale są powszechnym zjawiskiem. Szacuje się, że w 2025 roku przejętych zostało ponad 429 milionów kont w mediach społecznościowych, a aż co trzeci użytkownik lub użytkowniczka doświadczył incydentu bezpieczeństwa. W wielu przypadkach skutki są poważne – około 70% osób traci całkowicie dostęp do swojego konta, a proces jego odzyskiwania trwa średnio ponad dwa tygodnie. Co więcej, w 73% przypadków złamanie zabezpieczeń jednego konta prowadzi do przejęcia kolejnych, powiązanych usług[23].

Co istotne, twórcy i twórczynie internetowe są szczególnie atrakcyjnym celem, ponieważ:

- mają zaangażowaną społeczność,
- działają w oparciu o zaufanie,
- ich konta mają realną wartość finansową.

To sprawia, że przejęcie nawet jednego konta influencera lub influencerki może być dla atakujących znacznie bardziej opłacalne niż atak na zwykłego użytkownika/użytkowniczkę.

22 Verizon. (2025). *Data Breach Investigations Report*. https://www.verizon.com/business/resources/reports/dbir/ [dostęp: 01.04.2026 r.]

23 StationX. (2026). *Social Media Hacking Statistics*. https://app.stationx.net/articles/social-media-hacking-statistics [dostęp: 01.04.2026 r.]

WOJTEK KARDYŚ

NASK: **Czy w Twojej ocenie twórcy i twórczynie cyfrowe – jako osoby, które cały czas są obecne w sieci – są świadomi cyberzagrożeń?**

W. Kardyś: Ze względu na dużą aktywność w social mediach (i co za tym idzie, spore zasięgi) influencerzy stają się łatwym celem dla oszustów. Czasem wystarczy jedna fałszywa propozycja współpracy i ktoś może przejąć ich konto. Co, zresztą, dzieje się nagminnie. Jasne, coraz więcej osób pamięta o logowaniu dwuetapowym, ale wciąż wielu macha ręką na zasady bezpieczeństwa, bo liczy się tylko to, żeby wrzucić post na czas czy żeby nagrać pod trend rolkę. Influencerzy dopiero wtedy dowiadują się o cyberbezpieczeństwie, kiedy jest już za późno, czyli kiedy ich konto np. znika. Najwyższy czas, żebyśmy zaczęli uczyć się podstaw cyberbezpieczeństwa i ochrony swojej tożsamości w social mediach. W końcu to po prostu element bycia profesjonalistą!

JAK KONTA SĄ PRZEJMOWANE (I DLACZEGO TO TAKIE PROSTE)

W praktyce przejęcie konta rzadko przypomina sceny znane z filmów. Zazwyczaj nie polega na zaawansowanym hakowaniu, lecz na wykorzystaniu pośpiechu, emocji i odpowiednio przygotowanej treści, z którą ofiara zostaje nieoczekiwanie skonfrontowana. Taka „przynęta" może dotrzeć do osoby, której konto ma zostać przejęte, różnymi kanałami – jako e-mail, wiadomość w komunikatorze, powiadomienie z aplikacji czy link osadzony w reklamie albo w nagłówku posta lub artykułu. Często zdaje się być interesującą treścią, a kliknięcie w nią przekierowuje na inną, spreparowaną przez sprawców stronę. Nierzadko takie fałszywe witryny są przygotowane w bardzo wiarygodny sposób i na pierwszy rzut oka nie wzbudzają podejrzeń – w praktyce mają jednak na celu wyłudzenie danych logowania lub innych poufnych informacji od użytkownika/użytkowniczki.

Przykładowe scenariusze ataku:

- propozycja współpracy z linkiem do panelu kampanii,
- pilna informacja o rzekomym naruszeniu zasad, wymagająca natychmiastowego działania,
- fałszywa strona logowania łudząco podobna do oryginalnej.

Błędy i zaniedbania zwiększające ryzyko:

- używanie tego samego hasła w wielu miejscach,
- brak skonfigurowanego uwierzytelniania dwuskładnikowego (2FA),
- źle zabezpieczone powiązane konta – na przykład e-mail, który pozwala na reset uprawnień do konta w mediach społecznościowych,
- pozostawiony dostęp dla byłej współpracowniczki lub współpracownika po zakończeniu współpracy.

Podobne mechanizmy wykorzystywano m.in. w próbach przejęcia kont takich twórczyń jak Charli D'Amelio, gdzie ataki opierały się głównie na phishingu[24].

JAK TO WYGLĄDA W PRAKTYCE – CASE STUDY

W 2023 roku doszło do głośnego przejęcia konta MrBeast na platformie X (dawniej Twitter)[25]. Atak nie polegał na włamywaniu się do systemu, ale na przejęciu dostępu do konta poprzez socjotechnikę lub wyciek danych logowania. Po uzyskaniu dostępu osoba atakująca:

- opublikowała posty promujące fałszywe okazje do zdobycia kryptowalut (akcje typu giveaway),
- wykorzystała zaufanie społeczności odbiorców i odbiorczyń twórcy,
- próbowała skłonić odbiorców i odbiorczynie do otwierania szkodliwych linków i przekazania środków.

24 Forbes. (2023). *Hackers target influencers with phishing campaigns*. https://www.forbes.com/sites/johnkoetsier/2023/09/21/hackers-target-influencers [dostęp: 01.04.2026 r.]

25 BBC News. (2023). *MrBeast's X account hacked to promote crypto scam.* https://www.bbc.com/news/technology-66850821 [dostęp: 01.04.2026 r.]

W praktyce oznaczało to, że:

- konto zaczęło działać przeciwko własnej społeczności,
- wiarygodność twórcy została chwilowo podważona,
- odbiorcy i odbiorczynie byli realnie narażeni na straty finansowe.

Podobne historie opisywały również polskie twórczynie, m.in. Waleria Szewczyk[26] oraz Karolina Zientek[27], które publicznie pokazywały proces odzyskiwania kont i trudności z kontaktem z platformą.

Podczas prób odzyskania konta okazało się, że:

- kody potwierdzające trafiały już do osoby, która przejęła konto,
- standardowe metody resetu hasła nie działały,
- konieczna była dodatkowa weryfikacja tożsamości (np. nagranie wideo).

Co ważne – nawet wtedy odzyskanie nie było natychmiastowe i wymagało kilku prób oraz cierpliwości.

To pokazuje bardzo jasno: kiedy konto zostanie przejęte, sytuacja szybko wymyka się spod kontroli.

BEZPIECZEŃSTWO KONTA W PRAKTYCE: HASŁA, WERYFIKACJA DWUETAPOWA, DOSTĘPY I UPRAWNIENIA

Hasła – pierwsza linia dostępu

Hasło to pierwsza linia ochrony, ale też jeden z najważniejszych punktów ryzyka. W codziennej pracy warto przyjąć kilka zasad:

- każde konto powinno mieć inne hasło,
- hasło nie powinno być oczywiste ani powiązane z nazwą profilu, danymi osobowymi czy łatwo dostępnymi informacjami

26 Pomponik. (10 lipca 2021). *Waleria Szewczyk szczegółowo o kradzieży Instagrama!* Youtube. https://www.youtube.com/watch?v=-8STTdaoN4E [dostęp: 01.04.2026 r.]

27 Karolina Zientek. (22 listopada 2021). *O dwóch takich co ukradli mi Instagrama.* YouTube. https://www.youtube.com/watch?v=xpMBAvGvW0Q

(np. miejscem zamieszkania, datą urodzenia czy imieniem zwierzęcia), nie należy przekazywać haseł w wiadomościach ani mailach,

- dostęp dla osób z zespołu powinien być nadawany przez wewnętrzne narzędzia platform, nie poprzez podawanie im danych logowania.

Im mniej osób zna dane logowania, tym większe bezpieczeństwo.

Silne hasło – czyli jakie?

Silne hasło to takie, które trudno odgadnąć, ale łatwo zapamiętać. Najlepiej sprawdzają się:

- hasła o długości co najmniej 14 znaków,
- długie frazy (np. całe zdania),
- nieoczywiste połączenia słów,
- unikalne kombinacje dla każdego konta.

Weryfikacja dwuetapowa (2FA) – dodatkowa warstwa bezpieczeństwa

Weryfikacja dwuetapowa to jedno z najprostszych i najskuteczniejszych zabezpieczeń. Działa w dwóch krokach:

- wpisanie hasła,
- potwierdzenie logowania dodatkowym składnikiem (np. z kodem z aplikacji, SMS-em lub biometrią).

Nawet jeśli hasło zostanie wykradzione, konto nadal pozostaje chronione. To absolutna podstawa bezpieczeństwa.

Narzędzia wspierające bezpieczeństwo – co warto rozważyć

- **Menedżery haseł** to narzędzia, które bezpiecznie przechowują i automatycznie uzupełniają hasła, umożliwiając tworzenie silnych i unikalnych danych logowania. Menedżer haseł dodatkowo zwiększa bezpieczeństwo, ponieważ automatycznie uzupełnia dane logowania tylko na właściwych, zapisanych wcześniej stronach. Jeśli użytkownik trafi na fałszywą stronę (np. phishingową), menedżer haseł zazwyczaj nie wypełni danych logowania, co może być sygnałem ostrzegawczym.

- **Klucze U2F** (sprzętowe klucze bezpieczeństwa) to fizyczne urządzenia, które służą do potwierdzania logowania. Działają jako dodatkowy składnik uwierzytelniania – po wpisaniu hasła użytkownik musi podłączyć klucz (np. przez złącze USB lub czytnik NFC) i potwierdzić logowanie. Są jednym z najbezpieczniejszych rozwiązań, ponieważ nie da się ich łatwo przechwycić ani wykorzystać zdalnie, a dodatkowo chronią przed phishingiem.

Podział ról w zespole – porządek, który chroni

W pracy zespołowej wokół marki osobistej bezpieczeństwo zaczyna się od jasnych zasad. Warto określić:

- kto publikuje treści,
- kto odpowiada za ustawienia i bezpieczeństwo,
- kto ma dostęp do danych wrażliwych.

Dobre praktyki obejmują:

- różne poziomy dostępu,
- jedna osoba zarządzająca dostępami,
- szybkie odbieranie dostępów po zakończeniu współpracy.

SPRZĘT PRYWATNY I ZAWODOWY – JAK TO WYGLĄDA W PRAKTYCE

Rozdzielenie sprzętu prywatnego i zawodowego to jedno z prostszych działań zwiększających bezpieczeństwo. W przypadku twórców i twórczyń cyfrowych nie zawsze oznacza to jednak korzystanie z dwóch oddzielnych urządzeń – w praktyce większość działań odbywa się na jednym telefonie, laptopie lub tablecie. Dlatego kluczowe znaczenie ma nie samo posiadanie osobnego sprzętu, lecz świadome zarządzanie dostępem do kont.

Dlaczego to ma znaczenie?

- Ogranicza liczbę przypadkowych logowań w pośpiechu lub w niepewnym środowisku.
- Ułatwia kontrolę nad tym, gdzie i na jakich urządzeniach konto jest aktywne.
- Zmniejsza ryzyko sytuacji, w których dostęp do konta uzyskuje ktoś niepowołany.

W codziennej pracy oznacza to przede wszystkim większą uważność, czyli przede wszystkim:

- logowanie się tylko na zaufanych urządzeniach,
- unikanie korzystania z kont zawodowych na pożyczonym sprzęcie,
- kontrolowanie aktywnych sesji i miejsc logowania,
- oddzielanie – na ile to możliwe – działań prywatnych od zawodowych (np. poprzez różne konta czy profile).

Dodatkowo w przypadku utraty sprzętu dobrze uporządkowane logowania i dostępy znacząco zwiększają szansę na szybkie zabezpieczenie kont. Nie chodzi więc o idealne rozdzielenie sprzętu, ale o świadome korzystanie z urządzenia, które dla twórców i twórczyń jest centrum całej działalności.

GDY KONTO ZOSTAJE PRZEJĘTE – CO ZROBIĆ?

W przypadku przejęcia konta kluczowa jest szybka reakcja:

- próba wylogowania nieznanych aktywnych sesji (jeśli wciąż mamy dostęp),
- próba resetu hasła,
- zgłoszenie problemu do platformy,
- zabezpieczenie maila i innych kont,
- poinformowanie społeczności.

Warto jednak podkreślić: nawet szybka reakcja nie daje gwarancji odzyskania konta.

JAK ODZYSKAĆ KONTO?

Procedury odzyskiwania kont na platformach mogą się różnić, ale ich schemat jest podobny: weryfikacja tożsamości, odzyskanie dostępu i zabezpieczenie konta. Warto jednak pamiętać, że nie zawsze kończy się to sukcesem – dlatego kluczowe jest szybkie działanie.

Różnice pojawiają się w szczegółach – czyli w tym, jak wygląda weryfikacja i jakie narzędzia oferuje dana platforma.

W przypadku **Facebooka i Instagrama** proces odzyskiwania dostępu jest dość rozbudowany – może obejmować weryfikację tożsamości na podstawie zdjęcia, wcześniejszych aktywności czy kontaktów. W niektórych sytuacjach pomocne może być także zgłoszenie przejętego konta przez znajomych, co pozwala szybciej zareagować i ograniczyć jego dalsze wykorzystanie.

Jeśli nie ma dostępu do przypisanego adresu e-mail, warto skorzystać z alternatywnych metod odzyskiwania konta – np. numeru telefonu, wcześniej używanych urządzeń lub formularzy wsparcia dostępnych na platformie.

TikTok stawia przede wszystkim na szybkie działanie – zmianę hasła, usunięcie nieznanych urządzeń i zgłoszenie problemu, aby jak najszybciej ograniczyć dostęp osób trzecich.

YouTube, jako część systemu Google, korzysta z bardziej zaawansowanych zabezpieczeń – weryfikacja może obejmować kody, rozpoznanie urządzenia czy analizę historii logowania.

Z kolei **LinkedIn,** jako platforma zawodowa, często wymaga dodatkowej weryfikacji – na przykład potwierdzenia tożsamości przez e-mail, a w niektórych przypadkach także dokumentami.

Najważniejsze jest jednak to, że niezależnie od platformy jedna zasada pozostaje niezmienna: im szybsza reakcja, tym większa szansa na odzyskanie konta i ograniczenie strat.

Odzyskiwanie kont – szybkie linki

Facebook – odzyskiwanie konta:
facebook.com/hacked

Instagram – pomoc przy przejętym koncie:
instagram.com/hacked

TikTok – odzyskiwanie dostępu:
support.tiktok.com

YouTube / Google – odzyskiwanie konta:
accounts.google.com

LinkedIn – pomoc i odzyskiwanie konta:
linkedin.com/help

CYBERHIGIENA – CODZIENNE NAWYKI, KTÓRE ROBIĄ RÓŻNICĘ

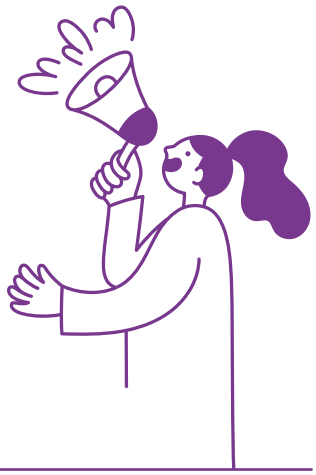
Codzienna checklista bezpieczeństwa:

- Stosujesz weryfikację dwuetapową (2FA).
- Używasz unikalnych haseł do każdego konta.
- Nie udostępniasz haseł osobom trzecim.
- Regularne sprawdzasz aktywne dostępy.
- Usuwasz dostępy po zakończeniu współpracy.
- Zachowujesz ostrożność wobec linków i pilnych wiadomości.
- Logujesz się wyłącznie na zaufanych urządzeniach.
- W swoim profilu podajesz aktualne dane kontaktowe.
- Regularnie aktualizujesz aplikacje i system.
- Szybko reagujesz na podejrzaną aktywność.

Dobrze dobrane ustawienia bezpieczeństwa działają w tle – nie przeszkadzają, ale zapewniają to, co najważniejsze: spokój i kontrolę nad własną marką.

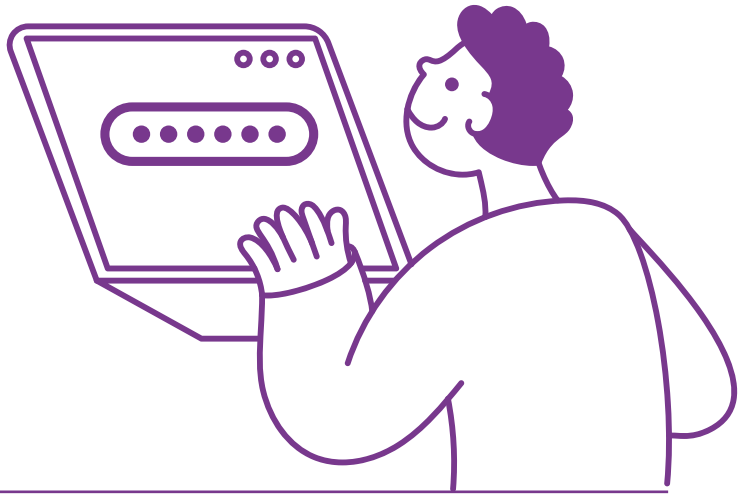
Pytanie do refleksji

Kiedy ostatnio sprawdziłaś/sprawdziłeś ustawienia bezpieczeństwa swoich kont – i czy dziś coś wymaga zmiany?



W pigułce

- Twórcy i twórczynie internetowe są atrakcyjnym celem ataków ze względu na zaangażowaną społeczność i rozpoznawalność, a ich **konta w mediach społecznościowych mają realną wartość** zawodową, wizerunkową i finansową.
- Przejęcia kont zdarzają się często i zwykle wynikają nie z użycia zaawansowanych technologii, lecz z socjotechniki oraz błędów użytkowników i użytkowniczek, a skutki ataku mogą dotknąć także odbiorców i odbiorczynie twórcy/twórczyni.
- Silne hasło to unikalna, nieoczywista fraza lub zdanie (min. 14 znaków, najlepiej 4–5 słów), oparte na własnym, nietypowym lub abstrakcyjnym skojarzeniu, a nie na znanym cytacie. **Słabe hasło można złamać w mniej niż sekundę.**
- W pracy cyfrowego twórcy/twórczyni rozdzielenie spraw prywatnych i zawodowych nie wymaga osobnego sprzętu, wystarczą oddzielne konta, dostępy i **świadome zarządzanie logowaniem, które zwiększają bezpieczeństwo danych i profili**.
- Podstawowe działania, takie jak silne hasła, weryfikacja dwuetapowa, kontrola dostępów oraz nawyki cyberhigieny, znacząco zmniejszają ryzyko ataku.



WIZERUNEK DZIECKA W SIECI, SHARENTING

Oliwia Chojnacka

Czym jest sharenting? Jakie ryzyko może wiązać się z publikowaniem zdjęć dzieci w mediach społecznościowych? Jak publikacje rodziców wpływają na cyfrową tożsamość dziecka? Jakie treści mogą narazić dziecko na ośmieszenie lub cyberprzemoc? Czy dzieci mają prawo do ochrony swojego wizerunku w internecie? Jak najlepiej chronić prywatność dziecka online?

O tym przeczytasz w tym rozdziale.

Sharenting to działanie polegające na publikowaniu przez rodziców lub opiekunów wizerunku i informacji o dziecku w internecie. Zjawisko najczęściej pojawia się w mediach społecznościowych oraz na platformach umożliwiających publikację materiałów wideo. Nazwa powstała z połączenia angielskich słów *share* (dzielić się) i *parenting* (rodzicielstwo).

Choć dzielenie się zdjęciami czy nagraniami dziecka może wydawać się niewinne, niesie ze sobą ryzyko poważnych konsekwencji. Jednym z nich jest powstawanie cyfrowego śladu – obejmującego zarówno publikacje, komentarze czy polubienia, jak i dane zbierane pasywnie, np. lokalizację czy sposób korzystania z urządzeń. Może on towarzyszyć dziecku przez całe życie.

Badania pokazują, że około 75% badanych rodziców podzieliło się materiałem zawierającym wizerunek ich dziecka w mediach społecznościowych, a ponad 80% użyło w publikacji jego prawdziwego imienia[28].

Około 75% rodziców publikuje wizerunek dziecka w SoMe, a ponad 80% podaje prawdziwe imię dziecka

Sharenting nie dotyczy wyłącznie rodziców – uczestniczą w nim także inni członkowie rodziny, znajomi czy nauczyciele. Każda publikacja współtworzy cyfrową obecność dziecka. Dodatkowo mechanizmy platform, takie jak polubienia czy udostępnienia, mogą wzmacniać potrzebę dzielenia się coraz bardziej osobistymi treściami.

28 Tosuntaş, Ş. B., Griffiths, M.D. (2024). Sharenting: A systematic review of the empirical literature. *Journal of Family Theory & Review, 16*(3), 525–562. https://doi.org/10.1111/jftr.12566

Co czwarty nastolatek odczuwa zawstydzenie publikacjami swojego wizerunku w SoMe rodziców

Zjawisko to wpływa na budowanie tożsamości cyfrowej dziecka, które często nie ma kontroli nad publikowanymi materiałami. Treści intymne, trudne lub ośmieszające mogą w przyszłości oddziaływać na jego prywatność, relacje społeczne i dobrostan psychiczny. Eksperci Dyżurnet.pl podkreślają, że nadmierne ujawnianie wizerunku dziecka może naruszać jego autonomię.

Z raportu NASK *Nastolatki 3.0* wynika, że blisko co czwarty nastolatek odczuwa zawstydzenie związane z publikacjami na swój temat, a niemal co drugi deklaruje, że jego wizerunek pojawia się w mediach społecznościowych rodziców[29].

PUBLIKOWANIE WIZERUNKU, LOKALIZACJI I CODZIENNOŚCI DZIECKA

Publikowanie wizerunku dziecka w internecie stało się powszechne wraz z rozwojem mediów społecznościowych, które zintensyfikowały potrzebę dzielenia się codziennością. Choć dla wielu osób jest to sposób na wyrażenie dumy i budowanie relacji, wiąże się z istotnymi zagrożeniami. Dziecko nie jest w stanie świadomie wyrazić zgody na publikację swojego wizerunku, dlatego decyzje podejmują dorośli – często bez pełnej świadomości konsekwencji. Materiały opublikowane w sieci mogą być kopiowane i wykorzystywane bez kontroli pierwotnie udostępniających je osób, a ich usunięcie bywa niemożliwe. Eksperci z zespołu Dyżurnet.pl podkreślają, że treści przedstawiające dziecko mogą zostać wykorzystane przez osoby trzecie w sposób nieetyczny lub przestępczy. Zdarza się również, że nawet zwyczajne fotografie są wykorzystywane przez osoby seksualnie zainteresowane małoletnimi.

Publikowanie treści ośmieszających, intymnych lub ukazujących dziecko w trudnych sytuacjach może prowadzić do hejtu, cyberprzemocy oraz negatywnie wpływać na jego dobrostan psychiczny. Ryzykowne jest także udostępnianie informacji o lokalizacji i codziennych zajęciach, takich jak adres szkoły czy plan dnia.

Długotrwała obecność dziecka w sieci może utrudniać budowanie tożsamości i granic prywatności. Dlatego każda publikacja powinna być poprzedzona refleksją, a ochrona bezpieczeństwa i prywatności dziecka powinna być priorytetem.

29 Lange, R. (red.). (2023). *Nastolatki 3.0: Raport z ogólnopolskiego badania uczniów i rodziców*. NASK.

Ryzyka płynące z sharentingu:

- brak kontroli nad publikacją,
- trwała dostępność danych w sieci,
- możliwość przerabiania i wykorzystywania materiałów przez osoby trzecie,
- negatywne komentarze,
- ujawnienie wrażliwych informacji.

W dłuższej perspektywie może to negatywnie wpływać na prywatność, poczucie bezpieczeństwa i dobrostan dziecka.

TREŚCI PRYWATNE I KOMERCYJNE – WIZERUNEK DZIECKA W INTERNECIE

Treści publikowane w internecie mogą mieć zarówno charakter prywatny, jak i komercyjny. Należy jednak pamiętać, że nawet materiały udostępniane na użytek osobisty mogą prowadzić do naruszenia prywatności dziecka oraz utraty kontroli nad jego wizerunkiem.

W przypadku treści komercyjnych, takich jak współprace reklamowe czy działalność w mediach społecznościowych, ryzyko to jest większe. Dziecko staje się częścią przekazu marketingowego, co wiąże się z jego większą ekspozycją oraz możliwością szerokiego i długotrwałego wykorzystania publikowanych materiałów.

Udział dziecka w reklamie lub modelingu może być postrzegany jako forma rozwoju czy budowania marki osobistej, jednak budzi również kontrowersje – zwłaszcza w kontekście czerpania korzyści finansowych z jego wizerunku. Szczególnym wyzwaniem jest sposób przedstawiania dzieci w przestrzeni publicznej. Zdarza się, że wizerunek dziecka jest stylizowany na bardziej „dorosły" – poprzez ubiór, makijaż, pozowanie czy kontekst publikacji. Tego rodzaju przedstawienia mogą prowadzić do jego seksualizacji, czyli przypisywania mu cech i znaczeń właściwych osobom dorosłym.

Seksualizowanie wizerunku dziecka – nawet nieintencjonalne – może prowadzić do jego uprzedmiotowienia oraz narażać je na niebezpieczne zainteresowanie ze strony osób trzecich, dlatego takie działania powinny być traktowane jako poważne naruszenie jego bezpieczeństwa i prawa do ochrony.

Dlatego decyzje o angażowaniu dziecka w działania komercyjne powinny zawsze uwzględniać jego dobro, potrzeby oraz prawo do prywatności. Istnieje bowiem ryzyko traktowania dziecka jako narzędzia do osiągania celów marketingowych, co może odbywać się kosztem jego komfortu, bezpieczeństwa i rozwoju.

MAŁGORZATA ROZENEK-MAJDAN

NASK: **W Polsce coraz więcej mówi się o negatywnym wpływie social mediów na dzieci i młodzież. W 2025 roku Australia wprowadziła zakaz używania mediów społecznościowych przez osoby poniżej 16. roku życia. O podobnych przepisach coraz częściej mówi się w Polsce. Co Pani, jako twórczyni internetowa, ale też mama i prawniczka, myśli o takim ograniczeniu? Czy ma to sens i czy w ogóle jest realne?**

M. Rozenek-Majdan: Dyskusja o ograniczeniu dostępu dzieci do mediów społecznościowych jest potrzebna i dobrze, że w ogóle się toczy, także w kontekście rozwiązań takich jak wprowadzony w Australii zakaz dla osób poniżej 16. roku życia. Natomiast samo postawienie granicy wieku, czy będzie to 14, 15 czy 16 lat, nie rozwiązuje problemu, jeśli nie idzie za tym realna możliwość jej egzekwowania. A z tym, jak wiemy, bywa bardzo różnie.

Z mojej perspektywy – jako twórczyni internetowej, mamy i prawniczki – kluczowe jest coś więcej niż same przepisy. Fundamentem powinna być edukacja cyfrowa, i to od najmłodszych lat. Dzieci i młodzież muszą nauczyć się poruszać w świecie online świadomie: odróżniać fakty od opinii, rozpoznawać manipulacje, rozumieć mechanizmy działania algorytmów i zagrożenia, jakie się z nimi wiążą.

Ogromną rolę mają tu do odegrania rodzice. Żadne prawo nie zastąpi rozmowy, uważności i budowania relacji. To właśnie w domu dzieci uczą się, jak reagować na hejt, jak radzić sobie z presją porównań i jak budować poczucie własnej wartości w oparciu o realne doświadczenia, a nie wirtualne oceny. Jako mama staram się, by moi synowie wiedzieli, że ich wartość nie zależy od komentarzy w sieci, tylko od tego, kim są i co robią w prawdziwym życiu.

Dlatego uważam, że sens mają zarówno regulacje, jak i działania systemowe, ale bez zaangażowania rodziców i mądrej edukacji cyfrowej ich skuteczność będzie ograniczona.

DŁUGOFALOWE SKUTKI CYFROWEJ OBECNOŚCI DZIECKA

Długotrwałe publikowanie wizerunku dziecka w internecie może mieć poważne i trudne do odwrócenia konsekwencje, które towarzyszą mu przez całe życie. Skutki te obejmują:

- **utrwalony cyfrowy ślad** – dziecko dorasta z wizerunkiem stworzonym przez dorosłych, bez możliwości jego kontroli lub zmiany;
- **naruszenie prywatności i autonomii** – brak wpływu na własny wizerunek może ograniczać poczucie sprawczości i kontroli nad samym sobą,
- **negatywny wpływ na zdrowie psychiczne** – wstyd, stres, presja społeczna oraz obniżone poczucie własnej wartości związane z oceną i komentarzami innych;
- **ryzyko ośmieszenia i cyberprzemocy** – publikowane treści mogą stać się przyczyną wyśmiewania, hejtu i trwałych negatywnych doświadczeń,
- **możliwość wykorzystania wizerunku** – materiały mogą zostać użyte przez osoby trzecie w sposób nieetyczny lub przestępczy;
- **zatarcie granic prywatności** – dziecko przyzwyczajone do ciągłej obecności w sieci może mieć trudność w rozpoznawaniu, co powinno pozostać prywatne.

RYZYKA PRAWNE ORAZ ODPOWIEDZIALNOŚĆ OPIEKUNÓW

Upublicznianie wizerunku dziecka wiąże się z obowiązkami prawnymi i etycznymi po stronie opiekunów. Wizerunek dziecka stanowi dobro podlegające szczególnej ochronie, a zgodę na jego rozpowszechnianie wyrażają rodzice lub opiekunowie prawni działający w imieniu małoletniego.

W przypadku starszych dzieci należy uwzględniać ich zdanie oraz prawo do współdecydowania o własnym wizerunku. Decyzje dotyczące publikacji powinny być podejmowane z rozwagą i zawsze uwzględniać dobro dziecka jako wartość nadrzędną.

Chociaż prawo nie reguluje kwestii związanych z upublicznianiem wizerunku dziecka przez rodziców, to istnieją stosowne przepisy mogące być pomocne w sprawach związanych z sharentingiem.

Regulacje prawne dotyczące wizerunku[30]

Art. 47 Konstytucji	Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.
Art. 16 Konwencji o prawach dziecka	Żadne dziecko nie będzie podlegało arbitralnej lub bezprawnej ingerencji w sferę jego życia prywatnego, rodzinnego lub domowego czy w korespondencję ani bezprawnym zamachom na jego honor i reputację. Dziecko ma prawo do ochrony prawnej przeciwko tego rodzaju ingerencji lub zamachom.
Art. 23 Kodeksu cywilnego	Dobra osobiste człowieka, jak w szczególności zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek [...] pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach.
Art. 81 Ustawy o prawie autorskim i prawach pokrewnych	Rozpowszechnianie wizerunku wymaga zezwolenia osoby na nim przedstawionej. W braku wyraźnego zastrzeżenia zezwolenie nie jest wymagane, jeżeli osoba ta otrzymała umówioną zapłatę za pozowanie.

ODPOWIEDZIALNOŚĆ ZA WIZERUNEK DZIECKA ZACZYNA SIĘ WCZEŚNIEJ

Odpowiedzialność za wizerunek dziecka nie zaczyna się w momencie publikacji, lecz już na etapie wykonania zdjęcia czy nagrania. Każdy materiał zawiera informacje o dziecku – jego wyglądzie, sytuacji czy otoczeniu – dlatego decyzja o jego utrwaleniu jest jednocześnie decyzją o potencjalnym ujawnieniu tych danych. Przed publikacją warto zadać sobie pytanie, czy dziecko – już jako osoba dorosła – chciałoby, aby dany materiał był dostępny w internecie.

Dlatego szczególnie istotne jest, aby materiały:

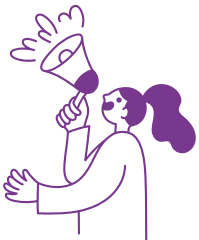
- w miarę możliwości ograniczały możliwości identyfikacji dziecka (np. poprzez kontekst, lokalizację czy nadmiar danych);
- nie prezentowały nagości;
- nie zawierały danych wrażliwych (np. medycznych);
- nie przedstawiały sytuacji ośmieszających.

30 Biuro Rzecznika Praw Dziecka. (2024). *Więcej szacunku dla młodego wizerunku*. https://brpd.gov.pl/wp-content/uploads/2024/12/Broszura.pdf [dostęp: 01.04.2026 r.]

ZANIM OPUBLIKUJESZ, ZATRZYMAJ SIĘ NA CHWILĘ

Zanim udostępnisz zdjęcie lub nagranie dziecka, zadaj sobie kilka pytań

- Czy moje dziecko – za kilka lat – chciałoby, żeby ten materiał był w internecie?
- Czy ta treść nie zawiera informacji, które mogą je zidentyfikować (np. szkoła, lokalizacja, plan dnia)?
- Czy materiał nie jest dla dziecka ośmieszający, zbyt prywatny lub intymny?
- Czy mam pewność, kto może zobaczyć ten post i co może z nim zrobić dalej?
- Czy publikuję to dla dobra dziecka, czy dla reakcji innych (polubień, komentarzy)?



Pytanie do refleksji

Czy ta publikacja za kilka lat nadal będzie bezpieczna i komfortowa dla mojego dziecka? Jeśli masz wątpliwości - to sygnał, żeby zrezygnować z publikacji!

W pigułce

» Sharenting wpływa na prywatność i bezpieczeństwo dziecka w internecie, a rodzice nie zawsze pamiętają, że **publikowanie materiałów o dziecku może być dla niego źródłem dyskomfortu, niezadowolenia lub zawstydzenia**.

» Każda publikacja tworzy cyfrowy ślad dziecka na lata, a udostępnianie jego wizerunku, lokalizacji, komentarzy czy prywatnych treści zwiększa ryzyko nadużyć i cyberprzemocy. **Opublikowane materiały mogą krążyć w sieci bez kontroli rodziców.**

» Odpowiedzialność za ochronę wizerunku dziecka spoczywa na rodzicach już od momentu wykonania zdjęcia. Prawo nie reguluje wprost kwestii sharentingu, ale ochronę wizerunku dziecka zapewniają m.in. Konstytucja, Konwencja o prawach dziecka, Kodeks cywilny oraz Ustawa o prawie autorskim i prawach pokrewnych

» **Prywatność i bezpieczeństwo dziecka powinny być ważniejsze niż potrzeba publikowania treści w mediach społecznościowych** – każdorazowo należy uwzględnić ich wpływ na obecne i przyszłe życie dziecka.

WIZERUNEK, DEEPFAKE I KRADZIEŻ TOŻSAMOŚCI

Ewelina Bartuzi-Trokielewicz
Alicja Martinek
Adrian Kordas

Czym są techniki deepfake i deepnude? Czy prawo chroni przed manipulacją wizerunkiem? Jakie są najczęstsze techniki manipulacji audiowizualnej? Jak powstają deepfake'i ? Na czym polega zasada „weryfikuj, zanim uwierzysz"? Co to jest prebunking? Jakie narzędzia pomagają wykrywać deepfake'i? Co zrobić, gdy ktoś wykorzystał Twój wizerunek?

O tym przeczytasz w tym rozdziale.

CZYM JEST DEEPFAKE I MANIPULACJA WIZERUNKIEM

Deepfake to technologia tworzenia lub manipulowania materiałami audiowizualnymi (zdjęciem, dźwiękiem, wideo) z wykorzystaniem sztucznej inteligencji. Umożliwia tworzenie treści, które wiarygodnie imitują konkretne osoby lub zdarzenia, mimo że przedstawione na nich sytuacje nie miały miejsca.

Termin ten obejmuje m.in. generowanie ścieżki dźwiękowej brzmiącej jak głos żywej osoby, podmianę twarzy na nagraniu, zmianę elementów wizerunku czy synchronizację ruchu ust z wygenerowanym dźwiękiem. Coraz częściej pojawiają się także cyfrowe postacie (awatary) sterowane tekstem lub głosem.

Dodatkowo rozwijają się tzw. *partial deepfake*, czyli materiały, w których modyfikowane są jedynie fragmenty (np. pojedyncze słowa lub elementy obrazu), co znacząco utrudnia ich wykrycie.

Szczególnie szkodliwą formą deepfake'ów są tzw. deepnude'y, czyli materiały o charakterze pornograficznym tworzone bez zgody przedstawionej w nich osoby. Zjawisko to dotyczy głównie kobiet i stanowi jedną z najczęstszych form przemocy wizerunkowej z wykorzystaniem technologii generatywnych.

Szacuje się, że nawet 95–98% deepfake'ów w sieci ma charakter pornograficzny. Zjawisko to określa się jako *image-based sexual abuse* i może ono prowadzić do poważnych konsekwencji psychologicznych, takich jak poczucie upokorzenia, lęk czy zespół stresu pourazowego (PTSD).

Przemoc z użyciem AI w formie deepnude'ów najczęściej dotyka kobiet

Nawet 95–98% deepfake'ów w sieci ma charakter pornograficzny

Jak powstaje deepfake?

1. **Zebranie materiałów**
   Do zbioru danych treningowych włączane są zdjęcia, nagrania wideo lub audio danej osoby.
2. **Analiza przez AI**
   Algorytmy uczą się wyglądu twarzy, mimiki i głosu.
3. **Tworzenie imitacji**
   Powstaje syntetyczny obraz lub głos (np. podmiana twarzy, klonowanie głosu).
4. **Połączenie z materiałem**
   Twarz lub głos są wstawiane do innego nagrania.
5. **Uwiarygodnienie i publikacja**
   Materiał jest poprawiany i udostępniany w sieci.

WIZERUNEK A DEEPFAKE – KONTEKST PRAWNY

W polskim systemie prawnym wizerunek rozumiany jest szeroko jako zestaw cech charakterystycznych danej osoby pozwalających na jej identyfikację. Obejmuje twarz, głos, a także sylwetkę, sposób poruszania się, czy charakterystyczne cechy wyglądu. Manipulacja wizerunkiem, w tym wykorzystanie technologii deepfake może prowadzić do naruszania różnych obszarów prawa, w tym:

- **przepisów o ochronie dóbr osobistych** – takich jak wizerunek, dobre imię i prywatność (Kodeks cywilny),
- **prawa autorskiego** – w zakresie rozpowszechniania wizerunku bez zgody (Ustawa o ochronie prawa autorskiego i praw pokrewnych),
- **prawa karnego** – w przypadkach podszywanie się i kradzieży tożsamości (Kodeks karny, art. 190a § 2),
- **przepisów o ochronie danych osobowych** – m.in. RODO (w szczególności art. 4 pkt 14 oraz art. 9, dotyczące danych biometrycznych i szczególnych kategorii danych osobowych), zwłaszcza gdy wykorzystywane są dane biometryczne (np. wizerunek twarzy)[31].

31 Rozporządzenie 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 (RODO). https://eur-lex.europa.eu/eli/reg/2016/679/oj [dostęp: 30.03.2026 r.]

TECHNIKI MANIPULACJI AUDIOWIZUALNEJ

Manipulacja wizerunkiem może mieć różny poziom zaawansowania – od prostego retuszu po zaawansowane deepfake'i tworzone z użyciem sztucznej inteligencji. Kluczowe znaczenie ma nie tylko technika, ale też intencja (czy dana przeróbka ma na celu wprowadzenie kogoś w błąd) oraz kontekst publikacji (np. reklama, fałszywe wiadomości, oszustwa).

Najpopularniejsze techniki manipulacji:

- **Lip-sync** – dopasowanie ruchu ust do fałszywego nagrania audio – efekt sprawia wrażenie, jakby osoba wypowiadała słowa, których nigdy nie powiedziała.
- **Face reenactment** – przenoszenie mimiki i emocji z jednej osoby na drugą – pozwala „sterować" wyrazem twarzy i reakcjami.
- **Face swap** – podmiana twarzy – nałożenie wizerunku jednej osoby na ciało innej (np. w filmie).
- **W pełni syntetyczne materiały (generatywne AI)** – obrazy lub nagrania wideo stworzone od podstaw przez sztuczną inteligencję, przedstawiające wydarzenia, które nigdy nie miały miejsca (w przeciwieństwie do metod, które modyfikują jedynie fragment istniejącego materiału).
- **Awatary** – cyfrowe postacie imitujące wygląd i sposób mówienia konkretnej osoby, sterowane tekstem lub głosem.
- **Manipulacja głosem** – deepfake to nie tylko obraz – równie niebezpieczne są fałszywe nagrania audio. Syntetyczny głos może naśladować barwę i sposób mówienia konkretnej osoby, a pod względem jakości bywa trudny do odróżnienia od oryginału.

Obecnie do stworzenia wiarygodnej kopii głosu wystarczy zaledwie kilka sekund nagrania, co znacząco zwiększa ryzyko nadużyć. Na podstawie takiej próbki algorytm może przenieść sposób mówienia, emocje i ton z jednej osoby na drugą albo wygenerować zupełnie nową wypowiedź w oparciu o zadany tekst.

W dobie łatwego dostępu do różnych metod generowania deepfake'ów i popularności mediów społecznościowych, które są niewyczerpanym źródłem danych, oszuści mają idealne warunki, by tworzyć szkodliwe materiały. Ale jakie cele mogą ich do tego motywować?

WPŁYW NA REPUTACJĘ

Dla twórczyń i twórców internetowych reputacja jest jednym z najważniejszych zasobów zawodowych. To na niej opiera się zaufanie ludzi, wiarygodność w roli ekspertów lub ekspertek, relacje z markami oraz skuteczność działań komercyjnych. Deepfake i manipulacja wizerunkiem mogą prowadzić do **tzw. fałszywego przypisania** – sytuacji, w której twórcy lub twórczyni przypisywane są słowa, działania lub rekomendacje, które nigdy nie miały miejsca (np. fałszywe reklamy czy wypowiedzi). Nawet jeśli treść jest nieprawdziwa, jej realistyczna forma może wywołać kryzys wizerunkowy.

Skala zjawiska jest istotna. Analizy incydentów wskazują, że w kampaniach wykorzystujących zmanipulowane treści audiowizualne bezprawnie wykorzystywane są wizerunki wielu znanych osób. Oszuści i oszustki najczęściej celują w osoby o wysokim wpływie społecznym, szczególnie związane z mediami, polityką oraz obszarem rozrywki, lifestyle'u, medycyny i biznesu.

REALNE KONSEKWENCJE

Fałszywe reklamy i materiały wykorzystujące wizerunek twórców i twórczyń mogą prowadzić do realnych strat po stronie ich publiczności, takich jak utrata pieniędzy, wyłudzenie danych czy inne formy manipulacji. Szczególnie niebezpieczne są tzw. oszustwa romantyczne, w których wykorzystuje się wizerunek znanej osoby do budowania relacji i zdobycia zaufania np. podszywanie się pod celebrytów, którzy rzekomo nawiązują prywatny kontakt i proszą o wsparcie finansowe. Przykładem jest sprawa kobiety, która uwierzyła, że pozostaje w relacji z Bradem Pittem i została oszukana na znaczną kwotę przez osoby wykorzystujące jego wizerunek oraz technologie generatywne[32].

Tego typu działania podważają również wiarygodność twórców i twórczyń i zaufanie ich społeczności. Problem pogłębia tempo rozprzestrzeniania się treści – raz opublikowane materiały mogą szybko stać się viralowe, a ich skutki są trudne do odwrócenia.

32 Euronews. (15 stycznia 2025). *French woman duped by AI Brad Pitt love scam faces cyberbullying*. https://www.euronews.com/culture/2025/01/15/viral-scam-french-woman-duped-by-ai-brad-pitt-love-scheme-faces-cyberbullying

W efekcie pojawiają się wielowymiarowe konsekwencje takie jak: naruszenie dóbr osobistych, utrata zaufania, wywoływanie silnych reakcji i lawinowego rozprzestrzeniania się fałszywych materiałów. Możliwe są również straty biznesowe, np. w wyniku zerwania współpracy lub powstania u internautów i internautek trwałego skojarzenia marki osobistej z nieuczciwymi praktykami biznesowymi.

FAŁSZYWE REKLAMY I PODSZYWANIE SIĘ

Jednym z najczęstszych zastosowań technologii deepfake są fałszywe reklamy oraz podszywanie się pod osoby publiczne. W takich przypadkach wizerunek twórczyni lub twórcy jest wykorzystywany bez ich wiedzy do promowania produktów i usług stanowiących w istocie oszustwo. Fałszywe reklamy bazują na zaufaniu, jakie odbiorczynie i odbiorcy mają do konkretnych osób, a rozpoznawalny wizerunek staje się narzędziem uwiarygodniania przekazu. Warto zaznaczyć, że w polskiej przestrzeni internetowej pojawia się miesięcznie nawet około 100 000 fałszywych reklam, które są stale rotowane i modyfikowane[33].

33 CERT Polska. (2024). *Oszustwa reklamowe na dużych platformach internetowych*. https://cert.pl/posts/2024/11/Oszustwa-reklamowe-na-duzych-platformach/ [dostęp: 27.03.2026 r.]

MAŁGORZATA ROZENEK-MAJDAN

NASK: **W social mediach nie brakuje treści szkodliwych. Wiele osób winą za to obarcza jedynie twórców i twórczynie takiego contentu. Jak Pani widzi rolę big techów: Mety, X, Tik Toka czy Google w kwestii reagowania na szkodliwe treści?**

M. Rozenek-Majdan: Zrzucanie całej odpowiedzialności za negatywny wpływ mediów społecznościowych wyłącznie na twórczynie i twórców cyfrowych to duże uproszczenie. Platformy takie jak Meta, X, TikTok czy Google nie są przecież biernymi pośrednikami – to one zarządzają zasięgami, moderacją i mechanizmami reklamowymi, które często umożliwiają rozprzestrzenianie się kontrowersyjnych treści na ogromną skalę.

Warto zauważyć, że dziś social media są wręcz rajem dla cyberoszustów – osób, które nie mają żadnej intencji budowania wartości czy relacji, a jedynie chcą szybko zarobić kosztem innych. Sama tego doświadczyłam, gdy w sieci pojawiły się materiały sugerujące, że promuję „aplikację do zarabiania pieniędzy". Zareagowałam natychmiast: ostrzegłam swoich obserwatorów i jasno powiedziałam, że to oszustwo.

I właśnie takiej samej szybkości i stanowczości oczekuję od big techów, a nie opieszałości czy przerzucania odpowiedzialności. To niedopuszczalne, że fałszywe reklamy czy dezinformacja potrafią funkcjonować na platformach przez długi czas bez reakcji. Użytkownicy i użytkowniczki mają pełne prawo wymagać, by firmy technologiczne wzięły realną odpowiedzialność za treści, które rozpowszechniają i aktywnie zwalczały nadużycia. Brak zdecydowanych działań w tej kwestii to nie tylko zaniedbanie, to przyzwolenie na oszustwa.

JAK DZIAŁAJĄ FAŁSZYWE REKLAMY?

Fałszywe reklamy bardzo często opierają się na konkretnych, powtarzalnych scenariuszach wykorzystania wizerunku twórczyń i twórców. Najczęściej polegają na przypisaniu im określonej roli w zmyślonej historii, która ma przekonać odbiorczynie i odbiorców do podjęcia zamierzonego przez sprawców działania.

W tego typu materiałach wizerunek znanych osób jest wykorzystywany w celu uwiarygodnienia treści – przedstawiane są one jako osoby, które rzekomo:

- polecają inwestycje, platformy finansowe lub aplikacje do zarabiania;
- występują w roli ekspertek i ekspertów dzielących się „sprawdzonym" rozwiązaniem lub odkryciem;
- udzielają wywiadu, w którym opowiadają o sposobie na szybki zysk lub przełomowej metodzie leczenia;
- potwierdzają wiarygodność konkretnej firmy, produktu lub usługi.

Fałszywym materiałom często towarzyszy narracja budująca poczucie pilności lub wyjątkowej okazji – np. sprawiająca wrażenie ograniczonej oferty albo przekazywania sekretnej wiedzy czy informacji, które ktoś próbuje ukryć. Wizerunek znanej osoby wzmacnia wiarygodność i zwiększa skuteczność oszustwa.

Oszuści i oszustki wykorzystują przy tym socjotechniki, wywołując silne emocje (strach, nadzieję) i poczucie presji czasu. W efekcie odbiorcy i odbiorczynie podejmują decyzje szybciej i rzadziej weryfikują źródło informacji.

GRAFIKA

Przykład jednej z najpopularniejszych kampanii w Polsce w drugiej połowie 2025 z użyciem wizerunku byłej Pierwszej Damy – Jolanty Kwaśniewskiej.

Źródło: NASK.

PODSZYWANIE

Podszywanie się polega na tworzeniu fałszywego wrażenia, że dana twórczyni lub dany twórca publikuje określone treści lub kontaktuje się z odbiorcami. Może przyjmować różne formy:

- fałszywe konta w mediach społecznościowych,
- spreparowane nagrania lub wypowiedzi,
- wiadomości prywatne (np. z prośbą o pieniądze lub dane).

JAK SIĘ CHRONIĆ I CO ZROBIĆ, GDY KTOŚ WYKORZYSTA TWÓJ WIZERUNEK?

Technologie generatywnej sztucznej inteligencji już są obecne w naszym życiu i cały czas szybko się rozwijają. Nasze czasy cechuje duże ryzyko manipulacji wizerunkiem, dlatego ochrona marki osobistej wymaga połączenia prewencji, gotowości operacyjnej oraz szybkiej reakcji. Duże znaczenie w tej sytuacji ma nie tylko ograniczanie ryzyka, ale także przygotowanie na ewentualne naruszenia wizerunku, tożsamości cyfrowej oraz dóbr osobistych.

Działania prewencyjne

Skuteczna ochrona przed manipulacją wizerunkiem i podszywaniem opiera się na świadomym zarządzaniu obecnością w sieci, spójnej komunikacji oraz stosowaniu codziennych zasad cyberhigieny (omówionych w innej części poradnika). Obejmują one:

- stosowanie znaków wodnych i stałych elementów identyfikacyjnych, np. podpisów, formatów komunikacji,
- budowanie rozpoznawalnych, oficjalnych kanałów komunikacji oraz wskazywanie ich jako jedynego źródła autentycznych treści,
- utrzymywanie jednego, oficjalnego punktu odniesienia dla odbiorców, czyli przykładowo strony internetowej z listą oficjalnych profili oraz zasad współpracy,
- jasne wskazanie, gdzie i w jakiej formie publikowane są informacje o współpracy ze sponsorami.

Znajomość procedur – reagowanie na naruszenia

Skuteczna ochrona wizerunku nie ogranicza się wyłącznie do działań prewencyjnych. Istotnym elementem jest również

znajomość procedur reagowania, zarówno tych obowiązujących na platformach społecznościowych, jak i wynikających z obowiązujących regulacji prawnych.

Osoby publiczne oraz zespoły odpowiedzialne za komunikację powinny wiedzieć, gdzie i w jaki sposób zgłaszać naruszenia. Platformy społecznościowe udostępniają specjalistyczne narzędzia umożliwiające zgłaszanie przypadków podszywania się, fałszywych reklam czy zmanipulowanych materiałów, co pozwala na podjęcie działań bez konieczności bezpośredniego kontaktu ze sprawcą.

W praktyce proces usuwania treści nie zawsze przebiega szybko i skutecznie. Dlatego rekomendowane jest podejmowanie działań zwiększających szanse na reakcję platformy, takich jak:

- zgłaszanie naruszeń z różnych kont (jeśli to możliwe),
- ponawianie zgłoszeń w przypadku braku reakcji,
- korzystanie z kilku dostępnych ścieżek zgłaszania,
- dokumentowanie naruszeń (zrzuty ekranu, linki, daty zgłoszeń).

Regulacje przyjęte przez Unię Europejską w ramach aktu w sprawie sztucznej inteligencji (AI Act) wprowadzają obowiązek oznaczania treści wytworzonych lub zmienionych przez AI, aby zwiększyć przejrzystość komunikacji i ograniczyć ryzyko wprowadzania odbiorczyń i odbiorców w błąd[34]. Jednocześnie Akt o usługach cyfrowych (DSA) nakłada na platformy obowiązek reagowania na nielegalne treści, w tym materiały wykorzystujące czyjś wizerunek bez zgody tej osoby[35]. Oznacza to formalne zobowiązanie serwisów do usuwania zgłoszonych naruszeń, choć tempo i skuteczność reakcji mogą się różnić w zależności od platformy i jakości zgłoszenia.

34 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. (akt w sprawie sztucznej inteligencji). https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng [dostęp: 27.03.2026 r.]

35 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 (Digital Services Act). https://eur-lex.europa.eu/eli/reg/2022/2065/oj [dostęp: 30.03.2026 r.]

Plan działania w przypadku naruszenia

W sytuacji bezprawnego wykorzystania wizerunku kluczowe jest szybkie i uporządkowane działanie

1. Zabezpieczenie dowodów	Należy wykonać zrzuty ekranu, zapisać linki i daty publikacji oraz – jeśli to możliwe – nagrać materiał. W poważniejszych przypadkach warto rozważyć notarialne potwierdzenie treści.
2. Zgłoszenie treści	Materiał należy zgłosić do administracji platformy, na której został opublikowany, z wykorzystaniem dostępnych formularzy. Aby ograniczyć dalsze negatywne skutki wykorzystania wizerunku, warto również przekazać sprawę do **CERT Polska**, który może podjąć działania, m.in. poprzez umieszczenie strony na Liście Ostrzeżeń, jeśli wizerunek jest wykorzystywany do wyłudzania danych lub środków finansowych – na podstawie przepisów ustawy o zwalczaniu nadużyć w komunikacji elektronicznej[36].
3. Reakcja prawna	W przypadku poważnych naruszeń zasadne jest rozważenie działań prawnych, takich jak formalne zgłoszenie: • **naruszenia dóbr osobistych** – na podstawie art. 23 i 24 Kodeksu cywilnego[37], • **podszywania się i kradzież tożsamości** – art. 190a §2 Kodeksu karnego[38], • **zmuszania do określonego działania lub szantażu** – art. 191 Kodeksu karnego[39], • **naruszenia danych osobowych** – RODO. • Możliwe działania obejmują wezwanie do usunięcia treści, zgłoszenie sprawy organom ścigania lub do Prezesa UODO.
4. Komunikacja kryzysowa	Należy opublikować szybkie i jasne sprostowanie w oficjalnych kanałach, wskazując, które treści są fałszywe oraz gdzie znajdują się wiarygodne źródła.
5. Prawo do bycia zapomnianym	W uzasadnionych przypadkach możliwe jest skorzystanie z prawa do bycia zapomnianym **(zob. str. 20).**

36 Ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz.U. 2023 poz. 1703).

37 Dz. U. z 2025 r., poz. 1071.

38 Dz. U. z 2025 r., poz. 383.

39 Tamże.

DLACZEGO NIE WARTO IGNOROWAĆ SYGNAŁÓW OSTRZEGAWCZYCH?

W praktyce zdarza się, że pierwsze sygnały o nieuprawnionym wykorzystaniu wizerunku – np. od odbiorców i odbiorczyń, którzy zauważyli fałszywy materiał – są bagatelizowane lub odkładane na później. Może to wynikać z niepewności, braku czasu lub przekonania, że pojedyncza publikacja nie ma większego znaczenia. Takie podejście wiąże się jednak z dużym ryzykiem.

Fałszywe materiały, zwłaszcza reklamy, mogą szybko osiągać dużą skalę oddziaływania – są powielane, modyfikowane i rozpowszechniane w różnych kanałach. Brak reakcji na wczesnym etapie może prowadzić do utrwalenia fałszywego przekazu oraz realnych strat wizerunkowych i finansowych.

Z perspektywy zarządzania marką osobistą każda informacja o możliwym naruszeniu powinna być traktowana jako sygnał do weryfikacji. Nawet jeśli zgłoszenie okaże się niezasadne, sam proces sprawdzenia wzmacnia kontrolę nad wizerunkiem i ogranicza ryzyko eskalacji.

Stosuj zasadę szybkiej reakcji – sprawdzaj i natychmiast zgłaszaj próby wykorzystania wizerunku

Rekomendowane jest przyjęcie zasady szybkiej reakcji – każda potencjalna próba wykorzystania wizerunku powinna być sprawdzona, a w razie potwierdzenia niezwłocznie zgłoszona i zakomunikowana publiczności.

EDUKOWANIE SPOŁECZNOŚCI

Edukowanie społeczności to jeden z kluczowych elementów ochrony wizerunku w środowisku cyfrowym. W czasach, gdy materiały mogą być łatwo modyfikowane lub generowane przez sztuczną inteligencję, odbiorcy i odbiorczynie często podchodzą do nich ze zbyt małym krytycyzmem. Twórcy i twórczynie, jako osoby o dużym zasięgu oddziaływania, odgrywają istotną rolę w budowaniu odporności swoich społeczności na manipulację i dezinformację.

PREBUNKING, CZYLI EDUKACJA Z WYPRZEDZENIEM

Najskuteczniejszym podejściem do edukowania społeczności jest działanie z wyprzedzeniem, określane mianem prebunkingu. Polega ono na wcześniejszym wyjaśnianiu mechanizmów manipulacji, zanim odbiorcy i odbiorczynie zetkną się z fałszywymi treściami, dzięki czemu są mniej podatni na impulsywne reakcje i łatwiej rozpoznają schematy dezinformacji.

Kluczowe jest uświadamianie swojej publiczności, że współcześnie materiały cyfrowe – obrazy, filmy czy nagrania audio – mogą być łatwo modyfikowane, oraz pokazywanie jej najczęstszych technik wpływu, takich jak presja czasu, silne emocje czy odwoływanie się do autorytetów. Badania oraz analizy organizacji fact-checkingowych wskazują, że prebunking zwiększa odporność na dezinformację i wspiera zdolność jej rozpoznawania[40].

NAUKA ROZPOZNAWANIA DEZINFORMACJI

Uzupełnieniem edukacji jest debunking, czyli reagowanie na już opublikowane fałszywe treści poprzez ich sprawdzanie i wyjaśnianie mechanizmu manipulacji. Nie polega on wyłącznie na oznaczeniu materiału jako nieprawdziwego – jego celem jest pokazanie, jakie techniki zostały wykorzystane i dlaczego przekaz może wprowadzać w błąd.

Skuteczny debunking powinien być jasny, zrozumiały, oparty na faktach i możliwy do zweryfikowania. Istotne jest także odniesienie do rzeczywistości – czyli wskazanie, w jaki sposób dana treść została wyrwana z kontekstu lub zniekształcona. Dzięki temu odbiorcy nie tylko wiedzą, że coś jest fałszywe, ale rozumieją, dlaczego.

W przypadku twórców i twórczyń oraz osób publicznych debunking pełni dodatkową funkcję – pomaga chronić wizerunek i ograniczać zasięg dezinformacji. Szybka, spokojna reakcja oparta na faktach może skutecznie zatrzymać rozprzestrzenianie się nieprawdziwych treści.

40 European Commission, Joint Research Centre. (2024). *Misinformation and disinformation: both prebunking and debunking work in fighting it.* https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/misinformation-and-disinformation-both-prebunking-and-debunking-work-fighting-it-2024-10-25_en

Równie istotne jest jednak rozwijanie umiejętności samodzielnego rozpoznawania sygnałów ostrzegawczych – szczególnie w przypadku treści audiowizualnych, które mogą wyglądać bardzo wiarygodnie, a mimo to zawierać błędy techniczne lub logiczne.

W praktyce warto znać proste sygnały ostrzegawcze, które pomagają szybko stwierdzić, że materiał może być nieprawdziwy:

- **w warstwie dźwiękowej** – nienaturalne brzmienie głosu, jednolite tempo mowy, brak pauz i oddechów, metaliczny pogłos, błędy w odmianie liczebników, nietypowa intonacja lub sposób mówienia, który nie pasuje do danej osoby,
- **w warstwie wizualnej** – nienaturalnie wygładzona skóra, rozmycia i deformacje (szczególnie w okolicy ust), niespójne oświetlenie, błędy w mimice i ruchach, nienaturalne proporcje lub detale,
- **w logice obrazu** – zaburzenia spójności całej sceny, relacji między postacią, otoczeniem, światłem i ruchem,
- **w warstwie językowej i narracyjnej** – nienaturalne konstrukcje składniowe, błędy w odmianie, treści niepasujące do stylu wypowiedzi danej osoby,
- **w kontekście** – nietypowe prośby (np. o pieniądze lub dane), presja czasu, obietnice wysokich zysków bez ryzyka, wykorzystanie wizerunku znanej osoby do uwiarygodnienia przekazu czy logotypów mediów do promowania produktów, które nie pojawiają się w wiarygodnych źródłach.

Pobierz przewodnik:

Należy podkreślić, że pojedynczy sygnał nie przesądza o fałszu, jednak ich połączenie powinno skłaniać do weryfikacji.

Więcej informacji można znaleźć w publikacji NASK *Przewodnik po cyberbezpieczeństwie i sztucznej inteligencji dla mediów i twórców cyfrowych*[41] oraz w materiałach dostępnych na kanale YouTube NASK[42].

41 Adamczyk, S. (red.). (2025). *Przewodnik po cyberbezpieczeństwie i sztucznej inteligencji dla mediów i twórców cyfrowych*. NASK.

42 NASK. (2025). *Usta, głos, treść, tło. Umiesz rozpoznać deepfake? Sprawdź! Pomogą ci w tym eksperci NASK*. https://nask.pl/aktualnosci/usta-glos-tresc-tlo-umiesz-rozpoznac-deepfake-sprawdz-pomoga-ci-w-tym-eksperci-nask/

ZASADA „WERYFIKUJ, ZANIM UDOSTĘPNISZ” W PRAKTYCE

Podstawą odporności społeczności na dezinformację jest wykształcenie przez nią prostych, powtarzalnych nawyków sprawdzania informacji. Zasada „weryfikuj, zanim uwierzysz” powinna być praktyką stosowaną podczas codziennego odbioru treści. W tym kontekście szczególne znaczenie ma uważność oraz fact-checking, czyli świadoma weryfikacja informacji przed ich dalszym rozpowszechnianiem. Proces ten obejmuje sprawdzanie źródła informacji, porównywanie wiadomości z innymi wiarygodnymi materiałami oraz analizę kontekstu, w jakim dana treść się pojawia.

Ważne jest także przyzwyczajenie do zachowywania czujności wobec treści, które wywołują silne emocje lub wprowadzają presję szybkiego działania, ponieważ właśnie takie mechanizmy są często wykorzystywane w manipulacjach i oszustwach. Duże znaczenie ma również ograniczenie impulsywnego udostępniania materiałów, w szczególności takich o charakterze sensacji.

Ostatnim istotnym elementem edukacji jest wzmacnianie postawy odpowiedzialności za obieg informacji. Odbiorczynie i odbiorcy powinni być zachęcani nie tylko do weryfikowania treści, ale również do ich zgłaszania w przypadku podejrzenia naruszenia. W ten sposób społeczność nie tylko unika powielania fałszywych materiałów, ale i aktywnie przyczynia się do ograniczania ich zasięgu.

Wybrane narzędzia do wykrywania deepfake’ów

Resemble AI	Narzędzie wielomodalne do wykrywania treści generowanych przez AI, szczególnie skuteczne w analizie dźwięku i materiałów wideo (syntetyczna ścieżka audio). https://www.resemble.ai/deepfake-detection/
Hive AI (Hive Moderation)	Rozwiązanie wielomodalne do analizy treści generowanych przez AI (obraz, wideo, tekst). Oferuje darmowy dostęp do testowania. https://thehive.ai/
Deepfake Total	Narzędzie skoncentrowane na analizie i wykrywaniu syntetycznego dźwięku oraz manipulacji głosem. https://deepfake-total.com
AI Image Detector (isitAI)	Proste narzędzie online do sprawdzania czy obraz został wygenerowany przez AI. https://isitai.com/ai-image-detector/

Narzędzia te stanowią wsparcie w analizie treści, jednak ich wyniki należy traktować jako wskazówkę, a nie jako ostateczny dowód, że ma się do czynienia z deepfake’iem.

Zadanie dla Ciebie

Znajdź w sieci materiał (wideo, nagranie lub zdjęcie), który wzbudza Twoje wątpliwości i spróbuj go przeanalizować:

- sprawdź źródło,
- oceń, czy pojawiają się sygnały ostrzegawcze (obraz, dźwięk, kontekst),
- spróbuj zweryfikować go w innych źródłach lub przy użyciu narzędzi.

Pytanie do refleksji

Czy potrafiłbym/potrafiłabym rozpoznać, że ktoś wykorzystuje mój wizerunek lub głos – i czy wiem, jak wtedy zareagować?

W pigułce

» Rozwój technologii sprawił, że manipulacja wizerunkiem przestała być zjawiskiem marginalnym i stała się realnym zagrożeniem dla osób aktywnych publicznie oraz użytkowników i użytkowniczek mediów społecznościowych.

» **Technologia deepfake**, umożliwiająca realistyczne tworzenie lub modyfikowanie obrazu, głosu i nagrań wideo, coraz częściej **wykorzystywana jest w oszustwach**, kampaniach dezinformacyjnych oraz innych działaniach naruszających dobra osobiste.

» W polskim prawie wizerunek jest dobrem osobistym, dlatego jego wykorzystanie bez zgody może prowadzić do odpowiedzialności cywilnej, a czasem także karnej.

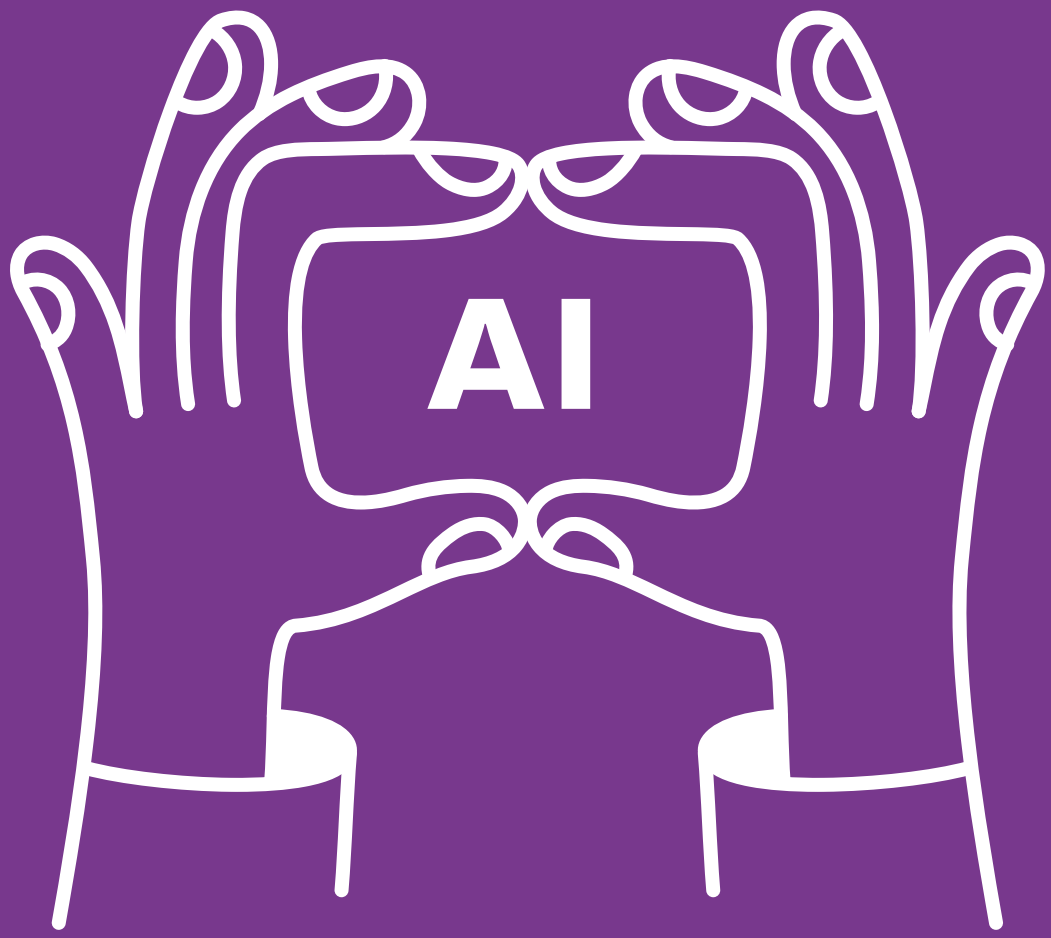
» Manipulacja audiowizualna przyjmuje różne formy – od prostego retuszu po techniki AI takie jak **lip-sync, face swap czy face reenactment**.

» W przypadku naruszenia kluczowa jest szybka reakcja: **zabezpieczenie dowodów, zgłoszenie treści** oraz w razie potrzeby podjęcie kroków prawnych i działań komunikacyjnych mających na celu zminimalizowanie szkód.

» Stosowanie prebunkingu oraz nawyku **„weryfikuj, zanim uwierzysz”** wzmacnia odporność na manipulację i dezinformację.

AI W DZIAŁALNOŚCI TWÓRCÓW – MOŻLIWOŚCI, RYZYKO I ODPOWIEDZIALNOŚĆ

Olga Zabolewicz



Czym są halucynacje AI? Czy sztuczna inteligencja pomaga, czy zagraża autentyczności twórcy? Kto jest autorem treści generowanych przez AI? Jakich danych nie wpisywać do publicznych systemów AI? Czym jest AI Act i co oznacza dla internetowych twórców i twórczyń? Jak oznaczać treści współtworzone przez AI w social mediach?

O tym przeczytasz w tym rozdziale.

AI JAKO NARZĘDZIE TWÓRCY I TWÓRCZYNI

Sztuczna inteligencja jest coraz częściej i chętniej wykorzystywana przez internetowych twórców i twórczynie. AI oferuje narzędzia, które są źródłem inspiracji, potrafi tworzyć tekst, obrazy oraz pliki wideo. Wielu influencerów i wiele influencerek zostało wykreowanych i istnieje dzięki AI[43].

GENEROWANIE POMYSŁÓW, TREŚCI I ANALIZA DANYCH

Najbardziej rozpowszechnionym zastosowaniem AI jest tworzenie treści. Narzędzia te wspierają:

- pisanie postów i opisów do social mediów,
- tworzenie scenariuszy wideo,
- edycję materiałów (np. skracanie nagrań do najbardziej angażujących fragmentów),
- generowanie i modyfikację grafik (np. zmiana tła, dodawanie lub usuwanie elementów).

AI wspiera również analizę danych – potrafi ocenić dotychczasowe treści twórcy lub twórczyni, przewidywać potencjalną popularność

43 Platz, L. (2024). Artificially Created, Truly Influential: How AI Influencers Are Taking Over Social Media. *European Youth Portal*. https://youth.europa.eu/news/artificially-created-truly-influential-how-ai-influencers-are-taking-over-social-media_en [dostęp: 30.03.2026 r.]

nowych materiałów oraz monitorować działania konkurencji pod kątem czynników wpływających na zasięgi.

Znaczącym ułatwieniem w tworzeniu ciekawych i angażujących treści przez influencerki i influencerów są narzędzia AI, które analizują dotychczasowe posty na profilu i przewidują popularność planowanego wpisu. Dodatkowo są w stanie monitorować treści konkurencji pod kątem tego, co wpływa na ich większą popularność i zasięgi[44].

HALUCYNACJE I BŁĘDY FAKTOGRAFICZNE

Istotnym ryzykiem korzystania z AI są tzw. halucynacje, czyli generowanie i przedstawianie w wiarygodny sposób informacji, które w rzeczywistości są nieprawdziwe. Systemy mogą tworzyć nieistniejące przepisy prawa, wydarzenia czy fakty[45].

Twórca lub twórczyni powinni zawsze upewnić się, że wygenerowany przez AI materiał, który jest zaplanowany do publicznego udostępnienia, nie zawiera mylących lub fałszywych treści. Jeśli nie ma pewności co do autentyczności materiału, lepiej powstrzymać się od publikacji.

AI A AUTENTYCZNOŚĆ

Zaufanie odbiorców i odbiorczyń opiera się na autentyczności, która wynika m.in. ze spójności, uczciwości, transparentności oraz rzeczywistego doświadczenia twórcy lub twórczyni.

Nadużywanie AI może tę autentyczność podważać, szczególnie gdy influencerzy i influencerki:

- generują opinie o produktach, których nie używali,
- wykorzystują AI do tworzenia nierealnych wizerunków (m.in. idealna sylwetka, „porcelanowa skóra", cyfrowe nakładanie ubrań, których się nie posiada, wygenerowane tło, np. rajska plaża, luksusowe pomieszczenie),
- nie informują o wykorzystaniu sztucznej inteligencji.

44 Marr, B. (2023). How Online Influencers And Idols Are Using Generative AI. *Forbes*. https://www.forbes.com/sites/bernardmarr/2023/12/01/how-online-influencers-and-idols-are--using-generative-ai/ [dostęp: 30.03.2026 r.]

45 Huang, L., Yu, W., Ma, W., Zhong, W., Feng, F., Wang, H., Chen, Q., Peng, W., Feng, X., Qin, B., Liu, T. (2025). A Survey on Hallucination in Large Language Models: Principles, Taxonomy, Challenges, and Open Questions. *ACM Transactions on Information Systems, 43*(2), artykuł 42. https://doi.org/10.1145/3703155

Dostępność i możliwości systemów AI sprzyjają takim praktykom, jednak istnieje duże prawdopodobieństwo, że zostaną one odebrane przez publiczność jako nieuczciwe. W konsekwencji twórca lub twórczyni ryzykuje utratą wiarygodności, spadkiem zasięgów oraz zakończeniem współpracy z markami[46].

WOJTEK KARDYŚ

NASK: **Czy sztuczna inteligencja jest zagrożeniem czy szansą dla twórców/twórczyń cyfrowych?**

Wojtek Kardyś: Sztuczna inteligencja dla twórców i twórczyn to z jednej strony potężny akcelerator kreatywności, jak i z drugiej strony medalu – poważne wyzwanie egzystencjalne. AI to szansa dla każdego trzeźwo myślącego przedsiębiorcy czy kreatora, bo pozwala na automatyzację żmudnych procesów, takich jak montaż wideo, obróbka dźwięku czy tłumaczenia, księgowość, co znacząco obniża barierę wejścia i koszty produkcji. Twórca zyskuje rolę dyrektora kreatywnego, który za pomocą agentów AI może realizować wizje wcześniej nieosiągalne bez wielkiego budżetu i ludzi pod sobą. Z drugiej strony AI stanowi realne zagrożenie dla praw autorskich i samej jakości contentu. To jest coś, czego ja osobiście się najbardziej boję, czyli ryzyko zalania rynku masową, niskiej jakości treścią, AI slopem, która niebezpiecznie zbliża nas do teorii martwego internetu. Kluczem do sukcesu będzie zatem symbioza: wykorzystanie AI do usprawnienia warsztatu przy jednoczesnym pielęgnowaniu autentyczności i osobistego stylu, którego algorytm nie jest w stanie w pełni podrobić.

ASPEKTY PRAWNE I ETYCZNE KORZYSTANIA Z AI

Autorstwo i prawa autorskie

Zgodnie z polskim prawem ochroną prawa autorskiego objęty jest utwór – każdy przejaw działalności twórczej o indywidualnym charakterze, który został ustalony w jakiejkolwiek postaci.

46 Duffek, B., Eisingerich, A. B., Merlo, O. (8 grudnia 2025). How to Do Influencer Marketing That Customers Actually Trust. *Harvard Business Review*. https://hbr.org/2025/12/how-to-do-influencer-marketing-that-customers-actually-trust [dostęp: 31.03.2026 r.].

To oznacza, że każda forma twórczości, która jest wyjątkowa i oryginalna, jest chroniona prawem autorskim. Prawem autorskim chronione są wyłącznie dzieła będące odzwierciedleniem kreatywnej pracy człowieka[47].

Korzystając z treści, grafik i innych form twórczości wygenerowanych przez sztuczną inteligencję i udostępniając je, należy pamiętać, że:

1. bezprawne jest wprowadzenie do systemu AI elementu zawierającego utwór chroniony prawem autorskim, a następnie wykorzystanie (z naruszeniem warunków korzystania), wyniku bazującego na utworze wprowadzonym do takiego systemu,
2. wykorzystanie wytworu wygenerowanego przez system AI, który jest identyczny lub bardzo podobny do już istniejącego utworu, powoduje ryzyko naruszenia prawa autorskiego twórcy oryginału.

Konsekwencje prawne

Wykorzystanie utworu niezgodnie z warunkami licencji (względnie umowy o przeniesienie autorskich praw majątkowych) może skutkować skierowaniem przeciwko naruszającemu (np. influencerowi lub influencerce) nie tylko roszczeń o charakterze cywilnoprawnym, określonych w prawie autorskim – np. żądania: zaniechania naruszania, usunięcia skutków naruszenia, naprawienia wyrządzonej szkody czy wydania uzyskanych korzyści – ale również zarzutów o charakterze karnym[48].

Wizerunek i dane osobowe

Korzystając z publicznych narzędzi generatywnej AI i umieszczając w nich swój wizerunek i dane osobowe, należy mieć świadomość, że narażamy swoją prywatność i tracimy kontrolę nad danymi wprowadzanymi do systemu. Sztuczna inteligencja przetwarza te dane, analizuje je i uczy się na nich; istnieje poważne ryzyko, że dane zostaną wykorzystane do trenowania przyszłych modeli. Wprowadzając takie dane do ogólnodostępnych narzędzi generatywnej AI, twórca/twórczyni nie ma pełnej wiedzy, gdzie i jak długo dane

47 ZAiKS Akademia. (b.d.). *Czy AI może być autorem?* https://akademia.zaiks.org.pl/wiedza/czy-ai-moze-byc-autorem-copy [dostęp 31.03.2026 r.].

48 Adamczyk, S. (red.). (2026). *Przewodnik po cyberbezpieczeństwie i sztucznej inteligencji*. NASK. https://www.nask.pl/magazyn/przewodnik-po-cyberbezpieczenstwie-i-sztucznej-inteligencji-dla-mediow-i-tworcow-cyfrowych

są przechowywane, w jakich dokładnie celach zostaną użyte i czy można te dane usunąć[49].

Oto niektóre kategorie danych, których nie należy wpisywać do publicznych narzędzi AI:

- **dane osobowe** – np. PESEL, numery dokumentów (również w postaci skanów dokumentów), adres, telefon,
- **informacje poufne** – np. umowy, bazy e-maili, strategie i plany działania,
- **dane finansowe** – np. numery kart, dane do logowania, dane z wyciągów bankowych,
- **dane wrażliwe** – np. informacje o zdrowiu, prywatne poglądy.

Zawsze należy unikać umieszczania w pytaniach kierowanych do publicznych narzędzi AI danych wrażliwych, poufnych lub takich, których wyciek będzie się wiązał z konsekwencjami prawnymi.

Możliwe konsekwencje prawne

Wprowadzenie do publicznych narzędzi AI danych osobowych, których przetwarzanie nie jest dopuszczalne lub do których nie ma się uprawnień, może skutkować odpowiedzialnością karną (art. 107 ustawy o ochronie danych osobowych) oraz cywilną – w tym obowiązkiem wypłaty odszkodowania osobie, której dane zostały naruszone (art. 82 RODO).

Powyższa lista danych i informacji ma charakter informacyjny i nie stanowi wyczerpującej listy. Każdorazowe wprowadzenie danych do ogólnodostępnego narzędzia AI powinno być poprzedzone indywidualną oceną. Warto zadać sobie pytanie: czy chcemy, aby ta informacja była publiczna?

49 Itoi, N. G. (15 października 2025). *Be Careful What You Tell Your AI Chatbot.* Stanford Institute for Human-Centered AI (HAI). https://hai.stanford.edu/news/be-careful-what-you-tell-your-ai-chatbot

TRANSPARENTNOŚĆ WOBEC ODBIORCÓW

Unijny Akt o sztucznej inteligencji (AI Act) to pierwsze na świecie kompleksowe ramy prawne regulujące rozwój, wdrażanie i użytkowanie systemów AI w UE

Wiele osób ma trudności z odróżnieniem treści generowanych przez AI od treści tworzonych przez człowieka. Aby ograniczyć ryzyko szkodliwego wykorzystania wygenerowanych treści, np. do prowadzenia kampanii dezinformacyjnych[50], wprowadzono przepisy prawa, które mają poprawić poziom transparentności użycia treści generowanych przez AI.

Unijny Akt o sztucznej inteligencji (tzw. AI Act)[51] wprowadza obowiązek ujawniania, że tekst został wygenerowany lub zmodyfikowany przy użyciu systemu AI, jeśli jest publikowany w celu informowania społeczeństwa o sprawach leżących w interesie publicznym.

Obowiązek ten nie znajduje zastosowania w przypadku, gdy treść została poddana weryfikacji przez człowieka lub kontroli redakcyjnej, a odpowiedzialność za jej publikację ponosi określony podmiot. Spełnienie tych warunków pozwala odstąpić od oznaczania materiału jako wygenerowanego lub zmienionego przez AI.

Odrębne zasady dotyczą treści wizualnych i audiowizualnych. W przypadku generowania lub modyfikowania obrazów, nagrań audio lub wideo – w szczególności z wykorzystaniem technologii deepfake – konieczne jest wyraźne poinformowanie odbiorców, że materiał został sztucznie wygenerowany lub zmanipulowany. W odniesieniu do treści o charakterze artystycznym, satyrycznym lub stanowiących fikcję obowiązek ten może zostać ograniczony do ogólnej informacji o wykorzystaniu AI, pod warunkiem, że nie utrudnia ona odbioru materiału.

Obowiązek ten nie znajduje zastosowania w przypadku, gdy treść została poddana weryfikacji przez człowieka lub kontroli redakcyjnej, a odpowiedzialność za jej publikację ponosi określona osoba lub firma. Spełnienie tych warunków pozwala odstąpić od oznaczania materiału jako wygenerowanego lub zmienionego przez AI.

50 Gallegos, I. O., Shani, C., Shi, W., Bianchi, F., Gainsburg, I. B., Jurafsky, D., Willer, R. (30 lipca 2025). *Labeling AI-Generated Content May Not Change Its Persuasiveness.* Stanford Institute for Human-Centered AI. https://hai.stanford.edu/policy/labeling-ai-generated-content-may-not-change-its-persuasiveness [dostęp: 31.03.2026 r.]

51 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji (akt w sprawie sztucznej inteligencji)

Jeśli masz wątpliwości, czy Twój materiał utworzony lub współtworzony przez sztuczną inteligencję należy oznaczyć, to oznacz go. W ten sposób udowadniasz, że działasz transparentnie i szanujesz swoich odbiorców[52].

ODPOWIEDZIALNOŚĆ MAREK I AGENCJI REKLAMOWYCH ORAZ REKLAMODAWCÓW

W omawianej branży oprócz influencerów i influencerek odpowiedzialność za sposób korzystania z systemów AI i skutki jego wykorzystania ponoszą również marki, reklamodawcy oraz agencje reklamowe. W przypadku publikacji wszelkich materiałów obowiązuje podstawowa zasada – to, że treść została stworzona przy użyciu sztucznej inteligencji, nie oznacza, że z prawnego punktu widzenia jest ona bez autora albo że nikt nie ponosi za nią odpowiedzialności[53].

Twórco, twórczyni – rekomendujemy sprawdzenie, czy w umowie pomiędzy Tobą a reklamodawcą lub agencją reklamową znajdują się odpowiednie postanowienia o zakazie/możliwości korzystania przez Ciebie z narzędzi AI, a w przypadku istnienia takiej możliwości – o konieczności oznaczania takich materiałów publikowanych w mediach społecznościowych.

DOBRE PRAKTYKI UŻYCIA AI W PROMOCJI

Kiedy i jak informować o użyciu AI

Influencer lub influencerka powinni oznaczać materiały utworzone lub współtworzone przez sztuczną inteligencję, które publikują na swoich kanałach w mediach społecznościowych, w sposób czytelny, jednoznaczny oraz zrozumiały dla każdego odbiorcy.

Oznaczenie powinno być widoczne zarówno dla stałych obserwatorów i obserwatorek, jak i dla tych, którzy zapoznają się z udostępnionymi materiałami po raz pierwszy.

52 Adamczyk, S. (red.). (2026). *Przewodnik po cyberbezpieczeństwie i sztucznej inteligencji.* NASK. https://www.nask.pl/magazyn/przewodnik-po-cyberbezpieczenstwie-i-sztucznej-inteligencji-dla-mediow-i-tworcow-cyfrowych

53 Zubrová, L. (2026). AI law in influencer marketing: what every publisher needs to know. *eHUB*. https://ehub.cz/en/blog/post/how-to-use-ai-for-content-creation-legally-and-responsibly [dostęp: 31.03.2026 r.]

Dodatkowo w przypadku treści reklamowych należy zaznaczyć zarówno wykorzystanie sztucznej inteligencji, jak i wszelkie formy współpracy reklamowej, zgodnie z rekomendacjami Prezesa UOKiK[54].

Weryfikacja treści generowanych przez narzędzia

Nie tylko twórcy i twórczynie, ale również publiczność powinna rozwijać umiejętność krytycznej oceny wyników generowanych przez AI, w szczególności pod kątem zgodności z prawem i stanem faktycznym.

Jeśli zdecydowałaś/zdecydowałeś się korzystać z narzędzi AI, to zawsze, przed udostępnieniem publicznie materiału, sprawdź go, obejrzyj lub przeczytaj, ewentualnie popraw i prawidłowo oznacz.

Pamiętaj – odpowiedzialność za treść materiału, który udostępniasz, zawsze spoczywa na człowieku, a nie na systemie AI.

**Powyższy rozdział odnosi się do twórców i twórczyń wykorzystujących narzędzia AI w swojej działalności. Publikacja nie obejmuje przypadków tworzenia i funkcjonowania tzw. wirtualnych influencerów i influencerek (wygenerowanych w całości cyfrowo, nieposiadających ludzkiego pierwowzoru).*

Sprawdź swój materiał przed publikacją

Zanim opublikujesz treść stworzoną lub wspartą przez AI, zadaj sobie kilka pytań

- Czy wszystkie informacje są prawdziwe i możliwe do zweryfikowania?
- Czy nie publikuję czegoś, czego sam/a nie rozumiem lub nie sprawdziłem/am?
- Czy materiał nie wprowadza odbiorców w błąd (np. co do efektów produktu, wyglądu, miejsca)?
- Czy jasno komunikuję, że treść została stworzona lub zmodyfikowana przy użyciu AI (jeśli jest to wymagane)
- Czy sam/a uznał(a)bym ten materiał za uczciwy jako odbiorca?
- Jeśli na któreś z tych pytań odpowiedź brzmi „nie” lub „nie wiem” – warto zatrzymać się i poprawić materiał przed publikacją.

54 UOKiK. (2022 r.). *Rekomendacje Prezesa UOKiK dotyczące oznaczania treści reklamowych przez influencerów w mediach społecznościowych*. https://uokik.gov.pl/influencer-marketing [dostęp: 31.03.2026 r.]

Pytanie do refleksji

Czy jestem w stanie wziąć pełną odpowiedzialność za ten materiał – nawet jeśli został stworzony przy wsparciu AI?

W pigułce

- Sztuczna inteligencja wspiera generowanie pomysłów, analizę danych i tworzenie treści, ale wiąże się także z ryzykiem błędów, utraty autentyczności oraz naruszeń prawa.
- Szczególnym zagrożeniem są tzw. halucynacje AI, czyli wiarygodnie brzmiące, ale nieprawdziwe informacje – systemy mogą tworzyć nieistniejące przepisy prawa, wydarzenia czy fakty, dlatego treści generowane przez **AI trzeba zawsze sprawdzać, aby nie ośmieszyć się i nie stracić zaufania odbiorców**.
- Twórcy i twórczynie internetowe podkreślają, że nadmierne lub nieoznaczone korzystanie z AI może osłabiać autentyczność przekazu i prowadzić do spadku zaufania społeczności oraz partnerów biznesowych.
- **Korzystanie z treści generowanych przez AI może naruszać prawa autorskie**, zwłaszcza gdy są one bardzo podobne do już istniejących utworów albo powstały na podstawie materiałów użytych bez odpowiedniej zgody.
- Nowe przepisy, w tym Akt w sprawie sztucznej inteligencji, wprowadzają obowiązek większej przejrzystości w korzystaniu z AI, m.in. poprzez oznaczanie treści tworzonych z jego pomocą. **Odpowiedzialność za takie materiały ponoszą nie tylko twórcy/twórczynie, lecz także marki, agencje i reklamodawcy.**

WIDOCZNOŚĆ W SIECI A DOBROSTAN PSYCHICZNY – PRESJA, MECHANIZMY I STRATEGIE RADZENIA SOBIE

Anna Pudłowska

Jaki wpływ mają liczba polubień i zasięgi na nastrój oraz samoocenę? Dlaczego work–life balance to coś więcej niż tylko modne hasło? Czy da się naprawdę „wylogować" z pracy w internecie? Jak rozpoznać pierwsze oznaki wypalenia twórczego? Czym jest przeciążenie informacyjne i jak wpływa na kreatywność? Czy można tworzyć angażujące treści bez presji „cyferek"? Jak dbać o higienę cyfrową, nie rezygnując z obecności online?

O tym przeczytasz w tym rozdziale.

Widoczność w mediach społecznościowych przestała być wyłącznie efektem obecności online – dziś oznacza funkcjonowanie w środowisku stałej oceny, porównań i mierzalnych wyników. Zasięgi, polubienia czy komentarze nie są już tylko danymi, ale coraz częściej stają się emocjonalnym punktem odniesienia, wpływając na samopoczucie, decyzje i ocenę własnej pracy.

W takim środowisku bardzo łatwo o przesunięcie: od analizy do emocjonalnej reakcji. To, co miało wspierać rozwój osobisty i budowanie marki, zaczyna pełnić rolę punktu odniesienia dla nastroju i poczucia własnej wartości. Badania pokazują, że intensywne korzystanie z platform oraz częste porównywanie się z innymi wiążą się z niższą samooceną i częstszym doświadczaniem trudnych emocji[55].

Widoczność staje się jednocześnie zasobem, narzędziem pracy i warunkiem utrzymania pozycji zawodowej. To sprawia, że presja nie wynika wyłącznie z indywidualnych predyspozycji, lecz jest wpisana w sposób działania platform, które premiują tempo, regularność i zaangażowanie. W praktyce łatwo wejść w powtarzalny cykl: publikowanie, sprawdzanie wyników, dostosowywanie treści i reagowanie na bieżąco. Taki rytm może być skuteczny, ale przy dłuższym utrzymaniu bywa obciążający – szczególnie wtedy, gdy liczby zaczynają być odbierane jako bezpośredni wskaźnik osobistej wartości.

55 Azayem, A. K., Nawaz, F. A., Jeyaseelan, L., Kair, H. M., Sultan, M. A. (2023), Beyond the filter: Impact of popularity on the mental health of social media influencers. Digital Health, 10. https://doi.org/10.1177/20552076241287843

W efekcie praca w mediach społecznościowych rzadko daje poczucie pełnej stabilności. Wysoka zmienność wyników, ciągła informacja zwrotna i nieprzewidywalność reakcji odbiorców sprawiają, że łatwo o napięcie, przeciążenie i stopniowe przesuwanie granic między pracą, tożsamością a odpoczynkiem.

MECHANIZMY, KTÓRE ZACZYNAJĄ PRZEJMOWAĆ KONTROLĘ NAD ZACHOWANIEM

Z czasem sprawdzanie wyników przestaje być elementem analizy, a zaczyna regulować emocje. Pojawia się nawyk częstego monitorowania, a liczby zaczynają wpływać na nastrój – ich wzrost przynosi ulgę, a spadek napięcie.

Mechanizm ten odpowiada uzależnieniom behawioralnym: obejmuje potrzebę coraz częstszego kontaktu z bodźcem, trudność w jego ograniczeniu oraz kontynuowanie praktyki mimo negatywnych skutków[56]. W przypadku mediów społecznościowych dodatkowo wzmacnia go system nieregularnych „nagród", takich jak nagłe wzrosty zasięgów czy zaangażowania.

Więcej czasu online i sprawdzania reakcji – większe napięcie i spadki nastroju

W efekcie liczby przestają być neutralną informacją, a zaczynają pełnić funkcję emocjonalnego barometru i sposobu odzyskiwania poczucia kontroli. Badania wskazują również, że intensywne korzystanie z platform wiąże się z większą liczbą negatywnych emocji[57]. Im więcej czasu spędzanego online i im częstsze sprawdzanie reakcji, tym łatwiej o napięcie, frustrację i spadki nastroju. Zmienność wyników oraz stała ekspozycja na ocenę sprawiają, że trudniej zachować dystans i spokój, wobec tego, co dzieje się wokół publikowanych treści.

Utożsamianie wyników z własną wartością

Jednym z najbardziej obciążających mechanizmów jest utożsamianie wyników z własną wartością. W takiej sytuacji spadek zasięgu bywa odczuwany jak osobista porażka, a wzrost jak potwierdzenie kompetencji.

56 Poli, R. (2017). Internet addiction update: diagnostic criteria, assessment and prevalence. *Neuropsychiatry (London), 7*(1), 4–8. http://doi.org/10.4172/Neuropsychiatry.1000171

57 Azayem, A. K., Nawaz, F. A., Jeyaseelan, L., Kair, H. M., Sultan, M. A. (2023), Beyond the filter: Impact of popularity on the mental health of social media influencers. *Digital Health, 10*. https://doi.org/10.1177/20552076241287843

Problem polega na tym, że wyniki w mediach społecznościowych są zmienne i nie w pełni zależne od jakości pracy. Gdy zaczynają być traktowane jako ocena osoby, pojawia się niestabilność emocjonalna i ciągłe napięcie.

Statystyki powinny pozostać narzędziem, a nie miarą wartości. Pomocne jest ograniczenie ich sprawdzania do konkretnych momentów, oddzielenie tworzenia od analizy oraz traktowanie potrzeby ciągłego monitorowania jako sygnału przeciążenia.

Presja ciągłej obecności oznacza poczucie, że trzeba być stale aktywnym – publikować, reagować i nie znikać z pola widzenia publiczności. W mediach społecznościowych brak aktywności bywa odczuwany jako ryzyko spadku widoczności, co utrudnia odpoczynek i sprzyja pracy bez wyraźnych granic. Zjawisku temu często towarzyszy FOMO (*fear of missing out*). W praktyce może on wzmacniać potrzebę ciągłego sprawdzania powiadomień i utrudniać pełne „wyjście z pracy".

FOMO (fear of missing out)
lęk przed tym, że coś nas omija: ważna informacja, reakcja odbiorców lub okazja do zwiększenia zasięgu. W kontekście pracy online może prowadzić do ciągłego sprawdzania powiadomień, trudności w odpoczynku i poczucia, że „trzeba być na bieżąco" niezależnie od pory dnia.

Takie środowisko premiuje dostępność i szybkie reakcje, dlatego łatwo wejść w tryb ciągłego bycia na bieżąco. Obejmuje to nie tylko publikowanie treści, ale też odpowiadanie na wiadomości, moderowanie komentarzy i reagowanie na wszelkie zaistniałe sytuacje w czasie rzeczywistym[58].

W efekcie pojawia się stan stałej gotowości, który utrudnia odłączenie się od pracy i zwiększa ryzyko przeciążenia.

58 Logan, K., Bright, L. F., Grau, S. L. (2018). "Unfriend me, please!": Social media fatigue and the theory of rational choice. *Journal of Marketing Theory and Practice, 26*(4), 357–367. https://doi.org/10.1080/10696679.2018.1488219 [dostęp: 30.04.2026 r.]

Porównywanie się do innych

Porównywanie się do innych to jeden z głównych mechanizmów powodujących obciążenie psychicznie. Występuje także poza mediami społecznościowymi, jednak w środowisku online jest znacznie intensywniejsze i częstsze. Najczęściej przyjmuje formę porównań „w górę" – do osób postrzeganych jako bardziej skuteczne lub rozpoznawalne. Badania pokazują, że im częstsze takie porównania, tym większy ich wpływ na obniżenie samooceny i pogorszenie nastroju[59]. Z czasem może to prowadzić do mierzenia własnej wartości cudzymi wynikami oraz poczucia, że dotychczasowe osiągnięcia są niewystarczające.

ZACIERANIE GRANIC MIĘDZY PRACĄ A ŻYCIEM PRYWATNYM

W środowisku cyfrowym granice między pracą a życiem prywatnym łatwo się rozmywają. Stała dostępność i szybka reakcja sprawiają, że aktywność zawodowa przenika do czasu odpoczynku. Telefon staje się jednocześnie narzędziem pracy, kanałem kontaktu i źródłem informacji zwrotnej. W efekcie odpoczynek często nie oznacza pełnego odłączenia, lecz jedynie zmianę aktywności. Z czasem pojawia się trudność w „wyjściu z pracy" i poczucie ciągłej gotowości.

Z perspektywy work–life balance oznacza to osłabienie granic między rolą zawodową a prywatną – w efekcie nawet czas wolny bywa zajęty analizą wyników, planowaniem treści czy sprawdzaniem reakcji.

KIEDY WORK–LIFE BALANCE JEST ZABURZONY

praca wchodzi w czas wolny

odpoczynek = „tylko szybkie sprawdzenie"

brak momentu wylogowania = rośnie zmęczenie i napięcie

59 Le Blanc-Brillon, J., Fortin, J.-S., Lafrance, L., Hétu, S. (2025). The associations between social comparison on social media and young adults' mental health. *Frontiers in Psychology, 16*, 1597241. https://doi.org/10.3389/fpsyg.2025.1597241

WYPALENIE TWÓRCZE

Wypalenie twórcze to stan wyczerpania emocjonalnego, poznawczego i motywacyjnego, wynikający z ciągłej presji tworzenia, utrzymywania uwagi i reagowania na zmienne oczekiwania. Nie oznacza braku talentu ani kompetencji – najczęściej jest efektem modelu pracy, który nie daje przestrzeni na odpoczynek, wymaga stałej obecności i sprowadza twórczość do osiągania założonych wyników. Objawia się zmęczeniem, spadkiem kreatywności, brakiem satysfakcji z pracy oraz poczuciem pustki nawet przy dobrych wynikach. Może też pojawiać się większa wrażliwość na komentarze i spadek motywacji do działania.

Badania pokazują, że wraz ze wzrostem liczby obserwujących i czasu spędzanego online rośnie poziom stresu, lęku oraz negatywnych emocji[60]. Z kolei raport badaczy z Uniwersytetu Harvarda wskazuje, że coraz więcej osób tworzących treści doświadcza problemów ze zdrowiem psychicznym związanych z presją widoczności, niestabilnością wyników i ciągłą oceną[61].

- **10% twórców i twórczyń** deklaruje myśli samobójcze związane z pracą.
- **Twórcy i twórczynie** są prawie dwukrotnie bardziej narażeni na takie myśli niż ogólna populacja.
- **Ponad 50% twórców i twórczyń** doświadcza pogorszenia zdrowia psychicznego (stres, wypalenie, presja wyników).

Przeciążenie informacyjne

Przeciążenie informacyjne pojawia się, gdy liczba bodźców i informacji przekracza możliwość ich spokojnego przetworzenia. W środowisku mediów społecznościowych jest to częste – jednoczesne analizowanie danych, odpowiadanie na wiadomości, śledzenie trendów i tworzenie nowych materiałów prowadzi

60 Azayem, A. K., Nawaz, F. A., Jeyaseelan, L., Kair, H. M., Sultan, M. A. (2023). Beyond the filter: Impact of popularity on the mental health of social media influencers. *Digital health, 10*. https://doi.org/10.1177/20552076241287843

61 Roeder, A. (2025). *Content creators are struggling with mental health, study finds*. Harvard T.H. Chan School of Public Health. https://hsph.harvard.edu/news/content-creators-are-struggling-with-mental-health-study-finds/ [dostęp: 06.04.2026 r.]

do nadmiaru bodźców. Problem dotyczy nie tylko ich liczby, ale też zmienności i presji szybkiej reakcji.

W efekcie trudno utrzymać koncentrację i dystans, a dłuższy czas spędzany na robiemiu wielu czynności na raz i to często online wiąże się z większym napięciem i negatywnymi emocjami.

KAROLINA CZAK

NASK: **Internet jest zalewany treściami, które generują silne, często negatywne emocje. Udział w tym mają też twórczynie i twórcy cyfrowi. Czy można tworzyć treści, które nie wywołują negatywnych emocji, bez utraty zasięgów?**

K. Czak: Na tym kiedyś polegała klikalność programów w TV, a teraz na tym polegają social media – najlepiej klikają się treści, które wywołują emocje, najlepiej te negatywne. To tam ludzie najchętniej się udzielają, komentują, wchodzą w (często agresywne) dyskusje, a algorytm to podchwytuje. Myślę, że można, a nawet i trzeba tworzyć treści, które nie sieją negatywnych emocji – żeby przełamać ten schemat. I nie poddawać się, jeśli nie wszystko pójdzie w viral. Część odbiorców odczuwa zmęczenie wszechobecnym natłokiem negatywnych emocji i zaczyna szukać spokojniejszych treści. Inni, widząc takie podejście, mogą pójść w tym kierunku – odciąć się od kontrowersyjnych i nieprzyjemnych materiałów, dzięki czemu wartościowe treści zaczynają osiągać coraz lepsze „cyferki". Nie „odczarujemy" internetu w pełni, ale możemy robić tyle, ile się da.

Nadreaktywność na komentarze

Nadreaktywność na komentarze oznacza silne i impulsywne reagowanie na opinie odbiorców. Może przejawiać się częstym sprawdzaniem reakcji, nadmiernym przeżywaniem pojedynczych uwag lub angażowaniem się w emocjonalne dyskusje. W takim środowisku komentarze przestają być tylko opinią – zaczynają być odbierane jako sygnał zagrożenia dla wizerunku. Dodatkowo ich publiczny i trwały charakter zwiększa presję oraz skłonność do reagowania. W efekcie komunikacja może przestać służyć relacji, a zaczyna pełnić funkcję ciągłej obrony.

KAROLINA CZAK

NASK: **Ludzie, którzy pracują na etacie po 8 godzinach kończą pracę. Praca twórcy internetowego to coś zupełnie innego, bo w internecie nie ma wolnych weekendów, ani urlopów. Czy Ty jako twórczyni odczuwasz FOMO? Czy potrafisz się „wylogować”? W jaki sposób odpoczywasz od swojej aktywności w internecie?**

K. Czak: To mnie zaskoczyło w tej pracy – to znaczy nie spodziewałam się, że będzie to aż taką trudnością. Człowiek niby wie, że nie musi cały czas sprawdzać powiadomień i być na bieżąco, ale w sumie jak już leży tu obok ten telefon, to czemu by nie zerknąć? Zaczęłam celowo wychodzić na spacery BEZ telefonu, żeby nie być w stanie w niego patrzeć. Organizowanie sobie pracy w „blokach” na kilka godzin i później brak (własnego) zezwolenia (ale to wymaga dyscypliny, wiadomo) na dotykanie telefonu i laptopa w przerwach między tymi blokami też było jakimś rozwiązaniem. Ale z drugiej strony, czy zrobienie kotom filmiku, jak się bawią, to moje prywatne życie czy praca? Skoro elementem pracy jest dzielenie się fragmentami swojej codzienności?

Granica się rozmywa, kiedy nasza twórczość jest o naszym życiu, bo nie zrobimy sobie np. służbowego telefonu do instagrama i drugiego do spraw prywatnych, skoro tymi prywatnymi często dzielimy się na socialach. Po pół roku pracy jako full time content creator odczuwałam mocno tę „zamułę” ekranem. Zaczęłam kombinować i szukać czegoś, co mogłoby mi pomóc. Na myśl przychodził wolontariat w schronisku dla zwierząt, ale po pierwsze nie miałam tam zbyt dobrego dojazdu zbiorkomem, a po drugie nieco bałam się, że zacznę przywozić te zwierzaki do domu bo, nie oszukujmy się, mam do nich miękkie serce.

Z tyłu głowy była też myśl o złapaniu jakiejś „normalnej” pracy np. na 1/4 etatu – w kawiarni bądź gdziekolwiek, nie dla pieniędzy, tylko dla konieczności odcięcia się od telefonu. Taki trochę problem pierwszego świata, który świadczy o bardzo uprzywilejowanej pozycji, jestem świadoma jak to brzmi i nie mówię, że, o Jezu, taka biedna nieszczęśliwa i tak mi ciężko – tylko że no, ludzki mózg odczuwa to przeładowanie światłem niebieskim. Ostatecznie wybrałam zwierzaki – ale nie psiaki w schronisku, tylko wróciłam do pasji z dzieciństwa,

czyli do jeździectwa. Kupiłam konia, zaczęłam być w stajni 6–7 razy w tygodniu. Mając pół dnia wyjęte z harmonogramu na dojazd tam i zrobienie z Ufo treningu, opieki, pielęgnacji, jakoś się „ożywiłam". Czyszcząc konia, nie scrollujemy instagrama, przy kowalu czy weterynarzu nie myślimy o powiadomieniach. Oczywiście z koni też (jak widać) robię trochę kontentu (co potwierdza tezę, że nigdy nie odetniemy się na 100%), ale wychodzi to przy okazji i dosyć nieinwazyjnie, bo idąc z koniem na trening szybko nagram kilkusekundowe ujęcie i z powrotem schowam telefon, a filmik obrobię i wrzucę z jakimś zabawnym opisem dopiero po powrocie do domu, kiedy usiądę do pracy.

Można więc wiele mówić o sposobach, takich jak pilnowanie regularnego ruchu, świeżego powietrza bez patrzenia w elektronikę, o czasie bez ekranu – ale wydaje mi się, że najbezpieczniej jest jednak (może nie od razu po przejściu na full time, ale po jakimś czasie na pewno) znaleźć sobie coś, co zmusi nas do wyjścia z domu i „dotknięcia trawy", porozmawiania z ludźmi, bo nikt nie jest stworzony do tego, żeby siedzieć w zamkniętych czterech ścianach i tylko nagrywać rolki. Poza tym, nie mając kontaktu ze światem, możliwe że skończą nam się na nie pomysły XD więc tak, zdecydowanie warto mieć chociażby jakiś wolontariat, spotkania, zajęcia – może tak jak ja sięgnąć po zapomnianą pasję.

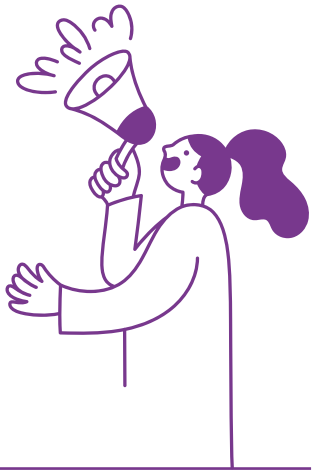
STRATEGIA HIGIENY CYFROWEJ

Zarządzanie obecnością w sieci wymaga świadomego dbania o równowagę i ograniczania przeciążenia informacyjnego. Poniższe zasady traktuj jako propozycję dobrych praktyk, które możesz dostosować do swoich potrzeb i stylu pracy:

- kontroluj kontakt ze statystykami i oddziel analizę od procesu tworzenia;
- traktuj wyniki jako informację zwrotną, a nie wyznacznik swojej wartości;
- ogranicz porównywanie się do innych i nadmiar bodźców;
- wyznaczaj granice w komunikacji i unikaj impulsywnych reakcji;
- dbaj o rytm pracy, regenerację i reaguj na sygnały przeciążenia.

Pytanie do refleksji

A Ty – co robisz, aby zadbać o swoją równowagę w sieci?



W pigułce

- **Zasięgi, polubienia i komentarze** – a także ich częste sprawdzanie – mogą negatywnie wpływać na nastrój i samoocenę. Statystyki powinny być jedynie wskazówką, **a nie wyznacznikiem sukcesu czy porażki** – najważniejsze jest tworzenie, a nie zapętlanie się w „cyferkach".
- Presja ciągłej obecności online utrudnia odpoczynek i zaciera granice między pracą a życiem prywatnym, co może prowadzić do przeciążenia informacyjnego i wypalenia twórczego – dlatego warto dbać o swoje granice.
- Najważniejsze jest **skupienie się na tworzeniu wartościowych treści**, a nie na samych wynikach. Pomaga w tym świadome podejście do statystyk, ograniczanie porównywania się z innymi oraz dbanie o higienę cyfrową.
- Sami twórcy i twórczynie przyznają, że praca w internecie wygląda inaczej niż wiele innych zawodów – często nie ma tu wyraźnych weekendów ani urlopów. Pojawia się FOMO i trudność z „wylogowaniem się" z pracy. **Odpoczynek jest jednak bardzo potrzebny.** Nie jest to łatwe, ale można się tego nauczyć, trzeba tylko poszukać sposobów, które pomogą zadbać o równowagę.

MAPKA POMOCOWA – GDZIE ZGŁASZAĆ I SZUKAĆ WSPARCIA

W przypadku naruszenia wizerunku, incydentu cyberbezpieczeństwa lub podejrzenia oszustwa warto działać szybko i korzystać z dostępnych form pomocy.

Poniższa mapa pokazuje, gdzie zgłosić problem i gdzie szukać wsparcia.

Zgłaszanie treści na platformach społecznościowych

W przypadku naruszenia wizerunku, hejtu lub fałszywych treści pierwszym krokiem powinno być zgłoszenie materiału bezpośrednio na platformie, na której został opublikowany.

Większość serwisów (np. Facebook, Instagram, TikTok, YouTube) posiada wbudowany przycisk „Zgłoś" dostępny przy poście, komentarzu lub profilu.

Jak to zrobić?

- **Kliknij w menu** (np. „..." obok treści),
- **wybierz opcję „Zgłoś",**
- **wskaż powód** (np. podszywanie się, hejt, naruszenie wizerunku),
- **prześlij zgłoszenie** zgodnie z instrukcjami platformy.

Cyberbezpieczeństwo i oszustwa internetowe

Zgłoszenie do CERT Polska można dokonać przez:

- formularz online: **https://incydent.cert.pl**,
- SMS: przekazując bez zmian podejrzaną wiadomość na numer **8080**,
- aplikację mObywatel: moduł „Bezpiecznie w sieci".

Nielegalne i szkodliwe treści

Materiały przedstawiające seksualne wykorzystywanie dziecka, twardą pornografię umieszczoną na ogólnodostępnych stronach, wpisy promujące rasizm i ksenofobię i inne nielegalne treści możesz zgłosić na stronie **Dyżurnet.pl**.

Dezinformacja i fałszywe treści

Jeśli materiał wprowadza w błąd lub jest manipulacją, możesz przekazać go ekspertom za pomocą strony: **NASK – Zgłoś dezinformację**.

Kradzież konta lub dostępów

Jeśli konto zostało przejęte:

- skorzystaj z opcji odzyskiwania konta na platformie,
- wyloguj pozostałe sesje – zakończ dostęp przestępców,
- zmień hasła (także do powiązanych usług),
- włącz weryfikację dwuetapową (2FA).

Naruszenie prawa i wizerunku

W poważnych przypadkach skontaktuj się z organami państwowymi:

- Policja (zgłoszenie przestępstwa – np. oszustwo, kradzież tożsamości),
- UOKiK (w przypadku oszustw konsumenckich i fałszywych reklam).

Wsparcie i pomoc psychologiczna

Dzwoniąc pod następujące numery możesz otrzymać pomoc ekspertów i ekspertek od zdrowia psychicznego oraz doradztwa kryzysowego:

- **800 70 2222** – Centrum Wsparcia (całodobowo),
- **116 123** – linia wsparcia emocjonalnego dla dorosłych,
- **800 108 108** – wsparcie w kryzysie psychicznym.

Hejt

Bezpośrednio na platformie

Każdy serwis społecznościowy (Facebook, Instagram, TikTok, YouTube, LinkedIn) umożliwia zgłaszanie obraźliwych treści, komentarzy czy wiadomości. To najszybszy sposób na ich usunięcie lub ograniczenie zasięgu.

Policja lub prokuratura

Jeśli hejt przybiera formę gróźb, stalkingu, zniesławienia lub naruszenia dóbr osobistych – można zgłosić sprawę organom ścigania. Warto zabezpieczyć dowody (zrzuty ekranu, linki, daty).

Pomoc prawna

Twórcy internetowi mogą skorzystać z pomocy prawnika – szczególnie gdy dochodzi do naruszenia wizerunku, reputacji lub działalności zawodowej.

Wsparcie psychologiczne

Długotrwały hejt może wpływać na zdrowie psychiczne. Warto skorzystać ze wsparcia specjalisty lub organizacji oferujących pomoc dla dorosłych.

PODSUMOWANIE

Współczesna obecność w mediach społecznościowych to nie tylko tworzenie treści, ale przede wszystkim świadome zarządzanie wpływem, odpowiedzialnością i własnym wizerunkiem. Rozwój mediów społecznościowych sprawił, że twórcy i twórczynie cyfrowe stali się nie tylko autorami i autorkami treści, ale także przewodnikami i przewodniczkami po świecie informacji, technologii i relacji online dla innych. Jak podkreślają sami influencerzy i influencerki, ich działalność nie ogranicza się do publikowania treści, wiąże się także z realnym wpływem na postawy, wybory czy zachowania odbiorców i odbiorczyń w internecie. Oddziałują oni na sposób myślenia swojej publiczności, na to, jak należące do niej osoby komunikują się w sieci oraz jakie wzorce zachowań mogą przyjmować i powielać w przestrzeni cyfrowej. W takim kontekście cyberbezpieczeństwo przestaje być zagadnieniem dodatkowym, staje się niezwykle ważnym elementem odpowiedzialnej obecności w sieci.

Treści przedstawione w publikacji pokazują, że bezpieczeństwo cyfrowe twórców i twórczyń obejmuje wiele wzajemnie powiązanych obszarów: ochronę prywatności, świadome zarządzanie wizerunkiem, reagowanie na dezinformację, odpowiedzialne publikowanie materiałów z udziałem innych osób (szczególnie najmłodszych użytkowników internetu) oraz rozumienie konsekwencji korzystania z nowych technologii, w tym narzędzi sztucznej inteligencji. Każdy z tych elementów wpływa zarówno na bezpieczeństwo działalności twórcy lub twórczyni, jak i na zaufanie odbiorców i odbiorczyń.

Z analizy omawianych zagadnień wynikają szczególnie istotne wnioski. Przede wszystkim cyberbezpieczeństwo influencerów

i influencerek zaczyna się od świadomego zarządzania własną obecnością w sieci. Obejmuje to nie tylko techniczne zabezpieczenie kont, ale także przemyślane decyzje dotyczące publikowania informacji o sobie, swojej rodzinie i codziennym życiu. Granica między sferą prywatną a publiczną powinna być wyznaczana w sposób celowy i konsekwentny.

Twórcy i twórczynie powinni zwracać szczególną uwagę na znaczenie publikowanych przez siebie porad, rekomendacji i opinii oraz na odpowiedzialność, jaka się z tym wiąże, ponieważ mogą realnie wpływać na decyzje i zachowania odbiorców i odbiorczyń. Szczególnej rozwagi wymagają zwłaszcza treści dotyczące zdrowia, finansów, bezpieczeństwa czy stylu życia, dlatego warto przekazywać je rzetelnie i jasno zaznaczać, czy wynikają z własnych doświadczeń, czy z wiedzy specjalistycznej. Takie podejście wzmacnia wiarygodność i pomaga ograniczyć ryzyko wprowadzania publiczności w błąd. Równie ważna jest rola twórców i twórczyń cyfrowych w przeciwdziałaniu dezinformacji. Ich wiarygodność oraz zasięgi sprawiają, że mogą zarówno nieświadomie wzmacniać fałszywe przekazy, jak i skutecznie je ograniczać poprzez odpowiedzialne udostępnianie treści, weryfikowanie źródeł oraz budowanie krytycznego podejścia do informacji wśród odbiorców i odbiorczyń.

Szczególnej uwagi wymaga publikowanie wizerunku dzieci, które powinno zawsze uwzględniać ich prawo do prywatności oraz długofalowe konsekwencje obecności w sieci. Decyzje podejmowane przez dorosłych dziś mogą wpływać na bezpieczeństwo i dobrostan młodych osób w przyszłości.

Istotnym wyzwaniem dla współczesnych twórców i twórczyń pozostaje także dynamiczny rozwój technologii generatywnych, w tym deepfake oraz narzędzi sztucznej inteligencji. Technologie te otwierają nowe możliwości pracy kreatywnej, ale jednocześnie zwiększają ryzyko manipulacji wizerunkiem, podszywania się pod inne osoby oraz nieuprawnionego wykorzystania ich treści. Wymaga to stałego rozwijania kompetencji cyfrowych i świadomego korzystania z nowych narzędzi.

Nie bez znaczenia pozostaje również znajomość procedur reagowania na naruszenia bezpieczeństwa oraz wiedza o dostępnych

formach wsparcia. Świadomość, gdzie zgłaszać incydenty i jak szukać pomocy, pozwala szybciej i skuteczniej ograniczać skutki zagrożeń.

I najważniejsze:

Cyberbezpieczeństwo w działalności twórców i twórczyń cyfrowych nie jest jednorazowym działaniem, lecz procesem wymagającym uważności, refleksji i systematycznego rozwijania kompetencji. To proces, o który trzeba dbać na co dzień. Influencerzy i influencerki, którzy traktują bezpieczeństwo jako część swojej odpowiedzialności, nie tylko chronią siebie, lecz także pomagają budować bezpieczniejszą i bardziej świadomą przestrzeń w internecie dla swoich odbiorców i odbiorczyń.

Cyfrowy Twórco, Cyfrowa Twórczyni, pamiętaj, że...

Odpowiedzialność to również Twoja przewaga konkurencyjna.

Jeśli działasz transparentnie, rzetelnie i zgodnie z zasadami, budujesz trwałe zaufanie odbiorców i odbiorczyń oraz partnerów biznesowych. To właśnie konsekwencja i wiarygodność w dłuższej perspektywie wzmacniają Twoją pozycję w sieci.

Bezpieczeństwo to element profesjonalizmu

Dbając o bezpieczeństwo cyfrowe, prywatność i dane, pokazujesz, że działasz świadomie i odpowiedzialnie. Kontrola dostępu do kont, przemyślane publikowanie treści oraz ochrona informacji wzmacniają Twój wizerunek i stabilność zawodową.

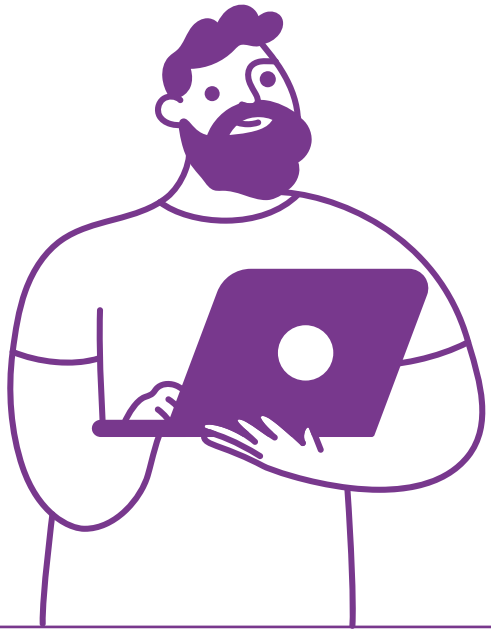
Relacja jest ważniejsza niż viral

Chwilowe zasięgi mogą przyciągać uwagę, ale w dłuższej perspektywie czasowej to autentyczne relacje budują wartość Twojej marki osobistej. Zaangażowanie odbiorców i odbiorczyń opiera się na spójności, wiarygodności i zaufaniu, a nie na jednorazowej popularności.

Cyberhigiena to fundament bezpieczeństwa
Stosuj silne hasła, włącz uwierzytelnianie dwuskładnikowe i regularnie kontroluj dostęp do swoich kont. Takie działania realnie zmniejszają ryzyko przejęcia profilu i pomagają chronić Twoje dane, wizerunek oraz relacje ze społecznością.

Co warto wdrożyć od razu?

- **Oznaczaj współprace i treści tworzone z użyciem AI** w sposób jasny i widoczny.
- **Weryfikuj publikowane treści** – szczególnie te generowane automatycznie.
- **Włącz weryfikację dwuetapową** i zarządzaj dostępem do kont.
- **Świadomie zarządzaj** granicą między życiem prywatnym a zawodowym.
- **Reaguj z dystansem** – nie pod wpływem emocji, lecz po analizie sytuacji.
- **Zgłaszaj podejrzane treści i naruszenia** (np. fałszywe strony, linki, dezinformację czy materiały typu deepfake) oraz dbaj o bezpieczeństwo i jakość informacji w swojej społeczności.



CZYM JEST NASK?

NASK to instytucja, która przyłączała Polskę do Internetu i od tamtej pory dba o to, by był szeroko dostępny i bezpieczny.

Od ponad 30 lat NASK prowadzi działania społeczne i edukacyjne, a także badania naukowe w obszarze sztucznej inteligencji i cyberbezpieczeństwa.

Docieramy do ludzi

Social media są dla nas ważne, ale znamy ich ciemne strony. Dlatego stawiamy na przyjazną, zrozumiałą komunikację, bez clickbaitowych nagłówków. Chcemy inspirować do rozważnego korzystania z technologii i budowania swojej wiedzy o cyfrowym świecie. W 2025 roku treści publikowane przez NASK w mediach społecznościowych zostały wyświetlone ponad **96 milionów** razy, a liczba opublikowanych materiałów przekroczyła **1500.**

Profile NASK obserwuje dziś blisko **100 tysięcy osób** – od użytkowników indywidualnych, przez media, po instytucje i firmy. Społeczność ta stale rośnie, skupiając zainteresowanych cyberbezpieczeństwem i świadomym korzystaniem z technologii.

Kampanie, które uczą

Działania NASK nie kończą się na publikacjach w mediach społecznościowych. Powadzimy ogólnopolskie kampanie społeczne i edukacyjne, które docierają do milionów odbiorców w różnych kanałach – od internetu przez prasę i radio, po telewizję i plakaty na nośnikach fizycznych.

W 2025 roku nasza największa kampania edukacyjno-informacyjna **„Bezpieczny dzień”**, realizowana wspólnie z Ministerstwem Cyfryzacji, dotarła do 28 mln odbiorców w kampanii telewizyjno-radiowej.

Jesteśmy tam, gdzie są ludzie

Jesteśmy obecni także offline – na wydarzeniach, festiwalach, konferencjach i warsztatach w całej Polsce i za granicą. To m.in. udział w wielkich wydarzeniach takich jak Pol’and’Rock Festival, Green Festival, międzynarodowe konferencje technologiczne (np. Web Summit w Lizbonie czy Mobile World Congress w Barcelonie), a także własne i partnerskie inicjatywy, w tym hackathony i zawody

cyberbezpieczeństwa (np. European Cyber Security Challenge – ECSC). To także szkolenia i działania prowadzone bezpośrednio z odbiorcami – w szkołach, instytucjach i przestrzeni publicznej.

Jesteśmy dla Was!

Obszar działalności NASK budzi coraz większe zainteresowanie. Cyberbezpieczeństwo, dezinformacja, sztuczna inteligencja i bezpieczeństwem użytkowników, cyberhigiena i ochrona najmłodszych to jedne z najczęściej wyszukiwanych dziś haseł w sieci. To tematy, w których łatwo o duże zasięgi – ale też o błędy, uproszczenia i powielanie nieprawdziwych informacji.Jeśli tworzysz treści w internecie, warto oprzeć się na wiedzy i informacjach udostępnianych przez NASK.

Dotyczy to przede wszystkim:

- aktualnych cyberzagrożeń (np. phishing, wyłudzenia, złośliwe oprogramowanie),
- dezinformacji i mechanizmów manipulacji w sieci,
- bezpieczeństwa dzieci i młodzieży w internecie,
- wpływu nowych technologii, w tym AI, na funkcjonowanie użytkowników w sieci,
- higieny cyfrowej i troski o własne zdrowie i samopoczucie w kontakcie z technologią.

Szukasz wiarygodnych informacji, chcesz włączyć się w działania dotyczące cyberbezpieczeństwa i promować wśród swoich obserwatorów *digital self-care* – Bądźmy w kontakcie!

Kontakt dla twórców internetowych w sprawie współpracy:

socialmedia@nask.pl

DZIĘKUJEMY INFLUENCEROM ZA ICH GŁOS W TEJ PUBLIKACJI

Janina Bąk

Statystyczka, influencerka i aktywistka. W sieci znana jako Janina Daily. Autorka dwóch bestsellerowych książek popularnonaukowych z cyklu *Statystycznie rzecz biorąc*, które sprzedały się w liczbie ponad 150 000 egzemplarzy. Wygłosiła trzy prelekcje TEDx – dwie o statystyce, a jedną o zdrowiu psychicznym. Każda z nich ma ponad 250 000 wyświetleń, a jedna była przez chwilę popularniejsza niż teledysk Zenka Martyniuka. W styczniu 2023 roku została zaliczona do grona 50 najlepszych prelegentów TEDx na świecie. Członkini Rady ds. Popularyzacji Nauki przy Ministerstwie Nauki i Szkolnictwa Wyższego, a także Rady Nowych Mediów przy Uniwersytecie SWPS. Wierzy w naukę i w ludzi.

Karolina Czak

Twórczyni internetowa i influencerka fitness, promująca zdrowe podejście do ciała i aktywności fizycznej. W swoich treściach przełamuje stereotypy związane z „idealnym" wyglądem i kulturą diet, pokazując, że trening może wynikać z troski o siebie, a nie presji. Buduje społeczność opartą na autentyczności, akceptacji i świadomym podejściu do zdrowia psychicznego i fizycznego.

Wojtek Kardyś

Ekspert w dziedzinie komunikacji internetowej, social mediów i digital marketingu. Konsultant, szkoleniowiec i twórca treści, specjalizujący się w strategiach online, marketingu influencerskim oraz zarządzaniu kryzysami w sieci. Założyciel agencji konsultingowej, Partner Biznesowy w Olive Media oraz inicjator wydarzeń edukacyjnych Social Town i audycji radiowej Cotygodniowy Przegląd Internetu. Szkoleniowiec i wykładowca akademicki. Współpracował z wieloma markami i instytucjami, wspierając rozwój komunikacji cyfrowej.

Małgorzata Rozenek-Majdan

Prezenterka telewizyjna, osobowość medialna, autorka książek oraz działaczka społeczna. W kontekście wystąpień i działalności publicznej, angażuje się w tematykę praw zwierząt oraz kwestie społeczne (m.in. in vitro). Założycielka i prezeska Fundacji MRM, podejmującej inicjatywy na rzecz wsparcia leczenia niepłodności. Z wykształcenia prawniczka. Od lat związana zawodowo z telewizją TVN, w której to współtworzyła wiele hitowych programów. Aktywna twórczyni cyfrowa, którą na Instagramie obserwuje 1,6 mln internautów. Chętnie publikuje zdjęcia i relacje z życia zawodowego i prywatnego, promując m.in. zdrowy styl życia. Prywatnie żona i matka 3 synów.

WSZYSTKIE FOTOGRAFIE POCHODZĄ Z ARCHIWUM PRYWATNEGO AUTORÓW

Dołącz do społeczności NASK i bądź bezpieczny/bezpieczna w sieci:

/NASKpl/

/NASK_pl

/company/nask

/nask.pl/

/@NASKPIB

Kontakt dla twórców internetowych w sprawie współpracy:

socialmedia@nask.pl

nask.pl

NASK