Przeciwdziałanie cybermobbingowi w pracy zdalnej

Materiały szkoleniowe dla pracodawców, specjalistów bhp oraz specjalistów HR

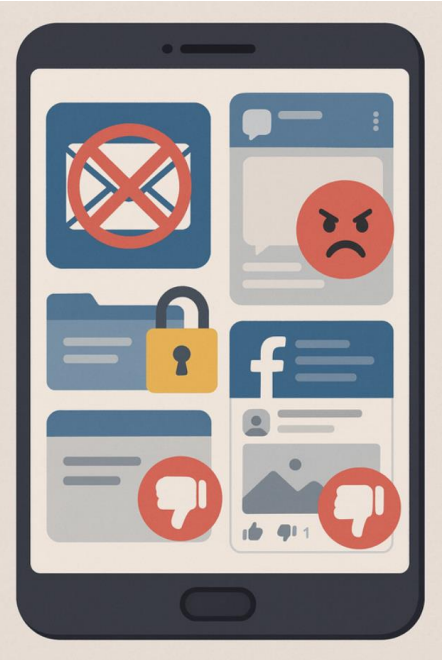
Auror: Magdalena Warszewska-Makuch
Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy

Wprowadzenie

- Cybermobbing (cyberprzemoc, cyberagresja, cyberbullying) stał się poważnym problemem ery cyfrowej
- Dynamiczny rozwój technologii informacyjno-komunikacyjnych (TIK) sprawił, że internet stał się miejscem nie tylko budowania interakcji, ale i stosowania agresji
- Cybermobbing dotyka zarówno młodzieży, jak i dorosłych, przenikając różne środowiska, w tym środowisko pracy

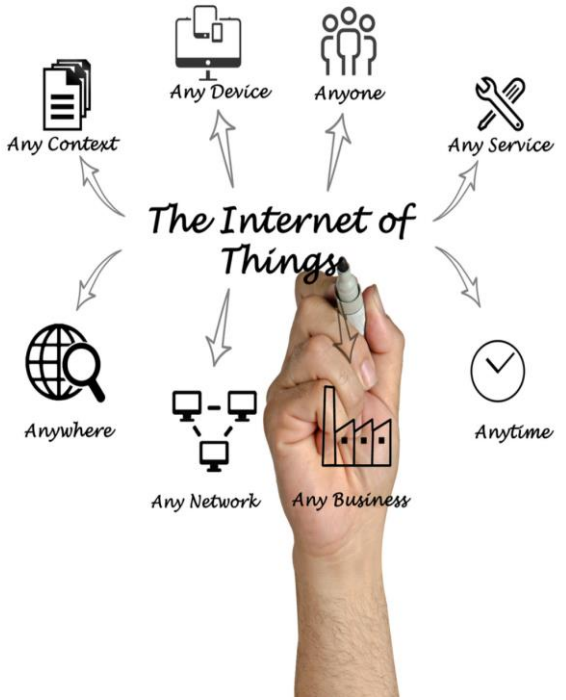
Czym jest cybermobbing w pracy?

„Wszelkie negatywne działania wynikające ze stosunków pracy, podejmowane za pomocą nowych technologii, występujące wielokrotnie i przez pewien okres czasu lub podejmowane co najmniej raz, ale istotnie ingerujące w życie osobiste pracownika i narażające go na publiczne ujawniane prywatnych informacji drogą *online*" (Vranjes i in., 2017).



Unikalne cechy cybermobbingu

- **Anonimowość sprawców** – sprawcy często ukrywają swoją tożsamość, co zwiększa ich poczucie bezkarności i utrudnia identyfikację
- **Wszechobecność** – cyberprzemoc może dotykać pracownika w dowolnym miejscu i czasie
- **Trwałość** – materiały udostępnione w sieci mogą pozostać dostępne przez lata
- **Szybkość rozpowszechniania** – szkodliwe treści mogą w krótkim czasie dotrzeć do ogromnej liczby osób



Przykłady cybermobbingu w pracy

- Ignorowanie wiadomości/e-maili od pracownika
- Publiczne krytykowanie pracy wykonywanej przez pracownika przy użyciu TIK
- Utrudnianie pracownikowi dostępu do niezbędnych plików
- Rozpowszechnianie plotek o pracowniku za pomocą TIK
- Obrażanie lub zastraszanie pracownika za pomocą TIK
- Udostępnianie prywatnych informacji pracownika
- Hakowanie i wykorzystywanie danych pracownika
- Kradzież w sieci tożsamości pracownika

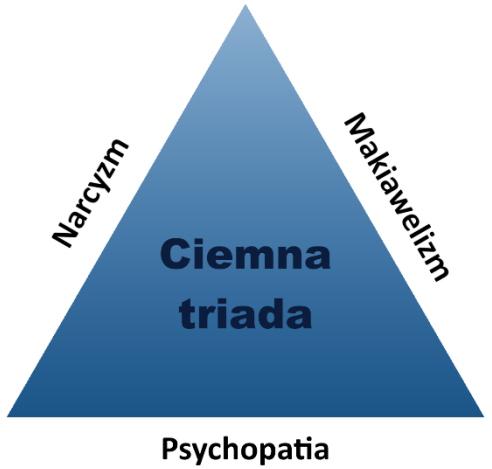
Cyberprzemoc w Polsce – badania Instytutu Psychologii Zdrowia

- Kobiety częściej zgłaszały przypadki cybermobbingu niż mężczyźni (15,2% vs. 10,4%)
- Osoby w wieku 31-40 lat najczęściej doświadczały cyberprzemocy w pracy (17%), w grupie powyżej 50. roku życia odsetek ten wynosił 8%
- Pracownicy zatrudnieni w organizacjach powyżej 500 osób rzadziej zgłaszali przypadki cybermobbingu niż osoby pracujące w małych firmach (do 50 osób)

Przyczyny cybermobbingu w pracy – cechy sprawcy

Cechy osobowości sprawców

- *Ciemna triada* (psychopatia, makiawelizm, narcyzm)
- Niska samoocena
- Potrzeba dominacji
- Skłonność do gniewu



Motywy sprawców

- Zazdrość i rywalizacja
- Zemsta
- Nuda

Przyczyny cybermobbingu w pracy - organizacja

Czynniki organizacyjne

- Niskie wsparcie społeczne
- Konflikt *praca-życie prywatne*
- Niska jakość przywództwa
- Niesprzyjający klimat społeczny

Czynniki technologiczne

- Anonimowość *online*
- Nieograniczony dostęp do narzędzi cyfrowych

Czynniki ryzyka cybermobbingu w pracy zdalnej

- Ograniczona komunikacja bezpośrednia –
  utrudnione odczytywanie emocji i intencji rozmówcy
- Presja ciągłej dostępności –
  oczekiwanie natychmiastowych odpowiedzi w komunikatorach
- Brak jasnych granic między pracą a życiem prywatnym
- Anonimowość i dystans cyfrowy, które zmniejszają empatię
  i odpowiedzialność za słowa
- Nadmierny nadzór technologiczny
  (monitorowanie ekranu, analiza aktywności online)
- Niedostateczne wsparcie ze strony przełożonych –
  brak indywidualnego kontaktu i informacji zwrotnej

Konsekwencje cyberprzemocy dla pracowników

PSYCHOLOGICZNE

CHRONICZNY STRES

OBNIŻONA SAMOOCENA

BEZSILNOŚĆ I LĘK

PTSD, DEPRESJA

FIZYCZNE

BÓLE GŁOWY

ZABURZENIA UKŁADU POKARMOWEGO

ZABURZENIA UKŁADU KRĄŻENIA

PROBLEMY ZE SNEM

SPOŁECZNE

UNIKANIE INTERAKCJI

POCZUCIE IZOLACJI

UTRATA ZAUFANIA DO LUDZI

Konsekwencje cybermobbingu dla organizacji

- Pogorszenie atmosfery w pracy i wzrost konfliktów,
- Spadek efektywności,
- Obniżenie zaufania w zespole,
- Wzrost absencji chorobowej,
- Wzrost rotacji pracowników i odpływ specjalistów,
- Straty wizerunkowe,
- Potencjalna utrata klientów,
- *Cyberloafing* jako forma radzenia sobie ze stresem, obniżająca produktywność.

Czym jest cyberloafing?

Cyberloafing – korzystanie z internetu lub technologii cyfrowych w celach prywatnych podczas godzin pracy, zamiast wykonywania obowiązków służbowych
(Blanchard & Henle, 2008; Lim, 2002)

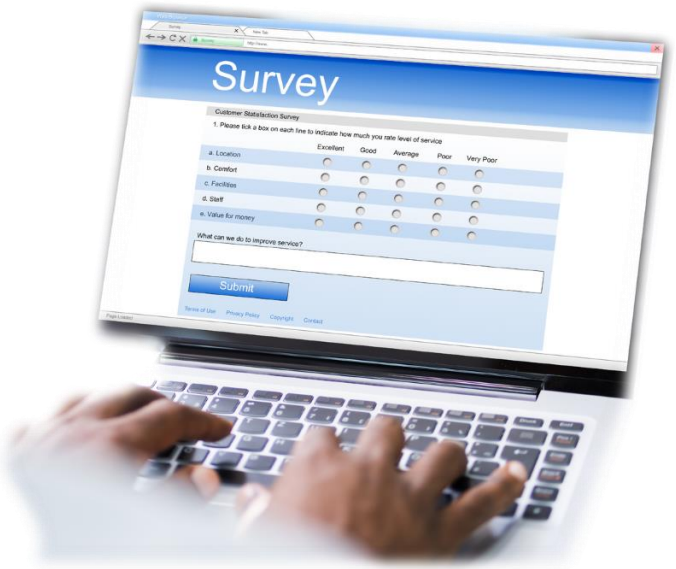
Cyberloafing może obejmować m.in.:

- przeglądanie mediów społecznościowych,
- robienie zakupów online,
- czytanie wiadomości niezwiązanych z pracą
- pobieranie plików online, w tym muzyki,
- gry/hazard online

Wyniki badań CIOP-PIB*

Korelacje między doświadczaniem cyberprzemocy w pracy a zaburzeniami zdrowia psychicznego, N=616 (*p<.05, **p<.001)

Zmienna	1	2	3	4	5	6
1.Cyberprzemoc w pracy	-					
2.Problemy ze snem	,38**					
3.Wypalenie	,26**	,62**				
4.Depresja	,40**	,61**	,75**			
5.Stres	,29**	,64**	,82**	,82**		
6.Stres poznawczy	,42**	,62**	,76**	,86**	,80**	
7.Stres somatyczny	,54**	,67**	,67**	,77**	,72**	,76**



*Warszewska-Makuch M., Mockałło Z. zadanie 2.ZS.01 pn. „Cybermobbing - negatywne konsekwencje w pracy zdalnej: moderująca rola technostresu i izolacji społecznej", 2025, CIOP-PIB

Wyniki badań CIOP-PIB*

Korelacje między doświadczaniem cyberprzemocy w pracy, cyberloafingiem, zaangażowaniem w pracę i poczuciem samotności, N=616 (*p<.05, **p<.001)

Zmienna	1	2	3
1.Cyberprzemoc w pracy	-		
2.Cyberloafing	,47**		
3.Zaangażowanie w pracę	,02	,10*	
4.Poczucie samotności	-,18**	-,06	,23**

*Warszewska-Makuch M., Mockałło Z., zadanie 2.ZS.01 pn. „Cybermobbing - negatywne konsekwencje w pracy zdalnej: moderująca rola technostresu i izolacji społecznej", 2025, CIOP-PIB

Regulacje prawne w Polsce

W Polsce nie ma odrębnej ustawy o cyberprzemocy w pracy!

Kodeks karny

- Pomówienie (art. 212 KK),
- Zniesławienie i znieważenie (art. 216 KK),
- Stalking i uporczywe nękanie (art. 190a KK),
- Groźby karalne (art. 190 KK).

Kodeks cywilny (art. 23, 24)

- ochronę przed naruszeniem godności, dobrego imienia oraz prywatności (art. 23 KC),
- Zaniechania działań naruszających jego dobra osobiste (art. 24 KC).

Kodeks pracy (art. 94^3)

- Kodeks pracy nie zawiera wprost regulacji dotyczących cybermobbingu, jednak odnosi się do mobbingu (art. 94^3 KP), który może obejmować również formy cyfrowe.

Inne regulacje ustawowe

- Ustawa z dnia 14 czerwca 2024 r. o ochronie sygnalistów, Dz. U. z 2024 r., poz. 928.

Regulacje międzynarodowe

Konwencja MOP nr 190
(zwalczanie przemocy i nękania w miejscu pracy)

Uchwalona w 2019 roku, uznaje cybermobbing jako formę przemocy i nękania. Nakłada na kraje członkowskie obowiązek wprowadzenia odpowiednich regulacji prawnych i środków ochrony przed przemocą w miejscu pracy. W Polsce trwają prace nad jej ratyfikacją.

Dyrektywa UE 2019/1937
(ochrona sygnalistów)

Dyrektywa zapewnia ochronę osobom zgłaszającym przypadki nadużyć, w tym mobbingu i cybermobbingu. Wprowadza mechanizmy ochrony przed represjami ze strony pracodawców.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2024/1385 (zwalczanie przemocy wobec kobiet i przemocy domowej)

Dokument zawiera konkretne definicje cyberprzemocy i dotyczy wszystkich sfer życia (a więc i życia zawodowego). Musi być wdrożona do 2027 r. przez wszystkie państwa członkowskie UE.

Narzędzie do diagnozy cybermobbingu w pracy

- ✓ opracowane przez Vranjes i in. (2018)
- ✓ polska adaptacja – Warszewska-Makuch (2025)

Kwestionariusz ICA-W

(Vranjes i in., 2018)

Jak często w ciągu ostatnich sześciu miesięcy, doświadczałaś/-eś w swojej pracy poniższych działań realizowanych przy użyciu narzędzi teleinformatycznych (Internet, e-mail, telefon komórkowy, telefon, tablet itp.)?

	1	2	3	4	5
	Nigdy	Jeden raz	Co miesiąc	Co tydzień	Codziennie

1.	Twoje e-maile, telefony lub wiadomości są w pracy ignorowane.	1 2 3 4 5
2.	Twoje e-maile są przekazywane osobom trzecim, aby wyrządzić Ci szkodę.	1 2 3 4 5
3.	Twoja praca jest publicznie krytykowana przy użyciu narzędzi teleinformatycznych.	1 2 3 4 5
4.	Ktoś wstrzymuje potrzebne Ci e-maile albo pliki, co utrudnia Twoją pracę.	1 2 3 4 5
5.	Ktoś rozpowszechnia na Twój temat pogłoski i plotki przy użyciu narzędzi teleinformatycznych.	1 2 3 4 5
6.	Jesteś obrażana/-y, zastraszana/-y lub są pod Twoim adresem kierowane groźby przy użyciu narzędzi teleinformatycznych.	1 2 3 4 5
7.	Ciągle pojawiają się uwagi na Twój temat i Twojego życia osobistego przekazywane za pomocą narzędzi teleinformatycznych.	1 2 3 4 5
8.	Twoje dane osobowe są hakowane i wykorzystywane, aby wyrządzić Ci szkodę.	1 2 3 4 5
9.	Ktoś udostępnia Twoje zdjęcia lub filmy w Internecie, aby się z Ciebie naśmiewać.	1 2 3 4 5
10.	Ktoś kradnie Twoją tożsamość.	1 2 3 4 5

Jak zapobiegać i radzić sobie z cyberprzemocą w miejscu pracy?

- Jasna polityka i procedury antyprzemocowe,
- Określenie zasad korzystania z technologii komunikacyjnych,
- Regularne szkolenia i kampanie edukacyjne,
- Mechanizmy anonimowego zgłaszania przypadków cyberprzemocy,
- Kształtowanie kultury organizacyjnej opartej na szacunku i etyce cyfrowej,
- Konsekwentne egzekwowanie sankcji wobec sprawców,
- Dostęp pracowników dotkniętych cyberprzemocą do profesjonalnego wsparcia m.in. psychologicznego.

Co może zawierać polityka antycyberprzemocowa?

- Jasna deklaracja, że **organizacja i kadra zarządzająca są zaangażowane w tworzenie środowiska wolnego od cyberprzemocy**
- **Opis kluczowych wartości, które wyznaje firma**, m.in. „wszyscy pracownicy powinni być traktowani z szacunkiem”, „każdy pracownik jest odpowiedzialny za reagowanie na jakiekolwiek akty cyberprzemocy”
- **Poradnik dotyczący zachowań cyfrowych w miejscu pracy**, dot. wykorzystania urządzeń do komunikowania się z innymi pracownikami (można podkreślać, że firmowe, mobilne urządzenia mogą być używane wyłącznie w celach zawodowych)
- **Wytyczne dotyczące używania poszczególnych narzędzi cyfrowych**, np. służbowe e-maile zawierające polecenia lub informacje zwrotne (szczególnie negatywne) nt. wykonanej pracy, nie powinny być wysyłane po oficjalnych godzinach pracy, np. późno w nocy

Co może zawierać polityka antycyberprzemocowa?

- Jasny **opis czym jest cyberprzemoc** i do czego prowadzi (podanie pracownikom przykładowych działań cyberprzemocowych)
- Zapis o **„zerowej tolerancji”** i **sankcjach dla sprawców**
- Opis **sposobu składania skargi,** tj. należy jasno określić punkt kontaktowy, w którym pracownik może zgłosić cyberprzemoc (zaleca się wskazanie więcej, niż jednego punktu kontaktowego, by osoby dotknięte cyberprzemocą mogły wybrać, z kim chcą się skontaktować)

Polityka antycyberprzemocowa będzie skuteczna jeśli w proces jej wdrażania będzie zaangażowane szerokie grono kierowników, specjalistów HR, przedstawicieli związków zawodowych itp., którzy udzielą informacji zwrotnych na temat polityki i będą ją współtworzyć z pracownikami (uwzględniając rzeczywiste doświadczenia i potrzeby pracowników)

Jak zapobiegać cyberprzemocy w sieci m.in. w mediach społecznościowych?

- Przekazanie pracownikom informacji o tym, że w związku z nieodpowiednimi treściami zamieszczanymi przez nich w sieci **mogą ponieść konsekwencje służbowe**
- Wyjaśnienie, że **nie należy używać w sieci obelg, osobistych zniewag czy wulgarnego języka**, które są niedopuszczalne w miejscu pracy
- Przypomnienie pracownikom, że raz zamieszczone w sieci treści są **niezwykle trudne do usunięcia** a ich konsekwencje mogą być odczuwalne przez długi okres czasu
- Wskazanie pracownikom, że komunikując się online powinni wyjaśnić, że **wyrażane przez nich poglądy są ich własnymi, a nie organizacji**

Podsumowanie

Cyberprzemoc to realne zagrożenie w środowisku pracy!

- Cyberprzemoc w pracy ma negatywne konsekwencje dla zdrowia pracowników i efektywności organizacji;
- Polskie prawo oferuje pewne możliwości reagowania, ale brakuje specyficznych regulacji;
- Kluczowa jest prewencja, edukacja i wdrożenie jasnych procedur postępowania w przypadku cyberprzemocy;
- Ważne jest budowanie kultury organizacyjnej opartej na szacunku i etyce cyfrowej.

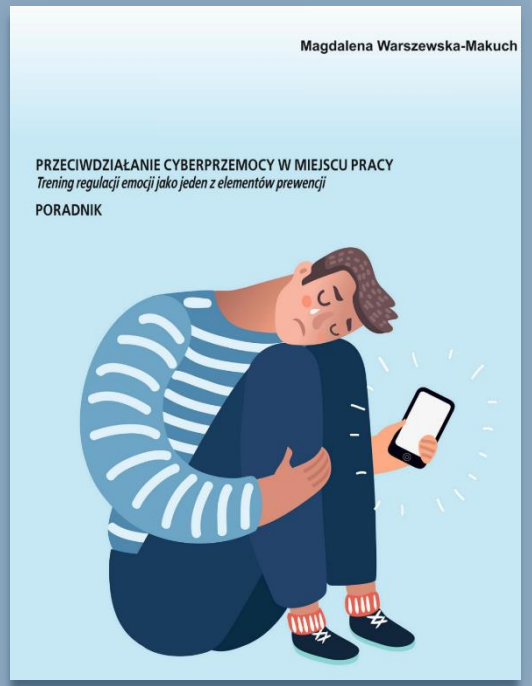
Poradnik

M. Warszewska-Makuch „Przeciwdziałanie cybermobbingowi w pracy zdalnej i hybrydowej”

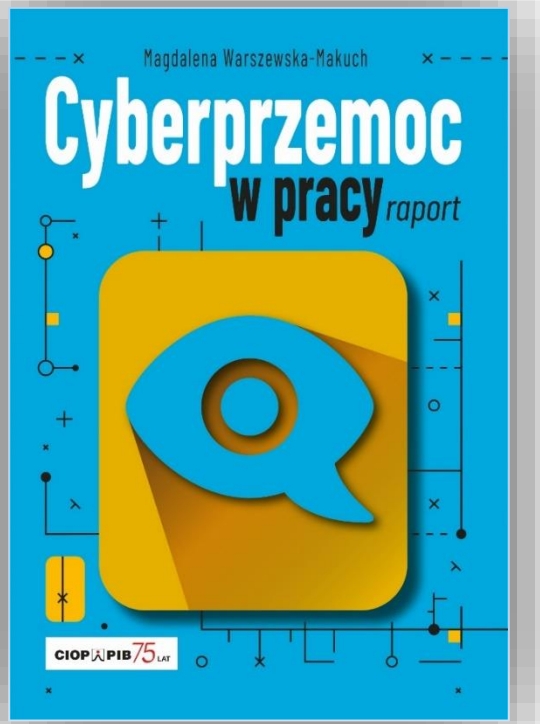
Poradnik dla pracodawców oraz specjalistów HR i bhp

Inne publikacje na temat cyberprzemocy w pracy dostępne w serwisie CIOP-PIB

https://www.ciop.pl/CIOPPortalWAR/file/95907/Poradnik_program_treningu_regulacji_emocji_redkj.pdf



http://www.ciop.pl/cyberprzemoc-raport



https://www.ciop.pl/CIOPPortalWAR/file/96144/Radzenie_sobie_z_cyberprzemoca_w_miejscu_pracy.pdf

Dziękuję za uwagę

Opracowano na podstawie wyników programu wieloletniego pn. Rządowy Program Poprawy Bezpieczeństwa i Warunków Pracy – VI etap (okres realizacji 2023-2025), finansowanego w zakresie zadań służb państwowych ze środków Ministerstwa Rodziny i Polityki Społecznej
Koordynator Programu: Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy