FUNDACJA DAJEMY DZIECIOM SIŁĘ

Dziecko Krzywdzone
Teoria Badania Praktyka

Modele instytucjonalne i prawne przeciwdziałania OCSAE: studium porównawcze wybranych jurysdykcji

Dorota Mroczkowska

Uniwersytet Warmińsko-Mazurski w Olsztynie

Przemoc seksualna wobec dzieci w środowisku cyfrowym stanowi jedno z istotnych współczesnych zagrożeń dla ich bezpieczeństwa i dobrostanu. Internet i media społecznościowe stwarzają nowe możliwości krzywdzenia dzieci, m.in. poprzez grooming, sextortion oraz rozpowszechnianie materiałów z ich seksualnym wykorzystaniem. Artykuł przedstawia przegląd systemów ochrony dzieci przed przemocą seksualną online w wybranych podmiotach prawa międzynarodowego, ze szczególnym uwzględnieniem rozwiązań prawnych, technologicznych i edukacyjnych funkcjonujących w Australii, Wielkiej Brytanii, Unii Europejskiej oraz Stanach Zjednoczonych. Omówiono rolę państwa, platform cyfrowych oraz instytucji wspierających dzieci w reagowaniu na przemoc i zapobieganiu jej eskalacji. Wskazano także kluczowe wyzwania związane z ochroną prywatności, skutecznością egzekwowania prawa oraz potrzebą spójnych działań systemowych. Celem artykułu jest ukazanie dobrych praktyk i kierunków rozwoju systemów ochrony dzieci w kontekście przemocy seksualnej online.

Słowa kluczowe:
ochrona dziecka; przemoc seksualna wobec dzieci; przemoc seksualna online; bezpieczeństwo dzieci w internecie; system ochrony dziecka

Wstęp

Rozwój technologii cyfrowych istotnie zmienił sposób funkcjonowania dzieci i młodzieży. W ostatnich latach technologia stała się integralną częścią ich codzienności, relacji społecznych oraz procesu rozwojowego. Jednocześnie środowisko cyfrowe stworzyło nowe formy zagrożeń, w tym możliwości krzywdzenia

dzieci poprzez przemoc seksualną online. Jako szczególnie niebezpieczne należy wskazać: uwodzenie (ang. *grooming*), wymuszanie treści seksualnych czy intymnych, gratyfikacji finansowej lub zachowań pod groźbą ujawnienia kompromitujących materiałów (ang. *sextortion*) oraz rozpowszechnianie materiałów przedstawiających seksualne wykorzystanie dzieci (ang. *child sexual abuse material*, CSAM); (UNICEF, 2021; WeProtect Global Alliance, 2019).

Przemoc seksualna online wobec dzieci często ma charakter ukryty i długotrwały, a jej skutki mogą być porównywalne z doświadczeniem przemocy w świecie realnym. Specyfika środowiska cyfrowego – anonimowość sprawców, łatwość dostępu do dziecka, trwałość raz opublikowanych treści oraz transgraniczny charakter zjawiska – znacząco utrudnia skuteczną ochronę małoletnich (Livingston, Stoilova, 2021a). Z tego względu problem ten wymaga kompleksowych, systemowych rozwiązań obejmujących prawo, praktykę instytucjonalną, działania platform cyfrowych oraz szeroko rozumianą prewencję.

W odpowiedzi na narastające zagrożenia wiele państw oraz organizacji międzynarodowych podejmuje działania mające na celu wzmocnienie systemów ochrony dzieci w środowisku cyfrowym. Obejmują one zarówno zmiany legislacyjne, jak i rozwój narzędzi technologicznych, mechanizmów zgłaszania przemocy oraz programów edukacyjnych skierowanych do dzieci, rodziców i profesjonalistów pracujących z dziećmi (Australian Government, 2021). Różnorodność przyjmowanych rozwiązań odzwierciedla odmienne podejścia do równoważenia ochrony małoletnich, praw użytkowników oraz odpowiedzialności podmiotów prywatnych (European Parliament & Council of the European Union, 2022).

Niniejszy przegląd ma charakter analizy porównawczej wybranych systemów ochrony dzieci przed przemocą seksualną online (ang. *Online Child Sexual Abuse and Exploitation*, OCSAE) funkcjonujących w Europie, Australii oraz Ameryce Północnej. Dobór przykładów nie wynika z perspektywy europocentrycznej, lecz z kryterium dostępności rozwiniętych, relatywnie dobrze udokumentowanych oraz instytucjonalnie ugruntowanych rozwiązań prawnych i operacyjnych, które umożliwiają analizę systemową oraz identyfikację mechanizmów regulacyjnych o znaczeniu międzynarodowym (WeProtect Global Alliance, 2023). Jednocześnie należy podkreślić, że przeciwdziałanie seksualnemu wykorzystywaniu dzieci w środowisku cyfrowym ma charakter transnarodowy i opiera się na współpracy wielopoziomowej. Obejmuje ona zarówno struktury państwowe, jak i sieci międzynarodowe oraz partnerstwa publiczno-prywatne. Do istotnych podmiotów w tym obszarze należą m.in. organizacje: International Association of Internet Hotlines (INHOPE), zrzeszająca hotline'y zgłoszeniowe (INHOPE, 2024); ECPAT International; International

Centre for Missing & Exploited Children (ICMEC) czy Tech Coalition (Tech Coalition, 2023). W wymiarze operacyjnym i ścigania sprawców fundamentalną rolę odgrywają wyspecjalizowane jednostki, takie jak australijski Argos, jednostka AP Twins w ramach Europolu (Europol, 2023; Europol, 2024) czy zespół ICSE Team w Interpolu. Globalne systemy ochrony dzieci pozostają jednak silnie zróżnicowane geograficznie i instytucjonalnie; w wielu państwach Azji, Afryki i Ameryki Łacińskiej rozwijane są odmienne modele reagowania, uwarunkowane poziomem rozwoju infrastruktury cyfrowej, zasobami systemów ochrony zdrowia i pomocy społecznej oraz lokalnymi tradycjami prawnymi. W ujęciu makrogeopolitycznym widoczne są też różnice pomiędzy rozwiązaniami charakterystycznymi dla państw tzw. Globalnej Północy i Globalnego Południa oraz między systemami zachodnimi i wschodnimi (WeProtect Global Alliance, 2023). Z tego względu prezentowane opracowanie ma charakter selektywny i analityczny, a jego celem jest przedstawienie wybranych modeli regulacyjnych i instytucjonalnych w szerszym kontekście międzynarodowych ram ochrony dzieci.

W niniejszym opracowaniu wykorzystano dane oraz dokumenty pochodzące głównie z lat 2019–2024, które w momencie przygotowywania artykułu stanowiły najbardziej aktualne i porównywalne źródła dostępne w analizowanych systemach prawnych oraz raportach międzynarodowych. Ze względu na dynamiczny rozwój technologii cyfrowych oraz szybkie zmiany legislacyjne w obszarze ochrony dzieci przed przemocą seksualną online należy podkreślić, że część rozwiązań instytucjonalnych i technologicznych może podlegać bieżącym modyfikacjom.

Konsekwencje przemocy seksualnej online dla zdrowia psychicznego dzieci

Doświadczenie przemocy seksualnej w środowisku cyfrowym, w tym ekspozycja na treści seksualne, uwodzenie oraz rozpowszechnianie intymnych materiałów bez zgody dziecka, wiąże się z istotnym ryzykiem zaburzeń funkcjonowania emocjonalnego i społecznego. Dzieci, których wizerunek został wygenerowany lub zmanipulowany (np. przy użyciu narzędzi sztucznej inteligencji), mogą doświadczać wstydu, poczucia utraty kontroli nad własnym ciałem, podmiotowością, poczuciem sprawczości i tożsamością oraz obaw związanych z trwałością treści cyfrowych. Badania i raporty eksperckie wskazują, że tego typu doświadczenia sprzyjają wtórnej traumatyzacji oraz utrudniają proces zdrowienia, nawet jeśli nie doszło do bezpośredniego kontaktu ze sprawcą, a w niektórych przypadkach ulegają wzmocnieniu ze względu na powtarzalność działań przestępczych lub szkodliwych, anonimowość sprawców

oraz brak możliwości definitywnego „zakończenia" doświadczenia w przestrzeni cyfrowej (Livingstone, Stoilova, 2021a; UNICEF, 2023).

W literaturze przedmiotu konsekwencje przemocy seksualnej online analizowane są m.in. w oparciu o adaptacje modelu dynamiki traumy Davida Finkelhora (ang. *Traumagenic Dynamics Model*). W kontekście online cztery kluczowe mechanizmy traumy przybierają specyficzną formę (Livingstone, Stoilova, 2021b):

11. traumatyczna seksualizacja – występuje poprzez ekspozycję na niechciane treści lub zniekształcony obraz seksualności generowany przez algorytmy;
12. zdrada – często dotyczy rówieśników udostępniających materiały lub dorosłych „groomerów", którzy budują fałszywą relację zaufania;
13. stygmatyzacja – w środowisku cyfrowym ulega drastycznemu wzmocnieniu ze względu na viralowy charakter treści i niemożność ich trwałego usunięcia (tzw. cyfrowy ślad);
14. bezsilność – poczucie utraty kontroli jest potęgowane przez anonimowość sprawców oraz technologiczną łatwość powielania wizerunku (np. przy użyciu *deepfake*).

W praktyce klinicznej dzieci po doświadczeniach przemocy seksualnej online mogą prezentować objawy zaburzeń lękowych (w tym PTSD) i depresyjnych, poczucie winy, wstydu, obniżone poczucie własnej wartości, a także zaburzenia snu i objawy psychosomatyczne (Finkelhor, Jones, 2006). Osoby pokrzywdzone często zgłaszają specyficzne poczucie „kradzieży tożsamości" i dysocjacji od własnego wizerunku (Livingstone, Stoilova, 2021b). U części dzieci pojawiają się trudności poznawcze związane z postrzeganiem relacji interpersonalnych, utratą zaufania do innych oraz nasilonym lękiem przed oceną społeczną. W sferze behawioralnej obserwuje się wycofanie społeczne, zachowania ryzykowne (w tym autoagresję) lub – paradoksalnie – podejmowanie ryzykownych zachowań seksualnych online jako formy odzyskiwania pozornej kontroli.

Kluczowym czynnikiem wpływającym na rokowanie jest jakość interwencji instytucjonalnej. Procedury prawne, choć niezbędne dla wymierzenia sprawiedliwości, niosą ryzyko wtórnej wiktymizacji (ang. *secondary victimization*). Wielokrotne przesłuchania, konfrontacja z materiałem dowodowym oraz przewlekłość postępowań stoją w sprzeczności z terapeutyczną potrzebą domknięcia doświadczenia traumatycznego. W przypadku przestępstw online dodatkowym stresorem jest „cyfrowa nieskończoność" dowodu przestępstwa – dziecko ma świadomość, że materiał może w każdej chwili wypłynąć ponownie, co utrudnia proces zdrowienia nawet po zakończeniu działań prawnych.

W świetle powyższego wydaje się zasadnym stwierdzenie, że ochrona dzieci wymaga wdrożenia modelu *Trauma-Informed Care* (opieki uwzględniającej traumę) we wszystkich służbach stykających się z dzieckiem. Kluczowe znaczenie mają:

- współpraca interdyscyplinarna: konieczna jest ścisła współpraca organów ścigania (usuwanie treści, zabezpieczanie dowodów) ze specjalistami zdrowia psychicznego, aby działania operacyjne nie naruszały dobrostanu dziecka;
- edukacja cyfrowa jako prewencja: praca z pokrzywdzonymi powinna obejmować elementy edukacji na temat zarządzania prywatnością i mechanizmów zgłaszania treści, co przywraca częściowe poczucie sprawczości;
- standardy Child-Friendly Justice: implementacja wytycznych Rady Europy w zakresie przyjaznego wymiaru sprawiedliwości, w tym przesłuchań w bezpiecznych warunkach (np. w trybie art. 185a k.p.k. w Polsce), minimalizujących stres związany z procedurą karną.

Ochrona dzieci przed przemocą seksualną online powinna być zatem traktowana nie tylko jako zagadnienie prawne lub technologiczne, lecz również jako istotny element profilaktyki zdrowia psychicznego dzieci i młodzieży.

W obliczu tych poważnych skutków psychicznych i społecznych powstała potrzeba ustanowienia międzynarodowych standardów i wytycznych chroniących dzieci przed przemocą seksualną online.

Najczęściej ratyfikowane instrumenty prawne oraz wytyczne międzynarodowe w ochronie dzieci przed przemocą seksualną online

Podstawą prawną ochrony dzieci są międzynarodowe konwencje i wytyczne określające standardy przeciwdziałania przemocy. Dobór przedstawionych instrumentów ma charakter selektywny i nie wyczerpuje całości międzynarodowych regulacji. Uwzględniono przede wszystkim dokumenty o szerokim zakresie ratyfikacji oraz znaczącym wpływie na kształtowanie współczesnych standardów ochrony dzieci przed przemocą seksualną, w tym w środowisku cyfrowym. Przedstawione instrumenty stanowią punkt odniesienia dla dalszej analizy krajowych i regionalnych modeli ochrony dzieci przed przemocą seksualną online.

Konwencja o prawach dziecka (ONZ, 1989) gwarantuje każdemu dziecku prawo do bezpieczeństwa i ochrony przed wszelkimi formami przemocy. Uzupełniający ją Protokół fakultatywny (ONZ, 2000) dotyczy handlu dziećmi, dziecięcej prostytucji i dziecięcej pornografii oraz nakłada na państwa obowiązek penalizacji

m.in. materiałów przedstawiających seksualne wykorzystywanie dzieci. Konwencja z Lanzarote (2007) zobowiązuje państwa do działań prewencyjnych, ścigania sprawców oraz zapewnienia wsparcia dzieciom doświadczającym krzywdzenia (Council of Europe, 2007). Jest to jeden z kluczowych europejskich instrumentów prawnych, który w sposób wyraźny odnosi się do przestępstw popełnianych z wykorzystaniem technologii informacyjno-komunikacyjnych, w tym *groomingu*.

Uzupełnieniem ram prawnych są wytyczne organizacji międzynarodowych, w tym Funduszu Narodów Zjednoczonych na rzecz Dzieci UNICEF, wskazujące na odpowiedzialność państw i podmiotów prywatnych – w szczególności firm technologicznych – w zakresie: raportowania nielegalnych treści, stosowania mechanizmów ochronnych oraz prowadzenia działań edukacyjnych skierowanych do dzieci i ich opiekunów (UNICEF, 2021; WeProtect Global Alliance, 2019). W dokumentach tych coraz wyraźniej akcentowana jest specyfika środowiska cyfrowego jako przestrzeni wymagającej systemowych rozwiązań ochronnych.

Dynamiczny rozwój technologii, w tym generatywnej sztucznej inteligencji (ang. *Artificial Intelligence*, AI), ujawnia istotne ograniczenia istniejących międzynarodowych instrumentów normatywnych i wytycznych.

Systemowe rozwiązania ochrony dzieci nie zawsze wprost obejmują zjawiska takie jak nadużycia tworzone przez sztuczną inteligencję (ang. *AI-generated abuse*), w tym zjawiska szantażu seksualnego wobec dzieci z wykorzystaniem syntetycznych treści wizualnych i audio. Wyzwanie to jest szeroko analizowane przez Tech Coalition, która w swoich raportach (m.in. *Addressing AI-generated child sexual exploitation and abuse*) wskazuje, że dynamiczny rozwój generatywnej sztucznej inteligencji wymaga od dostawców usług natychmiastowej adaptacji standardów bezpieczeństwa i wdrażania mechanizmów *safety by design* (Tech Coalition, 2023).

Coraz częściej identyfikowanym zjawiskiem w środowisku cyfrowym jest tworzenie i rozpowszechnianie materiałów o charakterze seksualnym z udziałem dzieci przy użyciu algorytmów AI, w tym *deepfake'ów*, tj. zaawansowanych technik manipulacji treściami multimedialnymi oraz syntetycznych wizerunków dzieci. Zjawisko to jest wskazywane przez instytucje międzynarodowe jako jedno z poważniejszych wyzwań dla współczesnych systemów ochrony dzieci, co znajduje odzwierciedlenie w danych sieci hotline'ów, notujących wzrost liczby zgłoszeń dotyczących syntetycznych materiałów CSAM (Europol, 2023; INHOPE, 2024; Internet Watch Foundation, 2023; WeProtect Global Alliance, 2023).

Poniżej przedstawiono kluczowe międzynarodowe instrumenty ochrony praw dziecka przed przemocą seksualną online oraz wytyczne organizacji międzynarodowych, a także ich implikacje dla krajowych systemów ochrony dzieci.

Konwencja o prawach dziecka (ONZ, 1989)

Konwencja o prawach dziecka (*Convention of the Rights of the Child*, CRC) jest fundamentalnym dokumentem międzynarodowym, gwarantującym każdemu dziecku prawo do ochrony przed wszelkimi formami przemocy, w tym przemocą seksualną. Państwa-strony zobowiązane są do wprowadzania rozwiązań prawnych i instytucjonalnych, które chronią dzieci przed wszelkimi zagrożeniami oraz umożliwiają interwencję w przypadku naruszenia ich praw. Konwencja o prawach dziecka podkreśla również rolę edukacji, świadomości społecznej i współpracy międzynarodowej w zakresie ochrony dzieci.

Konwencja Rady Europy o ochronie dzieci przed seksualnym wykorzystywaniem i niegodziwym traktowaniem

Konwencja Rady Europy o ochronie dzieci przed seksualnym wykorzystywaniem i niegodziwym traktowaniem (Lanzarote, 2007) jest pierwszym dokumentem międzynarodowym, który wprost odnosi się do ochrony dzieci przed wykorzystywaniem seksualnym, zarówno offline, jak i online. Nakłada na państwa obowiązki w zakresie:

- prewencji – edukacji dzieci i rodziców, szkoleń dla profesjonalistów, wczesnych interwencje w sytuacjach ryzyka;
- ścigania sprawców – harmonizacji prawa karnego, procedur współpracy transgranicznej, wymiany informacji między organami ścigania;
- wsparcia dla osób pokrzywdzonych – zapewnienia pomocy psychologicznej, prawnej i socjalnej dzieciom, które doświadczyły przemocy seksualnej.

Konwencja wskazuje również na konieczność współpracy z podmiotami prywatnymi, w tym z platformami internetowymi, które mają obowiązek raportowania i usuwania materiałów przedstawiających wykorzystywanie dzieci (Council of Europe, 2007).

Wytyczne organizacji międzynarodowych

Organizacje takie jak UNICEF czy WeProtect Global Alliance wydają rekomendacje i wytyczne dla państw, platform cyfrowych i organizacji pozarządowych. Koncentrują się głównie na (UNICEF, 2021; WeProtect Global Alliance, 2019):

- odpowiedzialności państw za zapewnienie skutecznych mechanizmów ochrony dzieci;
- obowiązkach platform cyfrowych – raportowaniu treści CSAM, wprowadzaniu zabezpieczeń, filtrowaniu treści, weryfikacji wieku użytkowników;
- edukacji i prewencji – rozwijaniu programów podnoszących świadomość dzieci, rodziców i profesjonalistów w zakresie bezpieczeństwa w sieci;
- współpracy transgranicznej – ze względu na charakter internetu zagrożenia często wykraczają poza granice jednego kraju, co wymaga wymiany informacji i wspólnych procedur interwencyjnych.

Implikacje wynikające z międzynarodowych uwarunkowań prawnych

Choć bezpieczeństwo dzieci w internecie pozostaje kwestią priorytetową, międzynarodowe wytyczne coraz częściej wskazują na potrzebę balansowania go z prawem do prywatności. Przykładem takich praktyk są:

- Europejska Konwencja o ochronie praw człowieka i podstawowych wolności, wpływająca na projektowanie regulacji cyfrowych z uwzględnieniem prywatności;
- ramy Organizacji Współpracy Gospodarczej i Rozwoju (OECD) i Organizacji Narodów Zjednoczonych (ONZ) dotyczące praw dziecka w środowisku cyfrowym, wskazujące, że ochrona dzieci nie może naruszać ich innych praw, np. dostępu do edukacji czy wolności wypowiedzi.

Analiza międzynarodowych uwarunkowań prawnych w zakresie ochrony dzieci w sieci prowadzi do następujących konkluzji:

- uznanie krzywdy: przemoc seksualna online jest traktowana jako realne doświadczenie krzywdzenia, wymagające kompleksowej reakcji systemowej, wykraczającej poza same rozwiązania technologiczne;
- integracja działań: skuteczna ochrona wymaga synergii różnych obszarów: legislacji, działań organów ścigania (obejmujących zarówno czynności operacyjno-rozpoznawcze, jak i procesowe) oraz skoordynowanego wsparcia psychologicznego dla osób krzywdzonych;
- koordynacja i współpraca: wdrażanie tych ram w praktyce wymusza ścisłą koordynację krajową i transgraniczną, obejmującą współpracę państw, organizacji pozarządowych oraz sektora prywatnego (firm technologicznych).

Dokumenty i wytyczne międzynarodowe stanowią punkt odniesienia, który pomaga krajom w opracowywaniu własnych systemów ochrony dzieci w sieci.

Rozwiązania krajowe i ponadnarodowe w zakresie ochrony dzieci przed przemocą seksualną online

W odpowiedzi na międzynarodowe zobowiązania poszczególne państwa wdrażają zróżnicowane modele ochrony dzieci przed przemocą seksualną w środowisku cyfrowym. Obejmują one rozwiązania legislacyjne, instytucjonalne oraz technologiczne, a także systemy wsparcia dla ofiar i działania edukacyjne. W kolejnych akapitach omówiono szczegółowo specyfikę i mechanizmy działania poszczególnych systemów ochrony dzieci przed przemocą seksualną online w Australii, Wielkiej Brytanii, Unii Europejskiej oraz Stanach Zjednoczonych.

Australia

Australia jest uznawana za jedno z państw, które najwcześniej rozwinęły spójny, centralnie koordynowany system ochrony dzieci przed przemocą seksualną online. Ramy prawne systemu ochrony dzieci w Australii wzmacnia Online Safety Act (2021), który znacząco rozszerzył odpowiedzialność dostawców usług cyfrowych, wprowadzając obowiązek aktywnego zarządzania ryzykiem dla dzieci oraz sankcje za brak współpracy z organem nadzorczym (Australian Government, 2021). Regulacja ta kładzie nacisk na prewencję oraz projektowanie środowisk cyfrowych w sposób uwzględniający potrzeby i ograniczenia rozwojowe dzieci.

Tamtejszy eSafety Commissioner jest niezależnym organem rządowym powołanym do ochrony obywateli – w szczególności dzieci i młodzieży – przed szkodliwymi treściami w środowisku cyfrowym (Australian Government, 2023; eSafety Commissioner, 2022). Obejmuje zakaz mediów społecznościowych dla osób poniżej 16. roku życia. Od grudnia 2025 r. obowiązuje nowelizacja (*Social Media Minimum Age Act*), która nakłada na platformy (m.in. Facebook, TikTok, Instagram, X) obowiązek uniemożliwiania zakładania kont osobom poniżej 16 lat. Ustawa daje eSafety Commissioner uprawnienia do nakazywania platformom usuwania m.in. materiałów CSAM oraz tzw. *cyberbullyingu* (cyberprzemocy) skierowanego przeciwko małoletnim.

Jako instytucja centralna eSafety Commissioner posiada szerokie uprawnienia regulacyjne i interwencyjne, obejmujące przyjmowanie zgłoszeń dotyczących materiałów przedstawiających seksualne wykorzystywanie dzieci, wydawanie nakazów usunięcia treści oraz współpracę z platformami cyfrowymi i organami ścigania (Australian Government, 2023; eSafety Commissioner, 2022). Charakterystyczną cechą australijskiego modelu jest niski próg zgłoszeniowy, umożliwiający reagowanie

nie tylko na jednoznacznie nielegalne treści, ale również na zachowania potencjalnie krzywdzące, takie jak *grooming online* czy szantaż seksualny wobec dzieci. Przykładowo w 2022 r. eSafety Commissioner otrzymał ponad 25 tys. zgłoszeń dotyczących nielegalnych treści wobec dzieci, w tym ok. 1,5 tys. związanych z szantażem seksualnym wobec dzieci (eSafety Commissioner, 2022). W jednym z przypadków eSafety Commissioner zareagował na zgłoszenie szantażu wobec trzynastoletniego dziecka. Platforma natychmiast usunęła materiały, a sprawa została przekazana lokalnej policji, co umożliwiło szybkie zatrzymanie sprawcy (Australian Government, 2023). Interwencja obejmowała także wsparcie psychologiczne dla dziecka, prowadzone przez wyspecjalizowaną jednostkę terapeutyczną.

Istotnym elementem systemu australijskiego jest ścisłe powiązanie regulacji prawnych z edukacją i wsparciem psychologicznym. eSafety Commissioner prowadzi programy skierowane do dzieci, rodziców, nauczycieli oraz specjalistów zdrowia psychicznego, podkreślając konsekwencje przemocy seksualnej online dla dobrostanu psychicznego dziecka. W dokumentach strategicznych akcentuje się, że doświadczenia takie mogą prowadzić do objawów traumy, obniżonego poczucia bezpieczeństwa, zaburzeń obrazu siebie oraz trudności w relacjach interpersonalnych (Quadara i in., 2015).

Z perspektywy klinicznej australijski model wyróżnia się uznaniem przemocy seksualnej online za realne doświadczenie krzywdzenia, wymagające analogicznej reakcji systemowej, jak przemoc w świecie rzeczywistym. Współpraca między instytucjami regulacyjnymi, organami ścigania i systemem ochrony zdrowia sprzyja wczesnej identyfikacji zagrożeń oraz kierowaniu dzieci i ich rodzin do odpowiednich form pomocy specjalistycznej (Quadara i in., 2015).

Doświadczenia Australii pokazują, że skuteczna ochrona dzieci w środowisku cyfrowym wymaga nie tylko jednego, wyraźnego centrum regulacyjnego, ale również wysokospecjalistycznych struktur policyjnych. Przykładem takiego rozwiązania jest jednostka Taskforce Argos (funkcjonująca w ramach policji stanu Queensland), uznawana za jedną z pierwszych na świecie grup dedykowanych wyłącznie zwalczaniu zorganizowanej przestępczości seksualnej wobec dzieci oraz identyfikacji ofiar CSAM. Australijski model opiera się zatem na synergii działań regulatora (eSafety Commissioner) oraz zaawansowanych operacji organów ścigania przy jednoczesnym konsekwentnym uwzględnianiu wymiaru psychologicznego i rozwojowego w projektowaniu rozwiązań prawnych.

Wielka Brytania

Wielka Brytania jest często wskazywana jako przykład państwa rozwijającego kompleksowy system ochrony dzieci przed przemocą seksualną online, łączącego regulacje prawne, wielowymiarowe działania organów ścigania (obejmujące zarówno czynności operacyjno-rozpoznawcze, jak i procesowe) oraz wsparcie psychologiczne. System ten opiera się na modelu współpracy instytucjonalnej, w którym poszczególne podmioty pełnią odmienne, komplementarne funkcje w ekosystemie przeciwdziałania CSAM.

Istotną rolę odgrywa instytucja Internet Watch Foundation (IWF), która przyjmuje zgłoszenia dotyczące materiałów przedstawiających seksualne wykorzystywanie dzieci i współpracuje z dostawcami usług internetowych na całym świecie oraz prowadzi działania zmierzające do szybkiego usuwania nielegalnych materiałów (Internet Watch Foundation, 2023). Warto podkreślić, że IWF działa w ramach międzynarodowej sieci hotline'ów INHOPE (zrzeszającej obecnie 57 punktów zgłoszeń na całym świecie), co zapewnia organizacji bezpośrednią kooperację operacyjną z partnerskimi zespołami, w tym z polskim Działem Reagowania na Nielegalne Treści w Internecie – Dyżurnet.pl (NASK). Ponadto IWF monitoruje przypadki szantażu seksualnego, realizując działania zapobiegawcze i edukacyjne w zakresie przeciwdziałania wymuszaniu treści seksualnych w internecie.

Z kolei kompetencje śledcze i operacyjne należą do organów ścigania, przede wszystkim do National Crime Agency – CEOP Command, czyli wyspecjalizowanej jednostki policyjnej odpowiedzialnej za identyfikację sprawców, analizę zgłoszeń przekazywanych m.in. przez hotline'y oraz ochronę małoletnich zagrożonych wykorzystaniem seksualnym, w tym groomingiem online (National Crime Agency, 2022). Relacja między IWF a CEOP ma charakter komplementarny: organizacja pozarządowa koncentruje się na analizie treści i współpracy z branżą technologiczną, natomiast organy ścigania prowadzą działania procesowe i operacyjne wobec sprawców.

Ramy regulacyjne systemu zostały wzmocnione przez Online Safety Act (2023), który nałożył na platformy cyfrowe obowiązek aktywnego zarządzania ryzykiem i zapobiegania zagrożeniom wobec dzieci, w tym wykorzystywaniu seksualnemu, poprzez projektowanie usług z uwzględnieniem bezpieczeństwa małoletnich (UK Parliament, 2023). Regulacja ta przesuwa ciężar odpowiedzialności z reaktywnego usuwania treści (rozumianego jako podejmowanie interwencji przez platformę dopiero w odpowiedzi na zgłoszenie lub wykrycie naruszenia) na prewencję systemową, obejmującą m.in. projektowanie usług z myślą o bezpieczeństwie dzieci.

Dane Internet Watch Foundation wskazują, że w 2022 r. spośród ponad 375 tys. zgłoszeń dotyczących podejrzeń CSAM aż 199 tys. dotyczyło materiałów samodzielnie generowanych przez dzieci (ang. *self-generated content*), często powiązanych z presją rówieśniczą, manipulacją lub szantażem seksualnym. Zjawisko to podkreśla, że zagrożenia w środowisku cyfrowym nie ograniczają się wyłącznie do klasycznych przypadków seksualnego wykorzystywania dzieci, lecz obejmują także materiały wytwarzane przez same dzieci, które stają się narzędziem wyzysku i przemocy. W praktyce klinicznej i prewencyjnej oznacza to konieczność uwzględnienia w interwencjach mechanizmów edukacyjnych, wsparcia psychologicznego oraz działań profilaktycznych skierowanych na umiejętności cyfrowego bezpieczeństwa dzieci i młodzieży (Internet Watch Foundation, 2023).

Z perspektywy klinicznej i pomocowej ważną rolę odgrywają organizacje takie jak National Society for the Prevention of Cruelty to Children (NSPCC), które łączą działania rzecznicze (ang. *advocacy*), obejmujące aktywności podejmowane w celu ochrony praw dzieci oraz wpływania na rozwiązania systemowe i prawne sprzyjające ich bezpieczeństwu, z bezpośrednim wsparciem małoletnich i rodzin doświadczających przemocy seksualnej, również w jej formach online (NSPCC, 2021). Organizacja ta prowadzi infolinię ChildLine oraz tworzy kampanie informacyjne – np. *Underwear Rule* (Zasada Bielizny), uczące dzieci zasad bezpieczeństwa.

Brytyjskie podejście coraz wyraźniej uwzględnia fakt, że przemoc seksualna w internecie może prowadzić do długotrwałych konsekwencji psychologicznych, porównywalnych z przemocą offline, w tym objawów traumy, zaburzeń lękowych oraz trudności w relacjach interpersonalnych (Livingstone, Stoilova, 2021a). Model brytyjski pokazuje, że skuteczna ochrona dzieci wymaga nie tylko narzędzi prawnych i technologicznych, ale także dostępnych ścieżek wsparcia klinicznego, które umożliwiają wczesną interwencję oraz długofalową pomoc ofiarom przemocy.

Unia Europejska

Unia Europejska (UE) rozwija system ochrony dzieci przed przemocą seksualną online przede wszystkim poprzez harmonizację regulacji prawnych oraz wzmacnianie współpracy między państwami członkowskimi.

Według raportów Agencji Praw Podstawowych UE (*Fundamental Rights Survey*, FRA) oraz organizacji partnerskich zjawisko wymuszeń seksualnych online wobec małoletnich wykazuje wyraźną tendencję wzrostową. Dostępne raporty ujawniają wzrost liczby zgłoszeń dotyczących szantażu seksualnego wobec dzieci i młodzieży w krajach UE, jednak skala zjawiska jest trudna do precyzyjnego oszacowania

z uwagi na ograniczenia metodyczne badań i wysoki poziom nieujawniania przypadków naruszenia (European Union Agency for Fundamental Rights, 2021).

Centralnym aktem prawnym w Unii Europejskiej jest Digital Services Act (DSA), który wprowadza jednolite obowiązki dla platform cyfrowych w zakresie reagowania na treści nielegalne, w tym materiały przedstawiające seksualne wykorzystywanie dzieci (European Parliament & Council of the European Union, 2022). DSA zobowiązuje największe platformy do prowadzenia ocen ryzyka systemowego, uwzględniających zagrożenia dla praw dziecka, oraz do wdrażania środków ograniczających ekspozycję dzieci na szkodliwe treści. Akt ten wskazuje ponadto, że platformy powinny uwzględniać ryzyko szantażu seksualnego wobec dzieci w ocenie treści oraz stosować mechanizmy zgłaszania i blokowania takich przypadków. Regulacja ta przesuwa punkt ciężkości z działań reaktywnych na odpowiedzialność strukturalną dostawców usług cyfrowych, choć pozostawia państwom członkowskim znaczną autonomię w zakresie interwencji klinicznych i pomocowych.

Równolegle Komisja Europejska proponuje odrębne rozporządzenie mające na celu zapobieganie i zwalczanie seksualnego wykorzystywania dzieci, obejmujące m.in. obowiązek wykrywania i zgłaszania treści CSAM, w tym przypadków szantażu seksualnego wobec dzieci, oraz wzmocnienie współpracy transgranicznej (European Commission, 2022). Propozycje te wywołują intensywną debatę dotyczącą proporcji między ochroną dzieci a prawem do prywatności, co pokazuje napięcie charakterystyczne dla unijnego modelu regulacyjnego.

Z perspektywy klinicznej system unijny pozostaje rozproszony, ponieważ dostęp do wsparcia psychologicznego i terapeutycznego zależy głównie od krajowych systemów ochrony zdrowia i pomocy społecznej. Jednocześnie dokumenty UE coraz częściej uznają przemoc seksualną online za doświadczenie potencjalnie traumatyczne, wymagające skoordynowanej odpowiedzi obejmującej identyfikację, ochronę oraz długofalowe wsparcie dla osób skrzywdzonych (European Union Agency for Fundamental Rights, 2021). Model unijny ilustruje znaczenie ram prawnych jako narzędzia porządkującego odpowiedzialność platform, jednak jego skuteczność kliniczna zależy w dużej mierze od implementacji na poziomach krajowych. Parlament Europejski popiera nieobowiązkową rezolucję o ustaleniu minimalnego wieku korzystania z mediów społecznościowych (European Parliament, 2023).

Uzupełnieniem wymiaru legislacyjnego są działania operacyjne koordynowane na poziomie wspólnotowym przez Europol (Agencję Unii Europejskiej ds. Współpracy Organów Ścigania). Mimo że UE nie posiada własnych sił policyjnych o kompetencjach wykonawczych, w strukturach Europolu funkcjonuje Europejskie Centrum Cyberprzestępczości (EC3), które wspiera państwa członkowskie w reagowaniu

na zagrożenia cyfrowe. Kluczową rolę w systemie ochrony odgrywa tu projekt analityczny Analysis Project Twins, dedykowany zwalczaniu poważnej i zorganizowanej cyberprzestępczości popełnianej na szkodę dzieci, w tym identyfikacji sprawców produkcji i dystrybucji materiałów CSAM.

Stany Zjednoczone

System ochrony dzieci w USA opiera się na obowiązkowym raportowaniu wykrytych treści CSAM do National Center for Missing & Exploited Children (NCMEC), który pełni funkcję centralnego węzła między platformami cyfrowymi, organami ścigania i instytucjami wsparcia (NCMEC, 2023). Federalne przepisy podkreślają znaczenie współpracy między sektorem publicznym a prywatnym oraz szerokiego wykorzystania narzędzi technologicznych do detekcji nielegalnych treści (U.S. Congress, 2008). Platformy cyfrowe mają ustawowy obowiązek zgłaszania podejrzeń dotyczących materiałów przedstawiających seksualne wykorzystywanie dzieci, a brak raportowania może skutkować odpowiedzialnością prawną. W ramach ochrony prywatności dzieci w internecie wprowadzono m.in. Children's Online Privacy Protection Act (16 C.F.R. §312, Federal Trade Commission, 2000), której celem jest zabezpieczenie danych osobowych dzieci poniżej 13. roku życia – zarówno amerykańskich, jak i spoza USA – korzystających z serwisów internetowych adresowanych do dzieci lub gromadzących dane osobowe dzieci poniżej 13. roku życia, o czym wiedzą operatorzy tych serwisów.

W dyskusji legislacyjnej znajdują się także projekty takie jak The EARN IT Act (Eliminating Abusive and Rampant Neglect of Interactive Technologies Act), które zakładają dalsze zmiany w prawie odpowiedzialności platform online. Zwolennicy argumentują, że firmy technologiczne powinny „zasłużyć" na swój immunitet prawny, przestrzegając standardów bezpieczeństwa dzieci, natomiast obrońcy prywatności ostrzegają, że przepisy te mogą wymusić osłabienie szyfrowania end-to-end (ang. *end-to-end encryption*), narażając wszystkich użytkowników na utratę prywatności (NCMEC, 2023).

W 2022 r. NCMEC odnotował ok. 21,7 mln zgłoszeń CyberTipline, w tym ok. 1,2 mln przypadków szantażu seksualnego wobec dzieci oraz materiałów samodzielnie generowanych przez dzieci, wykorzystywanych przez sprawców do wymuszeń seksualnych. Dane te wskazują, że zagrożenia obejmują zarówno tradycyjne przypadki seksualnego wykorzystywania dzieci, jak i treści tworzone pod presją rówieśników, manipulacją lub wymuszeniem.

Model amerykański przywiązuje szczególną wagę do instrumentów egzekwowania prawa oraz instytucjonalizacji obowiązków raportowania i analizy treści CSAM, realizowanych m.in. poprzez system CyberTipline NCMEC. W praktyce wykorzystuje się zaawansowane technologie analityczne, w tym systemy *hash matching*, służące identyfikacji znanych nielegalnych treści. Należy jednak podkreślić, że technologie automatycznej detekcji stosowane są również w innych jurysdykcjach, m.in. w Wielkiej Brytanii (Internet Watch Foundation), Australii (jednostka ARGOS) oraz na poziomie europejskim, gdzie EUROPOL rozwija wyspecjalizowane systemy analizy danych i bazy CSAM. Współpracę międzynarodową wspierają organizacje takie jak INHOPE, ECPAT, TechCoalition, Europol i Interpol. Różnice między systemami dotyczą przede wszystkim charakteru instytucjonalnego i regulacyjnego – alokacji odpowiedzialności między sektorem publicznym a prywatnym oraz proporcji między komponentem represyjnym, regulacyjnym i prewencyjnym – a nie samego stosowania zaawansowanych technologii.

Ramy prawne tworzą m.in. PROTECT Our Children Act oraz przepisy dotyczące obowiązków dostawców usług elektronicznych, które wzmacniają współpracę między państwem a firmami technologicznymi (U.S. Congress, 2008). W przeciwieństwie do modeli europejskich regulacje amerykańskie koncentrują się przede wszystkim na identyfikacji sprawców i zabezpieczeniu materiału dowodowego, a w mniejszym stopniu – na prewencji systemowej. Z perspektywy klinicznej system bywa krytykowany za ograniczone powiązanie procedur prawnych z kompleksowym wsparciem terapeutycznym dla dzieci i rodzin (Mitchell, Jones, 2015). Badania wskazują, że dzieci doświadczające przemocy seksualnej online mogą wymagać długotrwałej pomocy psychologicznej, niezależnie od skuteczności działań represyjnych wobec sprawców (Finkelhor i in., 2020).

Podsumowanie porównawcze analizowanych modeli

Aby uporządkować obowiązujące ramy prawne i mechanizmy ochrony dzieci przed przemocą seksualną w środowisku cyfrowym, poniżej przedstawiono porównawczą tabelę dotyczącą Australii, Wielkiej Brytanii, Unii Europejskiej i Stanów Zjednoczonych. Obejmuje ona cztery główne wymiary: konwencje międzynarodowe i prawa człowieka, najważniejsze krajowe lub unijne akty prawne, instytucje centralne odpowiedzialne za ochronę dzieci oraz fundamentalne mechanizmy reagowania i prewencji. Prezentacja w formie zestawienia umożliwia szybkie zorientowanie się w różnicach i podobieństwach pomiędzy systemami, a także podkreśla rolę zarówno regulacji prawnych, jak i instytucjonalnych w zapewnianiu bezpieczeństwa dzieci w internecie.

Tabela 1

Porównanie modeli ochrony dzieci przed przemocą seksualną online w wybranych jurysdykcjach

Jurysdykcja/ obszar	Kluczowe akty prawne i regulacje	Instytucje wiodące i wspierające	Specyfika modelu i mechanizmy ochrony
Australia	– **Online Safety Act 2021** (kompleksowa regulacja bezpieczeństwa online) – Social Media Minimum Age Act (nowelizacja z 2024/2025 r. wprowadzająca zakaz mediów społecznościowych dla osób poniżej 16. r.ż.)	– **eSafety Commissioner** (centralny organ regulacyjny) – Taskforce Argos (wyspecjalizowana jednostka policji Queensland)	– **Model scentralizowany:** silna pozycja regulatora (eSafety) z uprawnieniami do nakładania kar i nakazów usunięcia treści – **Safety by Design:** prawny obowiązek projektowania bezpiecznych usług – **Niski próg reakcji:** Interwencja nie tylko przy treściach nielegalnych, ale i szkodliwych (np. cyberprzemoc)
Wielka Brytania	– **Online Safety Act 2023** (obowiązek zarządzania ryzykiem przez platformy)	– **National Crime Agency – CEOP Command** (organy ścigania) – **Internet Watch Foundation (IWF)** (NGO/ Hotline) – **NSPCC** (wsparcie kliniczne/rzecznicze)	– **Model hybrydowy (publiczno-prywatny):** ścisła współpraca policji (CEOP) z sektorem NGO (IWF) – **Systemowa prewencja:** przesunięcie odpowiedzialności na platformy za zapobieganie szkodom – **Focus na treści wytwarzane przez dzieci:** reakcja na rosnącą skalę self-generated content
Unia Europejska	– **Digital Services Act (DSA)** – Rozporządzenie (UE) 2022/2065 (obowiązki dla platform w zakresie oceny ryzyka) – Projekt: Rozporządzenie dotyczące zapobiegania i zwalczania niegodziwego traktowania dzieci w celach seksualnych (tzw. CSAM Regulation) – Dyrektywa 2011/93/UE (zwalczanie niegodziwego traktowania seksualnego)	– **Europol** (European Cybercrime Centre – EC3; AP Twins) – **Komisja Europejska** (rola legislacyjna i nadzorcza w ramach DSA) – Sieć **INHOPE** (krajowe hotline'y)	– **Model regulacyjno-koordynacyjny:** harmonizacja prawa na poziomie wspólnotowym – **Odpowiedzialność strukturalna:** DSA wymusza na platformach ocenę ryzyka systemowego dla praw dziecka – **Napięcie regulacyjne:** silny nacisk na ochronę prywatności (RODO/e-Privacy), ścierający się z potrzebą detekcji treści (debata nad Chat Control)
Stany Zjednoczone	– **PROTECT Our Children Act 2008** – **COPPA** (Children's Online Privacy Protection Act – ochrona danych dzieci <13 r.ż.) – 18 U.S. Code §2258A (obowiązek raportowania)	– **National Center for Missing & Exploited Children (NCMEC)** – CyberTipline (centralny węzeł zgłoszeniowy) – Lokalne i federalne organy ścigania (FBI, ICAC)	– **Model obligatoryjnego raportowania:** ustawowy obowiązek zgłaszania CSAM przez dostawców usług do NCMEC – **Dominacja podejścia karnego:** system zorientowany na identyfikację sprawców i zabezpieczanie dowodów (hash matching) – **Słabsze ogniwo:** ograniczone systemowe powiązanie ścigania ze wsparciem terapeutycznym

Źródło: opracowanie własne na podstawie analizowanych aktów prawnych i raportów (stan na luty 2026).

Reasumując, analiza rozwiązań funkcjonujących w Australii, Wielkiej Brytanii, na poziomie Unii Europejskiej oraz w Stanach Zjednoczonych wskazuje, że ochrona dzieci przed przemocą seksualną online przyjmuje odmienne formy organizacyjno-prawne, jednak opiera się na kilku wspólnych założeniach. We wszystkich badanych jurysdykcjach przemoc seksualna w środowisku cyfrowym jest uznawana za realne doświadczenie krzywdzenia dziecka, wymagające reakcji systemowej, a nie jedynie problem technologiczny (Quadara i in., 2015; Livingstone, Stoilova, 2021a; European Union Agency for Fundamental Rights, 2021; Finkelhor i in., 2020).

Model australijski i brytyjski wyróżnia się wysokim stopniem integracji działań. Oba systemy posiadają wyraźnie zidentyfikowane instytucje centralne (eSafety Commissioner; IWF/CEOP), które łączą kompetencje regulacyjne, interwencyjne i edukacyjne (eSafety Commissioner, 2022; Internet Watch Foundation, 2023; National Crime Agency, 2022). Charakterystyczne jest tu uznanie, że skuteczna ochrona dzieci wymaga nie tylko usuwania nielegalnych treści i ścigania sprawców, ale również wczesnej interwencji oraz dostępu do wsparcia psychologicznego dla dzieci i ich rodzin (Quadara i in., 2015; NSPCC, 2021; Livingstone, Stoilova, 2021a).

Model unijny ma przede wszystkim charakter regulacyjno-koordynacyjny. Unia Europejska tworzy ramy prawne zwiększające odpowiedzialność platform cyfrowych i ułatwiające współpracę transgraniczną (European Parliament & Council of the European Union, 2022; European Commission, 2022), pozostawiając jednak państwom członkowskim znaczną swobodę w zakresie organizacji pomocy klinicznej. W efekcie ochrona dzieci przed przemocą seksualną online na poziomie UE jest silnie zależna od krajowych systemów ochrony dziecka i zdrowia psychicznego (European Union Agency for Fundamental Rights, 2021; European Parliament, 2023).

System amerykański opiera się głównie na obowiązkowym raportowaniu i egzekwowaniu prawa karnego, z centralną rolą instytucji pośredniczącej między platformami cyfrowymi a organami ścigania (NCMEC, 2023; U.S. Congress, 2008; Federal Trade Commission, 2000). Choć model ten umożliwia skuteczną identyfikację sprawców i szybkie zabezpieczanie materiałów dowodowych, jego słabą stroną jest ograniczone powiązanie procedur prawnych z kompleksowym wsparciem terapeutycznym dla osób krzywdzonych (Mitchell, Jones, 2015; Finkelhor i in., 2020).

Przedstawione rozwiązania pokazują, że systemy ochrony dzieci przed przemocą seksualną online są najbardziej efektywne tam, gdzie odpowiedzialność państwa, platform cyfrowych i instytucji pomocowych jest jasno określona i wzajemnie skoordynowana (eSafety Commissioner, 2022; Internet Watch Foundation, 2023; NCMEC, 2023; European Commission, 2022). W obliczu rozwoju nowych form przemocy cyfrowej, w tym wykorzystania sztucznej inteligencji, konieczne staje się dalsze

wzmacnianie mechanizmów prewencji oraz przygotowanie systemów ochrony dziecka i zdrowia psychicznego do reagowania na nowe, złożone formy krzywdzenia. Analizowane rozwiązania potwierdzają, że ochrona dzieci w środowisku cyfrowym wymaga podejścia wielowymiarowego, obejmującego zarówno prewencję, interwencję, jak i długoterminowe wsparcie rozwojowe (Quadara i in., 2015; Livingstone, Stoilova, 2021a; Finkelhor i in., 2020).

Zakończenie

Przeprowadzona analiza międzynarodowych ram prawnych wskazuje, że choć istnieje rozbudowany system instrumentów prawnych oraz instytucjonalnych mających na celu przeciwdziałanie przemocy seksualnej wobec dzieci w środowisku cyfrowym, mechanizmy te nie zawsze nadążają za dynamicznym rozwojem technologii informacyjnych. Szczególnym wyzwaniem stają się nowe formy nadużyć wykorzystujące generatywną sztuczną inteligencję, w tym *AI-generated abuse*, a także szantaż seksualny wobec dzieci, oparty na syntetycznych treściach wizualnych i dźwiękowych, które często wymykają się tradycyjnym definicjom prawnym i klasycznym modelom odpowiedzialności.

Porównanie rozwiązań przyjętych w Australii, Wielkiej Brytanii, Unii Europejskiej oraz Stanach Zjednoczonych pokazuje, że skuteczność ochrony dzieci nie zależy wyłącznie od zakresu penalizacji określonych zachowań, lecz w równym stopniu od istnienia wyspecjalizowanych instytucji, sprawnych mechanizmów egzekwowania prawa oraz zdolności systemów prawnych do adaptacji do nowych zagrożeń technologicznych. W analizowanych jurysdykcjach coraz wyraźniej widoczna jest tendencja do przesuwania akcentu z reaktywnego ścigania przestępstw na działania prewencyjne i wczesną interwencję, obejmujące obowiązki nakładane na platformy cyfrowe, rozwój narzędzi automatycznej detekcji treści oraz funkcjonowanie wyspecjalizowanych punktów zgłoszeń. Jednocześnie doświadczenia międzynarodowe jednoznacznie wskazują, że rozwiązania technologiczne nie mogą być traktowane jako wystarczające bez równoległego rozwoju systemów wsparcia klinicznego.

Z perspektywy psychologicznej przemoc seksualna online wiąże się z poważnymi i długofalowymi konsekwencjami dla zdrowia psychicznego dzieci, w tym zwiększonym ryzykiem zaburzeń lękowych i depresyjnych, objawów stresu pourazowego oraz trudności w budowaniu relacji interpersonalnych. Skuteczna ochrona dzieci powinna zatem obejmować nie tylko eliminowanie nielegalnych treści i identyfikację sprawców, lecz także zapewnienie dzieciom i ich rodzinom dostępu do długoterminowej pomocy psychologicznej.

Doświadczenia analizowanych krajów pokazują, że najbardziej efektywne systemy ochrony dzieci przed przemocą seksualną online charakteryzują się spójnością działań, jasnym podziałem odpowiedzialności oraz ścisłą współpracą między instytucjami publicznymi, organizacjami pozarządowymi i sektorem technologicznym. Wnioski te mogą stanowić istotny punkt odniesienia dla dalszych debat nad kształtowaniem kompleksowych strategii ochrony dzieci w cyfrowej rzeczywistości, uwzględniających zarówno wymiar prawny, technologiczny, jak i kliniczny.

E-mail autorki: **dor.mroczkowska@wp.pl**

Bibliografia

Australian Government (2021). *Online Safety Act 2021*. https://www.legislation.gov.au/Details/C2021A00058

Australian Government (2023). *eSafety Commissioner: Functions and powers*. https://www.esafety.gov.au/about-us

Council of Europe (2007). *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention)*. https://www.coe.int/en/web/children/lanzarote-convention

eSafety Commissioner (2022). *Protecting children from online sexual harm*. https://www.esafety.gov.au/reports/protecting-children-online

European Commission (2022). *Proposal for a regulation to prevent and combat child sexual abuse*. https://ec.europa.eu/info/publications/proposal-regulation-prevent-child-sexual-abuse_en

European Parliament & Council of the European Union (2022). *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065

European Commission (2022). *Proposal for a regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse. Publications Office of the European Union*.

European Union Agency for Fundamental Rights (2021). *Your rights matter: Security concerns and experiences. Publications Office of the European Union*. https://fra.europa.eu/

Europol (2023). *Internet organised crime threat assessment (IOCTA) 2023*. https://www.europol.europa.eu

Europol (2024). *Internet Organised Crime Threat Assessment (IOCTA) 2024. Publications Office of the European Union*. https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024

Federal Trade Commission (2000). *Final rule implementing the Children's Online Privacy Protection Act (16 C.F.R. §312)*. https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa

Finkelhor, D., Jones, L.M. (2006). Why have child maltreatment and child victimization declined? *Journal of Social Issues*, 62(4), 685–716. https://doi.org/10.1111/j.1540-4560.2006.00483.x

Finkelhor, D., Wolak, J., Mitchell, K.J. (2020). Online sexual exploitation of children: Consequences and responses. *Springer*. https://doi.org/10.1007/978-3-030-20786-3

INHOPE (2024). *INHOPE Annual Report 2024*. https://inhope.org/articles/inhope-annual-report-2024

Internet Watch Foundation (2023). *Annual report 2023*. https://www.iwf.org.uk/about-us/annual-report

Livingstone, S., Stoilova, M. (2021a). *The impact of online sexual abuse on children's mental health. London School of Economics and Political Science*. https://www.lse.ac.uk/media-and-communications/assets/documents/research/impact-of-online-abuse.pdf

Livingstone, S., Stoilova, M. (2021b). *The 4Cs: Classifying Online Risks to Children*. CO:RE – Children Online: Research and Evidence.

Mitchell, K.J., Jones, L.M. (2015). Technology-facilitated sexual abuse of children. *Child Abuse & Neglect*, 45, 1–3. https://doi.org/10.1016/j.chiabu.2015.02.002

National Center for Missing & Exploited Children (2023). *The scourge of child sexual abuse material: Annual report on online exploitation and protection initiatives*. https://www.missingkids.org/gethelpnow/cybertipline

National Crime Agency (2022). *CEOP Command: Protecting children from sexual exploitation*. https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/child-abuse

NSPCC (2021). *Online sexual abuse: Supporting children and families*. https://www.nspcc.org.uk/what-we-do/news-opinion/online-sexual-abuse/

Tech Coalition (2023). *Addressing AI-generated child sexual exploitation and abuse*. https://technologycoalition.org

Quadara, A., Wall, L., Higgins, D. (2015). *The impacts of child sexual abuse: A framework for understanding. Australian Institute of Family Studies*. https://aifs.gov.au/publications/impacts-child-sexual-abuse

UK Parliament (2023). *Online Safety Act 2023*. https://bills.parliament.uk/bills/3275

UNICEF (2021). *Protecting children online: Guidance for policymakers*. https://www.unicef.org/reports/protecting-children-online

United Nations (1989). *Convention on the Rights of the Child*. https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

U.S. Congress (2008). *PROTECT Our Children Act of 2008*. https://www.congress.gov/bill/110th-congress/house-bill/5281

WeProtect Global Alliance (2019). *Global threat assessment: Online child sexual exploitation*. https://www.weprotect.org/global-threat-assessment-2019

WeProtect Global Alliance (2023). *Global threat assessment on child sexual exploitation and abuse*. https://www.weprotect.org/global-threat-assessment-2023

WeProtect Global Alliance. (2024). *Global Threat Assessment 2024*. https://www.weprotect.org/global-threat-assessment-2024

Child Protection Systems Against Online Sexual Abuse in Selected Countries

Online sexual abuse of children constitutes one of the most significant contemporary threats to children's safety and well-being. The Internet and social media create new opportunities for the victimization of children, including grooming, sextortion, and the distribution of child sexual abuse material. This article presents a review of child protection systems addressing online sexual abuse in selected countries, with particular attention to legal, technological, and educational solutions implemented in Australia, the United Kingdom, the European Union, and the United States. The roles of the state, digital platforms, and child support institutions in responding to and preventing the escalation of online sexual violence are discussed. The analysis also highlights key challenges related to privacy protection, the effectiveness of law enforcement mechanisms, and the need for coherent and coordinated systemic responses. The aim of the article is to identify good practices and future directions for the development of child protection systems in the context of online sexual abuse.

Keywords:
child protection; child sexual abuse; online sexual abuse; child online safety; child protection system

Cytowanie:
Mroczkowska, D. (2026). Modele instytucjonalne i prawne przeciwdziałania OCSAE: studium porównawcze wybranych jurysdykcji. *Dziecko Krzywdzone. Teoria, badania, praktyka*, 25(1), 147–169.

Fundusz Sprawiedliwości
Ministerstwo Sprawiedliwości
Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości