BEZPIECZEŃSTWO DZIECI W CYBERPRZESTRZENI KLUCZOWE ZAGADNIENIA I PRZEPISY PRAWNE

OCHRONA OSÓB I MIENIA

7 STYCZNIA 2025

WSB SECURITY
MARCIN NIEDOPYTALSKI

W erze wszechobecnej cyfryzacji, intensywnie zmieniającej wszelkie aspekty życia społecznego i gospodarczego, cyberprzestrzeń stanowi nieodłączny element codziennego funkcjonowania zarówno dorosłych, jak i dzieci. Możliwości edukacyjne, rozrywkowe oraz komunikacyjne, jakie zapewnia internet, są bezprecedensowe w skali historii. Dzieci mają dziś dostęp do szerokiego wachlarza narzędzi online od platform e-learningowych, przez media społecznościowe, po gry sieciowe. Jednakże, obok licznych korzyści, dynamicznie rosnąca obecność najmłodszych w środowisku cyfrowym rodzi także poważne zagrożenia, na które warto zwrócić szczególną uwagę. W szczególności cyberprzemoc (ang. *cyberbullying*), nadużycia seksualne typu *grooming*, kontakt z nieodpowiednimi treściami, kradzież danych osobowych czy uzależnienie od internetu i gier komputerowych to zjawiska, które nabierają na sile w przestrzeni wirtualnej. Polskie prawo podobnie jak regulacje w innych krajach Unii Europejskiej – ewoluuje, by odpowiedzieć na nowe wyzwania. Odpowiednie przepisy krajowe i międzynarodowe koncentrują się na ochronie prywatności, sankcjonowaniu zachowań przestępczych oraz promowaniu edukacji w zakresie cyberbezpieczeństwa. Celem niniejszego opracowania jest ukazanie kluczowych aspektów związanych z bezpieczeństwem dzieci w cyberprzestrzeni. W artykule zostaną omówione główne zagrożenia, aktualne regulacje prawne, inicjatywy międzynarodowe, dostępne narzędzia i mechanizmy ochrony oraz znaczenie edukacji w kształtowaniu odpowiedzialnych postaw w internecie. Istotnym elementem będzie również przedstawienie wyzwań, jakie niesie przyszłość, w kontekście ciągle zmieniającej się natury środowiska cyfrowego.

Kluczowe zagrożenia dla dzieci w cyberprzestrzeni

2.1. Cyberprzemoc (cyberbullying)

Cyberprzemoc odnosi się do wszelkich form nękania, zastraszania, poniżania czy ośmieszania w internecie, na forach, portalach społecznościowych bądź przy użyciu komunikatorów. Kluczowym czynnikiem odróżniającym cyberprzemoc od klasycznego nękania jest ogromny zasięg i szybkość, z jaką treści mogą być udostępniane oraz trudność w usunięciu ich z przestrzeni wirtualnej. Dla dziecka konsekwencje tego zjawiska bywają bardzo dotkliwe psychicznie, nierzadko prowadząc do obniżonej samooceny, depresji czy w skrajnych przypadkach do prób samobójczych. Anonimowość, jaką zapewnia internet, jest czynnikiem ułatwiającym sprawcom działanie, a jednocześnie utrudniającym identyfikację. Dlatego szczególnie istotna jest współpraca rodziców, pedagogów oraz organów ścigania w procesie wykrywania i zwalczania cyberprzemocy.

2.2. Grooming

Grooming to proces uwodzenia dziecka w internecie w celu wykorzystania seksualnego. Sprawcy, podszywając się często pod rówieśników lub osoby godne zaufania, potrafią miesiącami manipulować dzieckiem, zdobywając jego przychylność i zaangażowanie emocjonalne. Ofiary, nieświadome faktycznej tożsamości rozmówcy, mogą być stopniowo nakłaniane do udostępniania treści intymnych bądź spotkań w świecie realnym. Grooming jest zjawiskiem szczególnie niebezpiecznym, wymagającym wzmożonej kontroli rodzicielskiej i edukacji dzieci w zakresie ostrożności w kontaktach z osobami poznanymi w sieci.

2.3. Nieodpowiednie treści

Internet, stanowiąc platformę niemal nieograniczonej wymiany informacji, zawiera także treści o charakterze pornograficznym, brutalnym czy promującym nienawiść. Dzieci mogą przypadkowo natrafić na materiały szkodliwe, których wpływ na ich psychikę i emocje bywa trudny do przewidzenia. Szczególnie negatywny wpływ mają treści przedstawiające przemoc, okrucieństwo względem ludzi czy zwierząt, a także promujące autodestrukcyjne zachowania. Wczesne zetknięcie się z takimi materiałami może zaburzać prawidłowy rozwój dziecka, kreować fałszywe wzorce i postawy.

2.4. Kradzież danych osobowych

Dzieci, nie mając dostatecznej świadomości zagrożeń wynikających z udostępniania danych osobowych, mogą łatwo paść ofiarą oszustw internetowych. Podawanie w sieci adresu zamieszkania, numerów telefonów, haseł czy danych o członkach rodziny stwarza liczne możliwości nadużyć, łącznie z kradzieżą tożsamości. Ponadto dane te mogą być sprzedawane w tzw. *darknecie*, wykorzystywane do podszywania się pod dziecko lub jego opiekunów w różnego rodzaju oszustwach czy kampaniach phishingowych.

2.5. Uzależnienie od internetu i gier komputerowych

Nadmierne korzystanie z urządzeń elektronicznych, gier sieciowych czy mediów społecznościowych przekłada się nie tylko na stan psychiczny dziecka, ale i na jego zdrowie fizyczne. Uzależnienie od internetu może prowadzić do zaburzeń koncentracji, trudności w kontaktach interpersonalnych i izolacji społecznej. Dodatkowo, brak aktywności fizycznej i długie godziny spędzane przed ekranem wpływają negatywnie na rozwój motoryczny, postawę ciała oraz mogą prowadzić do wad wzroku. Współcześnie psycholodzy i pedagodzy coraz częściej wskazują na konieczność świadomego balansowania między życiem offline a online.

Regulacje prawne dotyczące ochrony dzieci w cyberprzestrzeni

Wzrost świadomości społecznej na temat niebezpieczeństw związanych z korzystaniem z internetu przez dzieci skutkuje stopniowym zaostrzaniem regulacji prawnych. W Polsce oraz w obrębie Unii Europejskiej funkcjonuje szereg ustaw i przepisów mających na celu podniesienie poziomu bezpieczeństwa w sieci.

3.1. Ustawa o krajowym systemie cyberbezpieczeństwa (2018)

Ustawa ta określa zasady organizacji i funkcjonowania krajowego systemu cyberbezpieczeństwa, koncentrując się na infrastrukturze krytycznej i usługach kluczowych. Choć jej główne założenia dotyczą zabezpieczenia strategicznych zasobów państwa (np. sektora energetycznego, finansowego), to w praktyce wpływają również pośrednio na bezpieczeństwo dzieci w sieci. Mechanizmy współpracy operatorów usług kluczowych, dostawców usług cyfrowych oraz administracji publicznej przekładają się bowiem na wyższy ogólny poziom zabezpieczeń.

3.2. Rozporządzenie RODO (2016)

Rozporządzenie Ogólne o Ochronie Danych Osobowych (RODO) nakłada na podmioty przetwarzające dane szereg obowiązków, w tym dotyczących szczególnej ochrony danych dzieci. W Polsce wyznaczono granicę wieku na 16 lat – poniżej tej granicy wymagana jest

zgoda rodzica lub opiekuna prawnego na przetwarzanie danych osobowych. Administratorzy serwisów internetowych są zatem zobowiązani do weryfikacji wieku użytkowników, a także do informowania w sposób zrozumiały dla dzieci o celach i sposobach przetwarzania danych.

3.3. Ustawa Prawo oświatowe (2017)

Ustawa Prawo oświatowe wskazuje na obowiązek prowadzenia przez szkoły działań edukacyjnych w zakresie bezpieczeństwa w sieci. Placówki oświatowe mają obowiązek organizować zajęcia i warsztaty dotyczące cyberzagrożeń, w tym cyberprzemocy, uzależnień internetowych czy ochrony danych osobowych. Ważnym elementem jest także włączenie rodziców w proces edukacyjny poprzez spotkania informacyjne czy szkolenia dla rodziców na temat aktualnych trendów i zagrożeń w cyberprzestrzeni.

Kodeks karny

Polski Kodeks karny penalizuje zachowania zagrażające bezpieczeństwu dzieci w internecie:

1. **Grooming (art. 200a Kodeksu karnego)** – ustanawia odpowiedzialność karną za nawiązywanie kontaktu z małoletnim w celu wykorzystania seksualnego.
2. **Pornografia dziecięca (art. 202)** – penalizuje wytwarzanie, rozpowszechnianie oraz posiadanie treści pornograficznych z udziałem małoletnich.
3. **Cyberprzemoc** – choć nie jest zdefiniowana wprost, działania takie jak groźby (art. 190) czy znieważanie (art. 216) w internecie mogą być ścigane na mocy tych przepisów.

Dyrektywa NIS

Dyrektywa Unii Europejskiej o bezpieczeństwie sieci i informacji (NIS) zobowiązuje państwa członkowskie do podniesienia poziomu bezpieczeństwa usług kluczowych i infrastruktury cyfrowej. Dzięki temu powstają jednolite standardy ochrony, które – choć koncentrują się na skali makro – wpływają pozytywnie również na bezpieczeństwo indywidualnych użytkowników, w tym dzieci.

Inicjatywy międzynarodowe

4.1. Konwencja o Prawach Dziecka (1989)

Polska, jako sygnatariusz Konwencji o Prawach Dziecka, jest zobligowana do ochrony najmłodszych przed wszelkimi formami przemocy, wykorzystywania czy zaniedbania. W kontekście cyberprzestrzeni oznacza to konieczność wdrażania rozwiązań prawnych i instytucjonalnych mających na celu zapewnienie ochrony przed przemocą, uwodzeniem, a także gwarantujących poszanowanie prywatności dziecka.

4.2. UNICEF i kampanie edukacyjne

UNICEF prowadzi liczne globalne kampanie edukacyjne, skierowane zarówno do dzieci, jak i do rodziców oraz nauczycieli. Wśród nich znajdują się projekty mające na celu uświadamianie o zagrożeniach w sieci, zachęcanie do ostrożnego udostępniania danych osobowych i kształtowanie świadomych postaw. Dzięki międzynarodowemu zasięgowi, kampanie te przyczyniają się do wymiany doświadczeń i dobrych praktyk między różnymi krajami.

4.3. Międzynarodowy Dzień Bezpiecznego Internetu (Safer Internet Day)

Coroczne obchody *Safer Internet Day* mają za zadanie promowanie bezpiecznego i odpowiedzialnego korzystania z technologii cyfrowych. Organizowane w wielu krajach warsztaty, konferencje i akcje medialne sprzyjają budowaniu świadomości społecznej w zakresie odpowiednich zachowań online i znaczenia ochrony danych.

Narzędzia i mechanizmy ochrony dzieci w internecie

5.1. Kontrola rodzicielska

Mechanizmy kontroli rodzicielskiej pozwalają ograniczyć dostęp dzieci do niepożądanych treści, a także monitorować ich aktywność w sieci. Współczesne systemy operacyjne (Windows, macOS, Android, iOS) oferują wbudowane funkcje, takie jak:

- **Filtrowanie stron internetowych** – blokowanie stron zawierających treści erotyczne, przemoc czy wulgarne słownictwo.
- **Czasowe limity** – ustawianie przedziałów czasowych, w których dziecko może korzystać z urządzenia.
- **Monitorowanie aplikacji** – kontrola pobieranych programów i gier, weryfikacja ich kategorii wiekowych.

Podobne rozwiązania mogą być dostępne bezpośrednio w routerach (tzw. *parental control*) czy aplikacjach antywirusowych. Kluczowe jest jednak, by kontrola rodzicielska nie zastępowała rozmów i edukacji, ponieważ to przede wszystkim zaufany kontakt z opiekunem pozwala dziecku w pełni rozumieć zasady bezpiecznego korzystania z sieci.

5.2. Programy antywirusowe i zapory ogniowe

Dostęp do sieci, zwłaszcza poprzez różnorodne urządzenia mobilne, niesie ze sobą ryzyko infekcji wirusami, malware czy programami szpiegującymi. Zainstalowanie oprogramowania antywirusowego oraz regularne aktualizacje systemu operacyjnego stanowią podstawę ochrony przed tego rodzaju zagrożeniami. Z kolei zapory ogniowe (ang. *firewall*) pozwalają kontrolować ruch sieciowy, wykrywając potencjalnie niebezpieczne połączenia.

5.3. Edukacja dzieci

Najbardziej efektywną formą ochrony dzieci w cyberprzestrzeni jest kształtowanie ich świadomości w zakresie rozpoznawania zagrożeń i właściwych reakcji. Podstawowe zasady, które warto przekazać najmłodszym, obejmują:

- **Ostrożność przy nawiązywaniu znajomości** – przypominanie, że w sieci łatwo o fałszywe profile i podszywanie się pod rówieśników.
- **Nieudostępnianie danych osobowych** – wyjaśnianie, że adres zamieszkania, numer telefonu czy zdjęcia rodzinne to wrażliwe informacje.
- **Zgłaszanie niepokojących sytuacji** – zachęcanie, by dziecko zawsze informowało rodziców lub nauczycieli, gdy ktoś w sieci wzbudza jego niepokój lub prosi o dziwne rzeczy.

Współpraca międzyinstytucjonalna

W zwalczaniu cyberprzemocy, pedofilii w sieci i innych nadużyć internetowych istotną rolę pełni współpraca między policją, organami sądowymi, organizacjami pozarządowymi i szkołami. Coraz częściej powstają wyspecjalizowane jednostki zajmujące się cyberbezpieczeństwem (np. wydziały do walki z cyberprzestępczością w komendach policji), a także inicjatywy łączące różne podmioty w celu wymiany informacji, prowadzenia kampanii prewencyjnych czy pomocy ofiarom.

Edukacja jako kluczowy element ochrony dzieci

6.1. Rola szkół

Placówki oświatowe odgrywają kluczową rolę w szerzeniu wiedzy na temat zagrożeń w sieci i metod ich unikania. Poza obowiązkowymi lekcjami informatyki, coraz popularniejsze staje się prowadzenie warsztatów na temat:

- **Cyberprzemocy** – rozpoznawania i przeciwdziałania zachowaniom przemocowej w sieci.
- **Bezpieczeństwa w mediach społecznościowych** odpowiedzialnego korzystania z portali takich jak Facebook, Instagram, TikTok.
- **Ochrony danych osobowych i prywatności** – uświadamiania, jak proste może być przechwycenie i nielegalne wykorzystanie danych.

Wiele szkół we współpracy z ekspertami (np. organizacjami pozarządowymi) organizuje także spotkania z rodzicami, podczas których przedstawiane są aktualne zjawiska i trendy w cyberprzestrzeni, a także sposoby reagowania na zaobserwowane niepokojące zachowania dzieci.

6.2. Rola rodziców

Choć wiele osób oczekuje, że szkoła przejmie rolę edukatora w zakresie bezpieczeństwa online, to jednak to rodzice mają najwięcej możliwości, by kształtować postawy dzieci i kontrolować ich aktywność w sieci. Wspólne ustalanie zasad korzystania z urządzeń elektronicznych (np. limit dzienny, zakaz korzystania przed snem), rozmowy o ryzyku płynącym z nieodpowiedzialnych zachowań w internecie czy sprawdzanie ustawień prywatności w mediach społecznościowych to podstawowe działania, które powinny być podejmowane w każdym domu. Ważne jest także wzmacnianie więzi i zaufania między dzieckiem a rodzicem tak, by w razie trudnej sytuacji (np. próby zastraszania, podejrzanego kontaktu) dziecko nie obawiało się prosić o pomoc.

. Rola mediów społecznościowych

Serwisy społecznościowe, z uwagi na ogromną liczbę młodych użytkowników, stoją przed wyzwaniem zapewnienia im odpowiedniego poziomu ochrony. Wiele platform oferuje dziś narzędzia umożliwiające:

- **Zgłaszanie nieodpowiednich treści** – takich jak materiały pornograficzne, przemocowej czy mowa nienawiści.

- **Blokowanie niechcianych użytkowników** – prosta opcja pozwala dziecku uniknąć kontaktu z nękającą je osobą.
- **Algorytmy automatycznie wykrywające treści szkodliwe** – choć w praktyce narzędzia te nie są doskonałe, widać postępującą poprawę w ich działaniu.

Jednakże z perspektywy rodziców i dzieci istotne jest, by platformy kierowały się zasadą *privacy by design* i *privacy by default*, czyli uwzględniały kwestie prywatności już na etapie projektowania swoich rozwiązań oraz domyślnie stosowały najwyższe ustawienia ochrony.

Dynamiczny rozwój technologii

Postęp technologiczny obejmuje nie tylko nowe aplikacje, gry czy serwisy społecznościowe, ale także złożone systemy sztucznej inteligencji (AI). Z jednej strony AI może wspierać moderowanie treści (np. szybciej wykrywać pornografię dziecięcą, mowę nienawiści), z drugiej może stwarzać nowe zagrożenia. Przykładowo, algorytmy mogą zostać wykorzystane do tworzenia fałszywych tożsamości (tzw. *deepfake*), które posłużą przestępcom do uwodzenia dzieci bądź szantażowania ich. Kluczowe będzie opracowywanie nowych regulacji i standardów etycznych, które uchronią najmłodszych przed skutkami nieodpowiedzialnego wykorzystywania zaawansowanych technologii. Państwa członkowskie UE oraz organizacje międzynarodowe już podejmują działania legislacyjne, lecz tempo zmian w świecie cyfrowym wymaga stałej aktualizacji obowiązujących przepisów. Mimo wzrostu liczby kampanii edukacyjnych i dostępnych materiałów, wciąż istnieje grupa rodziców, nauczycieli czy samych dzieci, którzy nie są świadomi skali zagrożeń czy nie potrafią korzystać z dostępnych narzędzi ochrony. Szczególnie w małych miejscowościach lub mniej zasobnych regionach dostęp do edukacji cyfrowej bywa ograniczony. Problem ten potęguje się, gdy rodzice sami nie czują się kompetentni w zakresie korzystania z technologii. Ważnym wyzwaniem jest także dotarcie do dzieci z przekazem dopasowanym do ich języka i sposobu korzystania z internetu. Konieczne staje się zatem prowadzenie nowoczesnych kampanii edukacyjnych, które uwzględniają dynamiczny charakter trendów wśród młodych ludzi (np. krótkie filmy, infografiki, aplikacje mobilne uczące bezpiecznych zachowań). Internet nie zna granic państwowych. Cyberprzestępcy mogą działać z dowolnego miejsca na świecie, co znacznie utrudnia egzekwowanie prawa i ściganie sprawców przestępstw wobec dzieci. Współpraca międzynarodowa – zarówno między organami ścigania, jak i organizacjami pozarządowymi oraz firmami technologicznymi jest niezbędna, by skutecznie reagować na globalne zagrożenia. Instytucje takie jak Europol czy INTERPOL coraz częściej powołują wyspecjalizowane zespoły do walki z cyberprzestępczością, jednak ich skuteczność zależy od szybkości wymiany informacji i ujednolicenia procedur w różnych krajach. Zapewnienie bezpieczeństwa dzieci w cyberprzestrzeni to zadanie wieloaspektowe, wymagające zaangażowania i współpracy licznych podmiotów: rodziców, szkół, instytucji państwowych, międzynarodowych organizacji, sektora prywatnego oraz samych dzieci. Rosnące uzależnienie społeczeństwa od technologii cyfrowych sprawia, że minimalizowanie ryzyka związanego z internetem staje się priorytetem. Z jednej strony kluczową rolę odgrywają odpowiednie regulacje prawne. Polskie ustawodawstwo od ustawy o krajowym systemie cyberbezpieczeństwa, przez przepisy Kodeksu karnego, po ustawę Prawo oświatowe w coraz większym stopniu bierze pod uwagę potrzeby ochrony najmłodszych użytkowników sieci. Dodatkowo Rozporządzenie RODO nakłada na administratorów danych obowiązek szczególnego zabezpieczania informacji dotyczących dzieci. Z drugiej strony, prawo nie może

funkcjonować w próżni konieczne jest wprowadzenie realnych mechanizmów egzekwowania przepisów oraz rozwijanie infrastruktury i narzędzi, które pozwolą na skuteczne zwalczanie cyberprzestępczości. Ważnym czynnikiem jest edukacja, stanowiąca swego rodzaju „szczepionkę" przeciw zagrożeniom cyfrowego świata. Zarówno szkoły, jak i rodzice powinni kłaść nacisk na kształtowanie właściwych nawyków korzystania z internetu, począwszy od nieudostępniania danych osobowych, poprzez rozpoznawanie przejawów cyberprzemocy, aż po świadomość tego, jak działa phishing czy inne formy manipulacji online. Zbudowanie atmosfery zaufania między dziećmi a dorosłymi sprawia, że najmłodsi użytkownicy sieci są skłonni szukać pomocy i reagować w sytuacjach wymagających interwencji. Nie mniejsze znaczenie mają działania profilaktyczne i inicjatywy międzynarodowe, jak Konwencja o Prawach Dziecka czy kampanie UNICEF, które wyznaczają globalne standardy ochrony i promują współpracę ponad granicami. W tym kontekście należy pamiętać o *Safer Internet Day*, kiedy to na całym świecie organizuje się wydarzenia poświęcone edukacji i integracji różnych środowisk w celu wspólnej walki z zagrożeniami w sieci. Przyszłość z pewnością przyniesie dalszy rozwój technologii, co z jednej strony może ułatwiać wykrywanie i zwalczanie zagrożeń (np. dzięki sztucznej inteligencji), a z drugiej – stwarzać nowe niebezpieczeństwa, zwłaszcza w kontekście cyberprzemocy czy uwodzenia dzieci w sieci. Sprostanie tym wyzwaniom będzie wymagało nieustannego aktualizowania przepisów, rozszerzania kompetencji służb odpowiedzialnych za bezpieczeństwo, jak również ciągłej edukacji społeczeństwa. Ochrona dzieci w cyberprzestrzeni musi być postrzegana jako proces długofalowy i wielopłaszczyznowy, łączący aspekty prawne, techniczne, społeczne i edukacyjne. Tylko kompleksowe podejście pozwoli skutecznie minimalizować zagrożenia i umożliwi najmłodszym bezpieczne korzystanie z dobrodziejstw technologii cyfrowych. Współcześnie, gdy tempo rozwoju technologii przyspiesza w sposób wykładniczy, a globalna dostępność internetu wciąż się zwiększa, kwestia bezpieczeństwa dzieci w cyberprzestrzeni wymaga nie tylko uwagi, ale także proaktywnego działania ze strony wszystkich uczestników życia społecznego. Należy przy tym podkreślić, że dzieci, wchodzące dopiero w okres kształtowania swojej tożsamości i osobowości, są w szczególny sposób narażone na rozmaite niebezpieczeństwa sieciowe: począwszy od niewłaściwych treści, przez manipulację, aż po przestępczość zorganizowaną, która zyskuje nowe możliwości w ramach wirtualnych społeczności. Uwzględniając szeroki wachlarz ryzyk pojawiających się w internecie, nie sposób zignorować wyzwań związanych z rozwojem technologii immersyjnych, takich jak wirtualna rzeczywistość (VR) czy rozszerzona rzeczywistość (AR), które choć niosą ogromny potencjał edukacyjny i kreatywny mogą stanowić kolejny obszar nieetycznych działań dorosłych wobec najmłodszych lub rodzić niebezpieczne wzorce zachowań przekładających się na życie codzienne. Kolejnym zagadnieniem wymagającym uwagi jest postępująca miniaturyzacja urządzeń i cyfrowa konwergencja, która sprawia, że granice między światem online i offline zacierają się coraz bardziej. Smartfony, tablety, konsole do gier oraz inteligentne zegarki to dzisiaj standard w wielu gospodarstwach domowych, a dostęp do szybkiego internetu stał się czymś oczywistym dla większości społeczeństwa. Dzieci, które wychowują się w takim otoczeniu, bardzo wcześnie zaczynają posługiwać się urządzeniami elektronicznymi, często nie mając jeszcze wykształconej zdolności krytycznego myślenia ani umiejętności rozpoznawania zagrożeń. Skutkiem tego może być zwiększona podatność na zjawiska typu phishing, sexting czy inne formy internetowych manipulacji. Dodatkowo, wirtualne portale społecznościowe sprzyjają powstawaniu złożonych relacji interpersonalnych, w ramach których anonimowi użytkownicy w łatwy sposób docierają do nieletnich i mogą ich psychicznie bądź emocjonalnie

wykorzystywać. W kontekście tworzenia efektywnych strategii przeciwdziałania tym zagrożeniom kluczowe znaczenie ma interdyscyplinarność działań. Z jednej strony niezbędne są odpowiednie regulacje prawne, sankcjonujące zachowania zagrażające dobru dziecka. Z drugiej zaś istotne jest promowanie rozwiązań technologicznych, które zabezpieczają najmłodszych użytkowników, wspierając np. monitorowanie ich aktywności w sieci czy blokowanie treści niedostosowanych do wieku. Nie wolno jednak zapominać o równie istotnej płaszczyźnie psychologicznej i społecznej zarówno dzieci, jak i rodzice oraz nauczyciele powinni być edukowani w zakresie świadomego korzystania z zasobów online. Edukacja ta powinna obejmować nie tylko naukę obsługi komputera czy tabletu, ale również kształtowanie kompetencji miękkich: rozpoznawanie manipulacji, krytyczne myślenie, empatię, a także umiejętność budowania zdrowych relacji w wirtualnym otoczeniu. W świetle przytoczonych wcześniej zagrożeń, takich jak cyberprzemoc, grooming, dostęp do nieodpowiednich treści czy kradzież danych osobowych, niezbędne jest wypracowanie holistycznych metod prewencji. Wiele instytucji naukowych oraz organizacji pozarządowych zajmuje się badaniem i opisywaniem zagadnień związanych z bezpieczeństwem w internecie, publikując raporty i wskazówki dla rodziców i pedagogów. Niestety, nawet najbardziej szczegółowe wytyczne nie staną się skuteczne, jeśli nie zostaną wdrożone w praktyce, zwłaszcza w kontekście dynamicznych przemian społecznych i kulturowych. Współpraca różnych środowisk – administracji publicznej, sektora prywatnego, policji, placówek edukacyjnych oraz samych rodzin – ma tu znaczenie absolutnie fundamentalne. Tylko kompleksowe podejście pozwala bowiem na urealnienie przepisów, przełożenie ich z poziomu litery prawa na konkretne działania i procedury, a także na wzajemne wzmacnianie efektów w wymiarze profilaktyki. Zważywszy na globalny charakter cyberprzestrzeni, istotnym zagadnieniem staje się harmonizacja prawna między różnymi krajami. Dzieci mogą paść ofiarą przestępców działających spoza granic państwa, a ściganie takich osób wymaga współpracy międzynarodowej. W tym kontekście ważne są nie tylko konwencje dotyczące ochrony praw dziecka, takie jak Konwencja o Prawach Dziecka z 1989 roku, ale też ujednolicone regulacje z zakresu zwalczania cyberprzestępczości, np. konwencja budapeszteńska o cyberprzestępczości, czy też zobowiązania płynące z dyrektyw europejskich. Ponadto, globalne korporacje technologiczne, które prowadzą platformy społecznościowe i serwisy internetowe, są często zarejestrowane w konkretnych krajach, ale działają w skali międzynarodowej, co nierzadko rodzi trudności w egzekwowaniu krajowych przepisów. Z tego względu tak ważne jest, by kraje nawiązywały między sobą trwałe sojusze i partnerskie porozumienia, zakładające wymianę informacji, doświadczeń oraz wspólne opracowywanie rozwiązań. Ciekawym obszarem, który zyskuje coraz większe znaczenie w kontekście bezpieczeństwa dzieci, jest zjawisko tzw. cyfrowego śladu (ang. digital footprint). Wszystkie czynności wykonywane w sieci publikowane posty, udostępniane zdjęcia, komentarze czy polubienia tworzą swego rodzaju profil użytkownika. Dzieci i nastolatki niejednokrotnie nie są świadome, że to, co zamieszczają w mediach społecznościowych czy na forach, może być dostępne przez długi czas, a nawet trwale, i wykorzystywane przez nieupoważnione osoby, np. w kontekście tworzenia baz danych do celów marketingowych bądź prowadzenia działań przestępczych. Niewłaściwy dobór ustawień prywatności może skutkować ujawnieniem informacji o miejscu zamieszkania, planach wyjazdowych czy codziennych aktywnościach, co stanowi niemałe ułatwienie np. dla potencjalnych porywaczy czy złodziei. Dlatego tak ważne jest, by uwrażliwiać najmłodszych na kwestię zarządzania własną tożsamością w sieci, wskazywać im bezpieczne wzorce postępowania, a także tłumaczyć, jak istotne jest regularne sprawdzanie ustawień prywatności na kontach w

mediach społecznościowych. Nie można też pominąć rosnącej roli influencerów i tzw. e-celebrytów, którzy przyciągają uwagę milionów młodych ludzi, często będąc dla nich autorytetami silniejszymi niż nauczyciele czy rodzice. Z jednej strony zdarza się, że osoby te w odpowiedzialny sposób promują wartościowe treści edukacyjne czy angażują się w kampanie społeczne na rzecz bezpiecznego internetu. Z drugiej jednak strony, pojawia się niemałe ryzyko nadużyć lub wykorzystywania wizerunku dzieci w celach czysto komercyjnych czy wręcz manipulacyjnych. Jeśli popularny influencer zachęca do ryzykownych wyzwań czy publikuje rady sprzeczne z dobrem dziecka, konsekwencje dla niedojrzałych emocjonalnie odbiorców mogą być opłakane. Wobec tego zasadne jest wprowadzanie standardów etycznych dla twórców internetowych, które mogłyby być egzekwowane przez platformy społecznościowe i odpowiednie instytucje. Niemniej jednak, praktyka pokazuje, że samo wprowadzenie zapisów regulaminowych nie zawsze wystarcza, a kluczowe jest, by wszelkie działania były poparte skuteczną kontrolą i realnymi sankcjami w przypadkach naruszeń. Równolegle do postępujących zjawisk negatywnych, warto też odnotować wiele pozytywnych inicjatyw. Duża część organizacji pozarządowych, a także firm z sektora IT, stara się wspierać edukację cyfrową i kreować narzędzia w postaci specjalnych aplikacji, gier czy kursów online, które uczą dzieci rozpoznawania zagrożeń, budując w nich jednocześnie poczucie odpowiedzialności i umiejętność samodzielnego radzenia sobie w sytuacjach kryzysowych. Część z tych projektów jest współfinansowana przez organy publiczne, co pozwala na ich szersze propagowanie. Przykładem może być tworzenie platform e-learningowych, które w przystępny sposób uczą zasad bezpieczeństwa, przedstawiając je w formie interaktywnych historii czy quizów. Takie narzędzia działają nie tylko na rzecz edukacji, ale także wzmacniają zaangażowanie społeczne dzieci i młodzieży, poprzez możliwość dyskusji na forach, dzielenie się doświadczeniami czy wsparcie rówieśnicze w trakcie rozwiązywania konkretnych problemów. Jednocześnie, rodzice i opiekunowie muszą pamiętać, że żadne zabezpieczenia techniczne nie zastąpią świadomej obecności dorosłego w życiu dziecka i budowania z nim relacji opartej na zaufaniu. Nawet najlepsze blokady rodzicielskie mogą zawieść, jeśli dziecko nie rozumie, dlaczego pewne treści są dla niego nieodpowiednie, lub jeśli nie ma poczucia, że może porozmawiać z rodzicem o ewentualnych trudnościach, których doświadcza w sieci. Wychowanie w erze cyfrowej powinno zatem uwzględniać nie tylko aspekty techniczne (jak instalacja oprogramowania ochronnego), ale przede wszystkim codzienne dialogi na temat wartości, etyki i zdrowych granic w korzystaniu z internetu. Warto również, by rodzice edukowali się na temat trendów w popkulturze młodzieżowej, popularnych platform wideo, gier czy sposobów komunikacji dzieci. Tylko w ten sposób możliwe jest zbudowanie mostu zrozumienia między pokoleniami i prowadzenie skutecznej profilaktyki. Badania prowadzone przez specjalistów z zakresu psychologii rozwojowej wskazują, że zbyt wczesne korzystanie z urządzeń ekranowych może mieć wpływ na rozwój kognitywny i społeczny dzieci, dlatego niekiedy zaleca się ograniczanie czasu spędzanego przez małe dzieci w świecie wirtualnym. Dotyczy to w szczególności dzieci w wieku przedszkolnym, które uczą się komunikacji przez naśladowanie mimiki i gestów dorosłych, a więc bezpośredni kontakt twarzą w twarz jest dla nich kluczowy. W miarę, jak dziecko dorasta, warto wprowadzać zasady współdecydowania o sposobie i czasie korzystania z internetu, co pozwala mu uczyć się odpowiedzialności i konsekwencji swoich wyborów. Natomiast w okresie dorastania, kiedy młodzi ludzie intensywnie eksplorują nowe narzędzia, ważne jest, by rodzice byli świadomi, z jakich platform i aplikacji korzysta ich dziecko, i jakie mogą się z tym wiązać zagrożenia (np. nieletnich kuszą rzekomo darmowe gry bazujące na mikropłatnościach lub proponujące

hazardowe mechaniki). Oprócz kwestii psychologicznych i prawnych, z którymi wiąże się bezpieczeństwo dzieci w sieci, nie można zaniedbać także problemu etyki algorytmów i odpowiedzialności firm technologicznych za treści oraz reklamy, jakie docierają do najmłodszych. Sztuczna inteligencja, na przykład w serwisach wideo czy mediach społecznościowych, dobiera często treści w oparciu o historię oglądanych materiałów i zainteresowania użytkownika. Jeżeli algorytm nie jest odpowiednio dostosowany, dziecko może być narażone na nieodpowiednie dla niego treści tylko dlatego, że przypadkowo kliknęło w jakiś materiał. Co więcej, algorytmy reklamowe często nie rozpoznają wieku odbiorcy i kierują reklamy na podstawie słów kluczowych czy profilu zachowań, co może prowadzić do ekspozycji najmłodszych na materiały niebezpieczne, wulgarne czy wręcz patologiczne. Postulaty, by wprowadzać bardziej rygorystyczną regulację w tej dziedzinie, pojawiają się coraz częściej, zwłaszcza w kontekście prac nad tzw. Aktem o Usługach Cyfrowych (Digital Services Act) na poziomie Unii Europejskiej czy podobnymi inicjatywami w innych częściach świata. Na uwagę zasługuje również zagadnienie e-learningu i zdalnego nauczania, które w sposób spektakularny zyskało na znaczeniu w okresie pandemii COVID-19. Choć nauka zdalna umożliwiła kontynuowanie procesu edukacyjnego w warunkach ograniczonej mobilności, zrodziła też liczne komplikacje natury społecznej i psychologicznej. Dzieci spędzały (i w wielu przypadkach nadal spędzają) przed komputerem długie godziny, co może potęgować poczucie izolacji i wpływać na problemy zdrowotne, takie jak bóle kręgosłupa czy nadwyrężenie wzroku. Ponadto, w trakcie zajęć online nauczyciele mają ograniczone możliwości monitorowania tego, co robi uczeń w domu, co przekłada się na większe ryzyko niekontrolowanego korzystania z internetu i możliwej ekspozycji na niewłaściwe treści. W związku z tym rośnie znaczenie wdrażania wyraźnych zasad i protokołów dotyczących bezpieczeństwa informatycznego w edukacji zdalnej, a także zapewnienia wsparcia dla rodziców, którzy często nie posiadają wiedzy ani narzędzi potrzebnych do prawidłowego skonfigurowania domowego środowiska nauki. Co więcej, nie sposób pominąć znaczenia rozwoju kompetencji cyfrowych wśród nauczycieli. Pedagodzy powinni być nie tylko bieglejsi w obsłudze narzędzi edukacyjnych online, ale również wyczuleni na sygnały wskazujące, że uczeń może doświadczać problemów w sieci. Na przykład brak aktywności na lekcjach zdalnych albo podejrzane zmiany w zachowaniu mogą świadczyć o tym, że dziecko padło ofiarą cyberprzemocy ze strony rówieśników. Odpowiednie szkolenia i stałe poszerzanie kompetencji zawodowych w obszarze IT są w tym kontekście niezbędne, aby nauczyciele czuli się pewnie i mogli skutecznie reagować, a nie tylko bezradnie przyglądać się narastającym trudnościom. Dodatkowym wyzwaniem jest złożona rzeczywistość społeczno-kulturowa. Wiele rodzin, zwłaszcza w biedniejszych regionach czy na obszarach wiejskich, nie posiada wystarczających środków finansowych ani dostatecznych umiejętności technologicznych, by odpowiednio dbać o bezpieczeństwo dzieci w sieci. Z drugiej strony, nawet w rodzinach o wysokim statusie ekonomicznym zdarza się zaniedbanie w tym obszarze, wynikające z braku czasu bądź braku świadomości rodziców. Nierówności cyfrowe sprawiają, że część dzieci w ogóle nie ma dostępu do szybkiego internetu, co ogranicza ich szanse edukacyjne, a inna część nadużywa internetu, często bez żadnej kontroli. Tworzy to swoisty paradoks: technologia może być zarówno źródłem wykluczenia, jak i kluczem do poszerzenia możliwości rozwojowych. Dlatego każdy projekt edukacyjny czy reformujący prawo powinien brać pod uwagę zróżnicowane realia społeczno-ekonomiczne i stawiać na równość dostępu do informacji i narzędzi. Ciągła ewolucja cyberprzestrzeni, włącznie z pojawianiem się nowych trendów, językowych memów czy subkultur młodzieżowych, powoduje, że temat bezpieczeństwa dzieci w internecie nigdy nie

traci na aktualności. Z jednej strony mamy do czynienia z postępującą profesjonalizacją cyberprzestępczości wyrafinowane ataki phishingowym czy złośliwe oprogramowanie wymierzone w młodych użytkowników rosną w siłę. Z drugiej strony, narzędzia do walki z tym zjawiskiem stają się coraz bardziej zaawansowane, a sztuczna inteligencja może być używana do analizowania zachowań online i wykrywania przestępczych aktywności. Nie można jednak opierać się wyłącznie na technologii – to człowiek, ze swoją wrażliwością i umiejętnością empatycznej komunikacji, zawsze powinien odgrywać kluczową rolę w procesie wychowania i ochrony dziecka. W kontekście dalszej przyszłości należy przewidywać, że rosnąca popularność wirtualnych światów (tzw. metaverse) doprowadzi do kolejnego przedefiniowania granic prywatności i potencjalnie jeszcze bardziej złożonych form nadużyć. Dzieci, które będą przebywać w tych światach, mogą narażać się na interakcje z nieznajomymi osobami mającymi złe intencje, mogą także kreować swoje awatary w sposób sprzyjający zachowaniom ryzykownym. Tym bardziej konieczne będzie pogłębianie badań naukowych nad społecznymi i psychologicznymi skutkami intensywnego zanurzania się w rozszerzoną rzeczywistość, a także dalsza praca nad spójną legislacją, uwzględniającą specyfikę wirtualnych przestrzeni. Potrzebne będą systemowe rozwiązania, np. wprowadzanie certyfikacji treści w VR, narzędzi pozwalających pedagogom i rodzicom weryfikować, czy dany program spełnia standardy bezpieczeństwa, czy ogranicza kontakt z osobami dorosłymi mającymi potencjalnie złe zamiary. Niezależnie jednak od postępu technologicznego, przenoszącego nas coraz dalej w cyfrowy świat, istotną kwestią pozostaje rozwijanie umiejętności psychospołecznych wśród dzieci i młodzieży. Bez wypracowanych podstaw z zakresu komunikacji, współpracy, empatii, samoświadomości i rozumienia kontekstu emocjonalnego relacji międzyludzkich, najnowocześniejsze narzędzia nie będą w stanie w pełni zabezpieczyć najmłodszych przed krzywdą. Wręcz przeciwnie – brak fundamentalnych kompetencji może prowadzić do niebezpiecznego uzależnienia od technologii lub patologicznego zanurzenia w wirtualnej rzeczywistości, która będzie wydawać się bardziej atrakcyjna niż wymagający świat realny. Z tego względu wszelkie programy profilaktyczne i wychowawcze powinny łączyć elementy edukacji technologicznej z kształtowaniem umiejętności społecznych, a rodzice mimo często ograniczonego czasu – powinni starać się spędzać z dziećmi jak najwięcej chwil w realnym kontakcie, oferując im doświadczenia, których świat cyfrowy nie zastąpi. Warto podkreślić, że bezpieczeństwo dzieci w cyberprzestrzeni jest jednym z najważniejszych wyzwań naszych czasów, a jego charakter stale ewoluuje wraz z postępem technologicznym i przemianami społecznymi. Kluczem do skutecznej ochrony najmłodszych jest zrozumienie, że na ten obszar oddziałują liczne czynniki – od regulacji prawnych i międzynarodowych porozumień, przez narzędzia techniczne i produkty edukacyjne, po relacje interpersonalne i wartości wyznawane w społeczeństwie. Jeśli wszystkie te elementy będą harmonijnie współdziałać, jeśli uda się zbudować kulturę dialogu i wzajemnego wsparcia, wówczas istnieje szansa, że dzieci będą mogły czerpać z cyberprzestrzeni to, co najlepsze nieograniczone zasoby wiedzy, możliwość twórczej ekspresji, interakcji społecznej oraz rozrywki przy jednoczesnej minimalizacji ryzyka związanego z zagrożeniami wirtualnego świata. Jednak aby osiągnąć ten cel, potrzeba wspólnego wysiłku rodziców, pedagogów, prawodawców, ekspertów od technologii, a nade wszystko samych dzieci, które dzięki odpowiedniej edukacji i wsparciu będą w stanie świadomie i odpowiedzialnie korzystać z dobrodziejstw cyberprzestrzeni. Współczesne wyzwania związane z zapewnieniem bezpieczeństwa dzieci w cyberprzestrzeni są tak złożone, że konieczne staje się nieustanne rozwijanie i dostosowywanie działań zarówno przez rodziców, jak i nauczycieli. W erze szybkiego dostępu do internetu, urządzeń

mobilnych i mediów społecznościowych, najmłodsi użytkownicy nie tylko korzystają z niespotykanego dotąd bogactwa zasobów edukacyjnych i rozrywkowych, lecz także każdego dnia stykają się z potencjalnymi zagrożeniami. Cyberprzemoc, ryzykowne wyzwania, kontakt z nieodpowiednimi treściami, manipulacje dorosłych czy kradzież danych osobowych – to tylko część problemów, na które należy zwracać szczególną uwagę. W poniższym podsumowaniu przedstawione zostaną najbardziej istotne kwestie dotyczące rozpoznawania i przeciwdziałania zagrożeniom w sieci, ze szczególnym uwzględnieniem działań, jakie mogą i powinni podejmować rodzice oraz nauczyciele. Przede wszystkim warto zauważyć, że wprowadzanie dziecka w świat cyfrowy powinno odbywać się stopniowo, z uwzględnieniem jego wieku i etapu rozwoju. Nie należy zakładać, że maluch bez odpowiedniego wsparcia jest w stanie samodzielnie dokonywać selekcji treści, czy prawidłowo oceniać wiarygodność informacji. Zarówno rodzice, jak i opiekunowie w przedszkolach oraz szkołach początkowych powinni postawić na edukację w zakresie świadomego korzystania z internetu. Istotna jest tu rola rozmów z dzieckiem – tłumaczenie, dlaczego nie wolno podawać danych osobowych nieznajomym, co to są hasła i dlaczego powinny być silne i unikatowe, a także dlaczego nie każdy komunikat czy zdjęcie napotkane w sieci są godne zaufania. Już na etapie przedszkola można wprowadzać elementarne zasady bezpieczeństwa: dziecko powinno wiedzieć, że pytanie o adres zamieszkania w internecie czy prośba o przesłanie własnego zdjęcia to potencjalny sygnał alarmowy. Dla rodziców szczególnie ważne może być ustalenie jasnych reguł korzystania z urządzeń elektronicznych w domu. W praktyce oznacza to, że wspólnie z dzieckiem określamy godziny, w jakich może grać w gry komputerowe czy korzystać z komunikatorów, a także ustalamy konkretne zasady – na przykład brak elektroniki przy posiłkach czy przed snem. Ograniczanie czasu spędzanego przed ekranem pozwala nie tylko zadbać o zdrowie fizyczne i psychiczne dziecka, ale także zapewnia mu odpowiedni balans między światem cyfrowym a realnymi kontaktami społecznymi i innymi aktywnościami. Jednocześnie warto wspierać dziecko w rozwoju jego zainteresowań i pasji poza internetem, na przykład przez dodatkowe zajęcia sportowe czy artystyczne. Dzięki temu młody człowiek nie będzie traktować technologii jako jedynej lub najważniejszej formy rozrywki, a w razie ewentualnych problemów związanych z korzystaniem z sieci łatwiej mu będzie znaleźć alternatywę. Ważnym aspektem, często podkreślanym przez pedagogów, jest przykład, jaki dają sami dorośli. Dzieci z natury naśladują zachowania rodziców, w tym również sposób korzystania z komputera czy smartfona. Jeśli rodzic stale trzyma w ręce telefon i przegląda media społecznościowe, a wieczory spędza przy ekranie laptopa, to trudno oczekiwać, by dziecko zachowywało zdrowy dystans do technologii. Warto więc zastanowić się, w jaki sposób my sami korzystamy z sieci, i czy nie powielamy pewnych wzorców, które mogą być szkodliwe. W praktyce może to polegać na odkładaniu telefonu na bok w trakcie wspólnych posiłków, wyłączaniu powiadomień w czasie rodzinnych spotkań czy spędzaniu czasu na rozmowie i zabawie z dzieckiem zamiast pasywnego przeglądania internetu. Równocześnie dobrze jest przełamać bariery pokoleniowe: wykazać zainteresowanie tym, co dziecko robi w sieci, jakich gier używa, z kim najczęściej rozmawia i o czym. Otwartość na świat cyfrowy dziecka pozwala na bieżąco wychwytywać niepokojące sygnały i interweniować, jeśli coś wzbudzi nasz niepokój. Z perspektywy nauczycieli podstawowym narzędziem w budowaniu świadomości zagrożeń jest systematyczna edukacja informatyczna i wychowawcza. Podczas zajęć warto zwracać uwagę na takie zagadnienia, jak rozpoznawanie fake newsów, zasady tworzenia bezpiecznych haseł, konsekwencje cyberprzemocy i sposoby radzenia sobie w przypadku, gdy uczeń staje się jej ofiarą. Lekcje informatyki mogą być okazją do praktycznego ćwiczenia ustawień prywatności na portalach społecznościowych czy

pokazania, w jaki sposób działają programy antywirusowe. Jednocześnie dobrze jest, by nauczyciele zwracali uwagę na zjawisko FOMO (ang. Fear Of Missing Out), czyli lęku przed byciem wykluczonym z życia towarzyskiego online, który szczególnie dotyka nastolatków spędzających dużo czasu w mediach społecznościowych. Rozmawianie o FOMO w szkole może uświadomić młodzieży, że świat wirtualny nie powinien w pełni determinować ich poczucia własnej wartości i relacji z innymi. Ponadto, w szkołach niezbędne jest tworzenie programu wychowawczo-profilaktycznego uwzględniającego problematykę cyberbezpieczeństwa. Rozmowy z uczniami powinny dotyczyć zarówno kwestii rozpoznawania i przeciwdziałania groomingowi, jak i tego, co robić w sytuacji, gdy spotkają się z hejtem, nękaniem w sieci lub prośbą o udostępnienie treści o charakterze intymnym. Dobrze, jeśli w szkole powstaje punkt konsultacyjny (na przykład u pedagoga szkolnego) dla uczniów, którzy czują się zagrożeni czy przytłoczeni sytuacjami z internetu. Kluczowe jest, by młodzi ludzie mieli świadomość, że mogą liczyć na dorosłych i że problemy doświadczane w przestrzeni wirtualnej są traktowane z pełną powagą. Wciąż zdarza się, że dzieci lub nastolatkowie nie zgłaszają incydentów cyberprzemocy, bo obawiają się niezrozumienia ze strony dorosłych lub nawet kary (np. zabrania dostępu do sieci), co z ich perspektywy jest wyjątkowo dotkliwe. Właśnie dlatego pierwszym krokiem jest budowanie atmosfery zaufania, w której wychowawca, nauczyciel i pedagog zawsze służą wsparciem, zamiast straszyć sankcjami. W działaniach profilaktycznych istotne pozostaje zrozumienie specyfiki popularnych wśród dzieci i młodzieży platform, takich jak TikTok, Instagram, Snapchat, różnorodne fora tematyczne, komunikatory czy serwisy streamingowe typu Twitch i YouTube. Wiele niebezpieczeństw czyha właśnie tam, gdzie młodzi spędzają najwięcej czasu – oglądając filmy, transmisje na żywo czy uczestnicząc w wyzwaniach i trendach (challenge'ach). Nauczyciele i rodzice, nawet jeśli sami nie korzystają z tych aplikacji, powinni zdobywać podstawową wiedzę o ich mechanizmach. Przykładowo, na Tik Toku łatwo natknąć się na filmy promujące zachowania niebezpieczne, a młodsi użytkownicy mogą chcieć je naśladować w realnym świecie. Z kolei na Instagramie dzieci mogą być narażone na treści wywołujące niezdrowe porównywanie się z innymi, kompleksy lub zaburzenia odżywiania, jeśli napotkają na konta promujące nierealistyczne ideały urody. Rodzic czy nauczyciel, który rozumie specyfikę danej platformy, jest w stanie trafnie doradzić dziecku i w odpowiednim momencie zainterweniować, zanim dojdzie do eskalacji problemu. Drugim kluczowym obszarem, w którym powinniśmy wykazać się czujnością, jest cyberprzemoc rówieśnicza. Jej przejawy mogą być różne: obraźliwe komentarze, nękające wiadomości czy publikowanie kompromitujących zdjęć bez zgody. Dzieci i nastolatki bywają wyjątkowo okrutne wobec siebie nawzajem, a internet daje im dodatkowo poczucie anonimowości, co zachęca do eskalacji agresji słownej. Właśnie dlatego zarówno w domu, jak i w szkole niezbędne jest reagowanie na najmniejsze symptomy konfliktu czy wykluczenia w grupie. Nie wolno bagatelizować żadnych zgłaszanych przypadków obraźliwych zachowań w sieci, nawet jeśli z perspektywy dorosłego wydają się błahe. Warto również uczyć empatii i komunikacji bez przemocy, na przykład poprzez zajęcia warsztatowe, dramę, wspólne omawianie sytuacji problemowych podczas godzin wychowawczych. Dzięki temu dzieci mogą zrozumieć, jakie konsekwencje dla psychiki ofiary ma nękanie w internecie i jak to wpływa na jej poczucie wartości. Rodzice i nauczyciele powinni także zwracać dużą uwagę na to, czy dziecko przypadkiem nie wikła się w kontakty z dorosłymi, którzy mogą mieć nieuczciwe zamiary. Zjawisko groomingu polega na stopniowym zdobywaniu zaufania ofiary, a następnie wykorzystywaniu jej emocjonalnie bądź seksualnie. Agresorzy dążą do zbudowania więzi wirtualnej, podszywając się często pod rówieśników lub tworząc fałszywe

tożsamości. Dlatego tak ważne jest, by dzieci wiedziały, że nie powinny spotykać się z osobami poznanymi wyłącznie w sieci bez wiedzy i zgody rodziców. Trzeba też uczulać je na sytuacje, w których ktoś w internecie prosi o rozbieranie się przed kamerą, przesłanie zdjęć intymnych czy zdradzenie sekretów rodzinnych. W razie jakichkolwiek podejrzeń rodzic lub nauczyciel powinien reagować natychmiast – wspólnie z dzieckiem zabezpieczyć dowody (zrzuty ekranu, nagrania rozmów), a w razie potrzeby zgłosić sprawę policji. Ważne, by nie wywoływać przy tym u dziecka poczucia winy, lecz wyjaśniać, że takie działania agresorów nie są legalne i że to dorosły narusza granice, a nie dziecko „źle się zachowuje". Kolejną istotną kwestią jest edukacja na temat rozpoznawania tzw. fake newsów i teorii spiskowych. Choć mogłoby się wydawać, że dotyczy to głównie dorosłych, dzieci także często stają się adresatami treści dezinformacyjnych. Mogą natknąć się na niesprawdzone informacje o rzekomych zagrożeniach zdrowotnych, dziwnych praktykach religijnych czy manipulacjach politycznych. Nauczyciele poloniści czy wychowawcy mogą ćwiczyć z uczniami umiejętność weryfikowania źródeł, analizowania wiarygodności portali informacyjnych, sprawdzania dat publikacji i sensowności powoływanych argumentów. Dzięki temu młodzi ludzie rozwijają myślenie krytyczne i uczą się, że internet jest pełen zarówno wartościowych, jak i całkowicie fałszywych treści. Ważne jest też, by rodzice i pedagodzy mieli świadomość, iż pewne zachowania ryzykowne w sieci mogą wiązać się z problemami emocjonalnymi, które dziecko przeżywa w świecie rzeczywistym. Dotyczy to między innymi skłonności do samookaleczeń, zaburzeń nastroju czy niskiej samooceny. Niektóre grupy internetowe czy serwisy mogą wręcz promować destrukcyjne wzorce (np. w kontekście zaburzeń odżywiania lub samobójstwa). Jeżeli nauczyciel zauważy zmianę w zachowaniu ucznia, jego wycofanie społeczne, spadek motywacji, izolowanie się lub przejawy autoagresji, warto dyskretnie porozmawiać z nim i z rodzicami, a w razie potrzeby wspólnie skonsultować się z psychologiem. Podobnie rodzice nie powinni bagatelizować sytuacji, w których dziecko zamyka się w swoim pokoju na całe dnie i wygląda na rozdrażnione czy przygnębione – być może doświadcza czegoś trudnego w sieci, a wspólna interwencja i szczera rozmowa mogą okazać się kluczowe. Współpraca między rodzicami a nauczycielami jest tu nie do przecenienia. Nierzadko zdarza się, że dziecko w domu i w szkole prezentuje zupełnie inne zachowania, przez co ani jedna, ani druga strona nie ma pełnego obrazu sytuacji. Regularne kontaktowanie się rodziców z wychowawcami i nauczycielami, uczestnictwo w zebraniach, ale też otwartość na mniej formalne rozmowy (telefon, e-mail, komunikatory) stanowią fundament skutecznej profilaktyki. Dodatkowo szkoła może organizować warsztaty i prelekcje dla rodziców, na których specjaliści od cyberbezpieczeństwa czy psycholodzy dziecięcy pokazują najnowsze zjawiska i wyzwania, uczą podstawowych narzędzi kontroli rodzicielskiej oraz radzą, w jaki sposób rozmawiać z dzieckiem o jego aktywności w sieci. Oprócz działań edukacyjnych i wychowawczych, warto w praktyce stosować różnorodne techniczne środki bezpieczeństwa, takie jak: oprogramowanie antywirusowe, zapory sieciowe, filtry rodzicielskie czy ustawienia prywatności. Upewnijmy się, że urządzenia domowe (komputery, smartfony, tablety) mają zainstalowane aktualne programy ochronne i zawsze pobierają najnowsze aktualizacje systemu. Warto przejrzeć ustawienia w routerze, jeśli oferuje on funkcję kontroli rodzicielskiej. Można tam zdefiniować pory, w których internet jest dostępny dla urządzenia dziecka, albo zablokować określone strony internetowe. Takie działania nie zastąpią rozmów i edukacji, ale stanowią dodatkową barierę, która może wyhamować kontakt z groźnymi treściami. Równie istotne jest regularne sprawdzanie, jakie aplikacje i gry dziecko instaluje na swoim urządzeniu, zwłaszcza jeśli wprowadza do nich dane płatnicze. Nauczyciele natomiast, jeśli korzystają z narzędzi internetowych podczas

lekcji, powinni wybierać te platformy, które mają sprawdzoną renomę i nie wymagają od uczniów podawania zbyt wielu danych osobowych. Istnieje też potrzeba szczególnej uwagi w kontekście zdalnego nauczania. W sytuacjach, w których szkoła wprowadza lekcje online, czy to w wyniku pandemii, czy innych okoliczności, dzieci i młodzież spędzają przed ekranem znacznie więcej czasu niż zazwyczaj. Wówczas rodzice i nauczyciele powinni kłaść nacisk na ergonomię, zapewniając odpowiednie warunki pracy przy komputerze, dbając o przerwy i aktywność fizyczną między zajęciami. W trakcie lekcji nauczyciel powinien zachęcać uczniów do włączania kamer, aby móc na bieżąco reagować na ewentualne niepokojące sygnały: przygnębiony wyraz twarzy, brak koncentracji, znikanie z ekranu bez wyjaśnień. Z kolei rodzic może wspierać dziecko w organizowaniu sobie czasu pracy, przypominać o przerwach i pomagać w rozwiązywaniu problemów z oprogramowaniem. Takie wspólne działania zwiększają szanse na wczesne wychwycenie nieprawidłowości, w tym kontaktu z niebezpiecznymi osobami w sieci czy rozwojem uzależnienia od ekranu. Warto mocno podkreślić potrzebę ciągłego uczenia się i dostosowywania do nowych realiów. Cyberprzestrzeń jest dynamiczna i podlega nieustannym przemianom pojawiają się nowe platformy, nowe formy komunikacji, a także nowe formy zagrożeń. To, co było skuteczną praktyką rok czy dwa lata temu, dzisiaj może wymagać aktualizacji albo zupełnie nowych rozwiązań. Kluczowa jest tu elastyczność – zarówno rodzice, jak i nauczyciele powinni rozwijać swoje kompetencje cyfrowe, śledzić doniesienia o nowych trendach i mechanizmach bezpieczeństwa. Można korzystać z kursów e-learningowych organizowanych przez instytucje publiczne czy organizacje pozarządowe, uczestniczyć w konferencjach i warsztatach, a także wymieniać się doświadczeniami z innymi dorosłymi, którzy stoją przed podobnymi wyzwaniami. Najważniejsze dla rodziców i nauczycieli jest połączenie świadomej edukacji, empatii, otwartej komunikacji i odpowiedzialnego wdrażania rozwiązań technicznych. W praktyce oznacza to: **Ustalanie zasad i granic korzystania z urządzeń** (godziny korzystania, rodzaje dozwolonych treści). **Dawanie dobrego przykładu własnym zachowaniem** (ograniczanie nadmiernego korzystania z mediów społecznościowych, aktywne słuchanie dziecka w czasie rozmowy). **Rozwijanie kompetencji cyfrowych i krytycznego myślenia** u dzieci i młodzieży (omawianie źródeł informacji, ćwiczenie rozpoznawania fake newsów, uczenie bezpieczeństwa hasłowego). **Wzmacnianie więzi emocjonalnych z dzieckiem** i tworzenie atmosfery zaufania, w której zawsze można przyjść z problemem i liczyć na wsparcie bez obawy o karę czy wyśmianie. **Reagowanie na przejawy cyberprzemocy** i agresji w sieci (monitorowanie sytuacji w klasie, praca z ofiarą i sprawcą, budowanie empatii i kultury osobistej w internecie). **Kontrola rodzicielska i odpowiednie zabezpieczenia techniczne** (oprogramowanie antywirusowe, ustawienia prywatności, filtry blokujące treści szkodliwe). **Współpraca pomiędzy rodzicami, nauczycielami, pedagogami** oraz ewentualnie psychologami i policją w przypadku poważniejszych incydentów (zagrożenie groomingiem, cyberprzemocą, kradzieżą tożsamości). **Stałe dokształcanie się** w dziedzinie cyberbezpieczeństwa i wychowania w świecie cyfrowym (śledzenie nowinek technologicznych, udział w szkoleniach, konferencjach, webinariach). Jeżeli te elementy będą konsekwentnie wdrażane, znacząco wzrasta szansa na to, że dzieci będą korzystać z dobrodziejstw internetu i urządzeń mobilnych w sposób rozwijający, a jednocześnie bezpieczny. Oczywiście nie da się wyeliminować wszystkich zagrożeń sieć ma zasięg globalny i pojawiają się w niej coraz bardziej wyrafinowane sposoby na oszustwa i manipulacje. Mimo to, kluczowe jest zbudowanie w dziecku pewności, że zawsze może zgłosić się do zaufanej osoby dorosłej, a także wykształcenie w nim podstawowych kompetencji pozwalających rozpoznać sytuacje

niebezpieczne. Dzięki temu unikniemy wielu dramatów, a młodzież, zamiast obawiać się cyberprzestrzeni, będzie potrafiła z niej korzystać mądrze i z rozwagą. Tego rodzaju długofalowa praca – łącząca aspekty wychowawcze, edukacyjne i techniczne – wymaga czasu, cierpliwości oraz zrozumienia, że dzieci uczą się zarówno dzięki wskazówkom dorosłych, jak i na własnych błędach. Nie chodzi jednak o to, by pozostawiać młodych ludzi samych sobie w momencie, gdy w sieci czai się wiele potencjalnych zagrożeń, lecz by towarzyszyć im w poznawaniu świata wirtualnego i nieustannie wspierać w budowaniu pozytywnych relacji, również tych online. Świat technologii będzie się zmieniał, pojawią się nowe platformy i trendy, a wraz z nimi nowe niebezpieczeństwa. Jeśli jednak rodzice i nauczyciele będą stawiali na regularny dialog i rzetelną edukację, to dzieci zyskają solidne fundamenty, by świadomie i odpowiedzialnie korzystać z internetu przez całe życie, niezależnie od tego, jakie innowacje przyniesie przyszłość.