

Cybersecurity and Law

2025 Nr 2 (14)

DOI: 10.34567/cal/215965



Cybersecurity challenges in education

Wyzwania cyberbezpieczeństwa w oświacie

Wojciech FEDERCZYK

Uniwersytet Kardynała Stefana Wyszyńskiego

ORCID: 0000-0003-1242-9552

E-mail: w.federczyk@uksw.edu.pl

Abstract

Cybersecurity constitutes a fundamental requirement of contemporary civilization, stemming from the dynamic development of information technologies and their pervasive presence across all spheres of social life. Cyberattacks should be regarded not only as a form of criminal activity within the digital environment but also as potential instruments of modern warfare and acts of terrorism. In the virtual space, as in the physical world, legal violations occur, which justifies the necessity of addressing cybersecurity issues within the educational system.

The analysis of this matter reveals three essential dimensions: organizational, educational, and upbringing. First, educational institutions, relying on digital infrastructure, must ensure adequate technological safeguards encompassing both hardware and software. Second, in the educational dimension, it is indispensable to enhance teachers' digital competencies and to provide students with knowledge enabling safe functioning in the digital environment. Third, the upbringing aspect requires shaping attitudes conducive to observing social norms in cyberspace.

In this context, it is crucial to assess whether the existing legal framework provides sufficient grounds for educational administration and school principals to effectively implement these tasks, as well as to examine public policies and the degree of their implementation.

Keywords

cybersecurity, education law, upbringing, education

Streszczenie

Cyberbezpieczeństwo stanowi jeden z kluczowych wymogów współczesnej cywilizacji, wynikający z dynamicznego rozwoju technologii informatycznych i ich obecności we wszystkich obszarach życia społecznego. Cyberataki należy postrzegać nie tylko jako formę przestępczości w środowisku cyfrowym, lecz także jako potencjalne narzędzie współczesnych działań wojennych i aktów terroryzmu. W przestrzeni wirtualnej, podobnie jak w świecie rzeczywistym, dochodzi do naruszeń prawa, co uzasadnia konieczność uwzględnienia problematyki cyberbezpieczeństwa w systemie oświaty.

Analiza zagadnienia wskazuje na trzy zasadnicze płaszczyzny: organizacyjną, edukacyjną oraz wychowawczą. Po pierwsze, placówki oświatowe, korzystając z infrastruktury cyfrowej, muszą zapewnić odpowiednie zabezpieczenia technologiczne, obejmujące zarówno sprzęt, jak i oprogramowanie. Po drugie, w wymiarze edukacyjnym niezbędne jest podnoszenie kompetencji cyfrowych nauczycieli oraz przekazywanie uczniom wiedzy umożliwiającej bezpieczne funkcjonowanie w środowisku cyfrowym. Po trzecie, aspekt wychowawczy wymaga kształtowania postaw sprzyjających przestrzeganiu norm społecznych w cyberprzestrzeni.

W tym kontekście konieczna jest ocena, czy obowiązujące regulacje prawne zapewniają wystarczające podstawy do realizacji powyższych zadań przez administrację oświatową i dyrektorów szkół, a także analiza polityk publicznych oraz stopnia ich wdrożenia.

Słowa kluczowe

cyberbezpieczeństwo, prawo oświatowe, wychowanie, edukacja

Wprowadzenie

Początek XXI wieku charakteryzuje się dynamicznym rozwojem technologii informatycznych. Zjawisko to, określane mianem rewolucji cyfrowej, przeobraża otaczającą rzeczywistość, tworząc wirtualny świat, w którym funkcjonujemy na co dzień. Równolegle obserwuje się rozwój społeczeństwa informacyjnego, wynikający ze zdolności błyskawicznego przetwarzania i analizowania ogromnych zasobów danych oraz niemal nieograniczonego dostępu do informacji. Gospodarka oparta na wiedzy prowadzi m.in. do powstawania inteligentnych fabryk, a także globalnych produktów i usług, co z kolei powoduje konieczność nauczania i przygotowania do pracy w dynamicznie zmieniającym się otoczeniu.

Edukacja, jako fundament rozwoju najmłodszej części społeczeństwa, staje się obszarem, w którym cyfryzacja odgrywa kluczową rolę. Odpowiednia jakość oraz dostosowanie systemu kształcenia do wyzwań współczesności stanowią dla młodego pokolenia zarówno szansę rozwojową, jak i konieczność, ponieważ coraz częściej żyjemy równolegle w świecie rzeczywistym i wirtualnym. Jest to konsekwencją stałego dostępu do Internetu, jaki zapewniają smartfony i inne urządzenia przenośne wykorzystujące bezprzewodową transmisję danych.

Stale funkcjonowanie w środowisku cyfrowym wiąże się jednak dla dzieci i młodzieży z dodatkowymi zagrożeniami, wynikającymi z niedostatecznego poziomu krytycznego myślenia, ograniczonej umiejętności analizy faktów i zachowań, nadmiernego zaufania do nowych technologii oraz braku świadomości potencjalnych ryzyk.

Cyberbezpieczeństwo, rozumiane jako zapewnienie niezawodności sprzętu oraz ochrona użytkowników przed zagrożeniami, nie stanowi stanu możliwego do osiągnięcia raz na zawsze, lecz wymaga nieprzerwanego procesu prewencji i reakcji. Zapewnienie ochrony cybernetycznej w sektorze oświaty ma charakter wielowymiarowy, gdyż obejmuje uczniów, nauczycieli oraz szkoły. Celem niniejszego opracowania jest identyfikacja kluczowych obszarów ochrony oraz ocena, w jakim stopniu są one objęte działaniami administracji publicznej.

Zmiany w systemie edukacji muszą mieć charakter kompleksowy, ponieważ niewystarczające jest jedynie wyposażenie uczniów w umiejętności efektywnego korzystania z technologii cyfrowych i poruszania się w wirtualnej rzeczywistości. Niezbędne jest także zabezpieczenie przed zagrożeniami oraz kształtowanie postaw, które sprzyjają odpowiedzialnemu korzystaniu

z technologii i nie stanowią źródła dodatkowych ryzyk. Istotnym wyzwaniem pozostaje ponadto zapewnienie uczniom i nauczycielom bezpiecznego środowiska do rozwijania kompetencji cyfrowych oraz właściwe zabezpieczenie sprzętu i systemów informatycznych.

Cyfrowa transformacja oświaty

Wykorzystywanie technologii cyfrowych w edukacji stwarza realną możliwość indywidualizacji procesu kształcenia oraz wzmacniania zaangażowania uczniów¹. Cyfryzacja szkoły nie polega jednak wyłącznie na zastąpieniu tradycyjnych narzędzi dydaktycznych ich elektronicznymi odpowiednikami. Jest ona złożonym i wieloletnim procesem wymagającym sprostania licznym wyzwaniom technicznym i organizacyjnym, a jej celem jest systematyczna modernizacja polskiej oświaty.

Jednym z kluczowych elementów transformacji jest wyposażenie szkół, uczniów i nauczycieli w odpowiedni sprzęt – komputery, urządzenia mobilne oraz stabilne łącza internetowe. Równorządne znaczenie ma zapewnienie wysokiej jakości oprogramowania edukacyjnego, obejmującego platformy e-learningowe, systemy wspierające proces dydaktyczny oraz narzędzia służące zarządzaniu szkołą. Oprogramowanie to powinno spełniać wymogi bezpieczeństwa danych, zgodności z podstawą programową oraz intuicyjności użytkowania, gdyż brak adekwatnych i bezpiecznych treści cyfrowych prowadzi do obniżenia efektywności cyfryzacji.

Współcześnie zwraca się uwagę, że jednym z nadrzędnych celów edukacji jest kształtowanie kompetencji, rozumianych jako zdolność do samodzielnego podejmowania zadań i funkcjonowania w zmieniającym się środowisku społecznym². Wśród ośmiu grup kompetencji kluczowych sformułowanych przez Radę Unii Europejskiej³ znajdują się kompetencje cyfrowe, które polegają na umiejętności odpowiedzialnego korzystania z dostępnych technologii cyfrowych⁴. Aby przekazać tę umiejętność uczniom, muszą posiadać je nauczyciele, którzy są przedstawicielami starszych pokoleń. Z tego względu istotne jest wzmacnianie kompetencji nauczycieli zarówno w wymiarze technicznym, dotyczącym obsługi nowoczesnych narzędzi, jak i metodycznym, odnoszącym się do właściwego ich wykorzystania w procesie dydaktycznym⁵.

Odpowiedzią na wyzwania współczesnej edukacji jest koncepcja Edukacji 4.0, która zakłada przygotowanie uczniów do funkcjonowania w realiach gospodarki cyfrowej poprzez rozwijanie umiejętności niezbędnych do radzenia sobie z wyzwaniami przyszłości. Model ten opiera się na integracji najnowszych

¹ Raport OECD wskazuje, że wykorzystanie narzędzi cyfrowych w edukacji prowadzi do zwiększenia zaangażowania uczniów i rozwijania umiejętności 21. wieku, takich jak krytyczne myślenie, rozwiązywanie problemów oraz współpraca z innymi uczniami w wirtualnych przestrzeniach edukacyjnych. OECD, *Shaping Digital Education: Enabling Factors for Quality, Equity and Efficiency*, OECD Publishing Paris 2023, s. 22-25.

² P. Forma, A. Winiarczyk, Kompetencje cyfrowe – jako metakompetencje XXI wieku, „Edukacja ustawiczna dorosłych” 2024, nr 4, s. 41.

³ Zalecenie Rady z dnia 22 maja 2018 r. w sprawie kompetencji kluczowych w procesie uczenia się przez całe życie (2018/C 189/01).

⁴ Ibidem, s. 46.

⁵ M. Plebańska, A. Szyller, M. Sieńczewska, *Q edukacji cyfrowej*, Warszawa 2020, s. 23-25.

technologii oraz systemów informatycznych z procesem nauczania, a jego realizacja wymaga spójnych działań systemowych⁶.

Proces przekształceń w edukacji stanowi element szerszego procesu transformacji cyfrowej, rozumianej jako kompleksowa zmiana dotycząca wielu obszarów życia społecznego i indywidualnego, której pierwszym etapem jest cyfryzacja, lecz której zakres wykracza daleko poza samo wdrażanie technologii. element szerszego procesu transformacji cyfrowej, rozumianej jako kompleksowa zmiana dotycząca wielu obszarów życia społecznego i indywidualnego, której pierwszym etapem jest cyfryzacja, lecz której zakres wykracza daleko poza samo wdrażanie technologii.⁷

Pojęcie transformacji cyfrowej jest obecne w działalności administracji oświatowej. Przyjęta we wrześniu 2024 r. przez Radę Ministrów „Polityka Cyfrowej Transformacji Edukacji” (dalej: PCTE)⁸ stanowi dokument strategiczny, określający ramy zaangażowania państwa w obszarze cyfryzacji oświaty. Dokument ten wskazuje niezbędne działania, które powinny zostać zrealizowane do 2035 r., aby przygotować szkoły do funkcjonowania w warunkach społeczeństwa cyfrowego. Spośród dziesięciu obszarów interwencji jeden dotyczy bezpieczeństwa cyfrowego, obejmując przeciwdziałanie dezinformacji, rozwijanie umiejętności weryfikowania informacji oraz profilaktykę cyberprzemocy i promowanie higieny cyfrowej⁹.

Zagrożenia cyberbezpieczeństwa

Konsekwencją rozwoju rzeczywistości wirtualnej oraz przenoszenia coraz większej liczby aktywności zawodowych i osobistych do Internetu jest poszerzanie się katalogu zagrożeń cyfrowych. W literaturze zwraca się uwagę, że wraz z dynamicznym rozwojem technologii zmianie ulega również sama definicja cyberbezpieczeństwa¹⁰. Obejmuje ona nie tylko zapewnienie ciągłości działania sieci i urządzeń telekomunikacyjnych, lecz także bezpieczeństwo komunikacji, integralność i poufność informacji oraz ochronę użytkowników przed różnego rodzaju nadużyciami. W tym ujęciu do kluczowych zagrożeń zalicza się m.in. cyberterroryzm, cyberinwigilację, cyberprzestępczość oraz dezinformację. Jednakże cyberbezpieczeństwo powinno również obejmować zachowania i interakcje uczestników rzeczywistości wirtualnej (kwestie poufności czy legalności przetwarzanych informacji)¹¹.

Cyberbezpieczeństwo powinno być postrzegane jako proces, co wynika z faktu, że rozwój technologiczny prowadzi jednocześnie do ewolucji metod ataku i powstawania nowych form zagrożeń. Charakteryzują się one znaczną

⁶ K. Cłapa, P. Klasa, *Edukacja 4.0 – budowanie świadomego społeczeństwa* [w:] A. Zakrzewska-Półtorak (red.), *Spółeczeństwo, gospodarka i przestrzeń w globalnych uwarunkowaniach*, Wrocław 2023, s. 11-13.

⁷ A. Gryszczyńska, G. Szpor, *Pojęcie transformacji cyfrowej i jej uwarunkowania prawne* [w:] I. Lipowicz (red.), *System Prawa Samorządu Terytorialnego. Tom III. Samodzielność samorządu terytorialnego – granice i perspektywy*, Warszawa 2023, s. 613-614.

⁸ Uchwała nr 98 Rady Ministrów z 12 września 2024 r. (M.P. poz. 812).

⁹ Ibidem, s. 47.

¹⁰ K. Chałubińska-Jentkiewicz, *Cyberbezpieczeństwo – zagadnienia definicyjne*, „Cybersecurity and Law” 2025, nr 1 (13), s. 5-8.

¹¹ Ibidem, s. 11.

różnorodnością, wielopoziomowością oraz wysokim poziomem niepewności, który jest immanentną cechą środowiska cyfrowego¹².

Przenosząc powyższą definicję na realia placówek oświatowych w trakcie transformacji cyfrowej można wskazać co najmniej trzy płaszczyzny cyberbezpieczeństwa oświaty.

Po pierwsze jest to bezpieczeństwo infrastrukturalne, obejmujące ochronę sieci informatycznych, urządzeń końcowych oraz wykorzystywanych w szkołach systemów teleinformatycznych, platform edukacyjnych i baz danych. Placówki oświatowe mogą stać się celem ataków hackerskich, infekcji złośliwym oprogramowaniem czy prób wyłudzenia danych.

Po drugie uczniowie muszą uzyskać w procesie nauczania kompetencje cyfrowe, które pozwolą na bezpieczne funkcjonowanie w rzeczywistości wirtualnej. Są to zarówno kompetencje techniczne, korzystania z określonych urządzeń czy programów jak też umiejętność krytycznego myślenia czy analizy informacji.

Trzeci obszar stanowią aspekty wychowawcze, związane z kształtowaniem postaw odpowiedzialnego i etycznego korzystania z technologii. Uczniowie są bowiem nie tylko potencjalnymi ofiarami, lecz także mogą stawać się sprawcami czynów zabronionych w sieci lub zachowań naruszających normy społeczne.

Ważnym elementem systemowej ochrony cyberbezpieczeństwa placówek oświatowych są przepisy ustawy z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa¹³. Art. 4 pkt 7 wśród podmiotów tworzących system wskazuje kilka kategorii jednostek sektora finansów publicznych. W wyliczeniu tym mieści się większość publicznych placówek oświatowych, które są samorządowymi, a czasami rządowymi jednostkami budżetowymi. Podstawowe obowiązki takich jednostek, to zarządzanie incydentami w danej instytucji, ich obsługa oraz zgłoszenie do właściwego zespołu reagowania na incydenty bezpieczeństwa komputerowego¹⁴, a także wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa¹⁵.

W perspektywie kilkuletniej dokumentem określającym cele i priorytety rządu jest Strategia Cyberbezpieczeństwa RP. W aktualnie procedowanym projekcie Strategii na lata 2025-2029¹⁶ znajdują się także wskazania konkretnych działań w ramach edukacji dzieci i młodzieży. W pkt. 9.2. projektu wskazano potrzebę uwzględnienia w edukacji, już na etapie wczesnoszkolnym, problematyki m.in. konieczności ochrony prywatności i danych osobowych w Internecie. Natomiast programy nauczania informatyki mają obejmować także zasady zapobiegania i reagowania na cyberzagrożenia¹⁷. Uzupełnieniem mają być szkolenia z zakresu cyberbezpieczeństwa i higieny cyfrowej organizowane przez Ministerstwo Cyfryzacji we współpracy z Ministerstwem Edukacji Narodowej¹⁸.

¹² R. Siudak, Cyberbezpieczeństwo w Polsce. Od dyskursów do polityk publicznych, Kraków 2022, s. 282-283.

¹³ Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tj. Dz.U. z 2024, poz. 1077 ze zm.).

¹⁴ Art. 22 ustawy o krajowym systemie cyberbezpieczeństwa.

¹⁵ Art. 21 ustawy o krajowym systemie cyberbezpieczeństwa.

¹⁶ Projekt tego dokumentu trafił w 2025 do konsultacji społecznych. Dostępny na stronie <https://www.zpp.pl/storage/library/2025-07/cf7c082cf522e38345bf2df011c043a5.pdf> [dostęp: 20.10.2025].

¹⁷ Ibidem, s. 38.

¹⁸ Ibidem, s. 69.

Warto podkreślić, że Minister Edukacji Narodowej będący centralnym organem administracji oświatowej opracował poradnik dla szkół dotyczący zasad zabezpieczenia cyfrowego¹⁹. Jedną z rekomendacji strategicznych jest opracowanie w placówce planu bezpieczeństwa cyfrowego o charakterze kadrowym, edukacyjnym, wychowawczym i techniczno-inwestycyjnym, wraz z polityką bezpieczeństwa infrastruktury cyfrowej²⁰. Uszczegółowieniem planu może być szkolny kontrakt korzystania z Internetu podpisany przez uczniów i rodziców, nauczycieli oraz innych pracowników szkoły²¹. W poradniku słusznie wskazano, że wspólne wypracowanie zasad dostępu do sieci jest lepszym rozwiązaniem niż ograniczanie go w szkole. Daje szansę na wdrażanie higieny cyfrowej, której dzieci i młodzież potrzebują na co dzień, zwłaszcza poza szkołą.

Aspekt organizacyjny

Szkoły i placówki oświatowe w swojej codziennej działalności wykorzystują rozbudowaną infrastrukturę techniczną, obejmującą łącza internetowe, systemy teleinformatyczne, platformy edukacyjne oraz komputery i inne urządzenia cyfrowe. Prowadzą także własne strony internetowe, które – podobnie jak szkolne sieci informatyczne – mogą stanowić potencjalny cel ataków hakerskich, prób nieuprawnionego dostępu czy infekcji złośliwym oprogramowaniem²².

Najważniejszym projektem infrastrukturalnym w obszarze cyfryzacji oświaty jest Ogólnopolska Sieć Edukacyjna wdrażana na podstawie ustawy z dnia 27 października 2017 r. o Ogólnopolskiej Sieci Edukacyjnej²³. Ustawa ta reguluje funkcjonowanie systemu zapewniającego dostęp do szybkiego i bezpiecznego Internetu w placówkach oświatowych. Realizacją zadań wynikających z ustawy zajmuje się Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (NASK).

Na uwagę zasługuje pkt 3 art. 5 ustawy, który formułuje obowiązek świadczenia szkołom usług bezpieczeństwa teleinformatycznego, obejmujących ochronę przed szkodliwym oprogramowaniem, monitorowanie zagrożeń i bezpieczeństwa sieciowego oraz filtrowanie treści, które mogą stanowić zagrożenie dla prawidłowego rozwoju uczniów. Jest to istotne zadanie OSE wspierające realizację art. 27 Prawa oświatowego²⁴ zgodnie z którym szkoły mają obowiązek zapewnienia uczniom ochrony przed dostępem do treści nieodpowiednich lub mogących wywołać negatywne skutki wychowawcze. Chodzi w szczególności o treści pornograficzne, eksponujące przemoc, materiały patostreamingowe oraz treści zachęcające do używania alkoholu, papierosów czy substancji psychoaktywnych²⁵. Obowiązek ten obejmuje zarówno szkolne

¹⁹ Bezpieczna szkoła. Zagrożenia i zalecane działania profilaktyczne w zakresie bezpieczeństwa fizycznego i cyfrowego uczniów, MEN, Warszawa 2020.

²⁰ Ibidem, s. 62.

²¹ Ibidem, s. 64-65.

²² Rodzaje zagrożeń zostały opisane m.in. w poradniku MEN, Bezpieczna szkoła..., s. 102-103; a także w poradniku Bezpieczeństwo online w szkołach Ogólnopolskiej Sieci Edukacyjnej, NASK, Warszawa 2020, s. 24.

²³ tj. Dz.U. z 2024 r. poz. 1768.

²⁴ Ustawa z dnia 14 grudnia 2016 r. (tj. Dz.U. z 2025 r. poz. 1043).

²⁵ S. Wójcik, Zagrożenia dzieci i młodzieży w internecie, „Dziecko krzywdzone. Teoria, badania, praktyka” 2017, nr 1, s. 271-272.

środowisko cyfrowe wraz z siecią wifi jak i treści udostępniane uczniom w ramach infrastruktury szkolnej²⁶.

Podkreślić należy, że w ramach rozwoju technologicznego w formie cyfrowej prowadzona jest coraz częściej dokumentacja dotycząca uczniów oraz ich wyników w nauce i zachowaniu – księgi ewidencji, księgi uczniów, dzienniki elektroniczne²⁷. Zarządzanie placówką oświatową jest ponadto coraz częściej wspierane przez specjalistyczne oprogramowanie administracyjne. Oznacza to, że różnorodne informacje, w tym dane osobowe uczniów, a często ich rodziców oraz pracowników szkoły są przechowywane i przetwarzane w formie cyfrowej. Dlatego zgodnie z art. 32 RODO²⁸ szkoła jako administrator danych osobowych jest zobowiązana do właściwego ich zabezpieczenia z uwzględnieniem środków technicznych oraz organizacyjnych. Obejmuje to obowiązek zapewnienia poufności, integralności, dostępności oraz odporności systemów przetwarzania danych, a także regularnego testowania, analizowania i oceniania skuteczności stosowanych zabezpieczeń. Skuteczna ochrona danych stanowi zatem nieodłączny element organizacyjnego wymiaru cyberbezpieczeństwa w oświacie.

Aspekt edukacyjny

W wymiarze edukacyjnym cyberbezpieczeństwo obejmuje kształtowanie u uczniów umiejętności rozpoznawania i unikania zagrożeń, z którymi mogą zetknąć się w środowisku cyfrowym. Dotyczy to w szczególności ryzykownych zachowań podejmowanych wobec dzieci i młodzieży w Internecie, takich jak próby wyłudzenia danych osobowych lub wizerunku, kradzież tożsamości, hejt oraz różne formy cyberprzemocy. Część zachowań skierowanych wobec dzieci i młodzieży poprzez sieć teleinformatyczną ma charakter przestępczy – są to przede wszystkim przestępstwa związane z seksualnością, takie jak propagowanie i pochwalanie pedofilii, uwodzenie dzieci (grooming²⁹), prezentowanie treści pornograficznych w tym tzw. twardej pornografii³⁰. Rosnącym zagrożeniem jest również sexting, rozumiany jako przesyłanie własnych treści o charakterze seksualnym, w tym zdjęć i nagrań³¹.

Choć zagrożenia te mogą wystąpić także w środowisku szkolnym, dużo częściej pojawiają się poza placówką, gdzie poziom ochrony sieci, filtrowania treści i monitorowania aktywności jest znacząco niższy. Z tego względu kluczową rolę odgrywa edukacja w zakresie bezpiecznego korzystania z technologii, obejmująca zarówno rozpoznawanie typowych zagrożeń, jak i znajomość

²⁶ Ł. Korzeniowski [w:] G. Krawiec (red.), Prawo oświatowe. Komentarz, Warszawa 2025, s. 110.

²⁷ Pozwala na to Rozporządzenie Ministra Edukacji Narodowej z dnia 25 sierpnia 2017 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (tj. Dz.U. z 2025 r. poz. 50).

²⁸ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.U.UE.L.2016.119.1).

²⁹ Szerzej: M. Bartnik, Grooming jako przestępstwo przeciwko wolności seksualnej i obyczajności popełniane na szkodę małoletniego – przyczynek do rozważań, „Cybersecurity and Law” 2025, nr 2 (14) 2025, s. 1-3.

³⁰ Szerzej: M. K. Maciejczuk, K. Wnorowski, M. Olchanowski, Cyberbezpieczeństwo dzieci i młodzieży w prawie polskim, „Zeszyty Naukowe Zbliżenia Cywilizacyjne” 2019, XV, nr 1, s. 13-16.

³¹ Bezpieczeństwo online w szkołach..., s. 10.

sposobów reagowania oraz możliwości uzyskania pomocy. Wiedza ta stanowi ważny element profilaktyki i może pełnić funkcję dodatkowej ochrony przed cyberzagrożeniami.

Obowiązki edukacyjne w tym zakresie wynikają m.in. z Polityki Cyfrowej Transformacji Edukacji (PCTE), która zakłada konieczność dostosowania podstawy programowej i włączenia problematyki bezpieczeństwa cyfrowego do treści nauczania nie tylko informatyki, lecz także innych przedmiotów. Literatura przedmiotu wskazuje ponadto, że skutecznym uzupełnieniem dydaktyki szkolnej są działania prowadzone w ramach edukacji pozaformalnej przez wyspecjalizowane instytucje i organizacje, oferujące programy dotyczące cyberbezpieczeństwa i bezpiecznego korzystania z Internetu³².

Aby nauczyciele mogli efektywnie wspierać uczniów w nabywaniu kompetencji związanych z bezpieczeństwem cyfrowym, konieczne jest systematyczne rozwijanie ich własnych kompetencji technologicznych, metodycznych i pedagogicznych. Jest to warunek niezbędny do rzetelnego przekazywania wiedzy o sposobach ochrony przed zagrożeniami oraz do właściwego reagowania na incydenty³³.

Współczesne środowisko cyfrowe charakteryzuje się także nadmiarem informacji, co powoduje, że istotnym zagrożeniem dla uczniów są zniekształcenia przekazu, manipulacje oraz treści fałszywe, w tym fake news i materiały typu deep fake. W odpowiedzi na te wyzwania wśród podstawowych kierunków realizacji polityki oświatowej państwa w roku szkolnym 2025/2026³⁴ Minister Edukacji Narodowej wskazał również rozwijanie umiejętności krytycznej analizy informacji dostępnych w Internecie. Jest to podstawa świadomego i odpowiedzialnego korzystania z zasobów cyfrowych.

Aspekt wychowawczy

Wiedza dotycząca zagrożeń cyfrowych, choć niezbędna, nie stanowi wystarczającej podstawy do bezpiecznego i odpowiedzialnego funkcjonowania uczniów w środowisku wirtualnym. Dzieci i młodzież są bowiem nie tylko odbiorcami treści i potencjalnymi ofiarami ataków, lecz również aktywnymi uczestnikami życia cyfrowego, mogącymi – świadomie lub nieświadomie – inicjować zachowania stanowiące zagrożenie dla innych użytkowników. Z tego względu istotnym uzupełnieniem edukacji cyfrowej jest realizacja programu wychowawczego, którego obowiązek prowadzenia wynika z art. 26 Prawa oświatowego. Jego celem jest kształtowanie postaw sprzyjających odpowiedzialnemu korzystaniu z technologii i przestrzeganiu norm społecznych w środowisku cyfrowym.

Chociaż podstawowa rola wychowawcza przypada rodzinie, to wsparcie szkoły jest niezbędne, zwłaszcza w obszarze nowych technologii, które mogą stanowić wyzwanie dla części rodziców. Program wychowawczy powinien zatem obejmować zarówno utrwalanie pozytywnych postaw, jak i korygowanie

³² Szerzej: T. Warchoń, Rola edukacji pozaformalnej w kształtowaniu bezpieczeństwa cyfrowego uczniów szkół podstawowych, „Polityka i Społeczeństwo” 2024, nr 2(22), s. 278-280.

³³ W tym obszarze aktywność przejawiają zarówno władze publiczne: np. MC poprzez projekt „E-kompetencje” dla nauczycieli szkół i przedszkoli (<https://www.gov.pl/web/cyfryzacja/nowe-projekty-na-rzecz-kompetencji-cyfrowych-nauczycieli-w-polsce>, [dostęp: 20.10.2025] jak też podmioty trzeciego sektora oferujące wiele szkoleń.

³⁴ Dostępne na stronie: <https://www.gov.pl/web/edukacja/podstawowe-kierunki-realizacji-polityki-oswiatowej-panstwa-w-roku-szkolnym-20252026> [dostęp: 20.10.2025].

zachowań niepożądanych. Uczniowie powinni rozumieć, jakie konsekwencje – prawne, społeczne i etyczne – mogą wynikać z ich zachowań w sieci, w tym rozpowszechniania treści naruszających cudzą godność, prywatność lub bezpieczeństwo³⁵.

Aksjologiczną podstawą szacunku dla każdego użytkownika środowiska cyfrowego jest niezbywalna godność człowieka, o której mowa w art. 30 Konstytucji RP. W świetle tej zasady każdy ma prawo do korzystania z cyfrowych technologii bez narażenia na ataki, manipulacje czy przestępstwa. Ochrona ta wykracza poza przeciwdziałanie czynom zabronionym przez prawo karne i obejmuje również zachowania naruszające normy społeczne, takie jak posługiwanie się fałszywą tożsamością, uczestnictwo w patostreamingu czy rozpowszechnianie dezinformacji i treści typu fake news.

Podsumowanie

Ochrona prawna, obejmująca przepisy prawa karnego oraz mechanizmy ścigania cyberprzestępstw, stanowi jedną z kluczowych tarcz bezpieczeństwa cyfrowego. W połączeniu z obowiązkami administracji oświatowej w zakresie zapewnienia bezpiecznego dostępu do Internetu oraz ochrony danych osobowych tworzy to solidny fundament normatywny. Istotnym uzupełnieniem norm prawnych są dokumenty strategiczne, takie jak PCTE czy projekt „Strategii Cyberbezpieczeństwa RP”, które wyznaczają kierunki interwencji państwa i cele na kolejne lata.

Należy jednak podkreślić, że sam system regulacji prawnych nie jest wystarczający w obliczu dynamicznego rozwoju zagrożeń cyfrowych. Skuteczna ochrona wymaga działań o charakterze organizacyjnym, w tym wdrażania bezpiecznych rozwiązań technologicznych w szkołach oraz edukacyjnym – ukierunkowanym na rozwijanie kompetencji cyfrowych uczniów i nauczycieli. Równie ważny jest aspekt wychowawczy, obejmujący kształtowanie postaw odpowiedzialności, etycznego korzystania z technologii oraz świadomości konsekwencji działań podejmowanych w środowisku wirtualnym.

Dopiero kompleksowe, wzajemnie uzupełniające się działania w tych trzech obszarach – organizacyjnym, edukacyjnym i wychowawczym – realizowane we współpracy szkoły, rodziców i instytucji zewnętrznych, stwarzają szansę na zapewnienie dzieciom i młodzieży bezpieczeństwa zarówno w toku nauki szkolnej, jak i w ich codziennej aktywności online.

Bibliografia

Akty prawne i dokumenty programowe:

- Polityka Cyfrowej Transformacji Edukacji, uchwała nr 98 Rady Ministrów z 12 września 2024 r. (M.P. poz. 812).
- Projekt Strategii Cyberbezpieczeństwa RP na lata 2025-2029, https://www.zpp.pl/storage/library/2025-07/cf7c082cf522e38345bf2_df011c043a5.pdf.
- Rozporządzenie Ministra Edukacji Narodowej z dnia 25 sierpnia 2017 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (tj. Dz.U. z 2025 r. poz. 50).

³⁵ Na ten aspekt cyberbezpieczeństwa zwraca uwagę poradnik: Standard bezpieczeństwa online placówek oświatowych, NASK, Warszawa 2018, s. 15-16.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.U.UE.L.2016.119.1).

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tj. Dz.U. z 2024, poz. 1077. ze zm.).

Ustawa z dnia 27 października 2017 r. o Ogólnopolskiej Sieci Edukacyjnej (tj. Dz.U. z 2024 r. poz. 1768).

Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe (tj. Dz.U. z 2025 r. poz. 1043).

Zalecenie Rady z dnia 22 maja 2018 r. w sprawie kompetencji kluczowych w procesie uczenia się przez całe życie (2018/C 189/01).

Literatura:

Bartnik M., Grooming jako przestępstwo przeciwko wolności seksualnej i obyczajności popełniane na szkodę małoletniego – przyczynek do rozważań, „Cybersecurity and Law” 2025, nr 2 (14).

Bezpieczeństwo online w szkołach Ogólnopolskiej Sieci Edukacyjnej, NASK, Warszawa 2020.

Bezpieczna szkoła. Zagrożenia i zalecane działania profilaktyczne w zakresie bezpieczeństwa fizycznego i cyfrowego uczniów, MEN, Warszawa 2020.

Chałubińska-Jentkiewicz K., Cyberbezpieczeństwo – zagadnienia definicyjne, „Cybersecurity and Law” 2025, nr 1 (13).

Cłapa K., Klasa P., Edukacja 4.0 – budowanie świadomego społeczeństwa [w:] A. Zakrzewska-Półtorak (red.), Społeczeństwo, gospodarka i przestrzeń w globalnych uwarunkowaniach, Wrocław 2023.

Forma P., Winiarczyk A., Kompetencje cyfrowe – jako metakompetencje XXI wieku, „Edukacja ustawiczna dorosłych” 2024, nr 4.

Gryszczyńska A., Szpor G., pojęcie transformacji cyfrowej i jej uwarunkowania prawne [w:] I. Lipowicz (red.), System Prawa Samorządu Terytorialnego. Tom III. Samodzielność samorządu terytorialnego – granice i perspektywy, Warszawa 2023.

Korzeniowski Ł. [w:] Krawiec G. (red.), Prawo oświatowe. Komentarz, Warszawa 2025.

Maciejczuk M. K., Wnorowski K., Olchanowski M., Cyberbezpieczeństwo dzieci i młodzieży w prawie polskim, „Zeszyty Naukowe Zbliżenia Cywilizacyjne”, 2019, XV (1).

OECD, Shaping Digital Education: Enabling Factors for Quality, Equity and Efficiency, OECD Publishing Paris 2023.

Plebańska M., Szyller A., Sieńczewska M., Q edukacji cyfrowej, Warszawa 2020.

Siudak R., Cyberbezpieczeństwo w Polsce. Od dyskursów do polityk publicznych, Kraków 2022.

Standard bezpieczeństwa online placówek oświatowych, NASK, Warszawa 2018.

Wójcik S., Zagrożenia dzieci i młodzieży w internecie, „Dziecko krzywdzone. Teoria, badania, praktyka” 2017, nr 1.

Warchoł T., Rola edukacji pozaformalnej w kształtowaniu bezpieczeństwa cyfrowego uczniów szkół podstawowych, „Polityka i Społeczeństwo” 2024, nr 2(22).