

nr 54

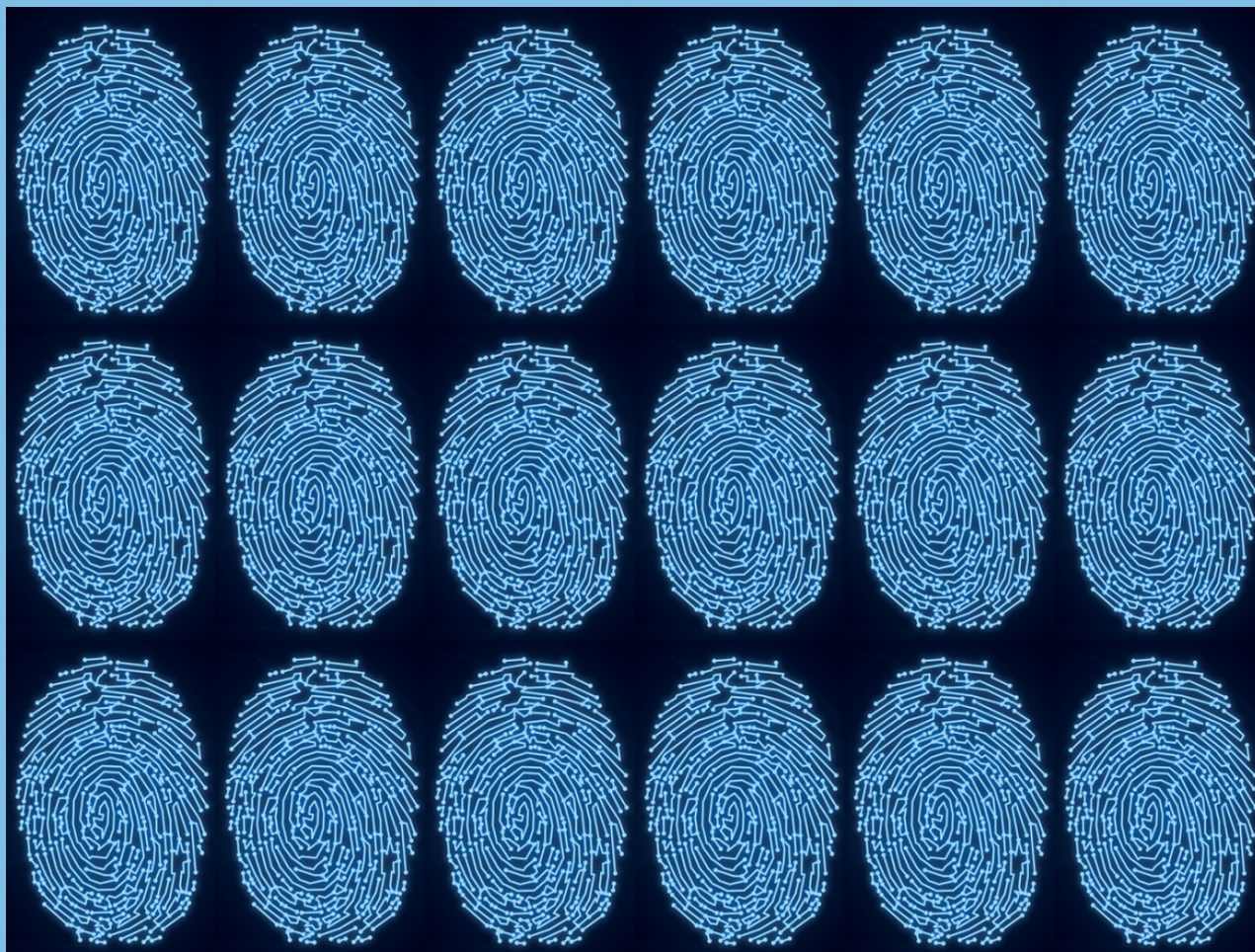
skrypty
belfra



Dolnośląski Ośrodek
Doskonalenia
Nauczycieli
we Wrocławiu
Filie w Jeleniej
Górze, Legnicy,
Wałbrzychu

Ewa Norkowska

Czy moje dane to moja sprawa? – o ochronie danych osobowych





Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym¹. Z tym konstytucyjnym prawem wiąże się ochrona danych osobowych. Pozyskiwanie, gromadzenie i udostępnianie danych dotyczących osób może odbywać się wyłącznie na podstawie obowiązujących przepisów prawa, które określają zasady i tryb gromadzenia oraz udostępniania informacji.

Zgodnie z ustawą zasadniczą (Konstytucja RP) każdy ma prawo do:

- 1) dostępu do dotyczących go urzędowych dokumentów i zbiorów danych,
- 2) do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.

Dane osobowe zostały zdefiniowane w Rozporządzeniu 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 (ogólne rozporządzenie o ochronie danych). Przez dane osobowe rozumie się wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Identyfikatorami danych osobowych są w szczególności: imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.²

Już od najmłodszych lat powinniśmy edukować dzieci w zakresie ochrony danych osobowych własnych i cudzych. Dzieci i młodzież, zwłaszcza kiedy korzystają z Internetu, nierozważnie udostępniają informacje o sobie, swoich bliskich i znajomych. Rodzi to poważne zagrożenia bezpieczeństwa osobistego i prywatności nie tylko dla nich samych, ale także osób, których dane zostały udostępnione. Najczęściej udostępniane dane to: imiona, nazwiska, adresy mailowe, wiek lub data urodzenia, zachowania i zainteresowania, oraz swoje zdjęcia i filmy. Dokładna analiza danych pozwala ich posiadaczowi nie tylko zidentyfikować lokalizację osób, ale także ich przyzwyczajenia, przekonania religijne, poglądy polityczne, zachowania konsumenckie, a nawet relacje z innymi osobami.

Pierwsze informacje dotyczące ochrony danych osobowych i prawa do prywatności każdy powinien uzyskać w domu, a potem poszerzać je w ramach edukacji formalnej i nieformalnej. Zgodnie z podstawą programową³ zadaniem przedszkol-

1 Art.47 i 51 Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r. (Dz.U. 1997 nr 78 poz. 483 ze zm.)

2 Art.4 pkt 1 Rozporządzenia 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 (ogólne rozporządzenie o ochronie danych)

3 Rozporządzenie Ministra Edukacji Narodowej z dnia 14 lutego 2017 r. w sprawie podstawy programowej wychowania przedszkolnego oraz podstawy programowej kształcenia ogólnego dla szkoły podstawowej, w tym dla uczniów z niepełnosprawnością intelektualną w stopniu umiarkowanym lub znacznym, kształcenia ogólnego dla branżowej szkoły I stopnia, kształcenia ogólnego dla szkoły specjalnej przysposabiającej do pracy oraz kształcenia ogólnego dla szkoły policealnej (Dz.U. 2017 poz. 356 ze zm.) i Rozporządzenie Ministra Edukacji Narodowej z dnia

la jest tworzenie sytuacji sprzyjających rozwojowi nawyków i zachowań, które mają kształtować u dzieci dbałość o bezpieczeństwo oraz systematyczne uzupełnianie, za zgodą rodziców, realizowanych treści wychowawczych o nowe zagadnienia, wynikające z pojawienia się w otoczeniu dziecka zmian i zjawisk istotnych dla jego bezpieczeństwa i harmonijnego rozwoju. W szkole podstawowej wiedzę na temat danych osobowych i ich ochrony uczeń uzyskuje podczas edukacji społecznej i przyrodniczej, a w klasach starszych – w ramach przedmiotu Wiedza o społeczeństwie. W szkole ponadpodstawowej zagadnienia związane z danymi osobowymi omawiane są w ramach „Podstaw przedsiębiorczości” oraz Wiedzy o społeczeństwie. W wielu placówkach oświatowych przedmiotowe zagadnienia poruszane są także podczas godzin wychowawczych, bądź w trakcie realizacji programów i projektów edukacyjnych. Takim programem jest np. ogólnopolski program edukacyjny „Twoje dane – twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli”⁴, który wpisuje się w działania edukacyjne Urzędu Ochrony Danych Osobowych, mające na celu podnoszenie świadomości społecznej w zakresie ochrony danych osobowych. Dolnośląski Ośrodek Doskonalenia Nauczycieli we Wrocławiu od 2 lat realizuje w/w program.

Ostatnie dwa lata (okres pandemii) w sposób szczególny pokazały konieczność znajomości zagadnień dotyczących ochrony danych osobowych, w tym w szczególności w cyberprzestrzeni. Wiele wątpliwości pojawiło się w związku z nauczaniem zdalnym – dotyczyły głównie ochrony wizerunku, myśli intelektualnej i poczucia bezpieczeństwa. Urząd Ochrony Danych Osobowych zamieścił na swojej stronie internetowej⁵ informacje dotyczące bezpieczeństwa danych osobowych podczas zdalnego nauczania. Zgodnie ze wskazaniem UODO obowiązki w tym zakresie mają zarówno dyrektor szkoły, nauczyciele, uczniowie i ich rodzice/prawni opiekunowie. Zgodnie z obowiązującymi przepisami⁶ szkoły mają dużą swobodę w zakresie wyboru właściwego narzędzia do nauki zdalnej, przy uwzględnieniu wszystkich aspektów związanych z możliwościami placówki, nauczycieli oraz możliwości techniczne i organizacyjne rodziców i uczniów. Dyrektor ma obowiązek poinformować nauczycieli, rodziców oraz uczniów o sposobie realizacji zdalnych zajęć. Jeżeli szkoła w celu realizacji nauki zdalnej będzie korzystać z nowych narzędzi lub usług świadczonych przez podmioty zewnętrzne, to musi także poinformować użytkowników o zakresie przetwarzania ich danych osobowych. Zgodnie z art. 35 ustawy – Prawa oświatowego⁷ w związku z art. 6 ust. 1 lit. e RODO⁸ dyrektor szkoły/placówki

30 stycznia 2018 r. w sprawie podstawy programowej kształcenia ogólnego dla liceum ogólnokształcącego, technikum oraz branżowej szkoły II stopnia (Dz.U. 2018 poz. 467 ze zm.)

4 <https://uodo.gov.pl/15> - dostęp 12.05.2022 r.

5 <https://uodo.gov.pl/pl/383/1475> - dostęp 11.05.2022

6 Rozporządzenie Ministra Edukacji Narodowej z 20 marca 2020 r. w sprawie szczególnych rozwiązań w okresie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19 (Dz.U. poz. 493 ze zm.).

7 Ustawa z dnia 14 grudnia 2016 r. - Prawo oświatowe (tj.: Dz.U. 2021 poz. 1082 ze zm.)

8 Rozporządzenia 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 (ogólne rozporzą-





może wymagać od ucznia, bądź jego rodziców/prawnych opiekunów jedynie danych niezbędnych do założenia dla niego konta w odpowiednim systemie zdalnego nauczania oraz w celu realizacji obowiązku nauki w formie zdalnej. Rodzice/prawni opiekunowie uczniów mają prawo wiedzieć, jak szkoła jako administrator będzie przetwarzała dane osobowe jego dziecka w trakcie nauki zdalnej oraz jakie w związku z tym przysługują im prawa. W przypadku wykorzystywania do zdalnej nauki platform innych administratorów pełnoletni uczniowie oraz rodzice/prawni opiekunowie niepełnoletnich uczniów powinni otrzymać klauzulę informacyjną o podstawowych zasadach i zakresie zbierania danych oraz administratorze. Dyrektor szkoły/placówki ma również obowiązek zabezpieczyć zgromadzone dane przez zastosowanie odpowiednich środków technicznych i organizacyjnych (dane te nie mogą być udostępniane osobom nieupoważnionym, należy je zabezpieczyć przed zniszczeniem, możliwością modyfikowania przez nieupoważnione osoby lub utratą). Taka praktyka ma szczególne znaczenie, gdy nauczyciele wykonują obowiązki służbowe poza szkołą. Należy przy tym pamiętać, że dyrektor ma prawo polecić nauczycielowi wykonywanie pracy zdalnej na terenie szkoły, z wykorzystaniem sprzętu znajdującego się w placówce, jeżeli jego warunki domowe nauczyciela nie spełniają przyjętych standardów i/lub nie zapewniają możliwości zapewnienia bezpieczeństwa danych.

Nauczyciele powinni wykorzystywać w nauczaniu zdalnym platformy edukacyjne lub narzędzia do e-learningu, które zostały wdrożone w szkole. Nauczyciele mogą przetwarzać dane osobowe uczniów i ich rodziców tylko w celach związanych z wykonywaniem swoich obowiązków służbowych, przy czym muszą pamiętać o bezpiecznym korzystaniu z komputerów i innych urządzeń zarówno wtedy, gdy zapewnił im je pracodawca, jak i wtedy, gdy korzystają z własnych. Przepisy RODO nie zabraniają wykorzystywania przez nauczycieli prywatnych komputerów, tabletów, czy telefonów do przetwarzania danych osobowych w związku ze zdalnym prowadzeniem zajęć. Ważne jest, aby te urządzenia były odpowiednio zabezpieczone, a nauczyciele powinni postępować zgodnie z polityką lub inną procedurą wprowadzoną w tym zakresie w szkole.

Podczas zajęć zdalnych uczniowie powinni aktywnie uczestniczyć w zajęciach. Wyrazem aktywności i zaangażowania ucznia podczas lekcji/zajęć jest m.in. zabieranie głosu podczas zajęć zdalnych. Stąd też mikrofon w większości przypadkach musi być włączony, gdyż nauczyciel ma prawo wzywać uczniów do udzielenia odpowiedzi na zadawane pytania. Taki obowiązek po stronie uczniów powinien być określony w regulaminach szkoły, dotyczących nauczania zdalnego. Nie ma natomiast podstaw prawnych do wymagania, by uczniowie posiadali kamery internetowe, umożliwiające przesyłanie obrazu podczas zajęć zdalnych (rozporządzenie o kształceniu na odległość nie definiuje formy komunikacji między nauczycielem a uczniami) - stąd też nie można nakazać uczniom włączania kamery internetowej podczas e-lekcji, a także wprowadzać konsekwencji za niekorzystanie z kamery (np. wystawienie oceny niedostatecznej, uwaga czy wstawienie

nieobecności). Także nauczyciele nie mają obowiązku udostępniać swojego wizerunku. Używanie kamer może nie być komfortowe dla obu stron z różnych powodów, np. osoby wstydzą się wyglądu swojego mieszkania lub znajdują się w krępującej sytuacji, występuje obawa, że ktoś nagrywa ekran, strach przed reakcją innych na mój wygląd.

Istotnym problemem z punktu widzenia ochrony danych osobowych jest też nagrywanie lekcji online. Nie ma przepisów, które wprost przewidywałyby możliwość nagrywania lekcji online. Jeśli nauczyciel chciałby nagrać lekcję, to muszą być spełnione określone warunki. Po pierwsze - należy wyraźnie wskazać cel nagrywania e-lekcji. Po drugie - należy podać, jak długo nagranie będzie przechowywane. Po trzecie – uczestnicy zajęć oraz ich rodzice/prawni opiekunowie muszą uzyskać informację kto uzyska do niego dostęp do nagrania i czy będzie ono rozpowszechniane. Po czwarte – obligatoryjnie wymagana jest zgoda ucznia pełnoletniego lub jeśli uczniowie nie są osobami pełnoletnimi - zgoda ich rodziców lub opiekunów prawnych. Zdarza się, że e-lekcje nagrywane są przez uczniów. Nauczyciel może zaakceptować takie nagrywanie, powinien jednak przed rozpoczęciem lekcji online poinformować uczniów, że nie wyraża zgody na rozpowszechnianie lekcji poza gronem uczniów danej klasy. Należy pamiętać, że nagrywanie zajęć zdalnych bez wiedzy i zgody ich uczestników jest naruszeniem norm społecznych, jednak nagrania zawierające wizerunek nauczyciela dokonane przez rodzica lub ucznia wykorzystywane do celów prywatnych, nie naruszają przepisów RODO.

Z nagrywaniem często wiąże się problem upubliczniania wizerunku zarówno uczniów, jak i nauczyciela. Wizerunek każdej uczennicy i każdego ucznia oraz wizerunek nauczyciela (zdjęcie/nagranie przedstawiające osobę) jest dobrem osobistym w rozumieniu cywilnoprawnym⁹ i nie może być dalej udostępniane bez zgody tej osoby. Jeżeli uczniowie lub nauczyciele upubliczniają zdjęcia/nagrania wykonane podczas prowadzonych zajęć, to w tej sytuacji osobie, której wizerunek został upubliczniony, przysługuje roszczenie z art. 78 ust. 1 ustawy – Prawo Autorskie¹⁰. Takie zachowanie może także zostać uznane za zniewagę na gruncie przepisów Kodeksu karnego¹¹, która jest przestępstwem ściganym z oskarżenia prywatnego na podstawie art. 216 Kodeksu.

Prowadzenie zajęć zdalnych może wymagać komunikowania się nauczycieli z uczniami i ich rodzicami/prawnymi opiekunami za pomocą poczty elektronicznej. Do tego celu powinny służyć służbowe skrzynki pocztowe, które zapewnia szkołę/placówkę. Szczególną uwagę należy zwrócić na zabezpieczenie danych osobowych udostępnianych w przesyłanych wiadomościach (sprawdzenie niezbedności danych, wybranie właściwego adresata, szyfrowanie wiadomości, korzystanie z opcji UWD przy korespondencji zbiorowej). Materiały edukacyjne nauczyciele mogą publikować na ogólnie dostępnych portalach lub stronach internetowych,

9 art.23 i 24 Ustawa z dnia 23 kwietnia 1964 r. - Kodeks cywilny (tj.: Dz.U. 2020 poz. 1740 ze zm.)

10 art. 83 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (tj.: Dz.U. 2021 poz. 1062 ze zm.)

11 Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny (tj.: Dz.U. 2021 poz. 2345 ze zm.)





nie mogą natomiast przetwarzać tam danych osobowych uczniów lub rodziców/prawnych opiekunów. Przy sprawdzaniu i monitorowaniu frekwencji uczniów nazajęciach prowadzonych zdalnego nauczyciela powinien zachować proporcjonalność i minimalizację danych.

W wirtualnej rzeczywistości coraz częściej mamy też do czynienia z cyberprzemocą i cyberatakami. Te zjawiska mają ścisły związek z ochroną danych osobowych.

Cyberatak – to każdy rodzaj ofensywnego działania w Internecie osób lub organizacji, którego celem mogą być systemy informatyczne, sieci komputerowe, komputery lub inne urządzenia osobiste¹². Cyberatak może przybierać różne formy. Typy cyberataków¹³, które mogą mieć miejsce w szkole lub organie prowadzącym:

- 1) Malware - jest to rodzaj złośliwego oprogramowania, które infekuje komputer i jednocześnie zmienia sposób jego działania w sposób zaplanowany przez atakującego. Najczęściej niszczy dane lub szpieguje użytkownika. Złośliwe oprogramowanie może rozprzestrzeniać się z jednego urządzenia na drugie, może też pozostawać na swoim miejscu, wpływając tylko na urządzenie gospodarza.
- 2) Cyberatak typu denial-of-service (DoS) prowadzi do przeciążenia zasobów systemu w takim zakresie, że system nie jest w stanie odpowiadać na uzasadnione żądania usług.
- 3) Cyberatak DDoS (distributed denial-of-service) ma na celu wyczerpanie zasobów systemu. Jest inicjowany przez ogromną liczbę zainfekowanych złośliwym oprogramowaniem maszyn kontrolowanych przez atakującego.
- 4) Cyberataki typu man-in-the-middle (MiTM) umożliwiają atakującemu podsłuchiwanie danych przesyłanych tam i z powrotem między dwiema osobami, sieciami lub komputerami - atakujący szpieguje interakcję pomiędzy nimi.
- 5) Phishing - atakujący wysyła wiadomości (e-mail, czat), które wydają się pochodzić z zaufanych, legalnych źródeł, próbując w ten sposób wyłudzić poufne informacje od swojego celu (atakujący wysyła link, który przeniesie użytkownika na stronę internetową, następnie ma miejsce pobranie złośliwego oprogramowania albo przekazania atakującemu informacji o ofercie).
- 6) Ransomware - cyberatak pozbawia czasowo administratora dostępu do jego danych. System „ofiary” jest przetrzymywany niejako w roli zakładnika, dopóki nie zostanie zapłacony okup atakującemu (w przypadku niezapłacenia okupu może dojść do trwałej utraty danych). Zmanipulowana „ofiara” pobiera oprogramowanie szyfrujące z witryny internetowej lub z załącznika do wiadomości e-mail. Wykorzystując luki na poszczególnych systemach, potrafi się ono zainstalować na wielu maszynach w danej sieci. Następnie, gdy atakujący zainicjuje szyfrowanie, wystąpi ono na wszystkich zainfekowanych systemach jednocześnie.

¹² <https://sjp.pwn.pl/sjp/cyberatak;5606168.html> – dostęp 10.05.2022 r.

¹³ Na podstawie <https://www.pbsg.pl/typy-cyberatakow/> - dostęp 11.05.2022 r.

7) Oszustwo nigeryjskie. Nadawca prosi o pomoc, zazwyczaj w formie wiadomości e-mail, ułatwieniu przekazania pewnej sumy pieniędzy. W zamian nadawca oferuje prowizję – dużą kwotę, a następnie prosi o przesłanie pieniędzy w celu pokrycia części kosztów związanych z przelewem. Jeśli pieniądze zostaną wysłane do oszustów, to oni znikają. Zdarza się, że oszuści próbują zdobyć więcej pieniędzy, twierdząc, że ciągle występują problemy z przelewem.

W celu zabezpieczenia szkoły/placówki na wypadek wystąpienia cyberataków, które mogłyby doprowadzić do nieuprawnionego pozyskiwania danych dyrektor powinien podjąć odpowiednie działania, np. edukowanie pracowników czy opracowanie procedur na wypadek wystąpienia zagrożeń związanych z nieuprawnionym pozyskiwaniem danych.

Słownik PWN definiuje cyberprzemoc¹⁴ jako wyzywanie, straszenie, nękanie, ośmieszanie itp. drugiego człowieka przy użyciu Internetu lub telefonu komórkowego. Wśród najpopularniejszych form cyberprzemocy należy wymienić:

- 1) publikowanie poniżających filmów lub zdjęć;
- 2) publikowanie ośmieszających, wulgarnych, komentarzy i postów;
- 3) włamania na konta serwisów społecznościowych;
- 4) flood, czyli przesyłanie wiadomości w komunikatorze, telefonami, SMSami
- 5) podszywanie się pod inne osoby;
- 6) wykluczanie z internetowych społeczności.

Specyficzną formą cyberprzemocy jest tzw. seksting i hejt. Seksting - jest to przesyłanie sobie nagich lub półnagich zdjęć. Pozornie delikatniejszą formą cyberprzemocy jest hejt, który polega na umieszczeniu w Internecie nienawistnych komentarzy, obrazków, filmów czy udostępnieniu takich treści.

Nie ma technicznych form ochrony przed cyberprzemocą, która może spotkać każdego, w dowolnym miejscu w sieci. Dlatego przede wszystkim należy jej przeciwdziałać. Wśród form przeciwdziałania cyberprzemocy wymienia się przede wszystkim edukację – uświadamianie występowania problemu agresji oraz wskazanie sposobów postępowania w przypadku wystąpienia zjawiska, poznanie i stosowanie zasad netykiety, uświadomienie odpowiedzialności karnej, wskazanie możliwości i sposobów zgłaszania nadużyć (procedury, nr telefonów, rozmowy ze sprawcami, poinformowanie szkoły, policji itd.), sposobów zabezpieczania dowodów (zrzuty ekranu, zachowanie SMS-ów, wiadomości e-mail), możliwość skorzystania telefonu zaufania dla dzieci i młodzieży. Istnieją też techniczne sposoby przeciwdziałania niepożądanym zachowaniom, ale wymagają znajomości programów, sposobów ich instalowania oraz aktualizacji.

Czy zatem moje dane to moja sprawa? Zasadnym wydaje się stwierdzenie, że moje dane to nasza wspólna sprawa: nauczycieli, uczniów i rodziców. Wiedza na temat udostępniania, przetwarzania i ochrony danych osobowych pozwoli nam wszystkim bezpiecznie funkcjonować we współczesnym świecie oraz uniknąć odpowiedzialności prawnej z tytułu naruszenia prawa do ochrony danych osobowych.



14 <https://sjp.pwn.pl/sjp/cyberprzemoc;5606169.html> – dostęp 11.05.2022



Podstawa prawna:

1. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r. (Dz.U. z 1997 r. nr 78. poz. 483 ze zm.)
2. 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 (ogólne rozporządzenie o ochronie danych)
3. Ustawa z dnia 23 kwietnia 1964 r. - Kodeks cywilny (tj.: Dz.U. 2020 poz. 1740 ze zm.)
4. Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (tj.: Dz.U. z 2021 r., poz. 1062 ze zm.)
5. Ustawa z dnia 6 czerwca 1997 r. - Kodeks karny (tj.: Dz.U. z 2021 r., poz. 2345 ze zm.)
6. Ustawa z dnia 14 grudnia 2016 r. - Prawo oświatowe (tj.: Dz.U. z 2021 r., poz. 1082 ze zm.)
7. Rozporządzenie Ministra Edukacji Narodowej z dnia 14 lutego 2017 r. w sprawie podstawy programowej wychowania przedszkolnego oraz podstawy programowej kształcenia ogólnego dla szkoły podstawowej, w tym dla uczniów z niepełnosprawnością intelektualną w stopniu umiarkowanym lub znacznym, kształcenia ogólnego dla branżowej szkoły I stopnia, kształcenia ogólnego dla szkoły specjalnej przysposabiającej do pracy oraz kształcenia ogólnego dla szkoły policealnej (Dz.U. z 2017 r., poz. 356 ze zm.)
8. Rozporządzenie Ministra Edukacji Narodowej z dnia 30 stycznia 2018 r. w sprawie podstawy programowej kształcenia ogólnego dla liceum ogólnokształcącego, technikum oraz branżowej szkoły II stopnia (Dz.U. z 2018 r., poz. 467 ze zm.)
9. Rozporządzenie Ministra Edukacji Narodowej z 20 marca 2020 r. w sprawie szczególnych rozwiązań w okresie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19 (Dz.U. z 2020 r., poz. 493 ze zm.).

Bibliografia:

1. Pyżalski J. (2012) Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży, Kraków, Oficyna Wydawnicza „Impuls”
2. Pyżalski J. (2009) Agresja elektroniczna i mobbing elektroniczny w kontekście zaangażowania w stosowanie nowych technologii komunikacyjnych, „Kwartalnik Pedagogiczny”, 4; 31-52
3. Knol K., Pyżalski J. (2011) Mobbing elektroniczny. Analiza rozwiązań profilaktycznych i interwencyjnych, „Dziecko krzywdzone. Teoria, badania, praktyka”, 1; 68-83
4. Jacek Pyżalski, EU Kids online 2018 Polska – raport z badań, Fundacja Orange [dostęp 4.05.2022 r.]
5. https://kancelariawyrzykowscy.pl/site/assets/files/1204/zdalne_nauczanie_poradnik-1.pdf [dostęp 11.05.2022 r.]
6. Poradnik dla szkół „Dane osobowe bezpieczne podczas zdalnego nauczania”, <https://www.gov.pl/web/edukacja-i-nauka/zdalne-nauczanie-uodo>, 2020 [dostęp 5.05.2022 r.]

Ewa Norkowska

Nauczyciel-konsultant

Dolnośląski Ośrodek Doskonalenia Nauczycieli we Wrocławiu



Dolnośląski Ośrodek Doskonalenia Nauczycieli we Wrocławiu

Dolnośląski Ośrodek Doskonalenia Nauczycieli we Wrocławiu jest jednostką organizacyjną Samorządu Województwa Dolnośląskiego, akredytowaną przez Kuratorium Oświaty we Wrocławiu. Posiada siedzibę główną we Wrocławiu oraz Filie w trzech lokalizacjach: w Jeleniej Górze, Legnicy i Wałbrzychu obejmując zasięgiem całe województwo dolnośląskie.

Zajmuje się organizacją i prowadzeniem różnorodnych form doskonalenia kadry kierowniczej szkół i placówek oświatowych oraz nauczycieli. Proponuje realizację programów wsparcia szkół w ich projakościowym rozwoju. Jest organizatorem wydarzeń edukacyjnych o charakterze lokalnym, regionalnym i międzynarodowym. W ramach statutowych zadań prowadzi działalność promocyjno-wydawniczą oraz konsultacje dla nauczycieli. Współpracuje z szeroko pojętym środowiskiem edukacyjnym - instytucjami działającymi na rzecz oświaty, wyższymi uczelniami, pracodawcami.

Zapraszamy dyrektorów szkół i placówek oraz nauczycieli do skorzystania z naszej oferty szkoleniowej. Proponujemy formy tradycyjne i prowadzone zdalnie. Różnorodna problematyka szkoleń zapewni Państwu podnoszenie kompetencji zawodowych w różnych obszarach, również związanych z realizacją kierunków polityki oświatowej państwa i województwa dolnośląskiego. Zapraszamy na stronę dodn.dolnyslask.pl/oferta/

Działamy skutecznie i profesjonalnie. Realizujemy różnorodne formy szkolenia: warsztaty, rady szkoleniowe, seminaria, konferencje i inne wydarzenia edukacyjne.

Oferta szkoleń jest różnorodna, z uwzględnieniem zgłoszonych przez Państwa potrzeb. Realizujemy międzynarodowe projekty edukacyjne.

Dedykujemy Państwu serię wydawniczą „Skrypty belfra” i „Skrypty metodyczne”.

Nie pozostajemy obojętni na bieżące problemy nauczycieli - nasi konsultanci i doradcy metodyczni prowadzą konsultacje indywidualne, w tym on-line.



ZAPRASZAMY

dodn.dolnyslask.pl