Gloria González Fuster oraz Dariusz Kloza (red.)

Europejski podręcznik: Nauczanie o ochronie danych i prywatności w szkołach

EAP

EUROPEJSKI PODRĘCZNIK:
NAUCZANIE O OCHRONIE DANYCH I PRYWATNOŚCI W SZKOŁACH

EUROPEJSKI PODRĘCZNIK: NAUCZANIE O OCHRONIE DANYCH I PRYWATNOŚCI W SZKOŁACH

Gloria González Fuster
Dariusz Kloza
(red.)

EAP

Europejski podręcznik: Nauczanie o ochronie prywatności w szkołach

Niniejszą książkę przygotowano w ramach projektu "Wprowadzenie kwestii związanych z ochroną danych i prywatnością do szkół w Unii Europejskiej" (ang. "Introducing d**A**ta p**R**ote**C**tion **A**n**D** privacy issu**E**s at school**S** in the European Union", ARCADES, www.arcades-project.eu) realizowanego między listopadem 2014 r. a majem 2015 r. i współfinansowanego z programu Unii Europejskiej Prawa Podstawowe i Obywatelstwo, zarządzanego przez Dyrekcję Generalną ds. Sprawiedliwości i Konsumentów (nr umowy o grant JUST/2013/FRAC/AG/6132).

Oświadczenie: Treści prezentowane w niniejszej książce nie odzwierciedlają poglądów Komisji Europejskiej.

ISBN 978-94-000-0768-0
D/2016/7849/111
NUR 822

Ilustracja na okładce: Femke Vanhellemont © 2016, na podstawie fotografii Nina Jelen © 2016.
Ilustracja na str. 89: Tomasz Soczyński. Ilustracje na str. str. 103 oraz 104: Anže Novak.

PODZIĘKOWANIA

Autorzy książki wyrażają swój dług wdzięczności wobec wielu nauczycieli, specjalistów z dziedziny edukacji, ekspertów ochrony danych osobowych i prywatności, aktywistów oraz dzieci i młodzieży, którzy służyli swoim wsparciem i zaangażowaniem podczas realizacji projektu ARCADES.

W szczególności chcielibyśmy wyrazić naszą wdzięczność wobec członków Międzynarodowej Grupy Roboczej ds. Ochrony Danych i Edukacji Cyfrowej, koordynowanej przez Pascale Serrier (Commission Nationale de l'Informatique et des Libertés (CNIL)), Gliwickiego Ośrodka Metodycznego i Kirsten Fiedler (Koalicja europejskich organizacji walczących o prawa cyfrowe (EDRi)) za cenne uwagi nt. podręcznika nauczyciela. Za bezcenny wkład chcielibyśmy również podziękować Autoritat Catalana de Protecciò de Dades (APDCAT) oraz Eticas Research & Consulting. Słowa podziękowania kierujemy także pod adresem European Schoolnet, Aídy Barquero oraz Ośrodka Edukacji Informatycznej i Zastosowań Komputerowych (OEIiZK).

Ponadto chcemy także podziękować wszystkim uczniom i nauczycielom, którzy brali udział w konkursach na scenariusze lekcji – tylko nieliczne mogły wygrać, ale wszystkie były bardzo inspirujące.

Zespół ARCADES

SPIS TREŚCI

WYKAZ SKRÓTÓW

ARCADES	Wprowadzenie kwestii związanych z ochroną danych oraz prywatnością do szkół w Unii Europejskiej
CNIL	Commission Nationale de l'Informatique et des Libertés (Krajowa Komisja ds. Informatyki i Wolności) (Francja)
DG	Dyrekcja Generalna
UE	Unia Europejska
GIODO	Generalny Inspektor Ochrony Danych Osobowych
IP RS	Republika Slovenija Informacijski pooblaščenec (Rzecznik Informacji Republiki Słowenii)
IT	Information Technology (Technologie Informacyjne)
LSTS	Grupa badawcza ds. Prawa, Nauki, Technologii i Społeczeństwa
NAIH	Nemzeti Adatvédelmi és Információszabadság Hatóság (Krajowy Urząd Ochrony Danych i Wolności Informacji na Węgrzech)
NGO	Organizacja pozarządowa
OEIiZK	Ośrodek Edukacji Informatycznej i Zastosowań Komputerów
VUB	Vrije Universiteit Brussel

WPROWADZENIE: DLACZEGO WŁAŚNIE ARCADES?

Wojciech Rafał WIEWIÓROWSKI*

Nie ma wątpliwości, że technologia ma ogromny wpływ na współczesne społeczeństwo i rozwój gospodarczy. Nie ma także wątpliwości co do tego, że nowe pokolenie czuje się znacznie swobodniej w świecie nowych Technologii Informacyjnych (IT) niż ich rodzice i dziadkowie. Jednocześnie towarzyszy temu rosnąca popularność „inteligentnych" urządzeń mobilnych i aplikacji, które w coraz szybszym tempie gromadzą informacje. Wobec ogromnej nierównowagi pomiędzy dostawcami takich urządzeń i aplikacji z jednej strony a konsumentem z drugiej, prowadzi to do sytuacji, w których korzyści społeczne płynące z korzystania z nowoczesnych technologii łączą się ze znacznymi zagrożeniami dla praw jednostki do ochrony danych i prywatności. Umiejętność zarządzania informacjami i umiejętności cyfrowe stają się więc niezbędne dla młodego pokolenia, stąd też misją organów ochrony danych jest zapewnienie, że młodzi ludzie są odpowiednio przygotowani do tego wyzwania, nie tracąc tym samym korzyści płynących z używania tych technologii.

Koncepcja projektu ARCADES oparta była na realizowanym w całej Polsce od 2009 r. programie skierowanym do szkół, zatytułowanym *Twoje dane – Twoja sprawa*, który cieszył się dużym zainteresowaniem ze strony nauczycieli. Stało się to źródłem inspiracji dla Generalnego Inspektora Danych Osobowych to tego, aby przenieść ten pomysł na szczebel europejski. Zespół projektu rozpoczynał jego realizację w przekonaniu, że szkoły powinny nauczać o ochronie danych osobowych i prywatności. Tematy związane z ochroną danych osobowych mogą

* Zastępca Europejskiego Inspektora Ochrony Danych.

zostać wpisane w programy nauczania różnych przedmiotów szkolnych. Stanowią one część umiejętności cyfrowych, które są fundamentem wiedzy na miarę XXI wieku i warunkiem *sine qua non* rozwoju nowoczesnych społeczeństw. Słusznie podkreśla się, że społeczeństwo demokratyczne potrzebuje, aby młodzi ludzie korzystali ze swoich umiejętności cyfrowych jako należnego im prawa, ale również narzędzia do zmieniania świata. Umiejętności cyfrowe są bowiem kluczem do aktywności społecznej i służą pomocą w rozwijaniu przedsiębiorczości, kreatywności i innowacji. Każda młoda osoba, która chce praktycznie i skutecznie korzystać ze swoich umiejętności cyfrowych, musi być świadoma tego, że podczas gdy dane są tlenem dla nowej ekonomii, użytkownik, który nie jest świadomy zagrożeń dla prywatności płynących z przetwarzania danych może stać się „produktem" w łańcuchu przemysłowym.

W *Opinii w sprawie ochrony danych osobowych dzieci* (Opinia nr 2/2009 Grupy Roboczej Artykułu 29) europejskie organy odpowiedzialne za ochronę danych podkreślają, że osoba, która nie osiągnęła jeszcze dojrzałości fizycznej i psychologicznej wymaga większej ochrony niż inni. Niemniej jednak poprawianie warunków dorastania dzieci oraz umacnianie praw dziecka do rozwoju własnej osobowości nie może się ograniczać jedynie do działań legislacyjnych i administracyjnych podejmowanych przez rządy, organy prawodawcze lub instytucje zajmujące się ochroną danych. Przede wszystkim można tego dokonać popularyzując wiedzę na temat aspektów nowych technologii związanych z prywatnością na każdym stadium edukacji młodych ludzi.

Dbałość i ochrona danych osobowych, tak niezbędne dla zapewnienia bezpieczeństwa dzieci, obejmuje także prawo dziecka do rozwoju oraz fakt, że z prawa tego można w pełni korzystać ze wsparciem lub ochroną zapewnianymi przez inne osoby. Odpowiedzialność za tę ochronę spoczywa na rodzinie, społeczeństwie i na państwie. Należy jednak pamiętać, że w celu osiągnięcia właściwego poziomu ochrony dzieci, niekiedy konieczne będzie szeroko zakrojone przetwarzanie ich danych osobowych, niejednokrotnie przez kilka podmiotów. Podejście do ochrony prywatności dzieci opiera się na kształceniu – przez rodziny, szkoły, organy ochrony danych, grupy rówieśnicze i innych – w zakresie potrzeby ochrony danych oraz prywatności oraz konsekwencji niepotrzebnego udostępniania danych.

Jeśli nasze społeczeństwa mają dążyć do prawdziwej kultury ochrony prywatności w ogóle i ochrony danych w szczególności, należy zacząć od dzieci –

nie tylko jako od grupy, która zasługuje na ochronę (lub jako podmiotów praw, które wymagają ochrony) ale także dlatego, że powinny one być świadome swoich obowiązków w zakresie poszanowania danych osobowych innych osób. Szkoły powinny odgrywać kluczową rolę dla osiągnięcia tego celu.

Dzieci i uczniowie powinni być zatem wychowywani tak, aby stać się niezależnymi obywatelami Społeczeństwa Informacyjnego. Dlatego też już od wczesnych lat życia powinni uczyć się o potrzebie ochrony danych osobowych i prywatności. Ta wiedza pozwoli im podejmować świadome decyzje dotyczące tego, które informacje chcą ujawnić, komu i pod jakimi warunkami. Ochrona danych powinna być systematycznie włączana w programy nauczania – niekoniecznie jako osobny temat, ale w każdym rodzaju zajęć, uwzględniając wiek uczniów oraz charakter nauczanych przedmiotów.

Rozwój umiejętności cyfrowych jest zazwyczaj oparty na relacji pomiędzy technologią a możliwymi do osiągnięcia rezultatami. Działania edukacyjne mające na celu ochronę prywatności powinny być oparte o ten sam scenariusz, przynosząc korzyści dla obydwu stron (ang. *win-win*). Powinny one jednak szanować fakt, że umiejętności cyfrowe mają charakter bardzo osobisty i indywidualny i będą różne u różnych dzieci.

Państwowe i prywatne instytucje edukacyjne oraz całe społeczeństwo obywatelskie zaangażowane w proces edukacyjny powinny rozumieć kwestie ochrony danych jako sedno umiejętności cyfrowych i promować innowacyjne metody nauczania o prywatności, jak również zapewniać narzędzia praktyczne służące prezentowaniu tej tematyki dzieciom.

Bruksela, maj 2016

WPROWADZENIE OD PARTNERÓW PROJEKTU ARCADES

Grupa Badawcza Ds. Prawa, Nauki, Technologii i Społeczeństwa (LSTS), Vrije Universiteit Brussel (VUB)

Szanowni Państwo,

Grupa Badawcza ds. Prawa, Nauki, Technologii i Społeczeństwa (LSTS) utworzona przez Vrije Universiteit Brussel (VUB) ze szczególną dumą prezentuje projekt ARCADES, a w szczególności niniejszy podręcznik.

Głównym celem projektu ARCADES było zintensyfikowanie wysiłków europejskich organów ochrony danych nakierowanych na zwiększanie świadomości kwestii dotyczących prywatności wśród dzieci i młodzieży poprzez edukację szkolną. W tym celu w projekcie połączono siły trzech organów ochrony danych oraz nasze – Grupy Badawczej LSTS na VUB, wiodącej grupy badawczej z uznanym w skali światowej doświadczeniem w dziedzinie prywatności i ochrony danych (oraz licznymi projektami realizowanymi wraz z organami ochrony danych na koncie). Naszą misją, jako jedynego partnera naukowego w projekcie ARCADES, było prowadzenie prac konsorcjum aż do ich ukoronowania w formie niniejszego podręcznika – tekstu praktycznego, innowacyjnego, bardzo europejskiego w swojej naturze i mocno zorientowanego na przyszłe wyzwania, stanowiącego punkt odniesienia dla nauczycieli.

Podczas tego projektu wiele się nauczyliśmy. Wiedzieliśmy, że organy zajmujące się ochroną danych aktywnie starały się edukować dzieci i młodzież, jak również ich nauczycieli. Dzięki ARCADES zdaliśmy sobie sprawę z istniejących inicjatyw, odkryliśmy siłę zaangażowania organów i dowiedzieliśmy się, że nauczyciele nie tylko potrzebowali praktycznych poradników, ale także byli żywo zainteresowani wykorzystaniem ich w codziennej pracy z dziećmi.

Zawsze wierzyliśmy, że dzieci i młodzież uważają prywatność za coś ważnego, i dlatego nie powinny być obwiniane za jej naruszanie, ale – zamiast tego – nauczane, jak jej bronić. W projekcie ARCADES poznaliśmy dzieci i młodych ludzi, którzy nauczyli nas, jak ważna jest umiejętność kontrolowania swoich danych osobowych, i że nigdy nie jest się za młodym na to, aby zacząć myśleć o prywatności.

Od początku postrzegaliśmy pracę nad tym podręcznikiem jako proces angażujący różne podmioty, uwzględniający wszystkie dostępne materiały i całą istotną wiedzę, toczący się w Brukseli i poza nią. Dlatego też zintegrowaliśmy kluczowe informacje, jakie otrzymaliśmy od nauczycieli i ich uczniów, ale także specjalistów w dziedzinie edukacji. Zwróciliśmy się także do ekspertów w obszarze społeczeństwa obywatelskiego i bezpieczeństwa w internecie, jak również szerokiej społeczności organów zajmujących się ochroną danych.

Podjęliśmy się tego zadania z perspektywy ochrony danych osobowych i prywatności jako praw podstawowych. Zawsze mieliśmy na uwadze fakt, że obydwa te prawa są wymienione w Karcie Praw Podstawowych Unii Europejskiej – i to z racji ich ogromnego znaczenia dla funkcjonowania społeczeństwa demokratycznego. Nauczanie o ochronie danych i prywatności nie powinno zatem dotyczyć (wyłącznie) zapewnienia „bezpieczeństwa" nieletnim. Musi ono także zapewniać, że będą oni świadomi swoich praw i gotowi ich dochodzić.

Publikacja niniejszego podręcznika to, naszym zdaniem, ważna wiadomość nie tylko dla nauczycieli, ale szerzej: także dla każdego, kto uważa, że edukacja powinna pomagać dzieciom i młodzieży w stawaniu się lepszymi (cyfrowymi) obywatelami.

Prof. dr Paul De Hert
Bruksela, maj 2016 r.

Generalny Inspektor Ochrony Danych Osobowych

Szanowni Państwo,

z dumą prezentujemy Państwu tę książkę będącą dowodem i owocem ponad półtorarocznej pracy poświęconej wprowadzeniu tematu ochrony danych i prywatności do szkół. Cieszę się bardzo, że Generalny Inspektor Ochrony Danych Osobowych miał możliwość udziału w tym projekcie.

W Unii Europejskiej dostępnych jest wiele materiałów edukacyjnych dotyczących ochrony danych osobowych w świecie cyfrowym, których adresatami są dzieci, młodzież i dorośli. Ich wartość jest nieoceniona – w erze szybkiego rozwoju technologicznego, dzieci zaczynają korzystać z internetu już w bardzo młodym wieku, używając go do nauki, zabawy i komunikacji. Niestety, bardzo często nierozważnie dzielą się informacjami o sobie i innych. Niezależnie od tego, ile materiałów edukacyjnych dostępnych jest online, rola, jaką w tym procesie do odegrania mają szkoły, jest niezastąpiona.

Kiedy zaczynaliśmy pracę nad projektem ARCADES, postawiliśmy sobie za cel stworzenie materiałów praktycznych dla szkół i nauczycieli, które pomogłyby im w nauczaniu młodych ludzi o potrzebie ochrony ich prywatności w sposób interesujący, a jednocześnie skuteczny. Jesteśmy przekonani, że wiedza dotycząca ochrony danych osobowych i prywatności oraz bezpiecznego korzystania z internetu powinna stanowić ważny element edukacji szkolnej. Niniejsza publikacja jest więc zbiorem praktycznych wytycznych dotyczących nauczania o ochronie danych i prywatności w szkołach.

Wartość tego rodzaju materiałów mogliśmy ocenić patrząc na popularność konkursu na najlepszy scenariusz lekcji zorganizowanego dla polskich szkół w ramach projektu ARCADES. Zaprosiliśmy nauczycieli do stworzenia – w oparciu o praktyczne wytyczne opracowane w ramach projektu – modelowego scenariusza lekcji na temat ochrony danych osobowych i prywatności. Otrzymaliśmy kilkanaście doskonałych propozycji spełniających wymogi

metodyczne obowiązujące w Polsce. Wiele z nich w bardzo oryginalny, a jednocześnie interesujący i skuteczny sposób demonstrowało, jak nauczać dzieci i młodzież o ochronie danych osobowych, o przysługujących im prawach oraz o tym, jak prawidłowo z nich korzystać.

Dlatego też z ogromną przyjemnością prezentujemy niniejszy podręcznik, mając nadzieję, że będzie on cieszyć się uznaniem zarówno wśród nauczycieli w UE i całego europejskiego środowiska edukacyjnego, ale także wśród organów ochrony danych UE.

dr Edyta Bielak-Jomaa
Warszawa, maj 2016 r.

Rzecznik Informacji Republiki Słowenii (IP RS)

Szanowni Państwo,

z ogromną przyjemnością prezentuję Państwu niniejszy podręcznik, wynik owocnej współpracy pomiędzy partnerami projektu ARCADES. Znajdą Państwo w nim wszystkie kluczowe informacje na temat ochrony danych i prywatności, których dzieci powinny być nauczane w szkołach, jak również praktyczne narzędzia, które mogą przydać się podczas nauczania o tych właśnie sprawach.

Dlaczego podjęliśmy się realizacji tego projektu? W naszej codziennej pracy organu odpowiedzialnego za ochronę danych często stykamy się z przypadkami i skargami dotyczącymi młodych osób – czy to jako ofiar, których prywatność została naruszona, czy – jeszcze gorzej – jako sprawców, znęcających się nad innymi w internecie lub mediach społecznościowych. Dlatego też wierzymy, że edukacja jest kluczowa – po to aby zapobiegać, a nie leczyć, aby nauczać młode osoby tego jak chronić własne dane osobowe i prywatność, a także aby dzieci i młodzież były w stanie korzystać ze wszystkich nowych technologii w sposób odpowiedzialny i z poszanowaniem innych osób.

Rzecznik Informacji Republiki Słowenii aktywnie działa w obszarze zwiększania świadomości w tym zakresie. Co roku publikujemy materiały mające na celu promowanie bezpiecznego i odpowiedzialnego korzystania z nowych technologii i nauczamy o tym, jak ważne są role, które odgrywamy jako rodzice, nauczyciele i eksperci w dziedzinie edukacji – w kształceniu dzieci do tego, aby były w stanie korzystać z wszystkich usług informacyjnych dla własnych celów, jednocześnie zachowując bezpieczeństwo i używając ich odpowiedzialnie. Dzieci mogą już teraz przewyższać nas swoją wiedzą o technicznej stronie korzystania z internetu. Ale to, czego im brak, to doświadczenie i świadomość tego, że mają przed sobą całą przyszłość – przyszłość, w której dane o nich dostępne w internecie mogą któregoś dnia stać się ich przekleństwem, uniemożliwić im dostanie stypendium, wymarzonej pracy, zdobycie zaufania partnera, w którym są zakochani. A to właśnie tę perspektywę i wiedzę jesteśmy w stanie im przekazać.

Rozpoczęliśmy projekt ARCADES półtora roku temu i w tym krótkim czasie zrealizowaliśmy ważne cele. Stworzyliśmy zbiór materiałów dla nauczycieli, zharmonizowanych i gotowych do użycia przez wszystkich pedagogów w UE. Zorganizowaliśmy bardzo udane szkolenia. Informacje, które otrzymaliśmy od nauczycieli w Słowenii były niezwykle pozytywne. Podkreślano, że seminaria dały im wiele cennych informacji w bardzo praktycznej formie wskazówek i treści interaktywnych, które będą mogli wykorzystać w pracy w swoich klasach. Zorganizowaliśmy także konkurs na najlepszy modelowy scenariusz lekcji – i z przyjemnością możemy pochwalić się, że zwycięzcy w Słowenii należeli do najmłodszej grupy wiekowej – dopiero zaczynali naukę w szkole podstawowej i byli u progu odkrywania całego potencjału internetu.

Podsumowując, w projekcie ARCADES możemy pochwalić się namacalnymi wynikami, które mają szanse na to, aby znacząco wpłynąć na zwiększanie świadomości dzieci na temat ochrony danych i prywatności. Życzę sobie, aby niniejsza publikacja dotarła do możliwie wielu szkół w różnych państwach członkowskich UE i podniosła poziom wiedzy na temat ochrony danych i prywatności.

Mojca Prelesnik
Lublana, maj 2016 r.

Krajowy Organ Ochrony Danych i Wolności Informacji na Węgrzech (NAIH)

Szanowni Państwo,

świat internetu ma realny wpływ na nawyki młodych ludzi we wszystkich aspektach życia. Powstają nowe słowa, używane są nowe formy komunikacji, wydarzenia globalne mają natychmiastowy wpływ na młodzież na całym świecie. Wszystko to kształtuje sposób myślenia i zachowania naszych dzieci. Te zmiany są nieuniknione, ale nie są w całości godne potępienia. Postawy młodych ludzi takie jak świadomość, ostrożność, krytyczne podejście i analityczne nastawienie są bardzo korzystnymi efektami tej zmiany.

Krajowy Organ Ochrony Danych i Wolności Informacji (NAIH) powstał z dniem 1 stycznia 2012 r. Przejął zadania realizowane przez poprzedniego rzecznika ochrony danych, który działał w latach 1995-2011. Węgierski Organ ds. Ochrony Danych otrzymuje skargi od obywateli, a w przypadku mocno uzasadnionych podejrzeń o poważne naruszenia takiej ochrony, może także inicjować postępowania administracyjne dotyczące ochrony danych.

Internet stanowi nieograniczone źródło danych osobowych – danych, które stanowią przedmiot zainteresowania z uwagi na niewiarygodnie wielką ilość informacji dostępnych online oraz powszechność internetu. Ochrona danych osobowych dzieci zawsze była priorytetem dla wszystkich nas, mających do czynienia z ochroną danych. Z racji swojego wieku i braku życiowego doświadczenia są one bardziej wrażliwe, a konsekwencje naruszenia ochrony ich danych mogą poważnie wpłynąć na ich osobowość i rozwój emocjonalny. Dlatego też Organ ds. Ochrony Danych zawsze zwracał szczególną uwagę na przetwarzanie danych osobowych dzieci przy użyciu internetu. Zapobieganie naruszeniom i działania edukacyjne podejmowane przez Organ mają niezwykłe znaczenie – zwiększanie poziomu świadomości osób, których dane dotyczą i ogółu społeczeństwa to zadania fundamentalne.

Jesteśmy przekonani, że wprowadzenie indywidualnych zajęć dotyczących ochrony danych w szkołach oraz zapewnienie najnowocześniejszej wiedzy w procesie kształcenia nauczycieli jest obecnie czymś nieodzownym, aby pomóc uczniom stać się wyedukowanymi i świadomymi użytkownikami nowoczesnych technologii informacyjnych i świadomymi obywatelami społeczeństwa informacyjnego. Sukces naszych projektowych publikacji – w tym także podręcznika dla nauczycieli, który znajdą Państwo w niniejszej publikacji – wyraźnie pokazuje, że wśród węgierskich ekspertów mających do czynienia z dziećmi (nauczycieli, specjalistów w dziedzinie ochrony dzieci, ekspertów organizacji dobroczynnych) istnieje ogromna potrzeba wymiany najlepszych praktyk i wiedzy fachowej w tym zakresie.

W ramach projektu zorganizowaliśmy także seminarium dla nauczycieli i ekspertów w dziedzinie edukacji. Spotkanie, które zgromadziło 200 zarejestrowanych uczestników zostało zorganizowane w dniach 20-22 października 2015 r. w Budapeszcie, na Narodowym Uniwersytecie Służby Cywilnej. Program seminarium podzielony był na dwie części: podczas sesji plenarnej zaprezentowano projekt ARCADES oraz podręcznik dla nauczycieli, natomiast kolejna część w formie warsztatów dawała możliwość omówienia z ekspertami konkretnych tematów, takich jak zaburzenia osobowości, skutki emocjonalne korzystania z internetu lub praktyczne wskazówki edukacyjne. Większość nauczycieli została poinformowana o tym wydarzeniu przez dyrektorów szkół, w których pracowali, połączonych z siecią Instytutu Edukacji, a niektórzy znaleźli informacje na stronie internetowej poświęconej ARCADES stworzonej przez NAIH. W oparciu o bezpośrednie reakcje, ale także opinie przedstawione na arkuszach ewaluacyjnych, seminarium można podsumować jako bardzo udane i użyteczne. Ponadto 15 prac nadesłanych do NAIH w konkursie na najlepszy scenariusz odnosiło się i obejmowało tematy i pomysły zaprezentowane w niniejszym podręczniku, jak również informacje i wiedzę, które staraliśmy się przekazać uczestnikom seminariów.

Co więcej, w marcu 2016 wraz z ministrem edukacji oraz uniwersytetami odpowiedzialnymi za kształcenie nauczycieli zainicjowaliśmy realizację specjalistycznych kursów dla nauczycieli poświęconych zagadnieniu ochrony danych osobowych – takim „nauczycielom przyszłości" Węgierski Organ Ochrony Danych z przyjemnością oferuje swoje doświadczenie, wiedzę oraz międzynarodowe kontakty.

dr Attila Péterfalvi
Budapeszt, maj 2016 r.

CZĘŚĆ I

KRAJOBRAZ NAUCZANIA O OCHRONIE DANYCH I PRYWATNOŚCI W SZKOŁACH

ARCADES, EUROPEJSKI PROJEKT WSPIERAJĄCY EDUKACJĘ W DZIEDZINIE PRYWATNOŚCI

Urszula GÓRAL i Paweł MAKOWSKI*

1. WIELE INICJATYW NA POZIOMIE KRAJOWYM

Współpracując w ramach licznych projektów, w tym projektów finansowanych przez Unię Europejską, okazało się, że wiele organów ochrony danych prowadzi działania edukacyjne. Te bardzo ciekawe inicjatywy rozwijane na poziomie krajowym były wdrażane niezależnie, równolegle, ale w istocie polegały na prowadzeniu bardzo podobnych działań. Współpracując z innymi organami, GIODO dostrzegł potrzebę skoordynowania tego typu inicjatyw poprzez dzielenie się dobrymi praktykami i ułatwianie dostępu do wiedzy – tak żeby nie „wyważać otwartych drzwi". Można zatem powiedzieć, że międzynarodowa współpraca pomiędzy organami ochrony danych doprowadziła do konkluzji, że wiele państw podejmowało samodzielnie działania edukacyjne, poświęcając czas i energię na tworzenie odpowiednich instrumentów i narzędzi edukacyjnych, podczas gdy inni osiągnęli już zadowalające efekty w tym obszarze. Dlatego wydawało się uzasadnione połączenie tych równoległych działań i stworzenie wspólnych rozwiązań umożliwiających bardziej efektywną realizację działań edukacyjnych przez oragny ochrony danych.

Niewątpliwie każdy organ napotyka w swoim kraju podobne problemy i wyzwania, gdy planuje podjęcie działań edukacyjnych we współpracy ze szkołami. Opracowanie odpowiednich pomocy dydaktycznych, stworzenie atrakcyjnych narzędzi dla nauczycieli i uczniów, a także przygotowanie kadry dydaktycznej wymaga dużych nakładów – zarówno merytorycznych jak

* Biuro Generalnego Inspektora Ochrony Danych Osobowych (GIODO), Polska.

i finansowych. Konieczna jest również współpraca z organami administracji publicznej nadzorującymi funkcjonowanie szkół. Jak pokazują doświadczenia organów ochrony danych, większość z nich – w bardziej lub mniej udany sposób – współpracuje z tymi instytucjami (na przykład wprowadzając treści związane z ochroną danych osobowych lub prawem do prywatności do programów nauczania). Analiza tych działań pozwala na stworzenie pewnego modelu, który mógłby posłużyć jako wzorcowy dla wszystkich organów zainteresowanych prowadzeniem działań edukacyjnych. Dlatego też uwzględniając niczym nieograniczoną naturę internetu, dostrzegamy potrzebę wypracowania wspólnego podejścia na szczeblu unijnym w celu stworzenia wspólnych i skutecznych metod edukowania nauczycieli w zakresie ochrony danych osobowych dzieci i młodzieży.

2. POLSKIE DOŚWIADCZENIA

W ostatnich latach GIODO w podejmowanych przez siebie działaniach stawiał edukację dzieci i młodzieży jako priorytet, dając temu wyraz poprzez szereg reliazowanych inicjatyw. Zmagając się z ograniczeniami finansowymi, udało się wypracować zadowalające rozwiązania – z nieocenioną pomocą innych organów ochrony danych i w oparciu o ich doświadczenie. Jednym z takich inspirujących doświadczeń były działania podejmowane przez czeskich kolegów. Bliska współpraca z tym organem pozwoliła na zapoznanie się z opracowanymi przez Czechów scenariuszami lekcji, wprowadzającymi treści dotyczące prywatności i ochrony danych osobowych do przedmiotów takich jak lekcje literatury, biologii czy historii. Ten sposób edukacji został z sukcesem wprowadzony do polskich szkół w ramach programu *Twoje dane – twoja sprawa*. Głównym celem tego programu, nieprzerwanie realizowanego przez GIODO od sześciu lat, jest poszerzenie oferty edukacyjnej placówek doskonalenia nauczycieli, szkół podstawowych, gimnazjów oraz szkół średnich poprzez wprowadzenie treści dotyczących ochrony danych osobowych oraz prawa do prywatności. Jednym z etapów programu jest szkolenie kadry pedagogicznej szkół i placówek doskonalenia nauczycieli oraz wyposażenie ich w materiały edukacyjne zawierające między innymi informacje dotyczące zasad ochrony danych osobowych oraz scenariusze lekcji, a tym samym przygotowanie nauczycieli do kształtowania świadomych, odpowiedzialnych i otwartych postaw wśród uczniów. Kolejnym elementem programu jest przeprowadzanie w szkołach i placówkach doskonalenia nauczycieli zajęć związanych z tematyką ochrony danych osobowych (m.in. spotkań i szkoleń) oraz opracowanie autorskich

scenariuszy lekcji i przygotowywanie raportów ewaluacyjnych dotyczących działań podjętych w trakcie programu.

3. PILNA POTRZEBA EDUKACJI W OBSZARZE OCHRONY DANYCH I PRYWATNOŚCI

Doświadczenie polskiego organu związane z kształtowaniem polityki w zakresie edukacji, wypracowanie obecnie funkcjonującego modelu edukacji oraz stosunkowo duże zainteresowanie wyrażone przez nauczycieli w Polsce dotyczące programu *Twoje dane – twoja sprawa* zainspirowały Generalnego Inspektora Ochrony Danych Osobowych do przeniesienia go na poziom europejski. Wynikiem powyższego była propozycja projektu ARCADES złożona do Komisji Europejskiej w marcu 2014 r. w ramach programu Prawa Podstawowe i Obywatelstwo, zarządzanego przez Dyrekcję Generalną ds. Sprawiedliwości. Została ona pomyślnie oceniona w lipcu 2014 r. i otrzymała dotację na działania dla czterech partnerów – Biura Generalnego Inspektora Ochrony Danych Osobowych jako koordynatora projektu, Rzecznika Informacji Republiki Słowenii, Krajowego Organu Ochrony Danych i Wolności Informacji (Węgry) oraz Grupy Badawczej ds. Prawa, Nauki, Technologii i Społeczeństwa (LSTS) na Vrije Universiteit Brussel (VUB) z Belgii. Konsorcjum projektowe zostało dobrane uwzględniając doświadczenie każdego z partnerów w tworzeniu pomocy naukowych dla szkół.

4. CELE ARCADES – O CO TU CHODZI?

Projekt wpisuje się w prowadzone na terenie Unii Europejskiej działania na rzecz podnoszenia świadomości na temat ochrony danych osobowych I prywatności. Jak już wspomniano, wiele takich inicjatyw podejmowanych jest przez organy ochrony danych osobowych w UE, które niezależnie od swoich kompetencji władczych, poświęcają także dużo uwagi działalności edukacyjnej. Ochrona danych osobowych i prywatności to prawa podstawowe, chronione tak przez prawodawstwo krajowe jak i prawo UE. Zadaniem takich organów jest ochrona tych praw. Mają one także do odegrania rolę polegającą na kształceniu ogółu społeczeństwa w tym obszarze. *Rezolucja w sprawie edukacji cyfrowej dla wszystkich* sporządzona podczas Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności, która odbyła się w Warszawie w 2013 r., jest tylko jednym z przykładów takiego zaangażowania. Rezolucja ta rekomenduje zapewnienie specjalnej ochrony nieletnim w kontekście wykorzystywania

technologii cyfrowych, była ona także bodźcem dla organów ochrony danych, aby zwrócić uwagę na działania edukacyjne skierowane wprost do szkół.

Jest to niesłychanie ważne szczególnie teraz, w erze szybko rozwijających się technologii cyfrowych, które są coraz bardziej wykorzystywane przez młode osoby. Dlatego też organy ochrony danych tworzyć powinny materiały edukacyjne skierowane do młodzieży, nauczycieli oraz rodziców. Bardzo ważne jest spójne kształcenie wszystkich tych grup w obszarze ochrony danych i prywatności.

Takie podejście do roli organów ochrony danych w Europie odzwierciedlone zostało także w przepisach ogólnego rozporządzenia o ochronie danych z 27 kwietnia 2016 r. Zgodnie z treścią artykułu 57 rozporządzenia, wśród licznych zadań stawianych przed organami ochrony danych, zapisano także obowiązek *upowszechniania w społeczeństwie wiedzy o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem oraz rozumienie tych zjawisk.* Niezwykle ważne jest, że wspomniany wyżej przepis podkreśla konieczność zwrócenia specjalnej uwagi działaniom skierowanym do dzieci.

Polskie doświadczenia w ramach wspomnianego programu *Twoje dane – twoja sprawa* pokazują, że w procesie upowszechniania wśród dzieci wiedzy na temat ochrony ich prywatności szczególne znaczenie ma wprowadzanie tych kwestii do prowadzonych w szkołach zajęć lekcyjnych. Codzienna praca nauczycieli uczestniczących w programie uświadomiła nam, że istnieje duża potrzeba przygotowania materiałów właśnie dla nauczycieli, tak by mogli oni skutecznie i ciekawie uczyć o ochronie danych osobowych w szkołach. Szczególną rolę szkoły w procesie edukowania dzieci i młodzieży na temat funkcjonowania w społeczeństwie oraz bezpiecznego zwiedzania cyfrowego świata dostrzegli także autorzy raportu raportu Eurobarometru z 2008 r. (*Towards a safer use of Internet for children in the EU – a parent`s perspective*). To właśnie szkoła jest pierwszym miejscem, gdzie dzieci i młodzież zgłaszają przypadki naruszenia ich prywatności. Stąd też głównym celem projektu ARCADES było stworzenie odpowiednich materiałów, które pomogłyby wprowadzić treści dotyczące ochrony danych osobowych właśnie do szkół.

5. OSIĄGAJĄC CELE

Aby nauczyciele byli w stanie skutecznie przekazać swoją wiedzę na temat ochrony danych osobowych i tym samym podnosić świadomość i umiejętności

dzieci i młodzieży w zakresie ochrony ich prywatności, niezbędnym było przygotowanie odpowiednich materiałów szkoleniowych. W tym celu partnerzy projektu ARCADES w pierwszej kolejności dokonali podsumowania istniejącej wiedzy dotyczącej kształcenia w zakresie ochrony danych osobowych i prywatności w szkołach w UE.[1] Raport zawiera zestaw podstawowych zasad ochrony danych osobowych i prywatności, a także przykłady materiałów i inicjatyw skierowanych do nauczycieli i uczniów, przedstawiając główne trendy w procesie nauczania o ochronie danych osobowych oraz przykłady najlepszych praktyk w tym zakresie. Dokument nie jest oczywiście wyczerpującym materiałem nt. wszystkich inicjatyw prowadzonych na terenie Unii Europejskiej, stanowi jednak przyczynek do otwarcia dyskusji na temat wymogów, które powinny spełniać materiały dla nauczycieli dotyczące tego ważnego zagadnienia.

Mając taki fundament mogliśmy zacząć przygotowywanie materiałów edukacyjnych, które byłyby dla nauczycieli inspiracją i pozwalałyby przygotować się im do prowadzenia lekcji poświęconych ochronie danych. Tak właśnie powstał podręcznik dla nauczycieli.[2] Materiał skierowany jest do nauczycieli szkół podstawowych, gimnazjów i szkół średnich, którzy chcą zwiększyć poziom swojej wiedzy w obszarze ochrony danych osobowych, a jednocześnie pozyskać materiały pomocne w prowadzeniu lekcji na ten temat. Podręcznik ten ma w założeniu stanowić użyteczne narzędzie dla nauczycieli w każdej szkole w UE, którzy chcą nauczać dzieci i młodzież na temat ochrony danych osobowych i prywatności. Jest on napisany prostym i zrozumiałym językiem, który pomóc ma nauczycielom znaleźć właściwe słowa do tego, aby wyjaśniać ten temat swoim uczniom. Każdy z rozdziałów podręcznika obejmuje inny aspekt ochrony prywatności i danych osobowych, przedstawia zbiór kluczowych zagadnień, zawiera również pomysły do dyskusji, zalecane ćwiczenia i szereg praktycznych wskazówek. Dokument, którego udoskonalona wersja znajduje się w niniejszym podręczniku, spotkał się z pozytywnymi ocenami krajowych ośrodków doskonalenia nauczycieli w Polsce, na Węgrzech i w Słowenii, co gwarantuje, że

[1] G. González Fuster, P. De Hert, i D. Kloza, *Deliverable 1.1: State-of-the-Art Report on Teaching Privacy and Personal Data Protection at Schools in the European Union*, ARCADES, marzec 2015 <http://arcades-project.eu/images/pdf/State_of_the_art_report.pdf> dostęp 01.05.2016.

[2] Wcześniejsza wersja materiału: G. González Fuster (red.), *Deliverable 1.2: The European Handbook for Teaching Privacy and Data Protection at Schools – the set of materials for teachers*, ARCADES, wrzesień 2015, <http://arcades-project.eu/images/pdf/The_European_Handbook_for_Teaching_Privacy_and_Data_Protection_at_Schools.pdf> dostęp 01.05.2016.

jest on dopasowany do wymogów dotyczących materiałów edukacyjnych używanych w czasie zajęć szkolnych.

Podręcznik ten był prezentowany podczas seminariów, które w ramach projektu ARCADES zostały zorganizowane w październiku 2015 r. przez partnerów z Polski, Słowenii i Wegier. Każde z trzech wydarzeń zgromadziło prawie 200 nauczycieli. Celem seminariów było przekazanie im kluczowej wiedzy w zakresie ochrony danych osobowych i prywatności tak, aby mogli oni w trakcie prowadzonych zajęć przedstawić ją swoim uczniom. Uczestnikom seminariów przedstawiono zarówno podstawowe informacje na temat ochrony danych, jak i praktyczne materiały edukacyjne w formie podręcznika. Informacje, które otrzymaliśmy od nauczycieli pokazują, że bardzo często brak im odpowiedniej wiedzy i materiałów niezbędnych do nauczania o ochronie danych i prywatności. Nauczyciele podkreślali także, że bardzo często właśnie szkołach dzieci opowiadają o incydentach związanych z naruszeniem prywatności i ochrony danych, ale brak jest wytycznych dla nauczycieli dotyczących sposobu, w jaki należy właściwie zareagować. Z tym większą satysfakcją przyjęliśmy ich pozytywne opinie na temat projektu ARCADES, co tylko potwierdziło nasze przekonanie, że materiały projektu mogą zostać docenione przez nauczycieli, którzy dostrzegają w nich praktyczną wartość dla prowadzonych przez siebie lekcji.

Powyższe znalazło także potwierdzenie w ilości prac zgłoszonych do konkursu, który został ogłoszony w Polsce, na Węgrzech i w Słowenii. Publikacja materiałów edukacyjnych lub czysto teoretyczne kształcenie dzieci i młodzieży już nie wystarczą – nowe metody, które spełniają potrzeby uczniów, powinny być włączone do programów nauczania w celu opracowania naprawdę skutecznego podejścia edukacyjnego. Stworzenie scenariuszy lekcji opartych na spersonalizowanych, realnych przykładach może wzbudzić zainteresowanie i zaangażować dzieci i młodzież oraz dostarczyć im wiedzę jak sobie radzić w codziennych sytuacjach. Stąd też przedmiotem konkursu uczyniliśmy przygotowanie modelowego scenariusza lekcji poświęconej ochronie danych osobowych. Wszystkie przygotowane w ramach konkursu scenariusze zostały przygotowane w oparciu o podręcznik zaprezentowany podczas seminariów, co potwierdziło w naszym odczuciu jego praktyczną przydatność.

Zwycięzcy krajowych konkursów na najlepszy scenariusz lekcji mieli okazję „odegrać" tę lekcję podczas konferencji kończącej projekt, która została zorganizowana w marcu 2016 r. Barcelonie. Aktywność konsorcjum ARCADES

została dostrzeżona także przez Międzynarodową Grupę Roboczą ds. Ochrony Danych i Edukacji Cyfrowej, prowadzoną przez francuski organ ochrony danych (CNIL), co doprowadziło do zorganizowania wspólnego warsztatu podczas konferencji w Barcelonie, tematem którego był modelowy zestaw szkoleniowy dla nauczycieli oraz wytyczne dotyczące „ram kompetencji" w obszarze ochrony danych i prywatności.

6. ISTOTNOŚĆ NA SZCZEBLU UE I PERSPEKTYWY NA PRZYSZŁOŚĆ

Dotychczas większość dostępnych materiałów edukacyjnych poświęconych ochronie danych i prywatności dla dzieci i młodzieży była tworzona na szczeblu krajowym. Wymiana doświadczeń pomiędzy partnerami projektu ARCADES pomogła stworzyć materiały nie tylko skuteczne, ale także trafiające w potrzeby szkół w całej Unii Europejskiej. W ostatecznym rozrachunku projekt ten zakończył się stworzeniem materiałów, które nie są ograniczone swoim zasięgiem tylko do jednego kraju, ale potencjalnie mogą mieć zastosowanie w każdym państwie członkowskim – nawet jeśli naturalnie wymagałoby to jakiejś elastyczności, aby zapewnić ich praktyczne zastosowanie i odniesienie do kontekstów lokalnych. Materiały przygotowane w trakcie tego projektu prezentują zatem szerszą perspektywę niż tylko krajową, dzięki czemu możliwe jest ich przeniesienie i bezpośrednie wykorzystanie we wszystkich państwach UE.

Mimo że projekt został już zakończony, wierzymy, że materiały ARCADES pozostaną źródłem inspiracji dla wielu nauczycieli w różnych państwach członkowskich UE. Mamy nadzieję, że będą one także użyteczne dla organów ochrony danych UE w ramach prowadzonych przez nie działań edukacyjnych, ponieważ treści prezentowane w niniejszej publikacji zawierają nie tylko kluczową wiedzę z obszaru nauczania o prywatności, ale także szereg porad praktycznych. Zachęcamy zatem Państwa do uważnej lektury niniejszej publikacji i aktywnego czerpania z zawartych tu informacji w celu wspierania działań edukacyjnych na temat prywatności dzieci i młodzieży w Europie.

SŁOWO OD GRUPY ROBOCZEJ DO SPRAW EDUKACJI CYFROWEJ

Pascale RAULIN-SERRIER i Sophie VULLIET-TAVERNIER[*]

Rezolucja w sprawie edukacji cyfrowej dla wszystkich[1] przyjęta podczas 35. Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności w Warszawie w 2013 r. wzywa organy ochrony danych do zwiększenia swojego zaangażowania w działania edukacyjne skierowane do ogółu społeczeństwa, które mają pomóc obywatelom stać się świadomymi i odpowiedzialnymi podmiotami w społeczeństwie cyfrowym, którzy potrafią skutecznie korzystać ze swoich praw i znają swoje obowiązki w tym obszarze. W ciągu ostatnich kilku lat wiele organów ochrony danych na całym świecie wymieniało się doświadczeniami i podejmowało istotne inicjatywy o charakterze globalnym dotyczące zwiększania świadomości potrzeby ochrony danych i prywatności wśród dzieci i młodzieży.

W ramach tych działań wspomniana rezolucja nałożyła na Międzynarodową Grupę Roboczą ds. Ochrony Danych i Edukacji Cyfrowej zadanie wdrożenia rocznych priorytetowych Planów Działania, takich jak „*Rozwój pakietu szkoleniowego mającego na celu przeszkolenie trenerów w zakresie ochrony danych i prywatności*" oraz „*Stworzenie platformy internetowej do dzielenia się treściami i materiałami edukacyjnymi w zakresie edukacji cyfrowej*" dla zrealizowania swoich głównych celów operacyjnych.[2]

---

[*] Departament Edukacji Cyfrowej, Commission Nationale de l'Informatique et des Libertés (CNIL), oraz koordynatorzy Międzynarodowej Grupy Roboczej ds. Ochrony Danych i Edukacji Cyfrowej.

[1] <https://icdppc.org/wp-content/uploads/2015/02/Digital-education-resolution.pdf> dostęp 15.05.2016.

[2] Obejmują one: (1) Promowanie edukacji w zakresie prywatności jako elementu programów nauczania kompetencji cyfrowych oraz (2) Przyczynianie się do szkolenia przyszłych osób szkolących poprzez organizowanie lub wkład w „doskonalenie zawodowe personelu szkolącego" w zakresie ochrony danych i prywatności.

Europejski projekt ARCADES oraz stworzenie w jego ramach zbioru materiałów edukacyjnych idealnie wpisuje się w działania mające na celu stworzenie zestawów edukacyjnych dla pedagogów w obszarze ochrony danych i prywatności. Na podstawie naszej analizy dostępnych materiałów edukacyjnych dla nauczycieli,[3] wynika, że nie istnieje żaden jednolity wzorzec zestawów edukacyjnych skierowanych do pedagogów poświęconych nauczaniu o prywatności i ochronie danych osobowych w szkołach w UE. Ten proces musi bowiem uwzględniać różne podejście krajów członkowskich do europejskiego prawodawstwa i różny stopień implementacji przepisów unijnych.

Dlatego też niniejszy podręcznik ma pomóc nauczycielom w przygotowywaniu dzieci i młodzieży do zmobilizowania i rozwinięcia kluczowych umiejętności, wiedzy i świadomości, aby odpowiednio i skutecznie reagować na liczne wyzwania i szanse, przed którymi stają każdego dnia w demokratycznym społeczeństwie – zarówno w świecie realnym, ale także świecie cyfrowym.

W tym kontekście niniejszy podręcznik, a w szczególności zbiór materiałów dla nauczycieli, ma na celu wykroczyć znacznie poza „edukację medialną" i „rozwój umiejętności cyfrowych", aby objąć także nowe wymiary związane z „edukacją prawną i etyczną", to znaczy zrozumieniem tego, w jaki sposób odpowiednie przepisy prawne definiują wytyczne i zachowania w środowisku online i offline.

Opinie i oceny otrzymane do tej pory od członków Międzynarodowej Grupy Roboczej ds. Ochrony Danych Edukacji Cyfrowej wskazywały na żywe zainteresowanie rozpowszechnianiem podręcznika jako bardzo użytecznego i wszechstronnego narzędzia wśród nauczycieli, pedagogów, władz publicznych odpowiedzialnych za edukację oraz innych podmiotów – tak aby umożliwić dzieciom i młodzieży pełne zrozumienie przysługujących im praw, swobód i obowiązków nałożonych na nie w społeczeństwie demokratycznym.

Oczywiście nauczyciele są zachęcani do tego, aby zapoznać się z niniejszym materiałem, a następnie korzystać, adaptować lub nawet odkrywać wszystkie obszary zainteresowań związane z prywatnością poprzez zawarte tu praktyczne porady. Zgodnie ze swoimi doświadczeniami pedagogicznymi mogą je

[3] Pokazują to dwa raporty z badań autorstwa Grupy Roboczej organów ochrony danych ds. edukacji cyfrowej z 2014 i 2015 r.

dopasowywać do potrzeb swoich uczniów. Dlatego też chcielibyśmy wyrazić nasze uznanie dla partnerów projektu ARCADES, którzy przyczynili się do stworzenia tego innowacyjnego materiału. Materiału, który można śmiało zaprezentować nie tylko nauczycielom, ale również samym nastolatkom i ich rodzicom.

WIELE WYMIARÓW NAUCZANIA O PRYWATNOŚCI W SZKOŁACH W EUROPIE

Gloria GONZÁLEZ FUSTER, Dariusz KLOZA oraz Paul DE HERT*

Mimo że nauczanie o prywatności stało się już codziennością w wielu szkołach w Europie, niejednokrotnie słychać głosy o potrzebie jego polepszenia. W niniejszym rozdziale staramy się zbadać przyczyny takiej sytuacji i wyciągnąć wnioski z krótkiego przeglądu bieżącej praktyki. Dlatego też w pierwszej kolejności uwagę poświęcamy samej potrzebie nauczania o prywatności i o ochronie danych osobowych w szkołach, a następnie – dotychczas podjętym wysiłkom, podejmując próbę ich oceny. Wniosek nasuwa się jeden: młodzi ludzie muszą być świadomi swojej prywatności nie tylko by być bezpiecznymi, ale przede wszystkim by mogli dorastać jako wolne osoby.

1. DLACZEGO NAUCZANIE O PRYWATNOŚCI?

1.1. PROBLEMY PRYWATNOŚCI SĄ PRAWDZIWE A ICH KONSEKWENCJE CZĘSTO POWAŻNE

Problemy prywatności są prawdziwe. Dla niektórych, np. nas naukowców zajmujących się nimi na co dzień, stwierdzenie to jest raczej bezsporne. Dla innych z kolei, zwykle zajętych innymi sprawami, istota i pilność problemów prywatności mogą nie być już tak oczywiste.

Zacznijmy od najbanalniejszego przykładu. Niewielu z nas czułoby się dobrze gdyby ich nazwiska, adresy zamieszkania i wykonywane zawody opublikowano na stronie internetowej parafii bez ich uprzedniej zgody. Podobnie niewielu z nas znalazłoby z zadowoleniem na takiej stronie szczegóły na temat swojego stanu zdrowia, nawet jeśli chodziłoby o małe przypadłości. Nie chodzi tu tylko o sam

* Vrije Universiteit Brussel (VUB), Grupa Badawcza ds. Prawa, Nauki, Technologii i Społeczeństwa (LSTS).

fakt publicznego udostępniania informacji, ale raczej o możliwość wydedukowania z nich innych aspektów życia, np. przynależności do związków wyznaniowych. Taką właśnie sprawą zajął się Trybunał Sprawiedliwości Unii Europejskiej już w 2003 r. Kwestia dotyczyła Szwedki, pani Bodil Lindqvist, oraz prowadzonej przez nią strony internetowej. Trybunał rozważał czy fakt umieszczenia przez nią, na parafialnej stronie internetowej, danych osobowych innych osób bez ich zgody stanowił naruszenie szwedzkiego prawa ochrony tych danych. Trybunał orzekł, że tak.[1]

Takie przykłady możemy podawać w nieskończoność. Kolejny: internetowe gry RPG (ang. *role-playing games*) cieszą się dużą popularnością na całym świecie. W wiele z nich można zagrać jedynie po rejestracji, wymagającej podania niektórych danych osobowych, i opłaceniu abonamentu. W 2011 r. należąca do Sony Corporation sieć Play Station Network padła ofiarą ataku hakerskiego. Dane osobowe około 77 milionów klientów zostały wykradzione i udostępnione publicznie. Dane te obejmowały nie tylko nazwiska i adresy mailowe, ale także loginy i hasła, daty urodzenia oraz numery kart kredytowych. Jeśli wyciekłyby tylko adresy mailowe, większość z nas prawdopodobnie zniosłaby kilka niezamawianych wiadomości (ang. *spam*) więcej tygodniowo. Jednakże ujawnienie informacji takich jak hasła i numery kart kredytowych powoduje poważniejsze problemy, tym bardziej że całkiem sporo osób używa jednego i tego samego hasła do zdecydowanej większości swojej aktywności internetowej. Sony Corporation niezwłocznie zwróciła się do swoich klientów o sprawdzenie historii własnej karty kredytowej.[2] Przykład ten nie jest odosobniony – naruszenia ochrony danych zdarzają się na całym świecie codziennie.[3]

Naruszenia ochrony danych, takie jak to w powyższym przykładzie, oraz – ogólnie ujmując – liczne problemy wynikające z przetwarzania danych, które rzutują na naszą prywatność, stawiają szereg pytań na temat naszych obowiązków i naszej odpowiedzialności za własną prywatność. Czasami mamy możliwość decydowania samodzielnie jakimi informacjami się podzielić, np. czy umieścić jakieś informacje o innych online czy nie. Czasami mamy jednak

[1] Sprawa C-101/01, *Bodil Lindqvist* [2003] ECR I-12971.

[2] PlayStation.Blog, *Update on PlayStation Network and Qriocity*, 26 kwietnia 2011 <http://blog.us.playstation.com/2011/04/26/update-on-playstation-network-and-qriocity> dostęp 25.05.2016.

[3] Interesującą wizualizację można znaleźć na: <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks> dostęp 20.05.2016.

niewielki wybór w tej kwestii, np. jeśli musimy zaakceptować konkretne warunki przetwarzania danych aby móc zagrać w grę, którą dopiero co kupiliśmy (albo dostaliśmy od rodziców czy krewnych). Niemniej, nie zawsze do końca jesteśmy świadomi konsekwencji swoich decyzji lub ryzyka związanego z podaniem określonych danych.

Wszystkie te kwestie można by określić jako dotyczące „prywatności", pojmowanej jako pojęcie obejmujące również ochronę danych osobowych. Często jednak pokrywają się one z kwestiami poufności i bezpieczeństwa. Podczas gdy perspektywa „prywatności" jest tylko jedną wielu, nie zmienia to faktu, że naruszenia prywatności mogą prowadzić do poważnych konsekwencji. Naruszenia prywatności są wystarczająco zgubne dla dorosłych. Z reguły, jako osoby dorosłe, chcemy niektóre informacje zachować tylko dla siebie i dla osób najbardziej nam zaufanych. Będziemy się jednak czuli niekomfortowo, gdy ktoś inny, w sposób przez nas niezamierzony, pozna nasze sekrety. Sprawy przyjmują gorszy obrót gdy nasze sekrety zostaną wykorzystane przeciwko nam. Próby poradzenia sobie ze spamem to błahostka w porównaniu z np. kradzieżą pieniędzy czy tożsamości, wirtualnym nękaniem (ang. *cyberbullying*) czy molestowaniem seksualnym. Ale sytuacja staje się dużo gorsza, gdy dziecko – osoba, która nie osiągnęła jeszcze dojrzałości i jest tym samym szczególnie podatna na niebezpieczeństwo – pada ofiarą takich nadużyć i przestępstw w taki czy inny sposób.

1.2. PRAWO O PRYWATNOŚCI UPODMIOTAWIA I GWARANTUJE UNIWERSALNĄ OCHRONĘ

Jeden ze sposobów ochrony prywatności to ostrożne obchodzenie się z własnymi danymi osobowymi. W tym sensie znaczna część ochrony zależy od nas samych. Jednak oprócz naszej należytej staranności istnieją także wymogi prawne nałożone na tych, którzy przetwarzają nasze dane osobowe. Wymogi te mają za zadanie chronić nas przed nadużywaniem naszych danych, potwierdzając tym samym, że nie wystarczy sama tylko nasza świadomość ryzyka i nasza odpowiedzialność za nie.

Korzenie tych wymogów sięgają roku 1890. W odpowiedzi na popularyzację fotografii i jej wzrastającą powszechność w prasie, co postrzegane było jako zbyt natarczywe, w Stanach Zjednoczonych narodziła się idea prywatności jako „prawa do bycia pozostawionym w spokoju", stanowiąca odbicie zmian

prawnych w Europie.[4] Współczesna ochrona prawna prywatności jest uniwersalna, tzn. obejmuje wszystkich, i ma swoje źródła w międzynarodowej ochronie praw człowieka, np. Europejskiej Konwencji Praw Człowieka (1950)[5] oraz Karcie Praw Podstawowych Unii Europejskiej (2000).[6] Równocześnie ochrona prywatności stopniowo zwiększała swoją obecność w porządkach prawnych państw członkowskich Unii Europejskiej. Europejskie prawo ochrony danych wyznacza warunki legalnego przetwarzania takich danych, przyznaje nam liczne prawa podmiotowe oraz ustanawia niezależne organy monitorujące przestrzeganie tego prawa.

Bardzo formalny ton zapisów prawa o prywatności często wymaga wysiłku z naszej strony. Prawdą jest, że zapisy tego prawa często utrzymane są w tonie niejako paternalistycznym i bardzo mocno preskryptywnym, ale celem jest ochrona naszej wolności, a same przepisy pozostawiają nam duże pole do manewru, przynajmniej co do zasady. Dbałość o naszą prywatność powraca w nasze ręce w postaci uprawnienia. Za każdym razem, gdy podejmujemy tego rodzaju wybór, ponosimy także jego konsekwencje; wyjaśnia to sens prawa podmiotowego do jasnych i zrozumiałych informacji na temat przetwarzania naszych danych osobowych. Np. często musimy wyrazić zgodę na rejestrację w serwisie internetowym i w ten sposób zgadzamy się także na konkretne sposoby przetwarzania naszych danych. Raz udzielona zgoda może na ogół być cofnięta w późniejszym czasie. Taki wybór jest, przynajmniej teoretycznie, bardzo potężnym narzędziem w naszych rękach.

1.3. PRAWO O PRYWATNOŚCI UZNAJE POTRZEBĘ SPECJALNEJ OCHRONY DZIECI

Współczesne dzieci, z racji swojej łatwej przyswajalności nowinek technologicznych (ang. *breezy familiarity*),[7] często są nazywane „cyfrowymi tubylcami" (ang. *digital natives*).[8] Używają one informacji inaczej niż ich starsi

[4] S. WARREN i L. BRANDEIS, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 5, 193. Por. także: G. GONZÁLEZ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer, Dordrecht 2014.

[5] Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności [1950] ETS 5; <http://www.echr.coe.int/Documents/Convention_POL.pdf> dostęp 20.05.2016.

[6] Karta Praw Podstawowych Unii Europejskiej [2000] Dz.U. C 361/1.

[7] Sprawa *American Libraries Association v. Pataki* [1997] 969 F. Supp. 160.

[8] M. PRENSKY, 'Digital Natives, Digital Immigrants' (2001) 9 *On the Horizon* 5, 1.

koledzy i koleżanki.[9] Coraz częściej korzystają z i tak już popularnych w swojej grupie wiekowej technologii. Już w 2011 r. ponad 75% dzieci w Europie używało Internetu z przeróżnych powodów: od komunikowania się z rówieśnikami (zwłaszcza za pomocą portali społecznościowych) przez odbieranie treści (np. słuchanie muzyki) aż po granie w gry. Niektórzy tworzą także własne treści w internecie, np. pisząc swojego bloga.[10] Wraz z upływem czasu, dzieci przebywają online coraz dłużej, poznają internet w coraz młodszym wieku i korzystają z niego w coraz bardziej różnorodne sposoby.[11] Nic dziwnego zatem, że to właśnie dzieci coraz częściej stają się celem rynkowym innowacyjnych praktyk przetwarzania danych. Udostępnione *selfie* z własnym świadectwem szkolnym jest już czymś powszechnym, a każdy dzień przynosi coś nowego: aplikacje na smartfony do pomiaru spożycia mleka czy *smart watch*, czyli inteligentne zegarki pozwalające mamie i tacie zawsze wiedzieć, gdzie znajdują się ich pociechy.[12] Nie oznacza to jednak, że dzieci są bardziej od dorosłych świadome tego, co dzieje się z ich danymi osobowymi, kiedy zostają one udostępnione innym. Niekoniecznie są też one świadome ryzyka związanego z takim przetwarzaniem oraz potencjalnego wpływu tego typu działań na ich życie, tak teraz, jak i w przyszłości.

Prawo o prywatności zapewnia uniwersalną ochronę. Logicznie rzecz biorąc, ochrona ta rozciąga się także na dzieci i młodzież. Dzieci jednakże to osoby bardzo podatne na zagrożenia. Nie zawsze wiedzą, jak chronić się przed niebezpieczeństwami wynikającymi z dzielenia się własnymi danymi osobowymi za pomocą nowych technologii. Kiedy dane dotyczące dzieci są przetwarzane, nie tylko zwiększa się istniejące ryzyko wyrządzenia tym dzieciom szkody, ale także te same dzieci narażane są na nowe jego rodzaje. Dlatego też dzieci wymagają specjalnej ochrony. Dopiero niedawno prawo Unii Europejskiej zaczęło otwarcie uwzględniać taką potrzebę. Niedawno zakończona (kwiecień 2016) reforma ochrony prawnej danych osobowych wyraźnie uznaje konieczność zapewnienia specjalnego poziomu takiej ochrony dla grup wrażliwych, między innymi dzieci. Preambuła do ogólnego rozporządzenia o ochronie danych podkreśla, że

[9] Ibid.

[10] S. LIVINGSTONE et al., *Risks and Safety on the Internet: The Perspective of European Children,* London Schools of Economics and Political Science, Londyn 2011, str. 33.

[11] S. LIVINGSTONE (red.), *EU Kids Online. Findings, Methods, Recommendations*, London Schools of Economics and Political Science, Londyn, 2015, str. 6.

[12] Ponadto na ten temat: G. GONZÁLEZ FUSTER, 'GDPR: we all need to work at it!', *Better Internet for Kids (BIK) Bulletin*, 31 marca 2016, <https://www.betterinternetforkids.eu/web/portal/news/detail?articleId=694148> dostęp 20.05.2016.

> [...] szczególnej ochrony danych osobowych wymagają dzieci, gdyż mogą one być mniej świadome ryzyka, konsekwencji, zabezpieczeń i praw przysługujących im w związku z przetwarzaniem danych osobowych. Taka szczególna ochrona powinna mieć zastosowanie przede wszystkim do wykorzystywania danych osobowych dzieci do celów marketingowych lub do tworzenia profili osobowych lub profili użytkownika oraz do zbierania danych osobowych dotyczących dzieci, gdy korzystają one z usług skierowanych bezpośrednio do nich.. […].[13]

1.4. NIEKTÓRYCH PROBLEMÓW PRYWATNOŚCI MOŻNA UNIKNĄĆ BĘDĄC ŚWIADOMYM ZAGROŻEŃ

Stare porzekadło mówi, że „lepiej zapobiegać niż leczyć". W niektórych przypadkach podjęcie środków zapobiegawczych leży wyłącznie w gestii tych, którzy przetwarzają nasze dane osobowe. Sami nie możemy zbyt wiele zrobić, jeśli np. dostawca usług internetowych pada ofiarą ataku hakerskiego. Odpowiedzialnością takich usługodawców jest zapewnienie odpowiedniego bezpieczeństwa swoich produktów i usług.

Są jednak sytuacje, w których podjęcie racjonalnych działań w celu zapobieżenia takiemu ryzyku i niebezpieczeństwom – lub przynajmniej ograniczenie prawdopodobieństwa ich wystąpienia – leży także w zasięgu naszych możliwości. Najprostszym sposobem jest chwila zastanowienia przed udostępnieniem danych osobowych lub wyrażeniem zgody na konkretne ich przetwarzanie.

Warunkiem powodzenia takiego podejścia w praktyce jest świadomość zagrożeń związanych z przetwarzaniem danych osobowych oraz sposobów ochrony przed nimi. Badania pokazują, że choć znacząca większość Europejczyków postrzega „udostępnianie danych osobowych jako coraz bardziej istotny element nowoczesnego życia", to jednak nie są oni wystarczająco świadomi sposobów ochrony własnych danych osobowych.[14] Jednostki są zazwyczaj przedstawiane jako „niedoinformowane i zdezorientowane", a co za tym idzie „często

[13] Motyw 38, Rozporządzenie (UE) 2016/679 Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych oraz uchylające dyrektywę 95/46 / WE (ogólne rozporządzenie o ochronie danych) [2016] Dz. U. L 119/1.

[14] Komisja Europejska, *Specjalna ankieta Eurobarometeru nr 359: Stosunek do ochrony danych i tożsamości elektronicznej w Unii Europejskiej*, Bruksela 2011, str. 5, <http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf> dostęp 20.05.2016.

niewłaściwie interpretujące własne zachowania".[15] Wspomnieliśmy już, że obowiązujące prawo daje nam możliwość podejmowania decyzji, a nasza zgoda jest potężnym narzędziem w naszych rękach. Ale powszechnym zjawiskiem jest klikanie „zgadzam się" bez nawet chwili zastanowienia się nad potencjalnymi konsekwencjami udzielenia zgody na przetwarzanie naszych danych. Co więcej, dane statystyczne pokazują, że Europejczycy nie mają wiedzy na temat potencjalnych środków zaradczych na wypadek gdyby coś poszło nie tak.[16] Nie są oni świadomi istnienia krajowych organów ochrony danych, które mogą zapewnić im pomoc w takiej sytuacji.[17] A nawet wśród tych, którzy są tego świadomi, z reguły brak jest dokładnego i wystarczającego zrozumienia zagrożenia.[18] Mówiąc prościej: zagrożenia te nie przemawiają do ich wyobraźni – „coś takiego nigdy by się mi nie przydarzyło, zbyt mało prawdopodobne" lub „będę się nad tym zastanawiać, jak się już wydarzy". Czasem jest po prostu za późno. Naruszenia prywatności niosą ze sobą ryzyko nieodwracalności ujawnienia informacji i są przez to z reguły nie do naprawienia.

Wyraźnie zatem widać, że świadomość jednostki i ochrona jej własnej prywatności nie zawsze idą w parze. Oczekuje się, że jednostki będą wystarczająco poinformowane i świadome zagrożeń, aby dokonywać właściwych wyborów. Jednakże powszechnie wiadomo, że – statystycznie rzecz ujmując – w większości przypadków tak nie jest. Ten paradoks jest jeszcze lepiej widoczny w przypadku dzieci – z definicji nie są one w stanie podejmować świadomych i odpowiedzialnych decyzji w takim stopniu, jak osoby dorosłe. Moglibyśmy niemniej zaryzykować tezę, że – aby sprawy miały się dobrze – dzieci powinny taką świadomość i odpowiedzialność mieć. Dlatego też coraz częściej nalega się, żeby dzieci – jeśli chodzi o ich prywatność – przestały zachowywać się jak dzieci.

1.5. UPODMIOTOWIENIE NAJBARDZIEJ PODATNYCH NA NIEBEZPIECZEŃSTWA

Nauczanie o prywatności skierowane do dzieci i młodzieży musi zatem wyjść ponad takie podejście poprzez zintegrowanie szerszej perspektywy. Ważne jest, aby powtarzać dzieciom, żeby zawsze pomyślały dwa razy o tym, co robią ze

[15] G. GONZÁLEZ FUSTER, 'How Uninformed Is the Average Data Subject? A Quest for Benchmarks in EU Personal Data Protection' (2014) 19 *IDP. Revista de Internet, Derecho Y Política*, 99.
[16] Agencja Praw Podstawowych Unii Europejskiej, *Access to Data Protection Remedies in EU Member States*, Urząd Publikacji Unii Europejskiej, Luksemburg 2014, str. 32–34.
[17] Komisja Europejska, *Specjalna ankieta Eurobarometru nr 359*, op. cit., str. 174.
[18] J.B. RULE, *The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies*, Elsevier, Nowy Jork 1980, str. 184.

swoimi danymi osobowymi. Równie ważne jest także, aby dzieci wiedziały, że ich dane osobowe zasługują na poszanowanie przez innych. Podejmowanie właściwych decyzji dotyczących ujawniania własnych danych osobowych jest kluczowym elementem ochrony prywatności, ale nie jedynym. Nauczanie takie nie tylko przyczynia się do zwiększenia bezpieczeństwa dzieci, ale także upodmiotowuje je (ang. *empowerment*) i wzmacnia ich pozycję w obrocie prawnym; te dwa cele idą ramię w ramię.

Upodmiotowiona jednostka będzie skuteczniej bronić się przed problemami prywatności. Upodmiotowienie oznacza świadomość niebezpieczeństw, ale także obowiązującego prawa oraz sposobów zaradzania problemom. A jeśli dzieci są upodmiotowione, to znaczy, że są świadome nie tylko problemów prywatności i ryzyka związanego z byciem online, ale także tego, do czego są uprawnione oraz kto jest do czego zobowiązany. Wówczas – koniec końców – powinny być bezpieczniejsze.

Dlatego też za wzorcowy uznaliśmy fakt, że zreformowane prawo o ochronie danych osobowych w Unii Europejskiej nie tylko wyraźnie podkreśla potrzebę specjalnej ochrony dzieci, ale także w dorozumiany sposób uznaje wartość podwyższania ich wiedzy o problemach prywatności. To samo prawo nakłada obowiązek zapewnienia tejże ochrony na niektóre organy publiczne, zwracając szczególną uwagę na dzieci. Organy te, zwyczajowo zwane „organami ochrony danych", są kluczowym komponentem prawa podstawowego do ochrony danych osobowych. Przepisy prawa powierzają tym organom wiele różnych ról.

W ujęciu historycznym, organy ochrony danych od początku swojego istnienia, czyli od lat 70-tych XX w., zajmowały się nie tylko „nadzorowaniem" czy prawo o ochronie danych jest przestrzegane, ale także odgrywały wiele innych ról: od rzeczników praw, audytorów, konsultantów aż po doradców politycznych.[19] Wszystkie te działania mają wspólny cel, jakim jest wyższy poziom ochrony, a jednym z zadań jest edukacja ogółu społeczeństwa.

Z upływem czasu prawo zaczynało odzwierciedlać poszerzenie misji tych organów. Nowo przyjęte ogólne rozporządzenie o ochronie danych, które

[19] C.J. BENNETT i C.D. RAAB, *The Politics of Privacy: Policy Instruments in Global Perspective*, MIT Press, Cambridge 2006. Por. także np. Komisja Europejska, *Evaluation of the Means used by National Data Protection Supervisory Authorities in the promotion of personal Data Protection. Final Report*, Bruksela 2009.

wejdzie w życie w maju 2018 r., wyraźnie nakłada ten obowiązek na te organy ochrony danych. Artykuł 57 unijnego rozporządzenia wylicza ich obowiązki i stwierdza m.in. że:

> organ nadzorczy na swoim terytorium [...] upowszechnia w społeczeństwie wiedzę o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem oraz rozumienie tych zjawisk. Szczególną uwagę poświęca działaniom skierowanym do dzieci.

Ogólne rozporządzenie o ochronie danych wyraźnie uznaje zatem, że dzieci muszą być świadome ryzyka związanego z przetwarzaniem danych osobowych, ale także obowiązujących zasad, mechanizmów ochrony i praw. Świadomość ryzyka powinna być dla nich pomocna do skutecznego korzystania ze swoich praw.

Warto także wspomnieć, że podnoszenie świadomości w zakresie prywatności wśród dzieci jest sprawą wykraczającą poza granice Europy. Np. Stany Zjednoczone były prekursorem w regulowaniu ochrony prywatności online. W 1998 r. przyjęto tam ustawę o ochronie prywatności dzieci w systemie online,[20] mającą zastosowanie do stron internetowych gromadzących informacje nt. dzieci poniżej 13. roku życia. Federalna Komisja Handlu USA, współodpowiedzialna za jej egzekwowanie, prowadzi szereg stron internetowych skupiających się na zwiększaniu świadomości wśród dzieci.

2. KRAJOBRAZ KSZTAŁCENIA O PRYWATNOŚCI W EUROPIE

W projekcie ARCADES przyjrzeliśmy się m.in. działaniom dotychczas podjętym w celu nauczania dzieci o prywatności w szkołach w Europie, uwzględniając przede wszystkim ich różnorodność.[21] Sednem projektu było przeanalizowanie dostępnych materiałów edukacyjnych.

2.1. KTO?

Tych, którzy przygotowują poradniki lub konkretne materiały do nauczania o prywatności w szkołach można podzielić na kilka ogólnych kategorii i przyjrzeć

[20] Ustawa o ochronie prywatności dzieci w systemie online z 1998 r., 5 U.S.C. 6501–6505.

[21] G. GONZÁLEZ FUSTER, P. DE HERT i D. KLOZA, *State-of-the-Art Report on Teaching Privacy and Personal Data Protection at Schools in the European Union*, Vrije Universiteit Brussel, Bruksela 2015, <http://arcades-project.eu/images/pdf/State_of_the_art_report.pdf> dostęp 25.05.2016.

się im z różnych perspektyw. Organizacje międzynarodowe, takie jak Organizacja Narodów Zjednoczonych do spraw Oświaty, Nauki i Kultury (UNESCO),[22] zajmuje się prawami dzieci, a tym samym także ich prawem do prywatności. To samo dotyczy Rady Europy, która jest zainteresowana polityką nauczania o prywatności z perspektywy praw człowieka. Unia Europejska zajmuje się tym tak z perspektywy bezpieczeństwa online, jak i z punktu widzenia praw podstawowych.

Aktywne w tej dziedzinie są także krajowe organy ochrony danych, których kampanie edukacyjne obejmują inicjatywy wprost skierowane do dzieci (np. przez ich stronę internetową) lub rodziców czy nauczycieli. Czasami nawet biorą one bezpośredni udział w procesie nauczania. Istotną rolę odgrywają także organizacje pozarządowe, czy to przez aktywny udział, czy przez przygotowanie pomocy naukowych.

Decyzja co do uwzględnienia problemów prywatności w szkolnych programach nauczania pozostaje w gestii właściwych organów państwowych, ale nie wszystkie państwa członkowskie Unii Europejskiej podjęły kroki w tym kierunku. Bezsporny pozostaje jednak fakt, że wszystkie wyżej wymienione podmioty generalnie współpracują ze sobą w kwestii nauczania o prywatności.

Dzieci są zazwyczaj typowym adresatem nauczania o prywatności w szkołach. Zdarzają się jednak inicjatywy adresowane w pierwszej kolejności do nauczycieli. Okazjonalnie inicjatywy te obejmują również rodziców w przekonaniu, że są oni kluczowym komponentem ochrony prywatności dziecka, i że najlepiej dotrzeć jest do nich przez szkołę.

2.2. GDZIE I KIEDY?

Nauczanie o prywatności może mieć miejsce na każdym poziomie kształcenia. Mimo że w niektórych państwach członkowskich Unii Europejskiej elementy nauczania o prywatności pojawiają się już w przedszkolach, z reguły są obecne w szkołach, od podstawowych przez gimnazja aż po szkoły średnie.

[22] Ponadto w tym temacie: P. HLADSCHIK i D. STEURER, 'Human Rights Education – Know Your Rights!' w: M. NOWAK, K.M. JANUSZEWSKI i T. HOFSTÄTTER (red.) *All Human Rights for All: Vienna Manual on Human Rights*, Intersentia, Wiedeń/Graz 2012, str. 606-612.

Szkoła jednak nie jest jedynym miejscem, w którym podejmuje się próby zwiększenia wśród dzieci świadomości nt. prywatności. Do dzieci, rodziców i nauczycieli można także docierać przez media, czy to tradycyjne (np. telewizję lub prasę) czy tzw. nowe media (np. strony internetowe), jak i przestrzeń publiczną (np. biblioteki czy targi edukacyjne) oraz wydarzenia masowe (np. Dzień Bezpiecznego Internetu).

2.3. JAK?

W państwach członkowskich Unii Europejskiej, w których nauczanie o prywatności zawarte jest w programie nauczania, jest ono realizowane na kilka sposobów. Np. mieści się w zakresie ogólnego nauczania o prawach podstawowych lub w zakresie edukacji informatycznej, która z kolei obejmuje bezpieczne korzystanie z technologii informacyjnych i komunikacyjnych. Dzieci uczą się tego pierwszego przeważnie w ramach zajęć z „wiedzy o społeczeństwie", natomiast tego drugiego – w ramach „informatyki" lub „edukacji medialnej", ale nazwy te mogą różnić się pomiędzy poszczególnymi krajami.

Nauczanie o prywatności wspierane przez organy ochrony danych jest elementem szerzej zakrojonych zadań dotyczących podnoszenia świadomości społecznej. Taka aktywność może być bezpośrednio lub pośrednio skierowana do dzieci. W tym drugim przypadku skierowana jest do rodziców i nauczycieli, specjalistów w zakresie edukacji oraz dyrektorów szkół, którzy następnie przekażą wiedzę dzieciom.

Angażując się bezpośrednio, organy ochrony danych zwykle oferują zasoby online (w tym dedykowane strony internetowe), prowadzą dedykowane kampanie informacyjne czy organizują konkursy. Zazwyczaj intensyfikują one swoje działania podczas specjalnych wydarzeń, jak np. Europejski Dzień Ochrony Danych (28 stycznia). Niekiedy biorą udział w dniach otwartych w szkołach czy bibliotekach oraz w targach edukacyjnych.

Angażując się pośrednio, organy takie udają się do szkół na wizyty studyjne lub szkolenia, wykłady, seminaria i warsztaty. Czasami są to działania jednorazowe, czasami stanowią część większej serii; uczestnictwo w nich jest zazwyczaj bezpłatne. Wiele organów ochrony danych wydaje materiały edukacyjne dla dzieci, tak w wersji elektronicznej, jak i drukowanej, w formie dedykowanych stron internetowych oraz plakatów, pocztówek, książeczek, broszur, ulotek, komiksów, filmów, testów, quizów, a niekiedy nawet wytycznych i scenariuszy lekcji. Zasoby te są z reguły dostępne nieodpłatnie.

Organy ochrony danych współpracują ze sobą tak na poziomie europejskim, jak i krajowym. Grupa Robocza Artykułu 29, organ doradczy złożony z organów ochrony danych z państw członkowskich Unii Europejskiej, w 2009 r. wydała wpływową opinię na temat ochrony danych osobowych dzieci.[23] Trzydziesta-piąta Międzynarodowa Konferencja Rzeczników Ochrony Danych i Prywatności (Warszawa, 2013) przyjęła *Rezolucję w sprawie edukacji cyfrowej dla wszystkich*,[24] która stała się bodźcem do rozpoczęcia prac Międzynarodowej Grupy Roboczej ds. Ochrony Danych i Edukacji Cyfrowej. Równocześnie organy ochrony danych z całego świata dzielą się nawzajem swoim doświadczeniem poprzez wizyty studyjne czy wymianę kadr.

Kooperacja organów ochrony danych nie ogranicza się wyłącznie do szkół – współpracują one również lokalnie, np. z radami miejskimi czy bibliotekami. Niektóre, jak np. francuski organ ochrony danych, stworzyły „EducNum" – kooperatywę na rzecz edukacji cyfrowej, łączącą ponad 60 partnerów z obszaru edukacji, badań naukowych, gospodarki cyfrowej, społeczeństwa obywatelskiego i instytucji politycznych.[25] Działania tych organów skierowane są także do decydentów, zwykle z zamiarem kształtowania programów nauczania lub innego rodzaju wpływu na politykę nauczania o prywatności. Nierzadko ich wkład opiera się o badania zlecone nt. szeroko rozumianego *status quo*, np. postrzeganie zagrożeń bezpieczeństwa wśród dzieci.

Organizacje międzynarodowe lub ponadnarodowe wyznaczają kierunki rozwoju i standardy nauczania o prywatności, ale także bezpośrednio angażują się w działania edukacyjne. Np. Rada Europy uczciła 50. rocznicę Europejskiej Konwencji Praw Człowieka premierą „COMPASSu", tj. cyfrowego narzędzia wspomagającego upowszechnianie wiedzy o prawach człowieka, umiejętności i postaw z nimi związanych. Jednym z tematów poruszonych w ramach tego

[23] Grupa Robocza Artykułu 29 ds. Ochrony Danych, *Opinia 2/2009 w sprawie ochrony danych osobowych dzieci (Ogólne wytyczne i szczególny przypadek szkół)*, WP 160, Bruksela, 11 lutego 2009 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp160_pl.pdf > dostęp 25.05.2016. Opinia ta została poprzedzona przez: Idem, *Dokument Roboczy 1/2008 w sprawie ochrony danych osobowych dzieci (Ogólne wytyczne i szczególny przypadek szkół)*, WP 147, Bruksela, 18 lutego 2008 <http://www.giodo.gov.pl/plik/id_p/1300/j/pl/ > dostęp 25.05.2016.

[24] Międzynarodowa Konferencja Rzeczników Ochrony Danych i Prywatności, *Rezolucja w sprawie edukacji cyfrowej dla wszystkich* (2013) <https://icdppc.org/wp-content/uploads/2015/02/Digital-education-resolution-PL.pdf > dostęp 20.05.2016.

[25] <http://www.educnum.fr> dostęp 18.05.2016.

projektu były prawa dzieci.[26] W 2007 r. po raz pierwszy ukazał się Podręcznik „Internet Literacy Handbook",[27] obecnie w trzecim wydaniu, a w 2012 r. Rada Europy współtworzyła Strategię na rzecz Praw Dziecka (2012-2015).[28]

Wysiłki Unii Europejskiej odnośnie nauczania o prywatności uzyskały wsparcie w postaci wartego 50 milionów euro programu „Bezpieczny Internet" w 1999 r. Po przyjęciu w 2012 r. europejskiej Strategii na rzecz lepszego internetu dla dzieci,[29] program ten funkcjonuje pod nazwą „Lepszy internet dla dzieci". Oparta na czterech filarach, w kontekście „Zwiększania świadomości i umacniania praw", Strategia podkreśla, że

> dzieci, ich rodzice, opiekunowie i nauczyciele powinni być świadomi zagrożeń, na jakie dzieci mogą być narażone w środowisku *online*, a także tego, z pomocą jakich narzędzi i strategii można uzyskać ochronę lub radzić sobie z takimi zagrożeniami.[30]

Strategia podkreśla także, że umiejętności cyfrowe i medialne są kluczowe w kontekście korzystania przez dzieci z internetu, oraz że „niezbędne jest rozpoczęcie edukacji w zakresie bezpieczeństwa w internecie w bardzo wczesnym dzieciństwie".[31] Zauważając, że bezpieczeństwo w internecie jako osobny obszar tematyczny został uwzględnione w programach szkolnych w ponad 20 systemach kształcenia w całej Europie, Strategia podaje, że

> miejscem, w którym można dotrzeć do większości dzieci, niezależnie od ich wieku, dochodów w rodzinie lub otoczenia, jak również do innych kluczowych odbiorców wiadomości dotyczących bezpieczeństwa w internecie, takich jak nauczyciele i (pośrednio) rodzice, są szkoły.[32]

Strategia zachęca państwa członkowskie Unii Europejskiej by zwiększyły wysiłki i włączyły tematyki bezpieczeństwa online do szkolnych programów nauczania do

[26] <http://www.eycb.coe.int/compass> dostęp 18.05.2016.
[27] Rada Europy, *Internet Literacy Handbook*, ed. 3, Strasbourg 2007, <http://www.coe.int/t/dghl/StandardSetting/InternetLiteracy/InternetLiteracyHandbook_3_EN.asp> dostęp 26.05.2016.
[28] Rada Europy, *Strategia na rzecz praw dziecka (2012-2015)*, CM(2011)171 wersja końcowa, Strasbourg, 15 lutego 2012, <http://www.coe.int/t/DGHL/STANDARDSETTING/CDcj/StrategyCME.pdf> dostęp 26.05.206.
[29] Komisja Europejska, *Europejska strategia na rzecz lepszego internetu dla dzieci*, COM(2012) 196 wersja końcowa, Bruksela, 02.05.2012.
[30] Ibid., str. 8.
[31] Ibid.
[32] Ibid.

2013 r., do wzmocnienia edukacji nieformalnej oraz do zapewnienia polityk „bezpieczeństwa online" w szkołach, jak również odpowiedniego przeszkolenia nauczycieli, także w partnerstwie publiczno-prywatnym. Z kolei biznes zaproszono do współpracy w zakresie rozwijania interaktywnych narzędzi i platform z materiałami edukacyjnymi i informacyjnymi dla nauczycieli i dzieci w oparciu o istniejące inicjatywy. Komisja Europejska natomiast zaangażowała się we wsparcie identyfikacji, wymiany i promowania najlepszych praktyk pośród państw członkowskich w obszarze edukacji formalnej i nieformalnej w zakresie bezpieczeństwa online. Takie kształcenie o „prywatności" przez pryzmat internetu skupia się przeważnie na popularyzowaniu wiedzy o zagrożeniach czyhających na dzieci w internecie, a nie kładzie nacisku na znajomość należnych im podstawowych praw i świadomość ich wielowymiarowości.

2.4. CO?

Wspólną cechą dostępnych obecnie materiałów jest fakt, że nie mają one na celu *wyłącznie* przekazywać dzieciom wiedzy, ale także zmierzać ku nauce i refleksji. Podstawowym zadaniem jest promocja przemyślanego i odpowiedzialnego korzystania z nowych technologii komunikacyjnych i informacyjnych, głównie z internetu. Materiały te nie skupiają się wyłącznie na problemach ochrony prywatności, jako że nauczanie o nich zwykle zazębia się z nauczaniem o bezpieczeństwie online, prowadząc tym samym do popularyzowania swoistej „cyfrowej odpowiedzialności".

Materiały te zwykle omawiają:

- definicję pojęcia „prywatność"; niektóre zgłębiają także „życie pod nadzorem" (ang. *surveillance*),
- poziom istotności tych pojęć we współczesnym społeczeństwie,
- sugestie w zakresie podejmowania decyzji o tym, czy w ogóle udostępniać dane osobowe czy nie,
- w sytuacjach, w których dane osobowe są udostępniane:
  - sugestie dotyczące bezpieczeństwa online, np. wybór bezpiecznego hasła lub ustawień prywatności w mediach społecznościowych, itd.,
  - jak udzielać ważnej zgody na udostępnianie danych (jeśli jest to możliwe w przypadku dzieci) i jak ją cofnąć,
  - uzmysłowienie, że gdy informacja zostaje udostępniona online, zazwyczaj trudno jest ją usunąć (np. „internet nigdy nie zapomina"),

  - dostępną pomoc i potencjalne środki zaradcze, np. prawo do zwrócenia się o pomoc do organu ochrony danych;
- rolę rodziców w ochronie danych osobowych ich dzieci.

Główne cele takich wysiłków edukacyjnych nie są jednak zawsze jasne. W wielu przypadkach nacisk wyraźnie kładziony jest na sposoby zwiększania ochrony prywatności dzieci oraz na zapoznawanie ich z prawami podstawowymi. W innych przypadkach, kwestie bezpieczeństwa online podyktowały nacisk na sposoby zapobiegania ryzyku w sieci, tym samym na trzymanie dzieci z dala od zagrożeń, w odróżnieniu od wyjaśnienia im, że mają one pewne prawa podmiotowe i że mogą domagać się przestrzegania pewnych zobowiązań dotyczących przetwarzania ich danych.

Na zakończenie, poniższy diagram ma zilustrować krajobraz nauczania o prywatności w Europie: kto kogo edukuje, gdzie, w jaki sposób, przekazując im jaki rodzaj wiedzy.

Tabela 1 – Krajobraz nauczania o prywatności

Kto?	Kogo?	Gdzie?	Jak?	Co?
– decydenci ▪ rządy krajowe ▪ organizacje ponadnarodowe ▪ organizacje międzynarodowe – podmioty ustanawiające standardy – organy ochrony danych – organizacje pozarządowe – biznes	– dzieci – rodzice – nauczyciele – opiekunowie	– przedszkola – szkoły ▪ podstawowe ▪ gimnazja ▪ średnie – media – przestrzeń publiczna – wydarzenia publiczne	– oficjalne programy nauczania – pośrednio ▪ zasoby dla nauczycieli ▪ zasoby dla rodziców – bezpośrednio ▪ zasoby dla dzieci	– definicje – poziom istotności – prawa – środki zaradcze – porady dot. bezpie–czeństwa

3. UWAGI KOŃCOWE

Zarówno sam fakt istnienia problemów prywatności, jak i poziom ich istotności, są często niedoceniane. Jest już wystarczająco źle, gdy sami padamy ich ofiarą, ale sprawy znacznie się pogarszają, gdy ich ofiarą staje się dziecko. Dzieci są wrażliwe i podatne na niebezpieczeństwo przede wszystkim z powodu swojej niewystarczającej świadomości zagrożeń w ogóle, a w szczególności tych

wynikających z korzystania z technologii, i dlatego też zasługują na specjalną ochronę. Jednocześnie są one także „cyfrowymi tubylcami", którzy bezproblemowo nawigują po świecie cyfrowym.

Ochrona prywatności zaczyna się od naszej własnej staranności. Następnie wkracza prawo, zapewniając nam wszystkim względnie wysoki poziom ochrony. Równocześnie prawo to pozostawia nam także spore pole do manewru, np. poprzez udzielanie zgody na przetwarzanie danych. Aby jednak z takich uprawnień skorzystać, musimy przede wszystkim wiedzieć, jakie są potencjalne zagrożenia i jak się przed nimi chronić. Dzieci, w równym stopniu jak ich rodzice i nauczyciele, mogą względnie skutecznie poradzić sobie z licznymi problemami prywatności, jeśli będą mieć wystarczającą wiedzę na ich temat. Nie wolno nam jednak wpaść w pułapkę myślenia, że prywatność dzieci będzie chroniona, jeśli poprzestaniemy na naleganiu, że zawsze powinny dwa razy zastanowić się, i jeśli założymy, że dzieci generalnie „znają się na rzeczy". Jeśli naprawdę znałyby się na rzeczy, prawdopodobnie już nie byłyby dziećmi.

Właśnie w tym miejscu wkracza szerokie podejście do nauczania o prywatności. Takie nauczanie nie obejmuje wyłącznie problemów prywatności lub ich znajomości. Stawia ono sobie za cel uświadomienie dzieciom zagrożeń, ale także ich praw i obowiązujących zasad. Przypomina nam ono o wymiarze prywatności jako prawa podstawowego oraz o tym, że młodzi ludzie potrzebują wiedzy o prywatności nie tylko dla bezpieczeństwa, ale przede wszystkim po to, by dorastać jako wolne osoby.

Nauczanie o prywatności jest obecne w szkołach w Europie już od jakiegoś czasu, a jego wartość jest powszechnie doceniana. Liczne wysiłki podejmowane przez wiele podmiotów na różnych poziomach zasługują na pochwałę, ale wciąż trzeba więcej. Przewidujemy tutaj specjalną rolę dla organów ochrony danych. Z racji ich roli w społeczeństwie, ale przede wszystkim z racji posiadanej wiedzy, mogą one odegrać kluczową rolę w stymulowaniu i doskonaleniu kształcenia w szkołach. Mogą one aktywnie dążyć w tym kierunku w imię swojej misji edukacji ogółu społeczeństwa. Mogą także skutecznie przyczynić się do jej jakości, zapewniając, że informacje, które są upowszechniane w szkołach, są w pełni zgodne z obowiązującymi przepisami prawa.

Naszym zdaniem godnym uwagi jest przepis ogólnego rozporządzenia o ochronie danych w Unii Europejskiej, na mocy którego organy ochrony danych są prawnie zobowiązane do szeroko rozumianego podnoszenia poziomu

świadomości o ochronie prywatności, a poprzez to są także zobowiązane do zwracania specjalnej uwagi na dzieci, adekwatnie do ich wrażliwości.

Dlatego też zdecydowanie nie możemy nie doceniać dzieci – nie powinniśmy jednakże zostawiać ich samych sobie podczas nawigacji w cyfrowym świecie, pełnym zakrętów i niebezpiecznych dróg. Ich „cyfrowa tubylczość" powinna być uzupełniana i równoważona „cyfrową odpowiedzialnością". Szkoły to jedno z najlepszych miejsc, tuż obok domu, ku temu, aby uczyć ich takiej odpowiedzialności, traktując je jak dzieci, ale jednocześnie jak pełnoprawne podmioty.

Rzecz jasna, nauczanie o prywatności nie jest lekarstwem na całe zło. Ochrona prywatności dzieci wymaga dużo więcej – w tym odpowiednio dostosowanej przejrzystości i surowych reguł dotyczących przetwarzania danych dzieci. Niemniej jednak jest to ważny element skomplikowanej układanki, jaką jest ochrona prywatności.

CZĘŚĆ II
PODRĘCZNIK NAUCZYCIELA

PODRĘCZNIK NAUCZYCIELA: WPROWADZENIE

Niniejszy podręcznik ma stanowić użyteczne narzędzie dla nauczycieli w każdej szkole w UE, którzy chcą nauczać dzieci i młodzież na temat ochrony danych osobowych i prywatności. Chcielibyśmy, aby mógł on być bezpośrednio stosowany w całej UE, dlatego też skupia się on na kluczowych informacjach, które dotyczą wszystkich państw członkowskich, i jest oparty o instrumenty prawne obowiązujące w całej Europie (przede wszystkim Kartę Praw Podstawowych UE). W celu uzyskania dodatkowych informacji prawnych, nauczyciele powinni kontaktować się z krajowymi organami ochrony danych.

Tekst jest napisany prostym i zrozumiałym językiem, który pomóc ma nauczycielom znaleźć właściwe słowa do tego, aby wyjaśniać ten temat swoim uczniom. Podręcznik podzielony jest na dziesięć rozdziałów obejmujących różne aspekty prywatności i ochrony danych osobowych, z których wszystkie mają specjalne znaczenie dla dzieci i nastolatków. Każdy rozdział wprowadza zbiór kluczowych pojęć i proponuje tematy do dyskusji, zalecane ćwiczenia lub konkretne porady, w zależności od tematu. Tam, gdzie to możliwe, w rozdziałach uwzględniono także „przypadki z życia wzięte" lub przykłady. Ponadto końcowa część każdego rozdziału uwypukla sprawy, które mogą być szczególnie ważne dla młodszych dzieci, oraz te, które mogłyby zainteresować uczniów starszych lub bardziej zaawansowanych. Zachęcamy nauczycieli do zapoznania się z całym podręcznikiem i swobodnego wykorzystywania różnych elementów poszczególnych rozdziałów zgodnie z potrzebami swoich klas.

Poniższej przedstawiono listę (w kolejności alfabetycznej) autorów, którzy przyłożyli się do powstania niniejszego tekstu: Viktor Árvay (NAIH), Jelena Burnik (IP RS), Paul De Hert (VUB), Piotr Drobek (GIODO), Gloria González Fuster (VUB), Urszula Góral (GIODO), Dariusz Kloza (VUB), Laura Kozma (NAIH), Paweł Makowski (GIODO), Marta Mikołajczyk (GIODO), Kata Nagy (NAIH), Anže Novak (IP RS), Zsófia Szántó (NAIH), Julia Sziklay (NAIH), Polona Tepina (IP RS) and Zsófia Tordai (NAIH).

1. WPROWADZENIE DO PRYWATNOŚCI

Czym jest prywatność? Dlaczego jest ona ważna?

CELE

- Nauka o prywatności.
- Ukształtowanie przemyślanego podejścia do prywatności.
- Zrozumienie wagi prywatności online i offline.

NAJWAŻNIEJSZE KWESTIE

Prywatność polega na ochronie tego, co **prywatne**, na zasłonięciu samego siebie i tego, co jest każdemu najbliższe, przed wzrokiem innych. Prywatność to także możliwość „**bycia sobą**" i szansa na życie zgodnie z własnymi preferencjami, kształtowanie własnego życia zgodnie ze swoją wolą. Prywatność zatem to możliwość odpierania prób naruszenia swojej sfery prywatnej przez innych – państwo, rodziców, przyjaciół, nauczycieli czy obcych.

Wartość prywatności doceniają psychologowie. Sugerują, że istnieje „ścisła prywatność" oraz „otwarta prywatność": „**ścisła prywatność**" dotyczy utrzymywania niektórych spraw w tajemnicy, zachowywania intymności własnego ciała, emocji lub myśli, podczas gdy „**otwarta prywatność**" to możliwość publicznego wyrażania swoich poglądów. Obydwa rodzaje prywatności są konieczne aby utrzymać poczucie własnej wartości oraz aby chronić własny wizerunek w społeczeństwie i relacjach społecznych.

Dzieciństwo to wyjątkowy okres w życiu każdego człowieka, w którym ochrona prywatności jest szczególnie ważna. **Wszystkie dzieci**, niezależnie od tego, gdzie mieszkają, mają prawo do życia i rozwoju, dorastania w środowisku, które szanuje wolność i godność, do **prywatności** i do **ochrony danych osobowych**.

Prywatność zawsze odgrywała kluczową rolę w funkcjonowaniu **współczesnych demokracji**, a co za tym idzie została uznana za jedno z **praw człowieka**. Prawne uznanie wagi prywatności przybrało na sile zwłaszcza po II wojnie światowej jako reakcja na totalitaryzm. Jej wartość jest powszechnie potwierdzona we wszystkich porządkach prawnych Europy – zazwyczaj jest ona w nich ujęta jako **prawo podstawowe** – jak również na szczeblu międzynarodowym. Państwo – generalnie rzecz biorąc – nie może naruszać prawa do prywatności, ale musi także zapewnić,

że to prawo jest chronione przed atakami ze strony innych, na przykład prywatnych firm.

Karta praw podstawowych Unii Europejskiej w artykule 7 odnosi się do prawa do poszanowania życia prywatnego.

Nowe technologie są źródłem nowych wyzwań dla ochrony prywatności. Coraz więcej komunikujemy się, pracujemy, uczymy się, bawimy korzystając z technologii – tak naprawdę coraz bardziej **żyjemy z i poprzez technologię**. Każdy – także dzieci – powinien być w stanie zawsze cieszyć się swoim prawem do prywatności, będąc **offline** oraz **online**, w sieci.

PRZYPADKI Z ŻYCIA WZIĘTE

Osoby sławne są szczególnie narażone na naruszenia prywatności. Media wiedzą, że publikowanie śmiesznych, zrobionych z zaskoczenia zdjęć takich osób może przyciągnąć wiele ciekawych oczu. Fotografowie znani jako „**paparazzi**" niekiedy przez wiele godzin czekają, aby zrobić takie zdjęcie celebryty. Jednakże nawet słynni ludzie mają prawo do prywatności, a co za tym idzie media nie powinny publikować ich zdjęć, które nie są szczególnie interesujące dla ogółu społeczeństwa (na przykład ponieważ przedstawiają taką znaną osobę przy codziennej czynności) lub jeśli ujawniają one coś, co taka słynna osoba wolałaby utrzymać w tajemnicy (na przykład wizytę w szpitalu na badaniach). Wiele znanych osób walczy z publikowaniem przedstawiających je zdjęć w prasie – są wśród nich aktorzy, modelki i księżniczki.

POMYSŁY NA DYSKUSJĘ

Uczniowie mogą omówić poniższe pytania:

1. ***Doświadczenia osobiste***: Czy wasza prywatność została kiedyś naruszona? Co się wydarzyło? Jak zareagowaliście?

2. ***Kształtowanie przemyślanego podejścia***: Czy możecie wyobrazić sobie społeczeństwo, w którym nie byłoby wcale prywatności? Jakby wyglądało takie życie? Czy przychodzą wam do głowy inne problemy, które mogłyby się pojawić? Postarajcie się pomyśleć o konkretnych kategoriach osób, które mogą mieć specjalne potrzeby dotyczące prywatności: osoby z problemami zdrowotnymi, o których nie chcą, żeby wszyscy wiedzieli, dziennikarze,

którzy chcą prowadzić poufne śledztwa, nauczyciele, którzy chcą zachować pewien dystans od swoich uczniów (i *vice versa*), ludzie, którzy chcą być aktywni politycznie, ale nie chcą być kontrolowani przez swoich przeciwników, itd.

ZALECANE ĆWICZENIA

1. To ćwiczenie może pomóc uczniom zrozumieć, co należy do ich prywatności, jak w niektórych kontekstach możemy potrzebować więcej „prywatności" niż w innych, i jak czuje się osoba, której prywatność została naruszona:
   - Uczniowie witają się z każdą osobą w klasie tak, jak gdyby nie widzieli się przez kilka miesięcy. **Obserwuj** różne sposoby witania się, a następnie **omówcie** te pytania: Czy bliscy przyjaciele witają się tak samo jak osoby, które nie są ze sobą tak blisko? Czy członka rodziny powitalibyście inaczej? Jak witają się osoby sobie obce, gdy spotykają się po raz pierwszy? Jak byście się czuli, gdyby obca osoba powitała was bardzo wylewnie?

2. Aby zgłębić różne wymiary prywatności zapisz na tablicy słowo „prywatność" i zachęć uczniów do **stworzenia mapy myśli** z powiązanymi pojęciami. Najpierw zapiszcie dowolne słowa odnoszące się do prywatności. Następnie postarajcie się pogrupować słowa według aspektu prywatności, do którego się odnoszą (na przykład: prywatność ciała, prywatność komunikacji, prywatność myśli i uczuć, itd.)

DLA NAJMŁODSZYCH

Małe dzieci powinny nauczyć się, że prywatność polega na zachowywaniu niektórych rzeczy dla siebie, ale także na posiadaniu własnej przestrzeni. Powinny wiedzieć, że inni **powinni szanować ich prywatność**, a one same powinny także **szanować prywatność innych**.

DLA STARSZYCH

Starsi uczniowie powinni zrozumieć, że prawo do prywatności jest **prawem podstawowym**, które odgrywa kluczową rolę w funkcjonowaniu społeczeństw demokratycznych. Wyznacza ono granice możliwości ingerowania przez państwo w życie jednostek, pomagając nam żyć w wolności.

2. WPROWADZENIE DO TEMATU OCHRONY DANYCH OSOBOWYCH

Czym są dane osobowe? Co to znaczy mieć prawo do ochrony danych osobowych?

CELE

- Poznanie znaczenia ochrony danych osobowych.
- Określenie, czym są „dane osobowe" i dlaczego powinny być chronione.
- Dowiedzenie się, czym są „dane szczególnie chronione" (nazywane często danymi wrażliwymi) lub dane zasługujące na specjalną ochronę.
- Zwiększenie świadomości praw przysługujących nam jako osobom, których dane dotyczą.

NAJWAŻNIEJSZE KWESTIE

Oprócz prawa do prywatności jednostkom przysługuje także **prawo do ochrony danych osobowych**. Prawo to traktowane jest jako prawo podstawowe we współczesnych społeczeństwach z powodu tragicznych skutków, jakie niewłaściwe użycie danych może spowodować: na przykład, jeśli dane osobowe są przez pomyłkę powiązane z niewłaściwą osobą w rejestrze publicznym, lub jeśli organizacja zdobywa zbyt dużą wiedzę o pewnych osobach gromadząc dużo rozproszonych informacji.

Pierwsze akty prawne dotyczące ochrony danych osobowych ujrzały światło dzienne w latach **70-tych XX wieku**, kiedy rządy i firmy zaczęły korzystać z komputerów do przechowywania i przetwarzania informacji o osobach. Pojawiły się obawy, że maszyny te dałyby wybranym, dużym podmiotom coraz więcej władzy nad ludźmi, a ludzie z kolei mieliby coraz mniej kontroli nad tym, co dzieje się z informacjami na ich temat. Obecnie przetwarzanie danych osobowych jest bardziej powszechne niż ktokolwiek przypuszczał, przez co prawo do ochrony danych osobowych jest bardziej konieczne niż kiedykolwiek.

Karta praw podstawowych Unii Europejskiej w artykule 8 odnosi się do prawa do ochrony danych osobowych.

Prawo chroni wszystkie „**dane osobowe**", to znaczy wszelkie dane, które można **powiązać z konkretną osobą**. Mogą być to informacje w formie pisemnej, zdjęcie, film, czy nawet nagranie dźwiękowe. Może być to numer telefonu, konto

mailowe lub czyjaś lista zakupów, o ile można je powiązać z konkretną osobą. Nawet jeśli dane wydają się na pierwszy rzut oka nieinteresujące lub nieistotne, mogą one stanowić dane osobowe, które zasługują na ochronę. Połączenie różnych, na pozór nieciekawych danych może w rzeczywistości wyjawiać wiele interesujących rzeczy o konkretnej osobie. Dlatego też prawo chroni ogólnie wszystkie dane osobowe, także wówczas, gdy są one tylko gromadzone.

Istnieją pewne rodzaje danych, które są szczególnie wrażliwe, a co za tym idzie objęte specjalną ochroną prawną. Za dane szczególnie chronione uznajemy na przykład te dane, które odnoszą się do **poglądów** politycznych, religijnych, **zdrowia**, **pochodzenia etnicznego** czy **życia seksualnego**. Tego rodzaju dane objęte są silniejszą ochroną, aby uniknąć dyskryminowania ludzi ze względu na powyższe kwestie, aby zapobiec jakiejkolwiek stygmatyzacji i aby pozwolić wszystkim ludziom, aby te informacje były tak prywatne jak sobie tego życzą.

Aby zapobiec niewłaściwemu wykorzystywaniu danych prawo nadaje **pewne prawa** każdej osobie, której dane osobowe są przetwarzane, nakłada **obowiązki** na tych, którzy chcą gromadzić lub wykorzystywać dane innych osób i przewiduje, że **niezależny organ ochrony danych** będzie monitorować poszanowanie wszystkich obowiązujących zasad.

Osoby, których dane są przetwarzane, nazywane są „**osobami, których dane dotyczą**" lub „podmiotami danych". Jako podmioty danych, wszyscy mamy prawo do:

- informacji o tym, **kto** wykorzystuje nasze dane, **jakie dane** są wykorzystywane i **do jakich celów** („prawo do bycia poinformowanym");
- **żądania** od tych, którzy wykorzystują nasze dane, informacji o tym, jakie dokładnie dane na nasz temat posiadają („prawo do dostępu do danych");
- żądania **poprawienia** nieprawidłowych danych („prawo do sprostowania danych);
- żądania **usunięcia** danych, jeśli podmioty, które je wykorzystują, nie mają ku temu żadnego ważnego powodu („prawo do wyrażenia sprzeciwu");
- **odmowy** lub **zgody** na niektóre sposoby wykorzystania naszych danych;
- **złożenia skargi** do niezależnego organu, jeśli nasze prawa nie są respektowane; oraz
- dochodzenia ochrony swoich praw w **sądzie.**

PRZYPADKI Z ŻYCIA WZIĘTE

W 2007 r. Max Schrems, student z Austrii, uczył się o prawie do prywatności i ochrony danych osobowych i zdecydował się przetestować swoje „prawo dostępu do danych". Miał on profil na Facebooku, zwrócił się więc do tego portalu i poprosił o kopię wszystkich danych, które na jego temat posiadał Facebook. Jako że używał tego portalu tylko przez kilka lat (ale z reguły rzadko z niego korzystał) ogromnie zaskoczył go fakt, że w odpowiedzi na jego żądanie Facebook przesłał mu ponad 1200 stron informacji na jego temat. Jeszcze większe było jego zdziwienie, gdy po przeczytaniu tych informacji, odkrył, że Facebook przechowywał zdjęcia, które myślał, że zostały wykasowane dawno temu, oraz inne dane, których jego zdaniem Facebook nie powinien mieć. Po tym wydarzeniu Schrems zapoczątkował ogólnoeuropejską inicjatywie mającą na celu wywarcie presji na portal Facebook, aby przestrzegał swoich obowiązków w zakresie ochrony danych osobowych – i wniósł przeciw portalowi sprawę do sądu.

POMYSŁY NA DYSKUSJĘ

1. ***Przemyślenie problemu.*** Ochrona danych osobowych dotyczy każdego przypadku, gdy ludzie gromadzą dane osobowe, nawet jeśli chcą je tylko zebrać, przechowywać i obiecują, że nigdy ich nie wykorzystają. Należy zachęcić uczniów do zastanowienia się, dlaczego tak jest: Dlaczego fakt, że organizacja lub firma zaczyna gromadzić mnóstwo danych o wszystkich mógłby być problematyczny? Czy waszym zdaniem powinny one móc gromadzić dane o was bez waszej wiedzy?

ZALECANE ĆWICZENIA

1. ***Zrozumienie, czym są dane osobowe.*** Ochrona danych osobowych dotyczy wszystkich danych osobowych, ale nie zawsze łatwo jest stwierdzić, czy konkretne dane są „danymi osobowymi" czy nie. Tak naprawdę dane mogą nie być „danymi osobowymi" w niektórych sytuacjach, a stawać się „danymi osobowymi" w innych. Aby lepiej to zrozumieć, uczniowie powinni **spojrzeć na zdjęcie** kogoś, kogo twarzy nie widać, i omówić, czy ich zdaniem jest to przykład danych osobowych czy nie. Powinni także zastanowić się, co by się stało, jeśli ktoś oznaczyłby to zdjęcie online dodając imię i nazwisko tej osoby. Czy byłyby to dane osobowe?

DLA NAJMŁODSZYCH

Najmłodszym uczniom należy uświadomić, że zawsze gdy ktoś chce posiadać dane ich dotyczące, przysługują im określone **prawa** dotyczące tych danych.

DLA STARSZYCH

Starsi uczniowie powinni wiedzieć, jak stwierdzić, które dane są ich danymi osobowymi, i dobrze rozumieć przysługujące im **prawa** dotyczące takich danych: kto posiada te dane i dlaczego, prawo dostępu do tych danych, ich poprawienia, a w niektórych przypadkach także usunięcia.

3. KTO CHCE TWOJE DANE OSOBOWE?

Dlaczego obecnie ochrona danych osobowych jest tak ważna?
Kto jest zainteresowany dostępem do naszych danych i jakie są jego obowiązki?

CELE

- Zrozumienie, dlaczego organizacje gromadzą, przechowują i wykorzystują nasze dane osobowe.
- Poznanie spoczywających na nich obowiązków związanych z wykorzystaniem naszych danych.

NAJWAŻNIEJSZE KWESTIE

Obecnie **wszyscy** każdego dnia **wytwarzamy ogromne ilości danych osobowych**. Tworzymy dane osobowe, gdy jesteśmy online – udostępniając lub dzieląc się informacjami, zdjęciami lub nagraniami wideo o innych lub po prostu sprawdzając nasze maile, czytając wiadomości online czy grając w gry online. Te czynności generują dane, które mogą być z nami powiązane. Dane osobowe tworzymy także będąc **offline**, kiedy do kogoś dzwonimy, gdy robimy zakupy i płacimy kartą płatniczą, kiedy korzystamy z publicznych środków transportu lub nawet po prostu idąc ulicą – jeśli nasz wizerunek uchwyci kamera monitoringu miejskiego. W rzeczywistości coraz większa część naszych działań **offline** często ma swój **wymiar online**: kiedy idziemy do kina, na koncert lub mecz piłki nożnej możliwe, że bilety kupimy online, generując tym samym jeszcze więcej danych.

Ogólnie rzecz biorąc, firmy i organizacje gromadzą, przechowują i wykorzystują nasze dane osobowe w celu zapewnienia konkretnych usług w najlepszy możliwy sposób. Często są to podmioty realizujące **bardzo ważne cele**, np. świadczące usługi opieki nad dziećmi lub opieki medycznej.

Niektóre firmy jednak lubią gromadzić **możliwie dużo danych** o ludziach w ogóle, a w szczególności o swoich klientach, zwłaszcza do tak zwanych „**celów marketingowych**". Pozwala im to ulepszać prowadzone działania i zwiększać liczbę klientów lub sprawiać, że będą oni wydawać więcej na usługi tej firmy.

Dlatego też dane osobowe mają niemałą **wartość ekonomiczną**. Dla wielu firm dane osobowe są przedmiotem zainteresowania i źródłem znaczących dochodów

– niektóre z nich wykorzystują nasze dane osobowe do celów reklamy, generując tym samym nowe lub zwiększając istniejące zyski. Dane osobowe mogą także być **bardzo interesujące** dla **organów publicznych**, ponieważ pozwalają im zyskać lepszy wgląd w życie osób lub grup.

Niekontrolowane wykorzystanie danych osobowych może jednak dawać firmom prywatnym i władzom publicznym zbyt dużą władzę, stawiając osobę w bardzo trudnej sytuacji.

Aby zapobiegać niewłaściwemu wykorzystaniu danych osobowych, prawo nakłada liczne obowiązki na podmioty, które chcą te dane przetwarzać. Podmioty te, zwane **„administratorami danych"**, są zobowiązane do:

- przetwarzania danych w sposób **rzetelny**;
- przetwarzania danych tylko w konkretnym, **określonym celu;**
- wykorzystywania niezbędnego minimum danych (to znaczy wykorzystania tylko tych danych, które są odpowiednie, istotne i proporcjonalne do celu, w którym są gromadzone i przetwarzane) i przechowywania ich **tylko tak długo, jak to konieczne** dla realizacji tego celu;
- dbania o to, aby dane były **dokładne**, **kompletne**, **aktualne,** zapewniając ich jakość oraz
- zapewnienia **bezpieczeństwa** danych i uniemożliwienia dostępu do nich komukolwiek, kto nie ma do tego prawa.

POMYSŁY NA DYSKUSJĘ

1. ***Naruszenia danych:*** Uczniowie powinni pomyśleć o tym, dlaczego tak ważne jest nałożenie obowiązków na firmy i organizacje, które wykorzystują duże ilości danych osobowych poprzez odniesienie się do naruszeń danych, to znaczy przypadków, gdy niewłaściwa osoba uzyskuje dostęp do danych osobowych przechowywanych przez firmę lub organizację. Powinni zastanowić się nad następującymi pytaniami: Czy kiedykolwiek słyszeliście o przypadku „naruszenia danych" lub o firmach lub organizacjach, które utraciły kontrolę nad posiadanymi danymi? Czy bylibyście zaniepokojeni, jeśli firma, która ma informacje na wasz temat, została zaatakowana przez hakerów? Jakiego rodzaju „naruszenia danych" byłyby dla was największym zmartwieniem? Dlaczego?

2. ***Hakerzy z dobrymi zamiarami?*** W nawiązaniu do poprzedniej dyskusji uczniowie powinni wziąć pod uwagę fakt, że niektórzy hakerzy twierdzą, że starają się bezprawnie uzyskać dostęp do danych tylko po to, aby pokazać, że zastosowane zabezpieczenia nie są wystarczające, że nadrzędnym celem ich nielegalnych działań jest skłonienie firm do zwiększenia poziomu zabezpieczeń, a tym samym zapewnienia skuteczniejszej ochrony danych. Uczniowie mogą pomyśleć na przykład o firmie produkującej urządzenia elektroniczne dla dzieci (np. aparaty-zabawki czy tablety-zabawki), która stałaby się ofiarą ataku hakerów mającego na celu ujawnienie poważnych braków w sposobie przechowywania przez tę firmę danych dzieci: Czy hakerzy mieliby do tego prawo? Jakie są potencjalne ryzyka związane z ich działaniem? Czy istniałyby lepsze sposoby na poradzenie sobie z tym problemem?

ZALECANE ĆWICZENIA

1. ***Lojalni klienci.*** Wiele sieci supermarketów i sklepów zachęca klientów do posiadania kart stałego klienta, które mogą lub muszą pokazywać przy każdych zakupach. To ćwiczenie ma na celu skłonić uczniów do refleksji na temat programów lojalnościowych oraz związanego z nimi przetwarzania danych osobowych.
   - Najpierw uczniowie **opowiadają** o tym, jak postrzegają karty lojalnościowe. Czy waszym zdaniem są one przydatne dla klientów? Czy waszym zdaniem są one przydatne dla firm? Jakie informacje gromadzą firmy dzięki takim kartom?
   - Następnie uczniowie wybierają kartę stałego klienta, z której korzystają sami lub ich rodzina, i krótko ją opisują: 1) informacje, które trzeba przekazać firmie, aby dostać kartę; 2) informacje, które firma zbiera, gdy używa się karty; oraz 3) cel zbierania danych podany przez firmę. Możliwe, że będzie to wymagało wejścia na stronę internetową firmy, sprawdzenie w broszurze informacyjnej lub zwrócenie się do niej bezpośrednio.
   - Jeśli są uczniowie, których rodziny nie używają kart lojalnościowych, **alternatywnie** mogą opisać wszelkie informacje, które sklepy gromadzą o nas, gdy robimy zakupy. Na przykład: gdy kupuję coś online, czy firmy rejestrują informacje o takich zakupach?
   - **Zaprezentujcie** i **porównajcie** wyniki indywidualnej pracy.
   - **Omówcie,** jakie korzyści może czerpać firma ze zbierania informacji o swoich klientach.

- **Pomyślcie**, czego nauczyliście się poprzez to ćwiczenie: Czy uczniowie byli świadomi tego, jakie dane dotyczące ich samych i ich rodzin są zbierane? Czy ich zdaniem ludzie wiedzą co do zasady, co dzieje się z ich danymi osobowymi? Czy dobrze byłoby, gdyby byli lepiej poinformowani?
- Na koniec **zastanówcie się** szczegółowo nad potencjalnymi ryzykami dla prywatności: Czy to, że firma przechowuje dane o tym, co konsumuje rodzina, może być problemem? Uczniowie powinni pomyśleć o tym, co można byłoby odczytać z nawyków żywieniowych, np. na temat żywności czy wyrobów lokalnych – kto mógłby być zainteresowany wiedzą o tym, czy członkowie rodziny jedzą zdrową żywność? Co można wywnioskować z książek lub filmów, które ktoś kupuje? Czy któreś z tych informacji mogą być danymi szczególnie chronionymi?

DLA NAJMŁODSZYCH

Najmłodsi uczniowie powinni dowiedzieć się, że dane ich dotyczące są **cenne**, że ludzie powinni gromadzić dane na ich temat tylko, jeśli mają ku temu dobry powód, oraz że mogą to robić jedynie, jeśli działają bardzo ostrożnie.

DLA STARSZYCH

Starsi uczniowie powinni zostać uwrażliwieni na **ogromną ilość** danych osobowych, które generują każdego dnia, liczne **powody**, dla których **różnorodne** firmy i organizacje mogłyby być zainteresowane ich wykorzystaniem oraz cele, do których dane te mogłyby zostać wykorzystane. Powinni także dowiedzieć się, że zawsze gdy ktoś przetwarza dane osobowe, musi także przestrzegać pewnych **obowiązków**, aby chronić osobę, której dane dotyczą.

4. PODEJMUJ MĄDRE DECYZJE I PAMIĘTAJ O TYM, ABY INNYM TEŻ POZWOLIĆ DECYDOWAĆ

Wszyscy mamy coś do powiedzenia, jeśli ktoś chce gromadzić lub wykorzystywać nasze dane osobowe. Oznacza to, że ludzie powinni brać pod uwagę nasze życzenia dotyczące tego, co dzieje się z naszymi danymi osobowymi, oraz że my powinniśmy robić to samo w odniesieniu do danych innych osób.

CELE

- Dowiedzenie się o możliwości **odmówienia** lub **wyrażenia zgody** na gromadzenie niektórych danych osobowych.
- Bycie świadomym tego, że taką zgodę można **cofnąć**.
- Zrozumienie, że niekiedy musimy poprosić o **zgodę innych osób** zanim udostępnimy jakieś treści online.

NAJWAŻNIEJSZE KWESTIE

Niekiedy jesteśmy **zobowiązani** do podania innym osobom określonych danych osobowych o nas samych. Jeśli chcemy, aby dostarczono nam do domu pizzę, jasne jest, że musimy podać swój adres – w przeciwnym razie nie będzie wiadomo, dokąd ją dowieźć.

W niektórych przypadkach firmy chciałyby jednak gromadzić **więcej danych niż to konieczne**. Mogą chcieć znać jakieś dodatkowe informacje o swoich klientach lub użytkownikach swoich usług, na przykład ich wiek, płeć lub hobby. Mogą prosić o te dane, ale muszą powiedzieć nam, co planują z nimi zrobić, i powinny dać nam możliwość **odmówienia** lub **wyrażenia zgody**.

Taka zgoda, aby była ważna, musi być **dobrowolna**, **konkretna**, **świadoma** i **jednoznaczna**. Oznacza to, że:

- nie można nas zmusić do wyrażenia „zgody" na podanie swoich danych;
- możemy zostać poproszeni jedynie o zgodę na konkretne przypadki wykorzystania danych, a nie ogólnie na wykorzystanie danych dla wszelkich celów, o jakich tylko można pomyśleć;
- możemy zostać poproszeni o zgodę tylko, jeśli otrzymamy szczegółowe informacje, na co się zgadzamy; oraz
- można mówić o tym, że udzieliliśmy naszej zgody jedynie, jeśli jednoznacznie to wyrazimy.

Przed podjęciem decyzji o tym, czy zaakceptować czy odrzucić prośbę o zgodę, osoby powinny poświęcić czas na zrozumienie, **jakie dane** będą zbierane, **do jakich celów**, kto będzie odpowiedzialny za zapewnienie ich bezpieczeństwa i **jak skontaktować się** z podmiotem gromadzącym dane, jeśli zmienimy zdanie i będziemy chcieli usunięcia danych. Jeśli nie jest to jasne, lub jeśli osoby, których dane dotyczą nie są czegoś pewne, nie należy **udzielać zgody**.

Jako że **dzieciom** trudno może być zrozumieć konsekwencje udostępnienia danych osobowych, **prawo stanowi, że w przypadku korzystania z usług online skierowanych do nich, nie można pytać ich o zgodę** przed osiągnięciem przez nie pewnego wieku. Dlatego też, jeśli firma lub organizacja chce zapytać dzieci, które są nieletnie, aby samodzielnie wyrazić zgodę na przetwarzanie danych osobowych, powinna **zwrócić się do ich rodziców** (lub opiekunów prawnych), którzy taką zgodę wyrażą lub odmówią udostępnienia danych dziecka. Nie oznacza to, że dorośli nie muszą brać pod uwagę opinii dzieci na ten temat – powinni uwzględnić ją w możliwie dużym stopniu. Dzieci mają bowiem prawo do **wyrażania swoich poglądów** we wszystkich sprawach, które ich dotyczą.

Nawet jeśli ktoś zgodził się na udostępnienie danych osobowych na swój temat, zawsze **może zmienić zdanie**. Jest to szczególnie istotne w odniesieniu do danych, które mogą pozwolić innym dowiedzieć się, gdzie osoby się znajdują, czyli tak zwanych „**danych dotyczących lokalizacji**". Może zdarzyć się, że osoba zaakceptowała lokalizowanie swojego telefonu komórkowego przez aplikację do wyszukiwania adresów, ale później chce poruszać się bez śledzenia przez innych. Ma prawo do cofnięcia swojej zgody. Urządzenia, które przekazują informacje o swojej lokalizacji, powinny regularnie przypominać ludziom o tym. Jest przecież możliwe, że ktoś zapomniał, że wyraził zgodę, lub że zgoda została udzielona przez inną osobę korzystającą z urządzenia.

Każdy, kto może udzielić zgody, ma także prawo do tego, by ją **cofnąć**. Co więcej jeśli rodzice wyrażają zgodę w imieniu swoich dzieci, a dziecko podrośnie i będzie mogło samo udzielać zgody, może wtedy dojść do wniosku, że chce cofnąć taką „zgodę rodzicielską" – ma do tego prawo.

Należy także pamiętać, że możemy **naruszyć prawa innych osób**, jeśli nie zapytamy, czy zgadzają się na to, żebyśmy udostępnili dane ich dotyczące. Kiedy chcemy umieścić online zdjęcie z innymi osobami, potrzebujemy na to ich

autoryzacji. Powinniśmy zapytać, czy zgadzają się na ten pomysł i **uszanować ich decyzję**, jeśli powiedzą, że wolą, aby ich zdjęcia nie były umieszczane online. Jeśli taka osoba jest nieletnia, powinniśmy zwrócić się do rodziców lub opiekunów prawnych.

POMYSŁY NA DYSKUSJĘ

1. ***Dobrowolna zgoda:*** Zasadniczo jesteśmy w stanie „wyrazić zgodę" na określone przetwarzanie naszych danych, jeśli mamy pełną swobodę powiedzenia 'nie'. Niekiedy jednak osoby, które proszą o naszą zgodę, wydają się być w szczególnej sytuacji, na przykład ponieważ są bardzo popularne, i trudno jest im odmówić. Uczniowie powinni zastanowić się, czy naprawdę czują się w pełni „wolni" odnośnie korzystania lub zaprzestania korzystania z serwisów online i aplikacji, których regularnie używają (i które gromadzą o nich dane osobowe), takich jak serwisy społecznościowe. Powinni zastanowić się nad następującymi pytaniami: Dlaczego korzystacie z konkretnego serwisu a nie innego? Czy dlatego, że większość waszych znajomych z niego korzysta? Czy czujecie presję, aby z tego powodu korzystać z danego serwisu?

ZALECANE ĆWICZENIA

1. ***Właściwe definicje i warunki:*** Ćwiczenie to skierowane jest do uczniów, którzy są już w takim wieku, że mogą wyrażać zgodę na przetwarzanie danych osobowych. Ma ono na celu pokazać, że niekiedy wyrażamy „zgodę" nie dowiadując się tak naprawdę, na co się zgadzamy.
   - Najpierw uczniowie powinni **zapisać nazwę** aplikacji lub serwisu online, który zbiera dane osobowe i z którego często korzystają. Najlepiej byłoby, gdyby nie wszyscy wybrali ten sam, ale kilka różnych serwisów.
   - Następnie powinni zapisać **wszystko, co pamiętają** z „warunków korzystania" lub „polityki prywatności" tego serwisu, które mają wyjaśniać, co firma robi z ich danymi, a które z pewnością musieli zaakceptować, żeby się zarejestrować. Jeśli nie pamiętają zbyt wiele, powinni przynajmniej postarać się przypomnieć sobie, czy w ogóle zetknęli się z „warunkami korzystania" lub „polityką prywatności".

- W kolejnym kroku uczniowie **porównują** swoje odpowiedzi z rzeczywistością sprawdzając rzeczywiste „warunki korzystania" lub „politykę prywatności" danego serwisu lub aplikacji.
- Na koniec klasa powinna omówić wnioski z tego doświadczenia: Czy uczniowie rzeczywiście wiedzą sporo o tym, co mówią im firmy? Czy poświęcili czas na przeczytanie tych dokumentów? Jeśli tak, czy są zdania, że wszystko zostało dobrze wyjaśnione?

DLA NAJMŁODSZYCH

Najmłodsi uczniowie powinni wiedzieć, że **nigdy nie powinni udostępniać swoich danych** bez pozwolenia rodziców. Powinni także rozumieć, że nie mogą udostępniać informacji o innych osobach (w tym przez dzielenie się zdjęciami i nagraniami wideo) bez uprzedniego zapytania się ich o zgodę.

DLA STARSZYCH

Starsi uczniowie powinni nabyć **umiejętności niezbędne do wyrażania (lub odmawiania) zgody**; kiedy ktoś zwraca się do nich o dane osobowe, powinni upewnić się, że rozumieją, jaki jest tego cel, jakie dane zostaną zabrane, kto będzie je przechowywał i jak długo, oraz jak skontaktować się z takim podmiotem w celu uzyskania szerszych informacji lub zmiany decyzji. Powinni zawsze mieć poczucie, że mogą powiedzieć nie, i dopytać o coś, czego nie zrozumieli. Podobnie przed wykorzystywaniem **danych osobowych dotyczących innych osób** powinni poprosić je o zgodę – i **uszanować** każdy wybór.

5. TOŻSAMOŚĆ CYFROWA

Jak dorastać z tożsamością cyfrową? Informacje na nasz temat dostępne online mogą mieć poważne konsekwencje w naszym życiu, stąd ważne jest, aby zadać sobie pytanie, co powinniśmy udostępniać, kiedy i w jakich okolicznościach.

CELE

- Uświadomienie sobie, czym jest obecność online i przyjęcie bardziej refleksyjnego podejścia do ujawniania informacji online.
- Przemyślenie wagi **tożsamości cyfrowej** innych.
- Refleksja nad tym, jak kontrolować nasze cyfrowe „odciski palców".

NAJWAŻNIEJSZE KWESTIE

Połączenie wszystkich informacji dostępnych o nas online tworzy coś, co można nazwać naszą „**tożsamością cyfrową**" lub „obecnością online". Jest to nasz obraz, który mógłby stworzyć ktoś kto nas nie zna, ale zna nasze imię i nazwisko, wyszukując informacje za pomocą wyszukiwarki internetowej. Można to postrzegać jako element naszej „tożsamości", która ma wiele wymiarów: nie jesteśmy tą samą osobą w oczach naszej babci i naszego przyjaciela, nie zachowujemy się w dokładnie ten sam sposób w swoim pokoju i w sklepie, może nie mamy tej samej reputacji w szkole jak w miejscu, gdzie byliśmy na wakacjach.

Jako że ludzie coraz więcej korzystają z internetu, „**tożsamości cyfrowe**" i „**reputacja online**" stają się bardzo ważne. Kiedy ktoś szuka pracy lub aplikuje o stypendium, potencjalni pracodawcy lub fundatorzy mogą przeszukać internet, aby uzyskać dodatkowe informacje o kandydacie i jeśli znajdą coś, co im się nie spodoba, mogą zdecydować się nie zatrudnić danej osoby lub nie przyznać jej stypendium. Jeśli pewnego dnia spotykacie kogoś, kogo chcielibyście mieć za przyjaciela lub nawet partnera, może okazać się, że ta osoba zdecyduje się poszukać w internecie więcej informacji o was.

Nasza „tożsamość cyfrowa" nigdy nie jest dokładnie taka sama jak nasza tożsamość rzeczywista. W niektórych przypadkach nasza „tożsamość cyfrowa" jest szczególnie **myląca** i sprawia, że ludzie myślą, że robiliśmy rzeczy, których tak naprawdę nigdy nie zrobiliśmy, lub przypomina wszystkim o czymś, co uważamy za sprawę dawno minioną.

Obecnie w Unii Europejskiej uznano, że każdy ma „**prawo do bycia zapomnianym**" (technicznie ujmując „prawo do usunięcia z wyników wyszukiwania"), które pozwala osobom na zażądanie, aby wyszukiwarki internetowe nie wyświetlały żadnych informacji **nieadekwatnych** lub **bez znaczenia**, jeśli ktoś będzie wyszukiwać informacji na ich temat. Fakt istnienia takiego prawa przypomina nam, że to, co można znaleźć o nas w internecie, może mieć realny wpływ na nasze życie.

Prawo to nie oznacza jednak, że można zwrócić się o usunięcie wszelkich danych osobowych, które są online. Tak naprawdę nawet jeśli mamy prawo do tego, żeby usunąć część informacji, możliwe, że **w praktyce niełatwe** będzie wykasowanie danych z internetu. Po ich usunięciu może okazać się także, że inni skopiowali już te informacje na swoje urządzenia i je rozpowszechniają.

Najlepiej jest zatem zastanowić się dwa razy zanim udostępnimy jakiekolwiek informacje online. Osoby nieletnie powinny być świadome tego, że dane ich dotyczące są jak „cyfrowe okruszki" lub „**cyfrowe odciski palców**", które pewnego dnia mogą do nich doprowadzić, a które jest bardzo trudno usunąć. Niektóre jest tak trudno usunąć, że lepiej chyba byłoby nazwać je „**cyfrowymi tatuażami**", które mogą grozić tym, że będą z nami na zawsze.

PRZYPADKI Z ŻYCIA WZIĘTE

- Pewien Hiszpan został kiedyś złapany podczas oddawania moczu w miejscu publicznym i ukarany za to. Zgodnie z hiszpańskim prawem, jako że policja nie wiedziała dokąd wysłać mandat, w popularnym dzienniku umieszczono pisemne powiadomienie, które zostało także opublikowane w formie elektronicznej i udostępnione w wyszukiwarkach. Mężczyzna ten zaczął pracować jako dyrektor szkoły. Jeden z uczniów wpisał nazwisko dyrektora w wyszukiwarkę, dowiedział się o tym mandacie i podzielił się tą informacją z wszystkimi uczniami. Poważnie wpłynęło to na wizerunek dyrektora w ich oczach, bardzo utrudniając mu pracę.

- Pewien węgierski student zrobił zdjęcia podczas lekcji historii na uniwersytecie, na których wyraźnie widać było jego twarz i symbole nazistowskie. Zdjęcia te zostały udostępnione online, a kiedy ktoś wyszukiwał nazwisko tego studenta w internecie, były one automatycznie wyświetlane. Bał się, że mogłoby to wpłynąć na jego szanse znalezienia pracy, poprosił więc wyszukiwarkę o niełączenie tych zdjęć

z wyszukiwaniami dotyczącymi jego nazwiska. Z pomocą organu ochrony danych udało mu się to osiągnąć.

PORADY

Czy w internecie jest coś o was, czego chcielibyście się pozbyć?

- Po pierwsze skontaktujcie się z osobą, która to opublikowała, i poproście o usunięcie tych materiałów.
- Jeśli to wy to opublikowaliście, spróbujcie to usunąć. Wszystkie serwisy internetowe powinny zapewniać użytkownikom możliwość pozbycia się całego profilu lub konta na życzenie.
- Jeśli to nie zadziała, skontaktujcie się z osobą lub firmą, która jest właścicielem danej strony internetowej lub platformy.
- Jeśli to nie zadziała, zwróćcie się o pomoc do kogoś dorosłego. Możecie także skontaktować się z organem ochrony danych w celu uzyskania informacji lub pomocy.

POMYSŁY NA DYSKUSJĘ

1. ***Dlaczego reputacja w internecie powinna być ważna?*** Uczniowie powinni pomyśleć o tym, kiedy i dlaczego ich tożsamość online staje się ważna. Możliwe podejścia:
   - Pomyślenie o **typowych sytuacjach**, w których ktoś może chcieć zebrać informacje online o innych osobach. Na przykład: w kontekście pracy (Czy poszukiwalibyście informacji online o kimś, komu chcielibyście zaproponować umowę o pracę w waszej firmie?), mieszkania (Czy poszukiwalibyście informacji online o kimś, z kim mielibyście dzielić mieszkanie?), relacji społecznych (Czy myślicie, że ludzie, których poznacie w przyszłości, mogą odczuwać pokusę ku temu, żeby dowiedzieć się czegoś o was szukając informacji w internecie?), itd.
   - Pomyślenie o **specjalnych kategoriach osób**, dla których reputacja online może być bardzo ważna. Uczniowie mogą omówić, co wydarzyłoby się, jeśli ktoś z nich miałby zrobić karierę polityczną lub stać się znanym aktorem, lub słynnym sportowcem: Czy ludzie byliby zainteresowani informacjami o takiej osobie? Dlaczego wówczas chcieliby, żeby ich zdjęcia czy ich dane nie były dostępne online?

2. ***Co jest absolutnie niewłaściwe online?*** Uczniowie powinni zastanowić się, jakie dane mogą być szczególnie problematyczne, jeśli będą dostępne online. W tym celu mogą odnieść się do doświadczeń osobistych i spróbować

przypomnieć sobie, czy kiedykolwiek widzieli coś, co wywołało w nich naprawdę złe wrażenie o kimś. Pomyślcie na przykład o:

- danych, które mogą być **zbyt intymne:** Czy są takie rzeczy, którymi lepiej nie dzielić się online? Jakie? Dlaczego?
- danych, które mogą być **niewłaściwie zrozumiane:** Czy istnieją rzeczy, które można by bardzo łatwo wyjąć z kontekstu? Czy są niejednoznaczne zdjęcia, które mogłyby zostać niewłaściwie zinterpretowane? Czy jakieś profile zbyt wybiórczo przedstawiają kim jesteś?
- danych, które mogą **szybko stać się przestarzałe**: Czy są jakieś rzeczy, które wyglądają fajnie dziś, ale jutro mogą być kompletnie niemodne? Czy kiedykolwiek czuliście wstyd z powodu czegoś, co zrobiliście kilka lat wcześniej?

ZALECANE ĆWICZENIA

1. Uczniów należy zachęcić do **sprawdzenia**, jakie **informacje na ich temat** są dostępne online. W niektórych przypadkach może pozwolić im to odkryć wiele nieoczekiwanych rzeczy – na przykład, że niektóre informacje, które uważali za prywatne, są tak naprawdę dostępne powszechnie, lub że coś, co uważali za dostępne tylko dla ich przyjaciół (internetowych) jest w rzeczywistości dostępne dla wszystkich. Aby uniknąć nieprzyjemności dla dzieci należy pozwolić im wykonywać to ćwiczenie samodzielnie – potencjalnie w domu.
   - Następnie można zachęcić dzieci do tego, aby przedstawiły **pisemnie** i/lub **omówiły** w klasie to, czego nauczyły się z tego ćwiczenia.
   - Poznając samodzielnie, jakie informacje o nich są dostępne online, niektórzy uczniowie mogą odkryć, że **istnieją na świecie inni ludzie, którzy nazywają się tak samo jak oni.** Uczniów należy zachęcić do tego, aby podzielili się swoimi odkryciami dotyczącymi informacji o osobach homonimicznych. W szczególności należy uwzględnić poniższe pytanie: Co mogłoby się stać, jeśli ktoś szukałby takiego ucznia, który nazywa się tak jak ktoś inny?

DLA NAJMŁODSZYCH

Młodsze dzieci powinny zdać sobie sprawę, że wszystko, co jest online, jest dostępne dla wielu różnych osób, oraz że różne informacje o nas w internecie

dają ludziom konkretne wyobrażenie o naszej osobie, zatem należy się dobrze zastanowić, co tam umieszczamy.

DLA STARSZYCH

Starsi uczniowie powinni zrozumieć, że informacje online mogą mieć poważne konsekwencje dla ich życia, stąd należy zwrócić na nie uwagę. Zasadniczo powinni unikać publikowania jakichkolwiek informacji, których nie chcieliby udostępnić ogółowi ludzi.

6. TARGETOWANIE ONLINE

Bycie w sieci oznacza nie tylko aktywne umieszczanie tam informacji i dzielenie się treściami, które wybieramy – za każdym razem, gdy korzystamy z usług elektronicznych, możemy wytwarzać lub wysyłać dane o samych sobie i o tym, co robimy. Dane te są szczególnie cenne dla firm, które sprzedają przestrzeń reklamową, które często gromadzą nasze dane oferując „bezpłatne" usługi.

CELE

- Uświadomienie, że działania online są często monitorowane.
- Uświadomienie, że firmy wyświetlają reklamy i propozycje produktów w oparciu o nasze wcześniejsze zachowania w internecie.

NAJWAŻNIEJSZE KWESTIE

Za każdym razem, gdy korzystamy z komputerów, telefonów komórkowych, iPad'ów, konsoli do gier i jakichkolwiek urządzeń do komunikowania się lub łączenia z internetem, **generujemy dane**. Niektóre z tych danych **dotyczą tego, co robimy**: stron, które odwiedzamy, filmów, które oglądamy, gier, w które gramy, ludzi, z którymi się komunikujemy, tego, co wyszukujemy, jak również wielu innych rodzajów danych. Niektóre z tych danych **dotyczą tego, kim jesteśmy**: te dane są wykorzystywane na przykład do lokalizowania nas na mapie lub do podłączenia nas do lokalnej wersji strony. Są też dane **o nas** (numer telefonu, adres e-mail, wszystkie dane identyfikacyjne), pozwalają one firmom na łączenie takich informacji i tworzenie całkiem szczegółowego obrazu tego, **kim jesteśmy**, naszego życia, tego, **co lubimy** oraz **jak moglibyśmy wydawać pieniądze**. Tak naprawdę mogą one mieć także całkiem dokładne pojęcie o tym, ile ich mamy. Firmy i inne organizacje wykorzystują wszystkie te informacje do „**profilowania**" ludzi, dzielenia ich na różne kategorie.

Nie zawsze jesteśmy **świadomi** takiego zbierania danych, nawet jeśli co do zasady każdy, kto zbiera nasze dane, powinien nas o tym wyraźnie poinformować. W praktyce ludzie z reguły akceptują wszelkie „**warunki**", **„polityki prywatności", itp.** przed korzystaniem z serwisu internetowego lub ściągnięciem aplikacji bez czytania ich. Jeśli je czytają, mogą ich nie zrozumieć – co może mieć miejsce, jeśli są osobami nieletnimi.

Strony internetowe, które gromadzą dane osobowe używając tak zwanych „**ciasteczek**" (ang. *cookies*), muszą informować wszystkich o tym, jakie dane są gromadzone i do jakich celów, dając możliwość wyrażenia na to zgody lub odmówienia jej. Większość osób jednak nie ma czasu na to, żeby myśleć o ciasteczkach podczas przeglądania każdej strony lub nie do końca rozumie, czym one tak naprawdę są.

Przez większość czasu firmy **tworzą charakterystyki** ludzi w oparciu o zachowania w internecie, aby **sprzedawać przestrzeń reklamową online**. Nazywamy to „**profilowaniem**".

Jeśli strona jest często odwiedzana przez dzieci, firmy będą starać się sprzedać przestrzeń reklamową na takiej stronie producentom zabawek, argumentując, że to właśnie dzieci są najlepszą grupą docelową. Tak naprawdę firmy są także w stanie **dopasować treść każdej reklamy do tego, co ich zdaniem zainteresuje każdego użytkownik**a. Kiedy wydaje się, że daną stronę odwiedzają dzieci, które lubią puzzle, wyświetlane będą na niej reklamy puzzli.

Praktyki takie nazywane są „**reklamą behawioralną**" lub „**targetowaniem**". Osoby nieletnie powinny być świadome tego, że treści online niekiedy są skierowane do nich w oparciu o ich dotychczasowe zachowania – linki, które wyświetlane są podczas wyszukiwania są częściowo determinowane przez zgromadzone o nich dane, podobnie jak produkty, które są im specjalnie oferowane w sklepach internetowych.

Osoby nieletnie powinny także być świadome tego, że firmy, które wydają się oferować swoje usługi „bezpłatnie", nie każą użytkownikom płacić za swoje usługi, ponieważ **zarabiają pieniądze** dzięki danym, które o nich gromadzą. Im więcej osób potrafią przyciągnąć, tym prawdopodobnie więcej pieniędzy zarobią i dlatego też wygodne jest dla nich oferowanie swoich usług „za darmo."

POMYSŁY NA DYSKUSJĘ

1. ***Czy małe niedźwiadki mogą szpiegować dzieci?*** Niektóre firmy, w tym producenci zabawek, tworzą „inteligentne zabawki", które mogą wchodzić w interakcję ze swoimi właścicielami i wysyłać firmie informacje o dzieciach. Informacje mają co do zasady sprawić, żeby reakcje tych zabawek były bardziej realistyczne i interesujące, ale mogą być także wykorzystywane przez te firmy, aby gromadzić dodatkowe dane o dzieciach. Uczniowie

powinni omówić, czy ich zdaniem dobrym pomysłem jest posiadanie misiów lub lalek z kamerami i mikrofonami, które mogą nagrywać dźwięki i obrazy i wysyłać je do producenta. Czy chcieliby mieć taką zabawkę? Jeśli tak, czy ich zdaniem powinna być możliwość wyłączenia takich funkcji? A co jeśli zapomną wyłączyć zabawkę i zarejestruje ona rzeczy, o których woleliby, żeby firma nie wiedziała?

2. ***Równe szanse?*** Kiedy jesteśmy online niektóre treści, które są nam wyświetlane, zależą od tego, co zdaniem firm może nas zainteresować, co moglibyśmy chcieć kupić, i są dobierane w oparciu o informacje, które taka firma o nas posiada (i ich interpretację tych informacji). Może to oznaczać na przykład, że uczniowie tej samej klasy widzą różne reklamy, kiedy odwiedzają tę samą stronę. Niekiedy treść wyświetlanej reklamy może nie być szczególnie ważna – niektórym uczniom wyświetlane są reklamy jednych ubrań, innym zaś wyświetlane są reklamy innych. Może się jednak zdarzyć, że różnice będą dotyczyć rzeczy, które są ważniejsze – możliwe, że zobaczycie reklamy wycieczek, o których inni nie widzą, reklamy innych szkół czy programów uniwersyteckich, innych ofert stypendialnych, czy nawet innych miejsc pracy. Uczniowie powinni omówić, czy ich zdaniem jest to sprawiedliwe, pomyśleć o przypadkach, gdy mogłoby to być problemem i porozmawiać o potencjalnych sposobach radzenia sobie z taką sytuacją.

ZALECANE ĆWICZENIA

1. ***Informacje anonimowe?*** Poniższe ćwiczenie to zachęta do pomyślenia o informacjach, które można wywnioskować z naszych działań i preferencji.
   - Każdy uczeń powinien wybrać **fikcyjne imię i nazwisko**, aby ukryć prawdziwą tożsamość, i zapisać na kartce – pod tym fikcyjnym imieniem i nazwiskiem – zbiór **informacji**, które określi nauczyciel, zależnie od wieku ucznia. Mogą być to: ulubione programy telewizyjne, ulubione ubrania, dyscypliny sportu, języki, którymi dana osoba mówi, ulubione rodzaje muzyki, niedawno oglądany film, niedawno czytana książka, itd. W pierwszej części nauczyciel nie wyjaśnia celu tej gry.
   - Wszystkie kartki należy wymieszać. Nauczyciel powinien losowo wybrać jedną kartkę i głośno przeczytać, co jest na niej napisane. Autor powinien starać się jak najlepiej ukryć swoją tożsamość, nie zdradzić się. Wszyscy uczniowie próbują **zgadnąć**, kto jest autorem: Czy mogą to odgadnąć na podstawie jednej informacji? Może dwóch? Może trzech?

- Następnie (lub jeśli nikt nie dał rady zgadnąć, kim był autor) uczniowie powinni pomyśleć, kto **mógłby być zainteresowany** skontaktowaniem się z osobą o takim profilu: czy takie dane mogłyby mieć wartość komercyjną nawet dla kogoś, kto nie wie, kim jest autor?
- Ćwiczenie to można **powtórzyć** wykorzystując różne profile.
- Starszych uczniów można poprosić o zastanowienie się nad tym, jak firmy mogłyby pozyskiwać online informacje podobne do tych podanych przez uczniów: Czy ktoś śledzi to, czego wyszukujemy? Czy ktoś pyta nas o to, co „lubimy"? Czy ktoś ma informacje o produktach, o których szukaliśmy informacji? Czy ktoś ma informacje o filmach, które lubimy oglądać? Itd.

DLA NAJMŁODSZYCH

Najmłodszym dzieciom należy powiedzieć, że wiele urządzeń elektronicznych, z których korzystają (lub mogą wkrótce korzystać) jest podłączonych do internetu i **generuje dane o ich zachowaniu:** telefony komórkowe, komputery, tablety, konsole do gier, itd. Poprzez wszystkie te urządzenia firmy starają się zdobyć informacje o tym, co robimy, aby móc nam sprzedać swoje produkty i usługi.

DLA STARSZYCH

Starsi uczniowie powinni zrozumieć, jak ich działania mogą być śledzone za pomocą różnych urządzeń, z których korzystają, i zdać sobie sprawę, że niektóre informacje, które widzą online, takie jak reklamy, mogą nie być takie same jak te, które wyświetlane są innym.

7. ABY SEKRET BYŁ SEKRETEM (A DANE NAPRAWDĘ ZABEZPIECZONE)

Pierwszy krok na drodze do zapewnienia, że nasze dane są chronione, należy do nas. Aby zagwarantować, że nasze dane są zabezpieczone, musimy zachowywać się ostrożnie i podjąć pewne podstawowe techniczne środki ostrożności.

CELE

- Świadomość istnienia potencjalnych zagrożeń dla danych.
- Dowiedzenie się, jak lepiej chronić swoje dane osobowe.
- Nauczenie się, czym są „**ustawienia prywatności**".
- Świadomość tego, czym jest „**kradzież tożsamości**" i „**phishing**".

NAJWAŻNIEJSZE KWESTIE

Nasze **dane cyfrowe** przechowujemy w różnych miejscach. Niektóre z nich są w urządzeniach, które posiadamy, takich jak komputery, tablety, smartfony. Niektóre są tak naprawdę przechowywane przez innych ludzi i możemy się do nich dostać logując się na konto lub profil. Ważne jest, abyśmy podjęli wszystkie niezbędne kroki, aby upewnić się, że nasze **dane są zabezpieczone**.

Dlatego też powinniśmy upewnić się, że chronimy nasze urządzenia, na przykład blokując dostęp do nich hasłem. Powinniśmy także dobrze chronić nasze profile i konta online. Jako że dostęp do większości z nich wymaga podania hasła, bardzo ważne jest, aby wybierać **silne hasła** i zachować je **wyłącznie dla siebie**.

Utrzymanie naszych haseł do kont i profili oznacza zachowanie ich **naprawdę wyłącznie dla siebie** i **nieudostępnianie ich nikomu**, nawet naszym najlepszym przyjaciołom lub partnerom. Zagwarantowanie bezpieczeństwa naszych haseł jest **naszą odpowiedzialnością** i nie powinniśmy się nimi dzielić z nikim.

Uczniowie powinni wiedzieć, że jeżeli ktoś poprosi ich o podanie osobistych haseł w dowód przyjaźni lub miłości, nie powinni się na to zgadzać, ponieważ mogłoby to zagrozić ich danym i danym wszystkich osób, które mają w kontaktach. Tak naprawdę, osoba, która o to prosi powinna – w dowód swojej przyjaźni lub miłości – w pełni uszanować prywatność i zaprzestać takich próśb.

Będąc online musimy zawsze mieć pewność, że mamy kontrolę nad tym, co dzieje się z naszymi danymi dokładnie poznając „**ustawienia prywatności**" serwisu, z którego korzystamy. Ustawienia prywatności to mechanizmy, które pozwalają użytkownikom serwisów na zdecydowanie (w pewnym stopniu), kto będzie mógł uzyskać dostęp do ich informacji profilowych oraz treści, które mogą chcieć udostępnić.

Nawet jeśli „ustawienia prywatności" mają pomóc użytkownikom w kontrolowaniu swoich danych, niekiedy **niełatwo** jest z nich skorzystać – może okazać się, że konieczne będzie dokonanie osobnych ustawień, aby kontrolować informacje na profilu, decydować, co dzieje się z postami, wybrać, kto może widzieć komentarze do postów innych osób, itd.

Ważne jest, aby osoby nieletnie:

- nie udostępniały publicznie informacji takich jak adres, numer telefonu lub adres mailowy;
- jasno rozumiały, że informacje, które udostępniają w postach, umieszczają w sieci lub którymi się dzielą mogą być dostępne dla każdego, chyba że one same to ograniczą tak, aby były dostępne tylko dla kilku osób – trzeba też wiedzieć, kim są te osoby;
- wiedziały, jakie informacje można znaleźć, jeśli wyszukuje się ich imienia i nazwiska lub pseudonimu.

Zabezpieczenie naszych danych wymaga także uważania na maile, które otrzymujemy. Niektóre wiadomości mogą być **oszustwem** lub być fałszywe. Na przykład można otrzymać mail z informacją o ogromnej wygranej lub odziedziczeniu wielkiej fortuny po kimś, o kim nigdy nie słyszeliśmy. Aby zdobyć fałszywą nagrodę lub nieistniejące pieniądze wymagane jest tylko, abyśmy podali nasze dane osobowe, które zostaną wykorzystane po to, aby zarobić na nas pieniądze.

Szczególnie niebezpieczną praktyką jest tak zwany „**phishing**", czyli oszukiwanie ludzi, że firma, którą dobrze znają, chce uzyskać dostęp do ich **poufnych danych**. Może być to wiadomość, która **wygląda jakby** została wysłana od kogoś, komu ufamy, na przykład bank, lub dostawcę usług e-mail lub firmę, która pozwala nam na zakup gier i aplikacji online.

Wiadomości phishingowe mówią o tym, że koniecznie musimy przekazać nasze hasło lub inne dane takie jak data urodzenia, numer telefonu lub adres, a następnie informacje te są wykorzystywane do tego, aby ktoś mógł uzyskać dostęp do naszego konta online podając się za nas – mamy wtedy do czynienia z „**kradzieżą tożsamości**". Używając naprawdę niewielu danych oszuści mogą próbować nawet wykorzystać nasze pieniądze (lub pieniądze naszych rodziców).

Dlatego też osoby nieletnie muszą być **bardzo ostrożne**, jeśli otrzymują takie maile i **nigdy nie podawać żadnych informacji poufnych**, nawet jeśli taka wiadomość wydaje się być bardzo ważna.

PORADY

Blokujcie swoje urządzenia tak, abyście tylko wy mogli je odblokować, na przykład za pomocą hasła.

- Sprawdzając historię waszego wyszukiwania w internecie ktoś może zobaczyć, jakie strony odwiedzaliście. Jeśli nie chcecie, aby miało to miejsce, pamiętajcie o wyłączeniu zapamiętywania w wyszukiwarce lub skasowaniu tego, co zostało już zapamiętane (zazwyczaj w menu „Narzędzia").

- Kiedy instalujecie aplikację na telefonie sprawdźcie, do jakich informacji chce ona mieć dostęp.

- Kiedy otrzymujecie spam (niechciane wiadomości mailowe), nie otwierajcie załączników – po prostu je zignorujcie. Mogą one zawierać linki do złośliwego oprogramowania.

- Wybierajcie **silne hasła** w sposób, który pozwoli wam je zapamiętać.
  - Nie używajcie jako haseł danych o sobie, takich jak data urodzin.
  - Nie trzymajcie hasła blisko komputera, telefonu lub tabletu.
  - Starajcie się używać długich haseł z różnymi znakami: małymi i wielkimi literami, cyframi, symbolami.
  - Unikajcie wpisywania liter, które po prostu są blisko siebie na klawiaturze.
  - Można z łatwością zapamiętać hasło, które pochodzi od zdania, na przykład: Lubię Silne Hasła i Ochronę Prywatności – LSHOP.

- Pamiętajcie o wylogowaniu się, jeśli korzystacie z komputerów publicznych lub wspólnych urządzeń.
- Zmieniajcie hasło od czasu od czasu, na wszelki wypadek.

- Jeśli otrzymacie maila z prośbą o dane, może być to oszustwo. Dokładnie go przeczytajcie, sprawdźcie wszystkie szczegóły i, kiedy będzie to możliwe, sprawdźcie w internecie, czy ktoś nie otrzymał już podobnego maila, na przykład wyszukując w wyszukiwarce któreś ze zdań użytych we wiadomości. Możecie też poprosić kogoś ze swojego otoczenia o radę. Pamiętajcie, żeby nigdy nie wysyłać swoich haseł mailem. Wiarygodne firmy nigdy nie proszą o wysłanie poufnych informacji mailem – jeśli otrzymacie wiadomość, która wygląda tak, jakby właśnie o to prosiły, najprawdopodobniej jest to próba **phishingu.**

ZALECANE ĆWICZENIA

1. ***Zdefiniuj swoją prywatność***. To ćwiczenie ma na celu pomóc uczniom zdać sobie sprawę, jak ważne jest zwracanie uwagi na „ustawienia prywatności" serwisów online lub aplikacji, z których korzystają. Uczniowie powinni:
   - Najpierw **wybrać** serwis online lub aplikację, z których często korzystają, a które mają „ustawienia prywatności" lub różne opcje prywatności. Najlepiej byłoby, jeśli nie wszyscy uczniowie wybraliby to samo, tak, aby była możliwość porównania różnych serwisów. Niemniej jednak kilku uczniów może pracować równolegle lub razem na tym samym serwisie.
   - Następnie opisać, jak działa serwis, jeśli użytkownik aktywnie nie zmieni niczego – innymi słowy, jakie są „**domyślne ustawienia prywatności**? Co się dzieje, jeśli ktoś się tylko rejestruje? Czy informacje profilowe będą dostępne dla wszystkich w wyszukiwarkach online? Czy te informacje profilowe obejmują dane takie jak prawdziwe imię i nazwisko, data urodzenia, zdjęcie z twarzą? Co się automatycznie stanie z danymi lub zdjęciami, które wysyłacie innym lub udostępniacie przez swoje konto?
   - Po trzecie opisać, jakie opcje prywatności są dostępne dla użytkowników: Co tak naprawdę można zmienić? Czy można ustawić, aby profil był prywatny? Czy można dzielić się informacjami tylko z kilkoma osobami? Czy naprawdę można kontrolować, kto ma dostęp do danych?

- Jeśli są uczniowie, którzy nie korzystają z żadnego serwisu online lub aplikacji z ustawieniami prywatności, mogliby alternatywnie popracować nad swoimi **zachowaniami offline dotyczącymi dzielenia się informacjami**: Jakie informacje o nich są udostępniane ludziom, gdy idą po ulicy? Jakimi informacjami lub zdjęciami dzielą się z innymi? Czy mogliby zmienić swoje „ustawienia prywatności", jeśli by chcieli? Jak? Mogą pomyśleć na przykład o: noszeniu okularów przeciwsłonecznych, dzieleniu się informacjami z kimś tylko wtedy gdy osoba ta obieca nikomu ich nie udostępniać, itd.
- Na koniec **porównajcie** i **omówcie** wyniki waszej pracy. Warto uwzględnić poniższe pytania: Czy uczniowie byli w pełni świadomi „ustawień prywatności" serwisów, z których korzystają? Czy ich zdaniem rzeczywiście pozwalają one na kontrolowanie danych? Czy jest łatwo je znaleźć i z nich skorzystać?

2. ***Jak kształtujemy naszą prywatność?*** Ćwiczenie to może być wprowadzeniem dla młodszych dzieci do tego, aby pomyśleć w jaki sposób dbamy o zachowanie naszej prywatności, oraz o różnych „narzędziach" i pomysłach, z których korzystamy.
   - W małych grupach lub pojedynczo uczniowie najpierw tworzą **listę** rożnych grup ludzi, w zależności od tego, jakimi informacjami się z nimi dzielą, na przykład: 1) mama i tata; 2) rodzeństwo; 3) przyjaciele; 4) inni uczniowie; 5) nauczyciele i inni dorośli, których dobrze znają; 6) nieznani ludzie na ulicy. Mogą istnieć także inne kategorie, na przykład „najlepsi przyjaciele", „sąsiedzi", „dziadkowie i inni członkowie rodziny", „ulubiona lalka", itd. – dzieci powinny same wybrać, które grupy są dla nich istotne;
   - Dla każdej grupy uczniowie **podają** informacje, którymi podzieliliby się tylko z tą grupą. Na przykład: Czy są takie rzeczy, które powiedzielibyście tylko (najlepszym) przyjaciołom? Czy rozmawiacie o tych samych sprawach z rodzicami i innymi członkami rodziny? Czy są jakieś rodzaje informacji, które waszym zdaniem powinni znać nauczyciele, ale raczej nie osoby obce na ulicy?
   - Klasa powinna zebrać odpowiedzi razem, porozmawiać **o tym, jak tak naprawdę zapewniamy**, że dzielimy się tym, co chcemy tylko z tymi, z którymi chcemy. Na przykład: nie wychodzimy na ulicę w pidżamie, rozmawiamy z niektórymi osobami na pewne tematy tylko, jeśli nikogo innego nie ma w pobliżu, czasem mówimy cicho, czasem prosimy ludzi o to, żeby obiecali zachować sekret, itd.

- Nauczyciel powinien **wyjaśnić**, że prywatność polega na kontrolowaniu tego, kto i co o nas wie, i że podobnie jak staramy się kontrolować to w codziennym życiu, tak będąc online także należy pamiętać o tym, by kontrolować, czym się dzielimy z innymi.

DLA NAJMŁODSZYCH

Najmłodsze dzieci powinny nauczyć się, że podobnie jak niektórzy ludzie chcieliby ukraść rzeczy, które są ich własnością, tak niektórzy ludzie chcieliby ukraść ich dane osobowe. Dlatego też powinny uważać na to, co robią ze swoimi danymi, zastanowić się, gdzie je przechowują i nigdy nie przekazywać danych obcym.

DLA STARSZYCH

Starsi uczniowie powinni nauczyć się odpowiedzialnie obchodzić się ze swoimi danymi: mieć silne hasła, zachowywać je dla siebie i uważać na zagrożenia takie jak phishing. Powinni także być w pełni świadomi „ustawień prywatności" serwisów lub aplikacji, z których korzystają.

8. RODZINA, PRYWATNOŚĆ I OCHRONA DANYCH OSOBOWYCH

Rodzice mogą pomóc dzieciom w ochronie prywatności i danych osobowych. Niekiedy jednak mogą także zbyt ingerować w te sprawy.

CELE

- Nauczyć się, jak ich rodzice mogą pomóc im w chronieniu swojej prywatności i danych osobowych.
- Zastanowić się, czy rodzice mogą także naruszyć ich prywatność i co z tym zrobić;.
- Zaproponować rozmowę na ten temat z rodziną.

Odnosząc się do powyższych kwestii uczniowie zagłębią się w zagadnienie danych osobowych, które wytwarzają i tego, kto ma do nich dostęp.

NAJWAŻNIEJSZE KWESTIE

Rodzice mogą odgrywać **kluczową rolę** w ochronie prywatności i danych osobowych swoich dzieci. O ile dzieci nie mogą wyrazić zgody nie niektóre sposoby przetwarzania danych, z reguły ich rodzice (lub opiekunowie prawni) są upoważnieni do **odmówienia** lub **udzielenia** na to zgody.

Nie oznacza to jednak, że rodzice powinni podejmować takie decyzje bez uwzględniania tego, czego chce dziecko. Wręcz przeciwnie, powinni słuchać swoich dzieci i pomagać w ich kształceniu tak, aby w przyszłości mogły one **podejmować właściwe decyzje** odnośnie tego, co zrobić ze swoimi danymi. Rodzice powinni zatem **pomóc dzieciom w obronie swoich praw** i pomóc im nauczyć się, jak to robić.

W praktyce jednak może zdarzyć się, że rodzice niestety odgrywają aktywną rolę w **naruszaniu** prywatności dzieci i ich praw ochrony danych.

- Rodzice z pewnością muszą wiedzieć, co robią ich dzieci, aby zapewnić ich bezpieczeństwo i kształcenie – są za to odpowiedzialni. Ich **nadzór** może jednak niekiedy sięgać za daleko i niepotrzebnie ingerować w zbyt wiele przestrzeni życia dziecka. W niektórych przypadkach dzieci są nieświadome tego, jak są śledzone, co jest szczególnie problematyczne.

- Rodzice mogą także „nadmiernie dzielić się" informacjami o swoich dzieciach z innymi ludźmi. Na przykład niektórzy rodzice umieszczają zdjęcia swoich dzieci lub filmy z nimi na swoich profilach w mediach społecznościowych bez kontrolowania tego, kto ma do nich dostęp, nie zdając sobie sprawy, że takie zdjęcia można na zawsze powiązać z imieniem i nazwiskiem dziecka. Takie zdjęcia lub filmy mogą dla nich być miłe, ale w innych kontekstach i po upływie pewnego czasu mogą być powodem zakłopotania lub nawet być niewłaściwie użyte.

Jeśli dzieci czują się niekomfortowo z którąkolwiek z powyższych kwestii powinny być w stanie **porozmawiać o tym** z rodzicami. Powinny być im zagwarantowane przynajmniej pewne sfery **prywatności**; należy im także **uświadomić**, jak wykorzystywane są dane na ich temat. Gdy dorastają, powinny mieć także coraz więcej do powiedzenia w decydowaniu o tym, co dzieje się z ich danymi, a z pewnością móc decydować o zdjęciach, filmach lub informacjach na ich temat udostępnianych online.

PRZYPADKI Z ŻYCIA WZIĘTE

Niektórzy użytkownicy serwisu społecznościowego **Instagram** stworzyli w celu dzielenia się zdjęciami trend **#BabyRP**, gdzie ludzie odgrywają role „dziecka", „mamy" i „taty" wykorzystując do tego celu zdjęcia rzeczywistych dzieci, które biorą od innych użytkowników nie pytając nawet o ich pozwolenie. W niektórych przypadkach rodzice odkrywali, że obce osoby wykorzystywały zdjęcia ich dzieci po tym, gdy zostały one powszechnie upublicznione przez ich fałszywe rodziny, pod fałszywymi imionami i nazwiskami i w wyimaginowanych sytuacjach.

POMYSŁY NA DYSKUSJĘ

Uczniów można poprosić o omówienie poniższych pytań:

1. ***Własne doświadczenia***: Czy kiedykolwiek czuliście, że ktoś naruszył waszą prywatność? Kiedy? Co z tym zrobiliście? Niekiedy rodzice naruszają prywatność dzieci nawet sobie z tego nie zdając sprawy, na przykład opowiadając podczas kolacji z innymi członkami rodziny lub przyjaciółmi anegdotę o swoim dziecku, która ich zdaniem jest bardzo miła lub po prostu śmieszna, a która dla dziecka jest ogromnie żenująca. Czy myślicie, że wasi

rodzice mają taką samą opinię jak wy o tym, co powinno być zachowane jako prywatne?

2. ***Poszukiwanie zasad:*** Czy waszym zdaniem rodzice mają prawo do monitorowania działań dzieci? Dlaczego mogliby potrzebować coś takiego robić? Czy powinny być jakieś granice ich nadzoru? Czy zasady powinny różnić się w zależności od wieku dziecka?

ZALECANE ĆWICZENIA

1. ***Dopuszczalne zachowania?*** To ćwiczenie może pomóc uczniom zastanowić się nad tym, co ich rodzice wiedzą o nich i o tym, co robią. Uczniowie powinni:

- **Wymienić** sposoby jakich rodzice mogą używać do monitorowania aktywności swoich dzieci. Warto pomyśleć na przykład o sprawdzaniu zachowań w internecie, kontroli nad komunikacją przez telefon, dostępie do ich kont na portalach społecznościowych, śledzeniu, jak wydają swoje (elektroniczne) pieniądze, itd.
- **Podkreślić** te zachowania, które ich zdaniem są niedopuszczalne.
- **Porównać** swoje odpowiedzi z odpowiedziami innych uczniów. Jeśli są jakieś różnice, wyjaśnić dlaczego.

2. ***Wy ich nauczcie.*** Czasem rodzicom może być trudno wspierać swoje dzieci w ochronie prywatności i danych osobowych, ponieważ nie wiedzą oni wiele o urządzeniach i serwisach, z których ich dzieci codziennie korzystają. Ćwiczenie to ma na celu skłonić dzieci do przemyślenia tego problemu i zdania sobie sprawy, że może posiadają jakąś bardzo cenną wiedzę, która może być użyta do tego, aby wzmocnić umiejętności cyfrowe całej rodziny. Pracując samodzielnie lub w małych grupach uczniowie powinni:
   - **Wyobrazić sobie lekcję** o urządzeniu, platformie społecznościowej, aplikacji lub innej usłudze cyfrowej, z której bardzo lubią korzystać, i którą bardzo dobrze znają, ale której ich rodzice wcale nie używają lub nie znają tak dobrze. Co powinni wiedzieć rodzice, jeśli mieliby zacząć z takiej usługi korzystać? Dlaczego jest to tak użyteczne, tak fajne? Opisać, jak funkcjonuje ta usługa i jakie są korzyści z używania jej.
   - **W lekcji należy uwzględnić także porady na temat prywatności** dla rodziców, tak, aby mogli oni chronić swoją prywatność i dane osobowe podczas korzystania z takiej usługi: Czy powinni stworzyć konto pod

swoim prawdziwym imieniem i nazwiskiem, czy raczej nie? Czy są jakieś ustawienia prywatności, które mogą zmienić? Czy firma będzie gromadzić o nich dane? Kto będzie widział informacje, które udostępniają?

DLA NAJMŁODSZYCH

Najmłodszym dzieciom należy uświadomić, że ich rodzice mają do odegrania kluczową rolę w pomaganiu im w ochronie prywatności i danych osobowych. Jeśli kiedykolwiek poczują, że rodzice ingerują w ich prywatność lub nie chronią ich praw tak, jak powinni, należy z nimi o tym porozmawiać. Rodzice mogą mieć konkretny powód ku temu, aby robić, co robią, lub w niektórych przypadkach mogą nie zdawać sobie sprawy, że ingerują w prywatność swojego dziecka.

DLA STARSZYCH

Starsi uczniowie powinni rozumieć, że ich rodzice mają do odegrania kluczową rolę w pomaganiu im w ochronie prywatności i danych osobowych, ale że to jednak oni są za to odpowiedzialni, i powinni wiedzieć, że ich opinia o tej sprawie się liczy.

9. JESTEM BEZPIECZNY, CZUJĘ SIĘ DOBRZE

W internecie możemy znaleźć wiele rzeczy, które nas ranią, ludzi, którzy nie są specjalnie mili ani uprzejmi, a nawet osoby ze złymi zamiarami. Dzieci powinny bardzo starać się unikać możliwych do przewidzenia zagrożeń i wszelkich zachowań, które mogłyby zranić innych.

CELE

Ten rozdział ma na celu pomóc uczniom:
- Zrozumieć potencjalne ryzyka online.
- Pomyśleć, czym są „**cyberbullying**" oraz „**mowa nienawiści**".
- Pomyśleć o potencjalnych niebezpieczeństwach „**sekstingu**".
- Zapobiegać ryzykownym zachowaniom.

NAJWAŻNIEJSZE KWESTIE

W internecie, podobnie jak w świecie realnym, **nie każdy jest naszym przyjacielem**. Poprzez sieci społecznościowe, w grach online lub po prostu poprzez komentowanie różnych rzeczy online można spotkać osoby, które wydają się bardzo przyjazne, ale to nie oznacza, że należy im ufać. Dzieci i młodzież muszą wiedzieć, że podobnie jak nie zaczęliby opowiadać szczegółów z życia osobistego nieznanej osobie napotkanej na ulicy, tak nie powinni nigdy przekazywać online jakichkolwiek informacji poufnych osobom obcym. W szczególności dotyczy to nieudostępniania nikomu **numerów telefonów** lub **adresów**, które ktoś mógłby później wykorzystać, aby ich nękać.

Tak naprawdę online, podobnie jak w rzeczywistości, nawet przyjaciele mogą nas czasem zranić. Wiemy, że ludzie mogą nieraz zachowywać się dziwnie, kiedy komunikują się online, może dlatego, że myślą, że nikt ich nie widzi lub też nie są w pełni świadomi **konsekwencji** swoich zachowań online.

Niekiedy ludzie krzywdzą innych celowo. „**Cyberbullying**" („**nękanie w internecie**") polega na krzywdzeniu lub molestowaniu kogoś przez internet, w szczególności jeśli jest to celowe i powtarzalne. Istnieje wiele rodzajów tego zjawiska, od rozpowszechniania fałszywych plotek przez media społecznościowe aż po nieustanne nagabywanie.

Wszystkie te zachowania mogą mieć **dramatyczne konsekwencje** dla ofiary. Dlatego też szalenie ważne jest, aby osoby nieletnie nie angażowały się w żadne działania (takie jak umieszczanie postów, komentowanie i dzielenie się treściami), które mogą mieć charakter „cyberbullyingu", i aby były gotowe wspierać swoich rówieśników, jeśli coś takiego się im przydarzy. Jeśli nieletni sami doświadczają takiej sytuacji, powinni być w stanie porozmawiać o tym z rodzicami (lub opiekunami) lub odpowiedzialnym dorosłym, aby **położyć kres** takiej sytuacji tak szybko, jak to możliwe.

Szczególnie skandaliczne krzywdzenie innych ma miejsce, gdy ludzie atakują jakąś osobę lub grupę, do której ona należy z powodu płci, pochodzenia etnicznego, religii, niepełnosprawności, orientacji seksualnej lub jakiejkolwiek innej „różnicy", którą niewłaściwie postrzegają jako powód do tego, aby ją poniżać. Niekiedy jest to nazywane „**mową nienawiści**" – sprawia to przykrość nie tylko osobie atakowanej, ale także całej grupie, której to dotyczy. Osoby nieletnie powinny wiedzieć, że takie zachowanie jest złe, że prawo przewiduje kary dla tych, którzy się go dopuszczają, oraz że powinny zgłaszać przypadki „mowy nienawiści", kiedy tylko się na nie natkną.

Uczniowie powinni także zrozumieć potencjalne niebezpieczeństwa związane z **„sekstingiem"**, czyli wysyłaniem i otrzymywaniem zdjęć, wiadomości lub filmów o wyraźnie erotycznym zabarwieniu – przez SMSy, maile czy portale społecznościowe. Młodzież, która odczuwa pokusę, aby wysyłać lub otrzymywać tego rodzaju obrazy, często nie rozumie, na jak wiele sposobów takie zdjęcia, wiadomości lub nagrania wideo mogą trafić w niewłaściwe ręce – dlatego też należy przypominać nastolatkom o tym, że ktokolwiek uzyska dostęp do takich informacji może podzielić się nimi lub udostępnić je wszystkim po prostu **przez własne zaniedbanie**, **przez pomyłkę**, **jako (kiepski) żart** lub nawet **w celu zdenerwowania kogoś**. Ponadto młodzi ludzie często nie wyobrażają sobie potencjalnych negatywnych konsekwencji takiego działania, a może ich ono narazić ich na wstyd, a nawet szantaż.

POMYSŁY NA DYSKUSJĘ

1. ***Osobiste doświadczenia dotyczące nękania w sieci (i jak położyć temu kres).*** Uczniowie powinni omówić poniższe pytania: Czy kiedykolwiek spotkaliście się z czymś, co wyglądało jak „cyberbullying"? Co z tym zrobiliście? Niektórzy eksperci mówią, że w takich sytuacjach ludzie powinni starać się

pokazać ofierze cyberbullyingu swoje wsparcie i że takie zachowania ich nie zastraszają. Czy łatwo jest to zrobić? Co jeszcze można zrobić?

2. ***Najbardziej prywatne sprawy.*** Uczniowie powinni porozmawiać o niebezpieczeństwach związanych z „sekstingiem" na przykład na podstawie zmyślonego scenariusza takiego jak ten:
   - **Scenariusz**: Fikcyjna dziewczyna, zwana D i fikcyjny chłopak, zwany C, oboje mający po kilkanaście lat, decydują się uczcić swoją rocznicę wysyłając sobie swoje erotyczne zdjęcia, ponieważ gdzieś przeczytali, że może być to fajne. Obiecują jednak sobie, że nie pokażą ich nikomu. Dzień później chłopak idzie na basen i przez przypadek zostawia swój telefon w szatni, na ławeczce. Gdy pływa, telefon zauważa inny chłopak, który przegląda to, co jest w telefonie, znajduje zdjęcie dziewczyny i decyduje się udostępnić je w bardzo popularnej sieci społecznościowej z konta C – czyli wszystkim jego „przyjaciołom" online. Zostawia telefon tam, gdzie go znalazł, i odchodzi. W międzyczasie D, która właśnie miała zacząć pisać na swoim blogu o ostatnich wakacjach, nagle widzi zdjęcie, które pojawia się na portalu społecznościowym – najwyraźniej wysłane z profilu jej chłopaka. Prawie natychmiast zaczyna dostawać drwiące i poniżające komentarze, także od ludzi, którzy nie byli „przyjaciółmi" online C. Rozzłoszczona i rozczarowana decyduje się na zemstę – na swoim blogu, który jest dostępny dla wszystkich umieszcza zdjęcie C i wysyła maila do jego ojca (którego adres mailowy znalazła w sieci), aby upewnić się, że będzie on wiedział, co robi jego syn.
   - **Dyskusja:** Co może wydarzyć się dalej? Czy D i C mogliby coś zrobić inaczej, aby uniknąć tej sytuacji? Co dokładnie? Czy waszym zdaniem taki scenariusz mógłby wydarzyć się w rzeczywistości? Jeśli nie, jakie inne problematyczne scenariusze możecie sobie wyobrazić?

ZALECANE ĆWICZENIA

1. ***Pomyśl zanim udostępnisz.*** Istnieje wiele powodów, dla których nieodpowiednie informacje mogą być udostępniane online przez dzieci lub nastolatki bez uprzedniego zastanowienia się nad konsekwencjami. Na przykład dzieci mogą myśleć, że po prostu zabawnie będzie, jeśli udostępnią publicznie zdjęcie, na którym ich przyjaciele wyglądają śmiesznie lub dziwnie, i nie myślą nawet, że takie zdjęcie może być następnie udostępniane wielokrotnie i stać się powszechnie dostępne, co tym przyjaciołom na pewno

się nie spodoba. Lub też w przypływie gniewu osoby nieletnie mogą pomyśleć o napisaniu o kimś w sieci czegoś szczególnie ohydnego nie zdając sobie sprawy, że może to nie tylko zdenerwować atakowaną osobę, ale zatruć ich życie na długi czas. Ćwiczenie to zachęca do **refleksji** na ten temat. Uczniowie powinni:

- **Opisać** sytuacje, w których ktoś mógłby umieścić lub udostępnić online informacje, które później stałyby się problemem, i jakiego rodzaju problematyczne treści mogłyby w ten sposób wylądować online – na przykład nastolatki na imprezie mogą udostępnić zdjęcia zachowań, o których powinny wiedzieć tylko osoby, które tam były, przyjaciele mogą po kłótni wyjawić sekrety, których mieli nikomu nie zdradzać,
- **Omówić**, co można by zrobić, aby zapobiec problemom: Czy są jakieś rodzaje danych, których nie powinno się nigdy udostępniać? Czy dobrym pomysłem jest pytanie kogoś o zgodę przed udostępnieniem danych na jego temat jest?

DLA NAJMŁODSZYCH

Najmłodsze dzieci powinny być świadome, że w internecie mogą natknąć się na najróżniejsze osoby. Nawet jeśli te obce osoby lub „nowi przyjaciele" zdają się być sympatyczni, nie można być stuprocentowo pewnym, że zasługują na zaufanie. Dzieci nie powinny nigdy przekazywać jakichkolwiek danych osobowych takich jak numer telefonu, adres zamieszkania czy zdjęcia obcym osobom lub „przyjaciołom" z internetu.

DLA STARSZYCH

Starsi uczniowie powinni w przemyślany sposób podejść do swoich zachowań online. Powinni pamiętać, aby zawsze zadać sobie pytanie, czy informacje, które udostępniają mogłyby mieć negatywny wpływ na kogoś (w tym także na nich samych!) – na przykład, jeśli zostałyby użyte w inny sposób niż początkowo przewidywano.

10. PODEJMOWANIE DZIAŁAŃ

Prawo do ochrony danych osobowych oznacza, że masz określone prawa, z których można korzystać, zatem nie należy się bać tego robić – bezpośrednio lub z pomocą kogoś dorosłego. W przypadku wątpliwości należy skontaktować się z organem ochrony danych w celu uzyskania informacji. Powinniście także wiedzieć, z kim należy się skontaktować w poważnych sprawach.

CELE

Ten rozdział ma na celu pomóc uczniom:

- Poznać ich **prawa do ochrony danych osobowych**.
- Dowiedzieć się, **co robić**, jeśli jakaś organizacja nie szanuje ich praw.
- Uświadomić sobie, że **istnieją organy ochrony danych**.
- Zapamiętać, **z kim się kontaktować** w przypadku trudnej, nagłej sytuacji.

NAJWAŻNIEJSZE KWESTIE

Ktokolwiek, kogo dane osobowe są wykorzystywane przez jakąś organizację lub firmę ma prawo do tego, aby zapytać, **jakie dane** posiada, zażądać **poprawienia** danych, które są niepoprawne oraz **usunięcia** danych, jeśli nie zachodzi już potrzeba ich posiadania. Jeśli **wyraziliście zgodę** na gromadzenie waszych danych osobowych przez firmę, ale potem zmieniliście zdanie, możecie ją o tym poinformować, a ona powinna niezwłocznie podjąć kroki w celu **usunięcia** danych. Są to przysługujące wszystkim podstawowe **prawa ochrony danych osobowych**, z których każdy powinien być w stanie korzystać poprzez zwrócenie się do firmy, która przetwarza jego dane osobowe.

Jeśli firma wysyła wam komunikaty handlowe lub nieustannie do was dzwoni, a wy nie jesteście zainteresowani tym, co mają wam do zaoferowania, możecie **powiedzieć im**, żeby przestali. Często można to zrobić „rezygnując z subskrypcji" ich maili. Wszystkie komunikaty handlowe powinny wyraźnie mówić, kto jest ich nadawcą i jak „zrezygnować z ich subskrypcji", żeby więcej ich nie otrzymywać.

Dzieci nie mogą samodzielnie korzystać z przysługującego im prawa do ochrony danych osobowych, ale mogą poprosić swoich **rodziców (lub opiekunów**

prawnych) lub zaufaną osobę dorosłą, aby pomogła im skutecznie chronić ich dane.

Jeśli firma lub organizacja przetwarzająca dane osobowe nie zareaguje odpowiednio lub nie będzie szanować decyzji osób, których dane dotyczą, zawsze można skontaktować się z **organem ochrony danych.** Jest to organ, którego funkcja polega na zapewnianiu, że dane osobowe są zawsze chronione zgodnie z obowiązującymi regułami (prawem) i że ktokolwiek korzysta z danych osobowych innych, robi to z poszanowaniem praw tych osób.

Organ ochrony danych może służyć informacjami i – w konkretnych przypadkach – przyjąć skargę. Może także skontaktować się z firmą lub organizacją aby rozwiązać problem.

Niektóre sytuacje wymagają jednak dużo **pilniejszych działań** i nie mogą być rozwiązane jedynie przez organ ochrony danych. Niekiedy osoby nieletnie odkrywają, że ktoś udostępnił online informacje na ich temat, które mogą wyrządzić sporo krzywd i które muszą zostać natychmiast usunięte. Niekiedy ma to miejsce przez pomyłkę, w innych przypadkach jest to działanie ludzi o złych intencjach, którzy nie chcą współpracować i usunąć tych informacji.

We wszystkich takich przypadkach dzieci i młodzież mogą próbować usunąć takie informacje możliwie szybko kontaktując się z administratorem strony lub usługodawcą takim jak portal społecznościowy. Nieraz może być to trudne, dlatego też powinni porozmawiać o tym ze **swoimi rodzicami lub opiekunem, lub zaufaną osobą dorosłą**, który powinien być w stanie im pomóc.

Jeśli wolą, mogą także bezpośrednio skontaktować się z **linią zaufania, jak np. Insafe**. Takie linie specjalizują się w pomocy dzieciom i nastolatkom, którzy przechodzą przez trudne doświadczenia online lub natkną się na nieodpowiednie treści, i są co do zasady bezpłatne i anonimowe. Mogą one także służyć pomocą w przypadkach **molestowania w internecie**. W przypadku poważnych problemów osoby nieletnie powinny nie wahać się przed zadzwonieniem na **policję**.

ZALECANE ĆWICZENIA

1. ***Korzystanie z naszych praw:*** Ćwiczenie to wymaga więcej czasu (przynajmniej kilka tygodni jest potrzebne, aby uzyskać odpowiedzi), ale

może być wyjątkowo użyteczne dla uczniów. Dzięki ćwiczeniu mogą zobaczyć co w praktyce oznacza ich prawo do ochrony danych osobowych. Każdy uczeń:

- **Wybiera** firmę lub organizację, która może mieć jego lub jej dane osobowe.
- **Zapisuje** dlaczego wybrał tę konkretną firmę lub organizację i jakie dane może ona mieć na jego temat.
- **Korzysta ze swojego prawa do dostępu** kontaktując się z tą firmą lub organizacją i prosząc o informacje, jakie dane na jego temat posiada.
- **Czeka** na odpowiedź co najmniej kilka tygodni.
- **Wyjaśnia** klasie, z jakim podmiotem się kontaktował, dlaczego akurat z nim, jakie dane przypuszczał, że mógł on posiadać, czy otrzymał odpowiedź, i czego zaskakującego się dowiedział (jeśli było coś takiego).
- **Porównuje** swoje doświadczenia z doświadczeniami innych uczniów. Analizując wszystkie wyniki, zastanówcie się nad następującymi pytaniami: Czy skorzystanie z prawa do dostępu do własnych danych osobowych może być użyteczne? Dlaczego? Czy łatwo jest uzyskać odpowiedź? Czy organ ochrony danych może być pomocny?

DLA NAJMŁODSZYCH

Młodsze dzieci powinny wiedzieć, że mogą **skorzystać z przysługującego im prawa do kontroli danych na swój temat** z **pomocą** rodziców lub zaufanej osoby dorosłej, oraz że istnieje **organ ochrony danych**, którego misją jest zapewnianie, że wszyscy przestrzegają zasad ochrony danych osobowych. Powinny także wiedzieć, że jeśli natkną się w internecie na coś, co ich zaniepokoi, lepiej jest wezwać pomoc.

DLA STARSZYCH

Starsi uczniowie powinni znać swoje **prawa do ochrony danych osobowych** i śmiało z nich **korzystać**. Powinni rozumieć, że mają prawo sprzeciwić się, jeśli ktoś niewłaściwie wykorzystuje dane na ich temat i wiedzieć, że istnieje **organ ochrony danych**, który może przekazać im więcej informacji lub w inny sposób pomóc. Ponadto powinni wiedzieć, że jeśli będą mieli kłopoty z powodu treści zamieszczonych online, dorośli mogą im pomóc.

MINI-KARTA PRAW DO PRYWATNOŚCI I OCHRONY DANYCH OSOBOWYCH

Poniższa „karta praw" to spis praw podstawowych przysługujących dzieciom i młodzieży na mocy prawa UE.

Masz prawo do prywatności. Wszyscy mamy prawo do prywatności od momentu urodzenia. „Wszyscy" oznacza także niemowlęta, dzieci i nastolatki. Dorośli też mają prawo do prywatności.

Masz prawo do ochrony swoich danych osobowych. Nikomu nie wolno przetwarzać danych innych osób bez poszanowania pewnych zasad, takich jak przetwarzanie wyłącznie danych, które są niezbędne, i dbałość o to, by dane te zawsze były zabezpieczone. Wykorzystując dane osobowe firmy i organizacje mogą osiągać duże korzyści, ale także zdobywać coraz więcej władzy. Zasady te pozwalają nam chronić nasze dane, siebie samych, ale także kontrolować, co robią takie firmy i organizacje.

Wszystkie twoje dane osobowe zasługują na ochronę. Nieważne, że dane są już publicznie dostępne ponieważ pewnego dnia zgodziliście się na ich

udostępnienie. Nieważne, że dane nigdy nie były „ściśle tajne", lub nie wydają się być szczególnie poufne. Zawsze gdy ktoś przetwarza dane osobowe na twój temat, musi przestrzegać zasad. Nawet nieciekawe, zwyczajne dane mogą być przyczyną kłopotów.

Masz prawo wiedzieć, kto ma dane na twój temat, do czego te dane są wykorzystywane i w jaki sposób. Masz prawo do kontrolowania – w pewnym zakresie – co dzieje się z danymi na twój temat, a jest to możliwe tylko wtedy, kiedy wiesz: kto wykorzystuje te dane, dlaczego i jak. Zatem ci, którzy chcą przetwarzać twoje dane osobowe, muszą cię o tym powiadomić.

Masz prawo otrzymywać jasne informacje. Informacje przekazywane ci przez administratorów danych powinny być zawsze zrozumiałe. Mają oni obowiązek do zachowania przejrzystości swoich działań, więc nie pozwól, żeby cokolwiek ukrywali. Jeśli coś jest niejasne, pytaj!

Masz prawo dokładnie wiedzieć, jakie dane są w posiadaniu administratorów danych. Wyobraźmy sobie, że wyjaśnili ci, po co chcieli twoje dane i jak będą je wykorzystywać. A może zapomnieli tego zrobić? A może udzielili ci niejasnych informacji? W każdym razie możesz zapytać ich o to, co o tobie wiedzą, a oni mają obowiązek ci odpowiedzieć.

Masz prawo poprawić wszelkie nieprawidłowe dane na swój temat. Czasem fakt, że inni mają o tobie nieprawidłowe informacje, może być naprawdę dużym problemem. Mogą z nich wyciągnąć niewłaściwe wnioski i podjąć niewłaściwe decyzje, które ciebie dotyczą. Jeśli zauważysz, że mają nieprawidłowe dane, możesz zwrócić się do nich o ich poprawienie, a oni mają obowiązek to zrobić.

Masz prawo do bycia wysłuchanym. Czasami organizacje lub firmy są zobowiązane do przetwarzania pewnych danych na twój temat. Często jednak nie mają ku temu dobrego powodu, więc proszą o twoją zgodę na wykorzystanie twoich danych. Dorośli i młodzież mają prawo do udzielenia zgody na takie przetwarzanie. Jeśli jesteś dzieckiem lub nastolatkiem prawdopodobnie nie ty, ale twoi rodzice mogą takiej zgody udzielić lub jej odmówić. Ale zanim podejmą decyzję, powinni porozmawiać z tobą i zapytać o twoją opinię.

Masz prawo do złożenia skargi. Jeśli ktoś nie szanuje zasad, powiedz mu, że jesteś świadomy swoich praw. Jeśli to do niego nie trafia, poproś kogoś o pomoc i nie odpuszczaj! Organy ochrony danych zostały utworzone w każdym kraju, aby

pomagać ludziom we wszystkich sprawach związanych z ochroną ich danych osobowych, mogą one być źródłem informacji i porad.

Znaj swoje prawa podstawowe i...

... korzystaj z nich! Staniesz się mistrzem prawa do prywatności i ochrony danych tylko jeśli będziesz z niego korzystać. Ludzie gromadzą dane o nas każdego dnia, więc niech wejdzie ci to w nawyk: pomyśl o tym, kto jakie dane gromadzi, jak je wykorzystuje i do jakich celów.

... korzystaj z nich mądrze! Z przysługujących ci praw korzystaj po to aby mieć pewność, że twoje dane są chronione – nie zaś po to aby naprawiać wcześniejsze lekkomyślne zachowanie. Najlepszym sposobem na to, aby nie stracić kontroli nad swoimi danymi osobowymi jest podejmowanie mądrych decyzji przed ich udostępnieniem.

... zawsze pamiętaj, że inni ludzie mają dokładnie takie same prawa. Upewnij się, że je szanujesz, na przykład nie udostępniając zdjęć przedstawiających innych lub informacji na ich temat bez ich zgody. Bądź miły i uprzejmy, także online.

WYBRANE SCENARIUSZE LEKCJI

Podręcznik nauczyciela został stworzony jako zachęta dla nauczycieli do tworzenia własnych scenariuszy lekcji, dopasowanych do potrzeb swoich uczniów. Podczas realizacji projektu ARCADES, organy ochrony danych z Polski, Słowenii i Węgier zaprosiły nauczycieli do przesyłania przykładowych scenariuszy lekcji, które można by powszechnie udostępnić, a które mogłyby być potencjalnie przydatne w innych krajach. Każdy organ krajowy wybrał najlepszy scenariusz spośród wszystkich nadesłanych w konkursach krajowych, po czym zostały one dołączone do niniejszego podręcznika, z krótkim wstępem od autorów.

Nagrodzone scenariusze przedstawiają różne możliwe podejścia do nauczania o prywatności i ochronie danych. Scenariusz lekcji 1, *Małe elfy*, to scenariusz dla młodszych dzieci, dzięki któremu poprzez zabawę można uczyć o podstawowej zasadzie, że trzeba pomyśleć zanim udostępni się dane w internecie. Scenariusz lekcji 2, *Kto chce twoje dane osobowe?*, skierowany jest do starszych uczniów i ma na celu przedstawić im szerszy obraz praktyk związanych z przetwarzaniem danych osobowych. Trzeci i ostatni opublikowany tu scenariusz lekcji, *Niebezpieczeństwa online*, skupia się z kolei na świadomości ryzyka, na które można natknąć się w internecie.

1. SCENARIUSZ LEKCJI 1: MAŁE ELFY

Nina JELEN

1.1. NAJLEPSZY ROK SZKOLNY W HISTORII!

To był naprawdę udany rok dla naszej szkoły podstawowej Podkum, OŠ Ivana Skvarče Zagorje. Zrealizowaliśmy mnóstwo projektów, dowiedzieliśmy się bardzo dużo i świetnie się przy tym bawiliśmy. A kiedy właśnie zdecydowaliśmy się trochę uspokoić, odpocząć trochę i skupić się tylko na programie szkolnym zaskoczyła nas nagroda Rzecznika Informacji! Sprawiło to, że ten rok szkolny był jednym z najlepszych w historii. Po ogłoszeniu, że wygraliśmy, naszą szkołę zalały wręcz elfy z wiersza ze zwycięskiej lekcji, elfickie piosenki i tańce. Nasze klasy były pełne śmiechu i szczęścia.

I nie tylko... Nasza mała, wiejska szkoła stała się jedną z najsłynniejszych szkół w Słowenii. Mówili o nas „najlepsza szkoła" i „odnosząca największe sukcesy", pisali o nas piękne artykuły, byliśmy w wiadomościach telewizyjnych i w radiu. Staliśmy się słynni jak elfy z naszej historii... ale w pozytywny sposób.

Tak naprawdę nie wyobrażałam sobie, że to my zwyciężymy w konkursie. Projekt był stworzony także z myślą o starszych dzieciach, a one mają tak rozległą wiedzę i pomysły dotyczące internetu, korzystają z niego codziennie. Myślałam, że jesteśmy zbyt młodzi i niedoświadczeni. Wielkim zaskoczeniem był telefon z biura Rzecznika Informacji i dobre wieści. Ale gdy się o tym naprawdę pomyśli....

W 100% zgadzam się, że musimy zacząć uczyć dzieci o internecie już kiedy są naprawdę małe. Są tak naiwne i nieświadome tego, jak wielka jest sieć. Nie zdają sobie sprawy, że można tam spotkać dobrych i złych ludzi... jak w prawdziwym życiu. Zanim zajęliśmy się tym tematem, nasi uczniowie byli gotowi dzielić się wszystkimi swoimi danymi osobowymi w internecie. Nie można odciąć dzieci od korzystania z sieci i nie należy nawet próbować. Jako że przygotowujemy je do prawdziwego życia, powinniśmy także przygotować je do życia online.

Bardzo cieszę się, że zaplanowałam i przeprowadziłam tę lekcję, nawet jeśli bym nie zwyciężyła. Myślę, że moi uczniowie wiele się z niej nauczyli. A jeśli za rok lub w kolejnych latach usłyszą coś o korzystaniu z internetu także od swoich rodziców, mam nadzieję, że będą pamiętać o naszych internetowych regułach, kiedy staną się prawdziwymi użytkownikami sieci.

Jestem bardzo wdzięczna za wszystko, co było naszym udziałem. Za wszystko, co zrobiło dla nas biuro Rzecznika Informacji. Dzięki tej nagrodzie doświadczyliśmy tak wielu rzeczy. Myślę, że było to coś unikalnego, coś, co nigdy się nigdy nie powtórzy ani w życiu moim, ani większości moich uczniów. Mieliśmy okazję grać na wielkiej scenie w Lublanie, dostaliśmy książki, komputery, byliśmy nawet w Barcelonie, co było niesamowite! Byliśmy w wiadomościach, w radiu, we wszystkich gazetach, zobaczyliśmy, jak tworzy się wiadomości w studio, jak pisze się artykuł prasowy... Nie znajduję słów, aby opisać, ile to znaczy dla małej szkoły. Nie tylko naszej, ale także każdej małej szkoły w Słowenii.

Nasza mała szkoła była WIELKA! Ponieważ udowodniliśmy, że nawet jeśli jesteśmy mali i jest nas niewiele, mamy wszystko i dużo więcej niż ci najwięksi! Dziękuję za wszystko!

1.2. SCENARIUSZ LEKCJI

1.2.1. Opis

Temat	Prywatność i ochrona danych w internecie
Czas trwania	45 min
Poziom	2. klasa szkoły podstawowej (system słoweński)
Wiek uczniów	7 - 8 lat
Cele	– Zrozumienie wagi danych osobowych. – Nauczenie się, czym są „dane osobowe" i dlaczego musimy je chronić. – Nauczenie się, czym są „dane wrażliwe", które wymagają specjalnej ochrony. – Podniesienie świadomości praw, które przysługują nam w odniesieniu do ochrony naszych danych. – Poznanie niebezpieczeństw związanych z internetem.
Formy pracy	Indywidualna, grupowa, prezentacja przed klasą
Metody pracy	Dyskusje, omówienie, demonstracje, scenki, czytanie i praca z tekstem.
Pomoce naukowe	– Wiersz (autorka: Nina Jelen) – Rekwizyty do scenki: kapelusze elfów, kamera, zabawki, fartuch, garnek, śrubokręt, sukienka do tańca... – Do rozdania uczniom: formularz rejestracyjny fikcyjnej strony *Fajne dzieciaki*

1.2.2. Rozwój lekcji

Wprowadzenie – motywacja	
Nauczyciel	**Uczniowie**
Nauczyciel ekspresyjnie czyta wiersz o *Elfach za górami* (poniżej) i pokazuje ilustracje. Historia jest następnie powtarzana z uczniami: Kim były elfy? Jakie były? Czy były dobre czy złe? Dlaczego inni chcieli je odwiedzać? (Przeczytaj część wiersza, która opowiada dlaczego, po niefortunnych wydarzeniach, inni chcieli odwiedzić elfy) Nauczyciel podkreśla, że cokolwiek zostanie upublicznione w internecie zostaje tam na zawsze. Jak skończyła się ta historia?	Uczniowie aktywnie uczestniczą w dyskusji i powtarzają oraz podsumowują historię.
Główna część lekcji	
Uczniom pokazane zostaje zdjęcie nowego portalu społecznościowego *Fajne dzieciaki*, skierowanego do młodszych dzieci, takich jak one. Oferuje ona gry, chat z innymi dziećmi i wiele innych ciekawych aktywności. Bez dalszych wyjaśnień, uczniom rozdane zostaną formularze rejestracyjne nowej strony *Fajne_dzieciaki.com*. Formularz wymaga wpisania wielu danych osobowych. Instrukcje dla uczniów: wypełnić formularz danymi, które uczniowie uznają za właściwe, i które bez obaw można udostępnić w internecie.	Uczniowie zostają poproszeni o podzielenie się opiniami o stronie internetowej. Czy chcieliby się tam zarejestrować? Uczniowie wypełniają formularz rejestracyjny ze strony internetowej *Fajne dzieciaki*.

Po wypełnieniu formularzy nauczyciel i uczniowie omawiają każdą kategorię danych osobowych, którymi byli gotowi podzielić cię w internecie. **Nauczyciel wyjaśnia, że nie należy w internecie udostępniać** swojego imienia, nazwiska, adresu, daty urodzenia, numeru telefonu, adresu mailowego lub haseł, danych na temat rodziców lub miejsc, gdzie się jest. To samo dotyczy zdjęć przedstawiających ich samych lub ich przyjaciół. **Nauczyciel wyjaśnia, że mamy specjalne prawa dotyczące naszych danych osobowych i że musimy je chronić.** Nauczyciel wyjaśnia, jak sklepy i firmy mogą wykorzystywać dane osobowe. **Podkreśla się wagę bezpieczeństwa.** W internecie, jak w realnym życiu, niektórzy ludzie mogą mieć złe intencje. Dlatego też uczniowie nigdy nie powinni ufać osobom, których nie znają. W internecie ktoś może z łatwością udawać, że jest kimś innym, jak w historii o elfach. **Nauczyciel wyjaśnia, że uczniowie muszą dbać o swoją tożsamość online.** W realnym życiu starają się być dobrzy i pracowici – powinni robić to samo odnośnie swojej tożsamości w internecie. Czy inni dostrzegali, że elfy w rzeczywistości były pracowite i dobre po tym, jak wstydliwe zdjęcia zostały udostępnione w internecie? **Nauczyciel wyjaśnia, że uczniowie muszą jednocześnie dbać o dane dotyczące ich**	Po dyskusji uczniowie stawiają wykrzykniki na formularzu przy tych danych, które podali, a które nie powinny być udostępnione w internecie. Uczniowie dzielą się swoimi doświadczeniami.

przyjaciół i ludzi, których znają. Dlatego właśnie Fotko (z aparatem) zrobił coś niewłaściwego udostępniając zdjęcia bez pytania o pozwolenie. Uczniom zostaje zaprezentowany plakat. *Złote zasady dla fajnych dzieciaków w internecie.* Plakat zostaje powieszony w klasie.	
Zakończenie lekcji	
Uczniowie odgrywają historię/wiersz o elfach za górami. Starają się grać możliwie ekspresyjnie.	

1.2.3. Materiały specjalne do wykorzystania

1.2.3.1. Wiersz

Elfy za górami
(lub jak małe elfy same zgotowały sobie kłopoty)

Za górami, za rzekami, za lasami
Była wioska z małymi elfami.
Były stworzeniami słodkimi i miłymi,
Sympatycznymi i bardzo grzecznymi.

Pomagały sobie w każdej czynności,
A w życiu ich było mnóstwo radości.

Z krain odległych przybywali do nich ludzie
Zobaczyć na żywo to, co słyszeli o elfim cudzie.

Pepe był elfim mechanikiem,
Naprawiał auta i był rzemieślnikiem.

Pepe*: O jaka fajna maszyna. Z pewnością będę ją reperował przez trzy dni i trzy noce. Myślę, że Vrtavka (Tkaczka) będzie bardzo szczęśliwa, gdy zobaczy, że naprawiłem jej samochód. Nie mogę się doczekać, gdy ją zaskoczę!*

Najprawdziwsza złota rączka była z niego,
Choć uszy miał zawsze pełne wosku żółtego.

Pepe: *Hmm... czy tą śrubę tez powinienem wykręcić?*

I kiedy myślał o tej śrubie, jak by ją odkręcił,
Palcem nieustannie sobie w uchu wiercił.

Vrtavka: *Pepe, czy naprawiasz mój samochód? Oh, jesteś moim bohaterem! Dziękuję!*

Smrdec (Smrodek) serce miał wielkie,
Pomagał wszystkim i rozwiązywał ich problemy wszelkie.
Smrdec: *Dzień dobry, panie Špegi. Proszę spojrzeć na pana piękne drzewo. Czy mogę je podlać? Ma pan tak dużo do zrobienia. Moje piękne słodkie drzewko...*
Ale czasem nie mógł oprzeć się ochocie,
Żeby sobie porządnie pierdnąć przy robocie.

Spak (Śmieszek) do łez rozśmieszał wszystkich,
Znał dowcipów mnóstwo z krajów dalekich i bliskich.
Spak: *Jeż wpada na kaktusa. I co mówi? „Oh, mamo!"*
Czasem któremuś elfowi się zdarzało
Przy nim upaść, potknąć lub że się coś wysypało
A on ze śmiechu zrywając boki
Zasikał sobie spodnie i od bluzy troki.

Vrtavka (Tkaczka) lubiła tkanie i szycie,
Ale to taniec kochała nad życie.
Elfia parkietu królowa, zgrabna i zwinna,
Choć czasem nogę stawiała nie tak jak powinna.
Vrtavka: *Hmm.. jak to było w tym przedstawieniu? Stajesz na palce, podnosisz się wysoko do nieba, potem w górę rękę i nogę… uuuuups…*
Nieraz też źle wychodziły piruety na jednej nodze,
I tańce kończyła dość szybko na podłodze.

Špegi kochała gotować kluski dla wszystkich dzieci –
Każdy wiedział, że z jej domu zawsze jeden dźwięk doleci:
Mniam, mniam, mniam…
Špegi: *Chodźcie tutaj moje małe dzieci. Špegi ma dla was makaron. Z mięsem, serem, ciepłe lub zimne... Chodźcie!*
Mała elfia kucharka tak kochała kluski,
Że je miała we włosach, na spódnicy i nawet wystawały jej z bluzki.

Fotko nigdy z domu nie wyszedł bez swojego aparatu.
Robił zdjęcia, kręcił filmy, by je potem pokazać całemu światu.
Fotko: *Mój aparat jest najlepszy na całym świecie! Najnowocześniejszy, najfajniejszy! Umieszczę te filmiki w sieci! Wszyscy będą chcieli to oglądać! Może zostanę słynną gwiazdą – Fotko Kuštroglavec!*
Udostępnię to teraz w sieci!

I krok po kroku, klatka po klatce do Internetu leci…
I wszystko – WSZYSTKO – udostępnił w sieci!
W oka mgnieniu dowiedział się o tym świat cały,
Jak się elfy bawiły, kiedy swoją prywatność miały!

I WSZYSCY mogli zobaczyć:
Jak Spak śmieje się zbyt donośnie,
Jak Smrdec pozwala sobie na pierdnięcie głośne,
Jak Špegi kluski kroi ukośnie.
Jak Vrtavka łapie zająca wielkiego,
Jak Pepe z uszu wyciąga coś żółtego.

Filmik od razu został sieci hitem,
A z Fotka zrobił od razu celebrytę,
Ale elfy wcale nie miały ochoty na żadne zabawy,
Zupełnie nie czuli się dobrze z tą falą nagłej sławy.

I z bardzo daleka ludzie przybywali tłumami,
Żeby się poznać z tymi dziwacznymi elfami!

O, Smrdec, co za ohydne pierdnięcie!
Špegi, patrz. Masz spaghetti w nosie.
A ty, Vrtavka, może przestań już tańczyć. Jesteś pokraką!
Nigdy nie będziesz prawdziwą tancerką!

Pepe, umyłbyś uszy! Jesteś taaaaaaki paskudny!
A ty, Spak.... twój brzuch jest jak galaretka, gdy się śmiejesz.

Biedne elfy, pod ziemię zapaść się chciały,
Uciec na koniec świata i zaszyć się pod skały,
I ze smutkiem myśleć o tych czasach,
Kiedy beztrosko mogły hasać po okolicznych lasach.

I cały czas płakały, płakały,
A ich łzy wcale nie wysychały.

Nawet Fotko chciał stać się niewidzialny,
Gdy zrozumiał, jakich szkód narobił nieodwracalnych.
Fotko: *Drogie elfy, gdzie jesteście? Co się stało naszej wiosce?*
Gdzie podziały się śmiech i szczęście?

Ale mleko się rozlało, szkody cofnąć się nie dało,
Wszyscy byli smutni, nikogo szczęście nie przepełniało.

Aby dojść do siebie, elfy potrzebowały całe lata
Po tym, jak w dziwnych sytuacjach zobaczyło ich ponad pół świata.

I mimo że Fotko film zrobił nowy,
Pokazujący prawdziwy świat elfów: wesoły i kolorowy:

Jak Pepe ciężko pracuje,
Jak Spak starszym rozrywkę gwarantuje,
Jak Špegi razem z dziećmi się bawi i gotuje,
Jak Smrdec stopą sąsiada się opiekuje.
Jak Vrtavka pięknie skacze, pląsa i tańcuje.

I mimo że znowu…
Z krain odległych przybywali do nich ludzie
Zobaczyć na żywo to, co słyszeli o elfim cudzie,
Ich uśmiechy już nigdy nie były tak szerokie,
O tym gorzkim dniu pamiętały z każdym krokiem.

1.2.3.2. Fikcyjny formularz rejestracyjny

www.fajne_dzieciaki.com

Pseudonim:*

Imię i nazwisko:*

Data urodzenia:*

Adres:

Numer telefonu:*

Numer karty kredytowej:

Adres e-mail:*

Hasło do konta e-mail:

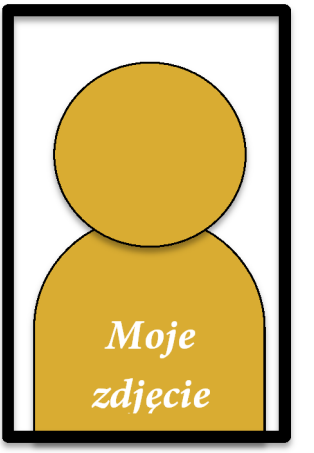
Moja szkoła:*

Zajęcia pozalekcyjne:

Miejsca, gdzie chętnie przebywam:

Hobby i zainteresowania:

Praca moich rodziców:



*** pola obowiązkowe**

1.2.3.3. Złote zasady korzystania z sieci

1. Nie udostępniaj swoich informacji osobowych, takich jak imię i nazwisko, data urodzin, numer telefonu, adres mailowy i hasło.
2. Nie wyjawiaj informacji o swojej rodzinie, przyjaciołach lub szkole.
3. Bądź zawsze uprzejmy.
4. Nie umieszczaj w internecie dziwnych lub nieodpowiednich zdjęć lub filmów.
5. Pamiętaj, że jeśli coś jest w sieci, bardzo trudno będzie to stamtąd usunąć!
6. Jeśli coś w sieci sprawia, że czujesz się niekomfortowo, powiedz o tym swoim rodzicom.
7. Nie rozmawiaj z obcymi, nie wysyłaj im żadnych zdjęć i nie próbuj spotkać się z nimi w rzeczywistości.

2. SCENARIUSZ LEKCJI 2: KTO CHCE TWOJE DANE OSOBOWE?

Małgorzata SZYSZKO i Katarzyna WIĄCZEK

2.1. WSTĘP

W ostatnich latach miał miejsce dynamiczny rozwój nowoczesnych technologii informacyjnych i komunikacyjnych. Internet oferuje liczne usługi, z których korzystają entuzjastycznie nastawieni młodzi ludzie, a którzy często bez skrupułów dzielą się mnóstwem informacji na własny temat. W świecie wirtualnym pozwala to na łatwe pozyskiwanie danych i identyfikację tych młodych osób. Może się to nawet stać zagrożeniem dla ich bezpieczeństwa i prywatności.

My, nauczyciele zauważamy to zjawisko i jesteśmy przekonani, że istnieje potrzeba działań mających na celu ochronę społeczności uczniowskiej. Jest to duże wyzwanie, ponieważ kwestie związane z ochroną danych osobowych i prywatnością są także czymś nowym dla nas – nauczycieli. Dlatego też doskonale jest, że różne instytucje, m.in. GIODO czy Fundacja Panoptykon przeprowadzają sesje informacyjne i edukacyjne oraz że możemy liczyć na ich wsparcie i współpracę.

W oparciu o materiały zapewniane przez te instytucje, wykorzystując własne doświadczenie w pracy pedagogicznej, znajomość różnych metod i form pracy z uczniami oraz przy użyciu ciekawych pomocy naukowych podejmujemy się edukowania młodych ludzi w obszarze ochrony danych osobowych i prywatności. Uczniom gimnazjów można zaproponować spotkania ze specjalistami, apele lub konkursy. Wydaje się jednak, że najlepszym sposobem na przekazanie trudnych treści dotyczących ochrony danych osobowych są lekcje prowadzone w dobrze znanych grupach, zespołach lub całych klasach.

Biorąc to pod uwagę, my, nauczycielki pracujące w Gimnazjum nr 119 im. Marszałka Józefa Piłsudskiego w Warszawie zdecydowałyśmy się przygotować scenariusz dla uczniów gimnazjum, który może zostać zrealizowany na różnych rodzajach lekcji, pozwalający na rewizję treści podczas lekcji. Zakładamy, że uczniowie mają już pewną podstawową wiedzę na temat danych osobowych i prywatności zdobytą w poprzednich latach kształcenia.

Uczniowie mogą aktywnie uczestniczyć w realizacji tematu. Scenariusz przewiduje pracę w grupach z użyciem materiałów przygotowanych uprzednio przez nauczyciela oraz prezentację wyników pracy grupowej. Zadania dla grup są bezpośrednio powiązane z treścią przedstawianą w prezentacji otwierającej i dyskusją, która z pewnością będzie miała miejsce w klasie.

W naszej szkole zrealizowałyśmy ten scenariusz na kilku rodzajach lekcji: informatyki z uczniami 1. kasy, lekcji wychowawczej z uczniami 2. klasy (wersja z nauczycielem wspierającym) oraz lekcji języka angielskiego z zaawansowaną grupą uczniów 3. klasy. Taka różnorodność wynika z założenia, że uczniowie w różnym wieku mają różny poziom wiedzy na temat ochrony danych osobowych i prywatności, a co za tym idzie zapewniamy różne poziomy trudności.

Scenariusz pozwala nauczycielowi na osiągnięcie zaznaczonego celu, ale trzeba bardzo ostrożnie przygotować się do takiej lekcji i dopasować ilość treści do poziomu każdej grupy. Powstała w ten sposób lekcja z pewnością wzbudza ogromne zainteresowanie wśród uczniów, czego dowodem jest ich aktywność podczas pracy w grupach, udział w dyskusjach i dodatkowa praca domowa.

2.2. SCENARIUSZ LEKCJI

2.2.1. Opis

Adresaci zajęć: uczniowie klas 1., 2. i 3. gimnazjum (system polski).

Rodzaje zajęć: zajęcia z wychowawcą, informatyka, język angielski.

Cel ogólny: Zajęcia pomogą młodym ludziom zrozumieć, dlaczego ochrona danych osobowych jest obecnie tak ważna. Uczniowie uczą się także, kto jest zainteresowany otrzymaniem ich danych oraz jakich zasad muszą przestrzegać takie osoby.

Cele szczegółowe:

Uczniowie:
- uczą się dlaczego instytucje, organizacje i firmy gromadzą, przechowują i wykorzystują nasze dane osobowe;
- poznają obowiązki podmiotów wykorzystujących nasze dane,

- uczą się, dlaczego swoje dane należy udostępniać odpowiedzialnie, i że trzeba sprawdzać informacje dotyczące polityki prywatności administratora danych.

Metody pracy:
- instrukcje podawane przez nauczyciela przy jednoczesnym rozdawaniu materiałów uczniom, praca w grupach;
- wyświetlenie prezentacji multimedialnej przygotowanej przez nauczyciela;
- rozmowa, dyskusja;
- korzystanie z narzędzi informatycznych.

Formy pracy:
- zwrócenie uwagi uczniów na informacje przekazane im przez nauczyciela;
- praca w grupach w oparciu o instrukcje i materiały przygotowane przez nauczyciela oraz komputer z dostępem do internetu;
- oglądanie prezentacji multimedialnej;
- rozmowa, dyskusja dotycząca kluczowych elementów oraz przykładów związanych z tematem lekcji.

Pomoce naukowe i materiały:
- wyposażenie sali – stoły ustawione do pracy w grupach;
- teczki z zadaniami dla konkretnych grup w formie wydruków;
- komputer z dostępem do internetu, projektor;
- kartki A4, kredki, flamastry;
- tablica magnetyczna (ewentualnie tablica korkowa lub duży arkusz kartonu).

Słowa kluczowe: dane osobowe, gromadzenie danych, bycie administratorem danych, przetwarzanie, bezpieczeństwo.

2.2.2. Rozwój lekcji

2.2.2.1. Wprowadzenie (wiedza podstawowa)

Obecnie ma miejsce bardzo szybki rozwój technologii informacyjnych i komunikacyjnych, który przynosi nam wielkie korzyści. Wytwarzane są duże ilości danych, które różne podmioty gromadzą online i offline. Skala i tempo tego zjawiska generuje problemy związane z odpowiednią ochroną udostępnionych danych osobowych.

Niekontrolowane wykorzystanie danych osobowych przez instytucje i firmy może wywoływać problemy dla wielu osób, których dotyczą dane, zwłaszcza nieletnich. Często wynika to z nieświadomości lub braku wiedzy na temat tego, co zrobić, aby zapewnić sobie bezpieczeństwo i ochronę prywatności. Korzystając z wiedzy, doświadczenia i zasobów informacyjnych takich instytucji jak organy ochrony danych i odpowiednie organizacje pozarządowe nauczyciele mogą – prowadząc interesujące lekcje i korzystając z metod aktywizujących – uświadomić dzieciom, dlaczego ochrona danych osobowych i prywatność są obecnie tak ważne.

Przygotowując lekcję na temat *Kto chce twoje dane osobowe?*, zakładamy, że uczniowie mają już pewną podstawową wiedzę dotyczącą danych osobowych i prywatności. Powtórzenie takich informacji będzie jednakże dobrym wstępem do wprowadzenia nowych treści.

2.2.2.2. Czynności nauczyciela przed lekcją

Aby przeprowadzić tę lekcję, nauczyciel powinien dokładnie przygotować: zadania dla uczniów w konkretnych grupach, sprzęt pozwalający na realizację tych zadań, prezentację na temat *Kto chce twoje dane osobowe?* oraz proponowaną pracę domową.

Bezpośrednio przed lekcją należy przygotować klasę – 3 stoły do pracy grupowej i wszystkie przedmioty niezbędne dla uczniów do wykonania zadań.

2.2.2.3. Kolejne etapy lekcji

1. Początek lekcji – powitanie, informacje o formie pracy, podział uczniów na grupy, rozdzielenie zadań – 5 minut;
2. Uczniowie wykonują swoje zadania – 10 minut;
3. Uczniowie prezentują swoje zadania i wyniki wspólnej pracy – 5 minut;
4. Prezentacja plus dyskusja sterowana przez nauczyciela na temat *Kto chce nasze dane?* – 20 minut;
5. Podsumowanie lekcji, omówienie pracy domowej – 5 minut.

2.2.2.4. Szczegółowy opis kolejnych etapów lekcji

1. Początek lekcji – uczniowie zostają zaproszeni do klasy i poinformowani, że będą pracować w grupach. Zostają poproszeni o dołączenie do jednej z trzech grup:
   - Uczniowie, którzy lubią robić gazetki, układanki zostają zaproszeni do grupy 1. Grupa otrzymuje tablicę magnetyczną, na której umieszcza posegregowane napisy oznaczające rodzaje danych osobowych, ich przykłady i podmioty, którym udostępniamy nasze dane online.
   - Uczniowie, którzy są dobrzy w wyszukiwaniu informacji online oraz ich szybkim zapisywaniu tworzą grupę 2, która dostaje komputer z dostępem do internetu i projektor.
   - Uczniowie, którzy lubią rysować i mają zdolności artystyczne tworzą grupę 3. Uczniowie otrzymują kartki papieru, kredki i flamastry niezbędne do zrobienia rysunków, które mogą być przykładami avatarów.

2. Dzieci wykonują swoje zadania. Mają na to około 10 minut. Nauczyciel nadzoruje pracę uczniów, sprawdza, czy zrozumieli swoje zadania, monitoruje postęp i przypomina im, ile mają czasu na wykonanie zadań. Jeśli to konieczne, dyscyplinuje uczniów.

3. Po wykonaniu zadań, reprezentanci grup prezentują zadania i wyniki wspólnej pracy każdej grupy.

4. Po zakończeniu etapu pracy grupowej, uczniowie zostają poproszeni o to, aby podejść do ekranu, na którym będzie wyświetlona prezentacja.

   Podajemy im temat zajęć: *Kto chce twoje dane osobowe?* Prezentacja jest połączona z rozmową i dyskusją. Jest ona wygłaszana w taki sposób, że uczniowie mogą porozmawiać przed pojawieniem się odpowiedzi na zadane pytania lub słów kluczy. Podkreślamy wagę zadań wykonywanych przez uczniów, kiedy konkretne treści pojawiają się w prezentacji.

Należy zwrócić szczególną uwagę na te informacje w prezentacji, które odnoszą się do konkretnych celów, które chcemy osiągnąć za pomocą przygotowanych materiałów i metod, tj.

- Uczniom należy dać odpowiedź na pytanie, dlaczego instytucje, organizacje, firmy gromadzą, przechowują i wykorzystują nasze dane osobowe;
- Trzeba wyjaśnić obowiązki tych, którzy wykorzystują nasze dane.
- Uczniowie uczą się, dlaczego swoje dane należy udostępniać odpowiedzialnie, i że trzeba sprawdzać informacje dotyczące polityki bezpieczeństwa administratora danych.

5. Zakończenie lekcji – podsumowujemy lekcję, podkreślając, że ochrona danych osobowych jest teraz bardzo ważna. Zadajemy kilka pytań, aby upewnić się, że uczniowie nauczyli się czegoś nowego i poszerzyli swoją wiedzę.

   Dajemy i krótko opisujemy pracę domową. Organizujemy wspólne porządkowanie sali lekcyjnej. Dziękujemy uczniom za udział w zajęciach.

Praca domowa:

- Praca domowa (lekcja z wychowawcą): Uczniowie muszą porozmawiać z rodzicami o kwestiach omawianych w czasie zajęć tj. *Kto chce twoich danych osobowych?*
- Praca domowa (informatyka):
  - Uczniowie muszą porozmawiać z rodzicami o kwestiach omawianych w czasie zajęć tj. *Kto chce twoje dane osobowe?*
  - Tworzą avatara z rysunku zgodnie z instrukcjami podanymi przez nauczyciela – dodatkowa praca domowa dla ochotników.
- Praca domowa (j. angielski): zapisanie nowych słów i użycie ich w zdaniach.

Ocena: Sprawdzamy wiedzę uczniów na koniec lekcji, ale także w jej trakcie. Prezentacja, która stanowi podstawę do rozmowy i dyskusji, zostaje wyświetlona w sposób, który daje uczniom możliwość porozmawiania zanim pojawi się odpowiedź na zadane pytanie lub słowo klucz. Obserwujemy ich reakcje. Na koniec lekcji pytamy, które informacje były dla nich nowe i zadajemy kilka pytań, aby sprawdzić, co zapamiętali.

Inne uwagi: Stworzony scenariusz jest dość uniwersalny i może być realizowany w czasie różnych lekcji, co pozwala na zaangażowanie różnych nauczycieli. Dodatkowo może być wprowadzony element sekretu poprzez niepodawanie uczniom tematu lekcji na początku, ale dopiero po wykonaniu zadań w grupach. Aby praca w grupach przebiegała bezproblemowo, zadania uczniów powinny być dokładnie przygotowane i należy im przekazać niezbędne materiały. W grupie, która układa napisy, najlepszym rozwiązaniem jest tablica magnetyczna. Jeśli nie mamy takiej tablicy, można użyć tablicy korkowej lub nawet dużego arkusza kartonowego, na którym będziemy przyklejać karteczki ze słowami. Lekcja dotycząca ochrony danych i prywatności nie jest jedną z wielu, wręcz przeciwnie – jest jedną z niewielu lekcji, które możemy zrealizować wzbogacając podstawę programową i dlatego też warto przygotować tę lekcję w sposób bardzo odpowiedzialny, dokładny i interesujący.

3. SCENARIUSZ LEKCJI 3: NIEBEZPIECZEŃSTWA ONLINE:

Eszter KESZY-HARMATH

3.1. PRZYSZŁOŚC WŁAŚNIE SIĘ ROZPOCZĘŁA...

W ostatnich latach pedagodzy coraz silniej odczuwają, że nasza sztuka nauczania wymaga nie tylko nieustannego dokształcania, ale także uwzględnienia nowych technologii. Współcześni studenci, pokolenie „Z", to osoby, które urodziły się w świecie technologii informacyjnych. Chcą się uczyć i są uważni tylko wtedy, gdy mogą wykorzystać nowe narzędzia, aby zdobywać informacje. Niestety, współcześni młodzi ludzie żyją w takim świecie nawet poza klasą, a duża część ich życia upływa z takimi mediami. Nie mają pojęcia, że oprócz korzyści płynących z technologii, w świecie tym kryje się wiele niebezpieczeństw. My – nieco mniej młodzi – możemy mieć trudności z tymi nowinkami. Ale potem zdajemy sobie sprawę, że mimo iż wszystkie dzieci korzystają z nowych platform komunikacyjnych (takich jak na przykład Facebook, Twitter, czy Skype) nie zdają sobie sprawy z ryzyk, którym mogą musieć stawić czoła. Istnieje potrzeba działań, a nauczyciele mogą nie wiedzieć, jak lub gdzie zacząć. Seminarium ARCADES dla nauczycieli zorganizowane przez węgierski Krajowy Organ Ochrony Danych i Wolności Informacji (NAIH) było ogromną pomocą w odnalezieniu właściwego sposobu, aby się za to zabrać. Otrzymaliśmy wiele użytecznych informacji i wytycznych dotyczących tego, jak pokazać uczniom, jak mogą stać się świadomymi użytkownikami internetu.

Po wykładzie rozmawiałam z moimi uczniami w *Karácsony Sándor Általános Iskola* w Budapeszcie i stworzyliśmy razem scenariusz lekcji, który dawał im zadania i pomagał zdać sobie sprawę z zagrożeń online, pułapek i rozwiązań. Personel NAIH uczestniczył w lekcji, a w końcu powiadomiono nas, że jako zwycięzcy krajowego konkursu będziemy reprezentować szkoły węgierskie na Konferencji kończącej Projekt ARCADES.

Udział w Konferencji pozwolił nam na poznanie innych czołowych zespołów, odkrycie nowych pomysłów i zapoznanie się ze scenariuszami lekcji stworzonymi w Polsce i Słowenii. Dowiedzieliśmy się, jak na inne sposoby można podejść do tego szerokiego i wielobarwnego tematu, skupiając się na uczniach w różnym wieku. Od nich oraz od przedstawicieli NAIH dowiedzieliśmy się wielu nowych, interesujących rzeczy o ochronie danych osobowych. Dziękujemy im za ich uprzejmość. Dziękujemy także wszystkim, którzy pracowali nad tym, aby

zaznajomić nas z tym palącym problemem i potencjalnymi rozwiązaniami, pomagając nam nauczyć naszych uczniów ostrożności i czujności.

3.2. SCENARIUSZ LEKCJI

3.2.1. Opis

Ten scenariusz lekcji został opracowany na zajęcia z edukacji medialnej, małego przedmiotu nauczanego w 8. klasie na Węgrzech. Główne tematy to zagrożenia online, w tym seksting i cyberbullying. Przedstawiony scenariusz obejmuje tylko część wiedzy o prywatności, którą należy przekazać uczniom. Można przewidzieć przynajmniej siedem podobnych lekcji, aby omówić wszystkie zagrożenia online, jak również różne aspekty ochrony danych.

Cele i zadania				
Rozbudowywanie umiejętności zapamiętywania	Poprawa percepcji wizualnej, uwagi i zdolności koncentracji	Pogłębienie wiedzy nabytej	Rozszerzenie słownictwa	Rozbudowywanie interoperacyjności
Rozbudowywanie umiejętności wypowiadania się	Rozbudowywanie umiejętności myślenia	Rozbudowywanie umiejętności monitorowania	Rozbudowywanie umiejętności komunikacji	Rozbudowywanie umiejętności współpracy

3.2.2. Rozwój lekcji

Ramy czasowe	**Jednostka**	**Opis ćwiczenia**	**Metody**	**Formy pracy w klasie**	**Pomoce**
3 minuty	Przygotowanie, rozgrzewka	Rozwiązywanie krzyżówki (zdefiniowanie umiejętności i zbadanie wiedzy) Wyrazy do odgadnięcia: ikona, nick, telewizja, podpis elektroniczny, router, netykieta, email, troll. Hasło to: INTERNET	Rozwijanie pamięci, aktywowanie wiedzy nabytej uprzednio	W parach	Podręcznik

2 minuty	Korekta	Dyskusja	Wyjaśnienie	Prezentacja przed klasą	Niezależna korekta
2 minuty	Dyskusja	Motto XXI wieku mogłoby brzmieć: *Obyśmy tylko byli zdrowi i mieli wystarczająco dobry zasięg internetu!* - Jakie jest znaczenie tego motto? - Zgadzacie się z tym?	Wyjaśnienie	Prezentacja przed klasą	Biurko interaktywne: projekcja
3 minuty	Obrazek:	Centralny element obrazka: INTERNET Zadanie: uzupełnić puste pola słowami związanymi z INTERNETEM	Stworzenie mapy myśli, wyjaśnienie, wolne skojarzenia	Prezentacja przed klasą	Biurko
3 minuty	Plakat	Interpretacja grafiki *Konfesjonał* autorstwa Pawła Kuczyńskiego	Interpretacja obrazu, dyskusja	Prezentacja przed klasą	Obraz
3 minuty	Efekt audiowizualny	Oglądanie filmu *Wo ist Klaus?* (dostępny w kilku językach na: http://www.klicksafe.de/ueber-klicksafe/downloads/klicksafe-werbespots/download-wo-ist-klaus/) Analiza materiału wideo na temat zagrożeń online	Dyskusja	Prezentacja przed klasą	Wideo
5 minut	Rozmowa	Zadanie: opisać znaczenie następujących słów: grooming, troll, flaming, mem, seksting, wirtualne nękanie	Wskazówki Promowanie autoekspresji Pobudzenie pomysłowości Zachęta	Prezentacja przed klasą	Biurko

7 minut	Scenka	Zadanie: wyciągnąć kartę i odegrać daną scenkę	2 scenki zgodnie ze wskazówkami nauczyciela związane z wirtualnym nękaniem i kradzieżą tożsamości	Praca grupowa	Karty
2 minuty	Opowiadanie niedokończonej historii	Ćwiczenie rekomendowane przez ARCADES: *Najbardziej prywatne sprawy*	Nauczyciel czyta klasie historię	Prezentacja przed klasą	Biurko interaktywne, podręcznik
10 minut	Dyskusja	Pytania: - Co mogło się wydarzyć? - Jak chłopiec i dziewczyna mogliby zapobiec takiej sytuacji? - Czy taka historia mogłaby się wydarzyć także w realnym życiu? - Jeśli nie, jakie inne historie możecie sobie wyobrazić?	Dyskusja, wyjaśnienie	Prezentacja przed klasą, praca w pojedynkę	
5 minut	Dyskusja mająca na celu zwiększenie świadomości podczas korzystania z internetu i przemyślenie ryzyk przed podjęciem decyzji	Pytania: Co byście zrobili w sytuacji ryzykownej lub niebezpiecznej? Gdzie szukać pomocy? - rodzice, - dorośli, - organy ochrony danych, - rzecznik praw człowieka, - internetowa infolinia, - internetowa informacyjna linia zaufania	Wypowiedź nauczyciela, wyjaśnienie, ocena	Prezentacja przed klasą	Biurko interaktywne, podręcznik

SŁOWNICZEK

Administratorzy danych: podmioty odpowiedzialne za przetwarzanie danych osobowych.

Cyberbullying (**wirtualne nękanie**): krzywdzenie, dręczenie, molestowanie lub grożenie komuś przy użyciu technologii, w szczególności jeśli jest to celowe i powtarzalne.

Dane osobowe: wszelkie dane, które można powiązać z konkretną osobą. Dane te mogą mieć różną formę: informacji pisemnej, zdjęcia, dźwięku, odcisku palca, itd.

Dane szczególnie chronione (wrażliwe): dane zasługujące na silniejszą ochronę, takie jak dane o poglądach, zdrowiu, pochodzeniu etnicznym czy życiu seksualnym.

Kradzież tożsamości: udawanie kogoś innego, w szczególności poprzez pozyskanie wystarczającej ilości informacji o tej osobie, aby móc się za nią podawać.

Osoba, której dane dotyczą: osoba, której dotyczą pewne dane osobowe, a która ma do tych danych liczne prawa.

Phishing: próba pozyskania informacji takich jak nazwa użytkownika, hasła lub szczegóły dotyczące karty kredytowej poprzez podszywanie się za godną zaufania osobę w komunikacji elektronicznej, zazwyczaj mailowej.

Prawo do ochrony danych osobowych: to prawo podstawowe chroni ludzi poprzez przyznanie im zbioru praw odnoszących się do ich danych osobowych przetwarzanych przez innych, nakładając jednocześnie na tych ostatnich obowiązki i ustanawiając organy ochrony danych w celu monitorowania przestrzegania zasad przetwarzania danych.

Prawo do prywatności: to prawo podstawowe, tradycyjnie opisywane jako „prawo do bycia pozostawionym w spokoju", jest w rzeczywistości pojęciem szerszym, które chroni poufność komunikacji, nienaruszalność domu, życia rodzinnego, danych osobowych oraz, ogólnie mówiąc, prawo każdej osoby do własnego życia, bez nieuzasadnionej ingerencji ze strony innych.

Profilowanie: proces polegający na zbieraniu i analizowaniu informacji o osobie. W oparciu o te informacje jednostki przypisywane są do kategorii/profili, które składają się z osób o podobnych cechach, preferencjach, działaniach. Dodatkowe informacje mogą być domniemywane lub implikowane w oparciu o zebrane dane.

Reklama behawioralna: wyświetlana w internecie w oparciu o dane zebrane uprzednio o użytkowniku zindywidualizowana reklama, mająca z założenia większą szansę na wpłynięcie na użytkownika.

Tożsamość cyfrowa: wizerunek osoby, który można stworzyć w oparciu o informacje dostępne o niej online.

Zgoda: udzielone dobrowolnie, konkretne, świadome i jednoznaczne wyrażenie akceptacji konkretnych sposobów wykorzystania danych osobowych przez osobę związaną z tymi danymi.

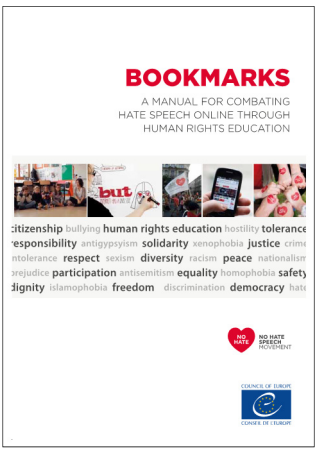
PRZYDATNE ŹRÓDŁA

Organy ochrony danych: Szukasz więcej informacji na temat zasad ochrony danych obowiązujących w twoim kraju lub też konkretnych wytycznych? Pełna lista krajowych organów ochrony danych w państwach UE oraz ich dane kontaktowe, podane według państw członkowskich, dostępne są na: http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm Na stronach wielu z nich można znaleźć materiały skierowane do dzieci i młodzieży oraz nauczycieli szkolnych.

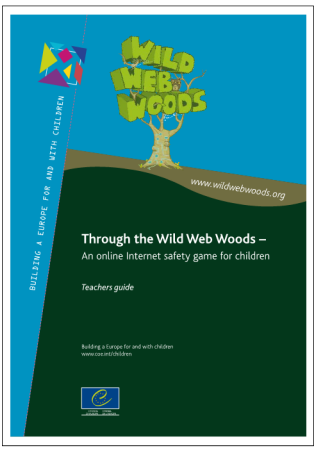
Centra Bezpieczniejszego Internetu: Potrzebujesz pomocy dotyczącej bezpieczeństwa nieletnich online? Centra Bezpieczniejszego Internetu zazwyczaj składają się z centrum informacyjnego, informacyjnej linii zaufania, infolinii i panelu młodych. Więcej informacji oraz linki do centrów krajowych można znaleźć na: https://www.betterinternetforkids.eu/web/portal/policy/insafe-inhope.

Karta Praw Podstawowych UE: Dokument ten to spis wszystkich praw podstawowych uznanych w prawie UE. Artykuł 7 tegoż dokumentu mówi o tym, że każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, domu i komunikacji, a artykuł 8 podkreśla, że każdy ma prawo do ochrony swoich danych osobowych. Dostęp do pełnego tekstu Karty we wszystkich oficjalnych językach UE: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A12012P%2FTXT.

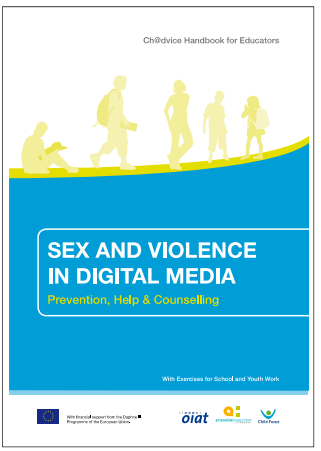
Podręcznik europejskiego prawa o ochronie danych: Doskonałym punktem wyjścia do tego, aby dowiedzieć się więcej na temat europejskiego prawa o ochronie danych, tak na szczeblu Unii Europejskiej, jak i Rady Europy, jest *Podręcznik europejskiego prawa o ochronie danych* opublikowany wspólnie przez Radę Europy oraz Agencję Praw Podstawowych UE (FRA) w 2014 r. Jest on dostępny bezpłatnie w wielu językach UE i kilku językach pozaunijnych na: http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law.



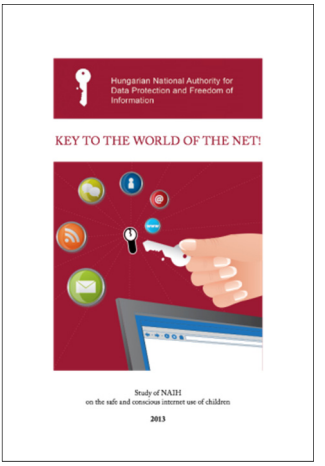
Zakładki: Podtytuł: *Przeciwdziałanie mowie nienawiści w sieci poprzez edukację o prawach człowieka.* Ta książeczka skierowana jest do pedagogów, którzy chcą zajmować się kwestią mowy nienawiści z perspektywy praw człowieka, tak w ramach jak i poza systemem edukacji formalnej. Stworzona została do pracy z uczniami w wieku od 13 do 18 lat, choć ćwiczenia można dopasować do innych grup wiekowych. Wersja angielska i francuska dostępne są na stronie Rady Europy, pozostałe wersje językowe dostępne są w krajowych punktach kontaktowych. Więcej informacji można znaleźć na: http://www.nohatespeechmovement.org/bookmarks.



Przez dzikie internetowe lasy: Gra online stworzona na zlecenie Rady Europy, aby pomóc dzieciom w bezpiecznym poruszaniu się w internecie. Jest dostępna w ponad 20 językach i opatrzona wytycznymi dla nauczyciela. Dostępna pod linkiem: www.wildwebwoods.org.



Seks i przemoc w mediach cyfrowych: Podręcznik dla nauczycieli z przydatnymi informacjami na temat przemocy w mediach i zjawisk takich jak nękanie w internecie, seksting i grooming. Stworzony przez Austriacki Instytut Telekomunikacji Stosowanej (OIAT) w kilku wersjach językowych jest dostępny pod poniższym linkiem: https://www.saferinternet.at/chadvice/.

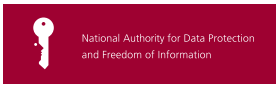


Klucz do świata Internetu!: Materiał poświęcony kwestiom bezpiecznego i świadomego używania internetu przez dzieci, przygotowany przez Krajowy Organ Ochrony Danych i Wolności Informacji na Węgrzech (NAIH). Publikacja ma na celu promowanie odpowiedzialnego korzystania z Internetu przez dzieci z uwzględnieniem ochrony przewidzianej w sferze praw podstawowych. Więcej informacji oraz inne wersje językowe dostępne są po linkiem: http://www.naih.hu/adatvedelemr-l-fiataloknak--kulcs-a-net-vilagahoz--projekt.html.

Niniejszy poradnik oferuje praktyczne wskazówki oraz narzędzia do nauczania dzieci i młodzieży uczęszczających do szkół w Europie o ochronie danych osobowych i prywatności. W jasny i przystępny sposób porusza on kwestie takie jak prawa podmiotowe osób, których dane dotyczą, bezpieczeństwo cyfrowe, tożsamość cyfrowa, reklama behawioralna, cyberbullying czy kontrola rodzicielska. Nauczyciele i eksperci w zakresie edukacji znajdą w tym poradniku nie tylko precyzyjnie wyjaśnione kluczowe zagadnienia, ale również pomysły do dyskusji, ćwiczenia oraz przydatne wskazówki, dostosowane do różnych kategorii wiekowych i poziomów nauczania, jak również wyróżnione plany lekcji. Ekspertom w dziedzinie ochrony danych osobowych i prywatności, w tym organom nadzorczym, poradnik oferuje nowe metody nauczania o prywatności oraz - bardziej ogólnie - podnoszenia wśród dzieci i młodzieży świadomości w tym zakresie. Poradnik ten zamykają: Mini-Karta Praw do Prywatności i Ochrony Danych Osobowych, słowniczek i przydatne źródła.

Publikacja niniejsza stanowi pierwszy tak kompleksowy poradnik tego rodzaju o zasięgu europejskim. Jest owocem skoordynowanych prac prawników oraz specjalistów z organów ochrony danych. Przygotowana w ramach projektu „Wprowadzenie kwestii związanych z ochroną danych i prywatnością do szkół w Unii Europejskiej" (ARCADES), współfinansowanego w ramach programu Unii Europejskiej Prawa Podstawowe i Obywatelstwo, stanowi rezultat wspólnych wysiłków wszystkich partnerów projektu – Biura Generalnego Inspektora Ochrony Danych Osobowych (GIODO), Rzecznika Informacji Republiki Słowenii (IPRS), Krajowego Organu Ochrony Danych i Wolności Informacji (NAIH, Węgry) oraz Grupy Badawczej ds. Prawa, Nauki, Technologii i Społeczeństwa (LSTS) na Vrije Universiteit Brussel (VUB).

Co-funded by
the European Union



ISBN 978-94-000-0768-0