KAMIL ŚLIWOWSKI, MICHAŁ "RYSIEK" WOŹNIAK

Prywatność w edukacji

KAMIL ŚLIWOWSKI
MICHAŁ „RYSIEK" WOŹNIAK

Prywatność w edukacji

WSTĘP

Czy można zapewnić powszechny, równy dostęp do edukacji wszystkim ludziom na świecie? Prawdopodobnie to zadanie będzie przerastać ludzkość jeszcze przez lata, ale robimy postępy. Jednym z nich było odkrycie i wykorzystanie potencjału internetu do maksymalnie otwartego, wolnego i taniego dostępu do wiedzy, często wcześniej zamkniętej w okowach fizycznych budynków uniwersytetów i bibliotek. Błyskawiczny rozwój edukacji w sieci ma jednak również konsekwencje, których nie przewidywano na początku, np. rozwoju usług i modeli biznesowych, które będą bazować na ogromnym zapotrzebowaniu na edukację prowadzoną w internecie. Te zaś często kopiują, na dobre i złe, komercyjne rozwiązania i wartości, które nie pasują do idei otwartej edukacji. Jednym z takich narastających konfliktów jest zarabianie na danych o osobach korzystających z usług edukacyjnych. Jakie granice powinniśmy sobie wyznaczać tworząc usługi i produkty edukacyjne, które będą dbać nie tylko o sprawiedliwy dostęp do edukacji, ale również o prawo do prywatności swoich odbiorców? Na co zwracać uwagę wybierając takie usługi jako rodzic, nauczyciel/ka, uczeń/nica? Poniższy przegląd, jak mamy nadzieję, trochę w tym pomoże.

NOWE TECHNOLOGIE W EDUKACJI

Cyfrowa Szkoła to nie tylko dobra nazwa dla programu rządowego, w ramach którego powstają cyfrowe, otwarte podręczniki, a do szkół trafia nowoczesny sprzęt. Ta nazwa dobrze oddaje zmianę praktyk jaka zachodzi we współczesnej edukacji, zarówno po stronie zachowań uczniów jak i działań podejmowanych przez nauczycieli i szkoły.

Internet i kwestia zbierania i przetwarzania danych o uczniach wkraczają do szkół na dwa różne sposoby:

- oddolnie, często nie planowane na poziomie systemowym, wykorzystywanie powszechnie dostępnych narzędzi przez uczniów i nauczycieli w codziennej pracy (np. prowadzenie komunikacji między nauczycielami a uczniami za pomocą Facebooka lub innych sieci społecznościowych, wykorzystywanie darmowych platform edukacyjnych takich jak Khan Academy, gier i serwisów do publikacji treści),
- odgórnie, poprzez wykorzystywanie w szkole w planowany sposób platform edukacyjnych i systemów zarządzania szkołą (np. e-dzienniki).

Dodatkowo, o czym nie można zapominać, w szkole co raz powszechniejsze jest wykorzystywanie urządzeń podłączonych do sieci, co ułatwia obu powyższym wariantom zbieranie jeszcze większej ilości danych.

W dyskusji nad wdrażaniem nowych technologii w szkole zdecydowanie dominują argumenty wychwalające zarówno jej wykorzystywanie jak i eksperymentowanie z nowymi technologiami. Można się z tym zgodzić, ale wyłącznie pod warunkiem, że ich stosowanie będzie objęte rygorystyczną ochroną dobra uczniów, do której należy zaliczyć ochronę ich danych osobowych, wolność od profilowania i komercyjnego wykorzystywania takich danych i bezpieczeństwo tych danych.

PRYWATNOŚĆ W KONTEKŚCIE NOWOCZESNYCH TECHNOLOGII

„Prywatność umarła", „jeśli nie masz nic do ukrycia, nie masz się czego bać" usłyszeć można z ust apologetów cyfrowej rewolucji, często opierających się w swojej działalności właśnie na luźnym podejściu do prywatności.

I do pewnego stopnia mają rację. Żyjemy w czasach wszędobylskiej technologii, komunikujemy się w coraz większym stopniu w sposób zapośredniczony, tym samym (chcąc, nie chcąc) dając dostęp do naszej komunikacji pośrednikom i ich partnerom biznesowym. Trzymamy informacje o naszych kontaktach i kalendarzu w urządzeniach i usługach, nad którymi nie mamy i nie możemy mieć kontroli.

Darmowe na pierwszy rzut oka usługi wydają się wspaniałym narzędziem, pozwalającym rozszerzyć ofertę edukacyjną, urozmaicić lekcje, dać dostęp do lepszych zasobów. Czego ich operatorzy oczekują w zamian?

Bardzo często danych (osobowych i innych), które potem są przetwarzane, a na ich podstawie budowane są profile psychologiczne wykorzystywane m. in. w marketingu (w tym politycznym).

Sieć natomiast nie zapomina. Dane raz w niej umieszczone nie są możliwe do usunięcia. Wrzucając dane do Sieci, tracimy *de facto* nad nimi kontrolę, czy raczej: oddajemy ją komu innemu. Mniejsza, jeśli jest to nasza własna, suwerenna decyzja. Co jednak jeśli jesteśmy do niej przymuszeni faktem, że większość naszej grupy używa konkretnej sieci społecznościowej? Czy powinniśmy zgadzać się na taką formę presji?

Czy — z drugiej strony — mamy prawo taką presję wywierać?

BIG DATA W EDUKACJI

Termin *big data* (którym opisuje się duże i różnorodne zbiory danych) wkroczył również do edukacji. Podobnie jak w innych obszarach życia gdzie dane o ogromnych grupach ludzi pozwalają na skuteczniejsze oraz bardziej ekonomiczne zarządzanie usługami oraz sprzedażą produktów, tak w edukacji termin ten odnosi się głównie do komercyjnej oferty dla publicznych systemów edukacji oraz dużych sieci szkół. Nawet specjaliści korporacji oferujących takie rozwiązania dostrzegają spore zagrożenia dla prywatności uczniów.

Jedną z podstawowych cech *big data* jest częsta przypadkowość zakresu danych i sytuacji ich zbierania, co powoduje, że w obszarze edukacyjnym zbierane i przetwarzane mogą być danymi nadmiarowymi, osobowymi i prywatnymi. Posiadanie i przetwarzanie takich danych, zwłaszcza w scentralizowany sposób, podatne jest na dużą liczbę zagrożeń technicznych oraz o charakterze nadużyć ich wykorzystywania.

W Stanach Zjednoczonych, gdzie branża ta rozwija się najprężniej, jedynie 7 procent dystryktów (najmniejszych jednostek terytorialnych, które odpowiadają również za szkoły publiczne), które mają umowy z różnymi dostawcami edukacyjnych usług sieciowych (w tzw. chmurze) ogranicza możliwość sprzedaży i komercyjnego wykorzystania przetwarzanych przez firmy danych uczniów[1].

ŚLEDZENIE UCZENIA — *LEARNING ANALITYCS*

Analiza danych edukacyjnych rozwija się w ostatnich latach błyskawicznie, powstają nawet firmy specjalizujące się wyłącznie w tym zagadnieniu. Zbieranie i analizowanie danych na temat postępów w nauce w celu optymalizacji procesu nauczania i usprawniania działania samych serwisów edukacyjnych, występuje dziś na porządku dziennym.

W większości przypadków jest to w pełni uzasadnione i bardzo pozytywne. Niestety niesie za sobą również ogromne ryzyko związane zarówno z bezpieczeństwem danych jak i wykorzystaniem ich wbrew pierwotnym celom.

Skala zbieranych danych pozwala już nie tylko na optymalizację, ale wręcz profilowanie odbiorców, co może grozić pogłębianiem występującego powszechnie w sieci zjawi-

[1] *Privacy and Cloud Computing in Public Schools*, Fordham University School of Law, 2013, dostęp online http://law.fordham.edu/center-on-law-and-information-policy/30198.htm.

ska tzw. *filter bubble* czyli otrzymywania wyłącznie informacji i wyników wyszukiwania utwierdzających nasze poglądy i zainteresowania.

Mimo deklarowania przez większość twórców chęci przeciwdziałania temu zjawisku, właśnie poprzez wykrywanie w wyniku analizy danych obszarów czy kompetencji, które warto dodatkowo rozwijać u konkretnych uczniów, to należy pamiętać, że sama taka możliwość może być wykorzystywana wbrew poglądom, a co najważniejsze wolnemu wyborowi uczniów.

Jak zaś pokazują nam problemy ze zbieraniem i analizą danych w innych obszarach niż edukacja, nawet same metadane i informacje statystyczne pozwalają na identyfikowanie pojedynczych osób.

Aby wykorzystać dobrodziejstwo danych w edukacji trzeba zadbać o odpowiednie organicznie ich zakresu, dostępu do nich oraz możliwości ich wykorzystania i tego jak będą mogą wpływać na cały proces nauczania. Nie bez znaczenia pozostaje również problem tego kto takie dane będzie posiadał (czy pozostaną po kontrolą uczniów i instytucji edukacyjnej), czy będą w rękach instytucji, które mogą je wykorzystywać komercyjnie lub sprzedać.

Nawet deklaracje takich ograniczeń w regulaminach aktualnie dostępnych usług nie dają nam zwykle gwarancji, że warunki te nie zmienią się w przyszłości.

URZĄDZENIA

Nasze dane w sieci nie biorą się znikąd. Informacje o sobie musimy jakoś dostarczyć lub ktoś musi je o nas zebrać. W szkole, zwłaszcza tej coraz bardziej cyfrowej, nie jest to żaden problem, ponieważ powszechniejsze staje się używanie komputerów i urządzeń przenośnych (smartphony, tablety). Niegroźne same w sobie, mogą niestety zasilać problemy związane z ochroną danych i prywatnością.

Po pierwsze, zwłaszcza urządzenia przenośne, wyposażone są w stałe połączenie z siecią oraz masę czujników (np. lokalizacji GPS, żyroskopy etc.), które można świetnie i ciekawie wykorzystać na lekcji np. podczas eksperymentów. Mogą być jednak wykorzystywane, co próbują wprowadzać już niektóre szkoły w USA i Wielkiej Brytanii, do śledzenia uczniów. Z racji na kontrolę szkoły nad sprzętem dostarczanym uczniom istnieje również ryzyko, że szkoła lub dostawca przygotują sprzęt w sposób, które będzie takie śledzenie ułatwiać, mimo woli i wiedzy uczniów i ich opiekunów. Do takiej sytuacji doszło w amerykańskim dystrykcie Merion[2], który zamówił (z dostępnej oferty) dla swoich szkół laptopy z możliwością zdalnego uruchamiania kamerek. Szybko funkcja ta doprowadziła do poważnych naruszeń prawa prywatności uczniów i ich rodzin. Skandal w Merion jest jednak poważnym ostrzeżeniem nie tylko przed ludzką skłonnością do nadużywania narzędzi kontroli, ale również przed pozornie niegroźnymi decyzjami systemowymi (takimi jak zamówienie sprzętu i oprogramowania). Zwłaszcza nauczyciele i rodzice powinni być wyczuleni na ochronę praw i wolności swoich podopiecznych.

Poza komputerami i telefonami szkoły dysponują również wieloma innymi narzędziami technicznymi, które mogą być poważnym naruszeniem prywatności uczniów. Na czele listy stoją powszechnie montowane w imię poprawy bezpieczeństwa, kamery. Niestety, jak dowodzi większość badań, nie osiągają one zamierzonego efektu, wręcz przeciwnie wzmagają niektóre problemy, przesuwając je do innych obszarów i obniżając poczucie wspólnej odpowiedzialności za bezpieczeństwo[3].

Czasem możemy usłyszeć również o eksperymentach w szkołach z takimi technologiami jak śledzenie uczniów przez nadawanie im identyfikatorów lub ubrań z czipami RFID lub innymi rozwiązaniami pozwalającymi na śledzenie ich w przestrzeni. Warto zadać sobie poważne pytanie czy funkcją szkoły jest posiadanie pełnej kontroli nad uczniami, czy jednak edukowanie ich i tłumaczenie świata w jakim funkcjonują, również wtedy kiedy popełniają błędy lub wagarują. Próba zabezpieczenia szkoły i uczniów za wszelką

[2] Robbins v. Lower Merion School District, http://en.wikipedia.org/wiki/Robbins_v._Lower_Merion_School_District.

[3] *Życie wśród kamer. Przewodnik*, Fundacja Panoptykon, 2013, dostęp online https://zycie-wsrod-kamer.panoptykon.org/.

cenę za pomocą analizy każdego ich kroku (lub zapytania w wyszukiwarce) to ucieczka dorosłych przed odpowiedzialnością i bezpośrednim kontaktem i rozmową z dziećmi o zagrożeniach. Tylko te zaś są w stanie uczyć młode osoby zarówno odpowiedzialności za siebie, innych oraz dbania o swoją wolność oraz prawa.

JAK NIE WPAŚĆ W *FILTER BUBBLE* CZYLI RYZYKA INFORMACJI SKROJONYCH POD ODBIORCĘ

Jednym z kluczowych niebezpiecznych zjawisk informacyjnych występujących w sieci i przenoszących się z łatwością do edukacji jest „bańka informacyjna" po angielsku zwana *filter bubble*. Nie jest to zjawisko nowe, ale na zmiany w tym jak współcześnie poszukujemy i dostarczamy sobie informacji, znacznie silniejsze w sieci niż w okresie dominacji mediów tradycyjnych. Najsilniej zjawisko to uwidacznia się w wynikach wyszukiwania, które w przypadku największych dostawców tej usługi są bardzo silnie personalizowane i profilowane na bazie naszych wcześniejszych zapytań, podobieństw z innymi osobami oraz zapytań osób z nami związanych lub do nas podobnych.

Negatywnym efektem bańki informacyjnej jest odcinanie nas od informacji nowych, wychodzących poza zakres naszych standardowych zainteresowań lub poglądów. Klasycznym już przykładem jest porównywanie wyników wyszukiwania osób z dwóch różnych krajów na temat Egiptu, gdzie mieszkaniec Egiptu lub krajów z tego regionu otrzyma najnowsze informacje dotyczące polityki i aktualnych konfliktów natomiast mieszkaniec USA lub Europy jedynie informacje turystyczne. Konsekwencje takiego zjawiska w edukacji są niestety jeszcze groźniejsze, ponieważ mogą nie tylko kształtować określone poglądy lub wiedzę, ale również uniemożliwiać rozwój i przełamywanie barier edukacyjnych związanych z płcią, pochodzeniem oraz dotychczasową wiedzą i poglądami.

Źle konstruowane usługi edukacyjne oraz wykorzystanie w edukacji powszechnie dostępnych narzędzi już teraz narażonych na to zjawisko (najpopularniejsze wyszukiwarki internetowe) może działać w dwie strony. Wykluczać pewne informacje dla określonych osób np. nie proponować wyników związanych z nauką programowania dziewczynom lub błędnie proponować innym np. podawać informacje na temat sportu niezainteresowanym nim chłopcom.

KOMERCJALIZACJA EDUKACJI

Problemy o których wspominaliśmy wcześniej, zwłaszcza te, które wynikają z narastającej ilości danych zbieranych w edukacji oraz coraz powszechniejszej obecności podłączonego do sieci sprzętu w szkole, mają jedną wspólną cechę. Nie jest ona zła w sama w sobie, ale obserwowany dziś brak ograniczeń i publicznych regulacji, które by sobie z nią radziły powoduje, że jest to jedno z największych zagrożeń dla systemu edukacji. Mowa tu o komercjalizacji systemu edukacji oraz podporządkowywaniu go zasadom rynkowym bez odpowiedniego zabezpieczenia interesu uczniów, rodziców i nauczycieli.

W Polsce zaburzenie takiej równowagi mogliśmy zaobserwować w 2013 roku — wyniki kontroli kuratorium w Katowicach pokazały masowe zjawisko przyjmowania prezentów przez dyrektorów szkół od wydawców w zamian za wybór konkretnych podręczników. W przypadku współpracy szkół z komercyjnymi podmiotami dostarczającymi sprzęt komputerowy lub usługi sieciowe ryzyka są jeszcze większe. Poza korupcją i walką o kontrakty dla szkół, które są świetnymi, masowymi i stałymi klientami, razi nierówność sił między podmiotami komercyjnymi a szkołami czy instytucjami państwowymi odpowiadającymi za zamówienia dla szkół. Po stronie edukacji brakuje kompetencji do oceny oraz negocjacji warunków korzystnych zarówno dla uczniów jak i całego systemu edukacji. Czy będzie to zagwarantowanie możliwości serwisowania i modyfikowania zakupionego sprzętu bez konieczności opłacania kolejnych licencji jego producentom czy odpowiednie zabezpieczenie przetwarzanych przez komercyjny podmiot danych uczniów.

W przypadku Polski należy pamiętać, że prawo do edukacji oraz równe szanse w dostępie do niej zagwarantowane są w konstytucji, a celem systemu oświaty nie jest zysk, a realizacja tych zadań. Zarówno Państwo jak i podmioty komercyjne działające w ob-

szarze edukacji, muszą o tym pamiętać kierując się najpierw dobrem uczniów, a dopiero potem kalkulacją finansową.

KTO POWINIEN MIEĆ DOSTĘP DO DANYCH?

Ograniczenie ryzyk związanych z przetwarzaniem danych uczniów zależy od wielu czynników technicznych, ale również proceduralnych i osobowych. Z racji na wrażliwość danych generowanych podczas procesu nauczania, dostępność ich dla osób trzecich powinna być wyjątkowo dokładnie ograniczona i kontrolowana. Przykładowo dostępność danych o problemach w nauczaniu powiązana z danymi osobowymi powinna być dostępna wyłącznie dla nauczycieli danego ucznia czy uczennicy, natomiast poza szkołą dane te powinny zostać zanimizowane tak by mogły być wykorzystywane wyłącznie w celach statystycznych.

Należy pamiętać, że szeroki dostęp do danych to nie tylko problem ewentualnego ich wycieku czy ujawnienia, ale również wykorzystania przeciw osobom, których dotyczą. Jest to zagrożenie związane zarówno z czynnikiem ludzkim (np. dyrektor będący w konflikcie z uczniem nadużywający informacji o nim) lub wykorzystaniem komercyjnym (firma posiadająca dane i dbająca o nie może w pewnym momencie być zmuszona sytuacją finansową do sprzedania ich firmie, która nie będzie już tak samo respektować prawa do prywatności uczniów).

KIEDY DOJDZIE DO WYCIEKU DANYCH...

Prawdopodobieństwo wycieku danych rośnie wraz z ilością (i, co za tym idzie, wartością!) danych składowanych w jednym miejscu. Podobnie jak duże sumy pieniędzy zgromadzone w jednym miejscu stanową łakomy kąsek dla ewentualnych włamywaczy, tak duże ilości danych przyciągają uwagę osób i organizacji, które mogą chcieć się na nie połasić.

Czy zatem dane u dużych dostawców, mogących zapewnić lepsze procedury bezpieczeństwa, są bezpieczniejsze, niż trzymane na własnym serwerze? Niekoniecznie. Również dużym dostawcom zdarzały się poważne naruszenia bezpieczeństwa, a dane u nich przechowywane mogą paść ofiarą włamywaczy szukających czegoś innego.

Podstawową zasadą powinno zatem być przechowywanie minimum danych, zwłaszcza danych prywatnych (jak lokalizacja, imię, nazwisko, czas dostępu do zasobu, itp). Im mniej danych przechowujemy, tym mniej danych może potencjalnie wycieknąć i tym mniejsza ich wartość (a zatem i pokusa).

UZALEŻNIENIE OD USŁUG

Rozwiązania „chmurowe" przyniosły nową wersję starego zjawiska *vendor lock-in*. *Vendor lock-in* to przywiązanie do rozwiązań jednego dostawcy, pozostawiające klienta na jego pastwie. Doskonale znane ze świata oprogramowania każdemu, kto jeszcze parę lat temu próbował zmienić pakiet biurowy, zjawisko to uzyskało z „chmurą" zupełnie nowy wymiar: dawniej trudność polegała na konieczności ustalenia, jak dany plik jest zbudowany, dziś — użytkownik może w ogóle nie mieć dostępu do samego pliku!

Buduje to uzależnienie od jednego usługodawcy, od konkretnej usługi. Uzależnienie to ma wymiar tak technologiczny (polegający na technicznej trudności zmiany usługi), jak i psychologiczny (przyzwyczajenie jest drugą naturą człowieka, nawet małe różnice w interfejsie i sposobie działania usługi wydają się czasem nie do przeskoczenia).

Oczywiście dostawcy usług wykorzystują to do swoich celów. Tym ważniejsze jest świadome podejmowanie decyzji dotyczących wyboru konkretnej usługi i jej dostawcy. Rozwiązania oparte na wolnym oprogramowaniu budują najmniej tego rodzaju barier.

MOBILNOŚĆ NASZYCH DANYCH

Wybór usługi nie powinien być jednorazowy i nieodwołalny. Musi istnieć możliwość zmiany dostawcy w wypadku, w którym usługa stanie się zbyt droga lub przestanie speł-

niać oczekiwania (w tym te dotyczące zapewnienia bezpieczeństwa danych prywatnych i prywatności samych użytkowników).

By możliwa była zmiana usługi, musi istnieć możliwość wyeksportowania danych i przeniesienia ich do nowego dostawcy lub zaimportowania ich do rozwiązania, które uruchomimy na własne potrzeby. Operacja taka przebiegać powinna w jak największym stopniu automatycznie — im więcej pracy taka migracja będzie wymagała, tym większa jest bariera związana ze zmianą rozwiązania.

Czy zatem dana usługa oferuje eksport danych? W jakim formacie — czy jest to otwarty format, obsługiwany przez wiele różnych rozwiązań, czy też zamknięty format konkretnego producenta rozwiązania? Zamknięty format oznaczać będzie, że możliwość eksportu danych jest czysto iluzoryczna, ponieważ niewiele będziemy mogli potem z nimi zrobić.

PSYCHOLOGICZNE SKUTKI NADZORU

Nadzór ma konkretne skutki psychologiczne. Osoby, które czują się nadzorowane, mniej chętnie próbują nowych rzeczy, zachowują się znacznie bardziej zachowawczo, konformistycznie. Celem staje się nie rzucanie się w oczy, nie odstawanie od średniej. Następuje autocenzura, zarówno w zakresie wyrażanych myśli, jak i podejmowanych działań.

Świadomość, że informacje o jakości prac domowych, wynikach sprawdzianów i kartkówek, oceny semestralne i roczne służyć będą budowaniu profilu psychologicznego i będą nieusuwalne, może zatem negatywnie wpłynąć na uczniów i uczennice korzystające z narzędzi edukacyjnych.

PRYWATNOŚĆ I EKOLOGIA CZYLI O DBANIU NIE TYLKO O SIEBIE, ALE RÓWNIEŻ O NASZE OTOCZNIE

Ostatecznie, prywatność jest też kwestią pewnej ekologii — moje wybory wpływają na możliwości wyboru innych w moim otoczeniu i *vice versa*.

Mogę nie mieć konta na danym portalu społecznościowym, ale jeśli moi znajomi wrzucają tam moje zdjęcia, podpisujące je moim nazwiskiem i opisując, co przedstawiają, podejmują za mnie decyzję o udostępnieniu wizerunku i informacji, których mogę nie chcieć udostępniać.

Mogę nie mieć ochoty zakładać konta na danym portalu społecznościowym, ale gdy okazuje się, że koło naukowe, do którego chcę należeć, czy mój nauczyciel, publikują bieżące informacje wyłącznie tam — wszak przecież „każdy ma konto" na tej czy innej, popularnej w danym momencie sieci społecznościowej — zmuszony jestem do dokonania trudnego wyboru między moją prywatnością, a możliwością korzystania z danej oferty edukacyjnej. I tak zgoda na warunki świadczenia usługi przez jakiś koncern stają się warunkiem koniecznym do korzystania z konstytucyjnego prawa do edukacji.

Pamiętajmy, że co trafi do sieci, już z niej nie zniknie. Podejmowanie za kogoś takiej decyzji lub wywieranie takiej presji (nawet nieświadomie!) nie powinno być częścią procesu edukacyjnego.

USŁUGI BEZ WYJŚCIA

Ochrona danych i prawa do prywatności uczniów (oraz nauczycieli) zależą niestety coraz częściej nie tylko od ich indywidualnych wyborów, ale od tego z jakich usług korzystali oni lub szkoła wcześniej. Podobnie jak w wypadku uzależniania się od jednej usługi indywidualnie, szkoły, a czasem nawet całe państwo i jego system edukacyjny potrafi dokonać wyboru, który utrudni lub uniemożliwi mu zmiany w przyszłości (np. nie pozwalając zabrać i przenieść danych do innego systemu).

Wielu dostawców usług i produktów adresowanych do szkół oferuje im darmowe lub o obniżonych cenach rozwiązania, które będą wymuszać na dalszych etapach zakup kolejnych lub znacząco podwyższać koszty zmian dostawcy usługi. Przykładem takiego działania jest dostarczenie za darmo lub taniej sprzętu np. tabletu, którego aktualizacje

lub rozbudowa o nowe aplikacje może odbywać się wyłącznie pod kontrolą pierwotnego dostawcy. Często modele te są jednak bardziej zaawansowane i opierają się na podnoszeniu kosztów zmiany, a nie jej całkowitemu uniemożliwianiu. Ważnym problemem stojącym na przeszkodzie przezwyciężaniu takich sytuacji jest siła przyzwyczajenia. Nawet jeśli inne rozwiązanie mogło by być lepsze dla szkoły (np. pod względem ochrony danych), to często pozostaje się przy rozwiązaniach gorszych, ale już znanych. W takich sytuacjach należy próbować osobom decydującym o wyborze rozwiązań technicznych dla szkoły przedstawiać efekty długofalowe uzależnienia od takich usług oraz pozytywne efekty początkowej inwestycji, np. w doszkolenie lub przeznaczenie dodatkowych zasobów czasowych na przyzwyczajenie się do nowych rozwiązań.

Klasycznym przykładem dyskusji o kosztach początkowych zmiany rozwiązania technicznego na bardziej elastyczne jest Linux w szkołach. Choć większość osób kojarzy go z czymś trudniejszym od systemów komercyjnych takich jak Windows, to w szkołach, które go wybrały sprawdza się dzięki szybko przerastających inne systemy możliwościach. Niestety ograniczeniem dla jego wdrożenia często są stereotypowe dyskusje o trudnościach nauczenia się nowego systemu. System edukacji nie powinien się jednak bać uczenia rzeczy nowych.

Tekst opracowany na podstawie:

Materiał powstał dzięki wsparciu Open Society Institute.

Redakcja techniczna: Paulina Choromańska