

Twoje dane – Twoja przyszłość

8 grudnia 2014

Choć uczymy się całe życie, tylko w szkole – jeszcze jako osoby niepełnoletnie – dostajemy od reszty społeczeństwa czas i częściowe przyzwolenie na popełnianie błędów, eksperymentowanie. Zdobywamy pierwsze doświadczenia, weryfikujemy porady i przestrogi dorosłych, wchodzimy „na próbę” w różne role i tożsamości. Tak było zawsze, ale odkąd przenieśliśmy wiele społecznych interakcji do Internetu, ten etap zaczął nieść ze sobą specyficzne ryzyko. Z jednej strony, stajemy się bardziej podatni na wpływ innych, z drugiej – te młodzieńcze eksperymenty i błędy mogą zostać wykorzystane przeciwko nam w dorosłym życiu. Nic nie zostanie zapomniane.

W sieci roi się od memów, w których starsze (czasem tylko o kilka lat) pokolenie cieszy się, że należało do ostatniego, którego wybryków młodości nie udokumentowały powszechne telefony z aparatami i Internet. Jest to swoisty głos w dyskusji o tym, co zmienia powszechność podłączonych do sieci narzędzi, dzięki którym młodzi mogą się nie tylko komunikować, ale także krzywdzić. Jedno zdjęcie nierozsądnie opublikowane w sieci (lub którego odpowiednio nie zabezpieczyliśmy) potrafi zaszkodzić nam na całe życie. Być może kolejne kryzysy, wywoływane przez wycieki zdjęć z aplikacji, takich jak chmura Apple czy Snapchat, są oznaką pewnego przesilenia i odrodzenia społecznej potrzeby prywatnej komunikacji. To jednak odpowiedź tylko na jeden aspekt bardziej złożonego problemu.

Konsekwencje przeobrażania się systemu edukacji w poligon doświadczalny dla najnowszych technologii – służących zbieraniu, analizie i sterowaniu za pomocą danych – nadal pozostają wielką niewiadomą. Korzystanie z technologii edukacyjnych równa się dziś zbieraniu danych, a dzieci od najmłodszych lat są przyzwyczajane do oddawania informacji o sobie. Dane o każdym zachowaniu uczniów są zbierane w ramach platform, aplikacji edukacyjnych, kursów e-learningowych. W

tzw. learning analytics inwestują największe firmy zarabiające na komercyjnym profilowaniu i reklamach tj. Facebook i Google, a nowe firmy wchodzące na ten rynek należą do najlepiej doinwestowanych. Skąd taka atrakcyjność danych o tempie, efektywności czy stylach uczenia się?

Nowoczesne platformy edukacyjne, takie jak Knowton, inBloom, czy znana też polskim nauczycielom Edmodo, mogą na bazie zbieranych danych budować szczegółowe profile psychologiczne uczniów. Firmy deklarują, że służy to wyłącznie personalizacji procesów nauczania. Co innego wynika jednak z ich „polityk prywatności”, którym kilka miesięcy temu przyjrzało się czasopismo Education Week. Dostawcy najpopularniejszych aplikacji edukacyjnych za pomocą ciasteczek zbierają i przekazują dane zbierane podczas uczenia się w sieci firmom reklamowym.

Niestety, sprzedaż danych i wykorzystywanie ich przez inne firmy to nie jedyne poważne zagrożenie.

Tzw. personalizacja nauczania może nie tylko wspierać edukację i indywidualny rozwój ucznia, ale również zakłócać ten proces. Poprzez odpowiedni dobór informacji spersonalizowane aplikacje zamykają ucznia w bańce informacyjnej, potwierdzając dotychczasowe kompetencje i tok myślenia. Świetnie znamy ten efekt z analizy zjawiska filter bubble w wyszukiwarkach takich jak Google. W systemie edukacji można go wykorzystać do walki politycznej i światopoglądowej. W Polsce znamy ten problem ze wieloletnich sporów o podręczniki lub wprowadzanie takich przedmiotów jak etyka czy edukacja seksualna. O ile jednak brak przedmiotu da się łatwo zauważyć i oprotestować, o tyle dobór zasobów edukacyjnych, które pojawią się na ekranach różnych uczniów, wydaje się prawie niemożliwy do skontrolowania przez nich samych i ich rodziców.

Wreszcie, chmura edukacyjna to technologia wysokiego ryzyka z perspektywy prywatności i bezpieczeństwa danych. Jedną z podstawowych cech tzw. big data – również w obszarze

edukacyjnym – jest częsta przypadkowość zakresu danych i sytuacji ich zbierania co powoduje, że zbiera się i przetwarza dane nadmiarowe, często prywatne i wrażliwe. Dane przetwarzane w scentralizowanych systemach są też zwyczajnie podatne na typowe zagrożenia, takie jak wycieki danych, przy czym ich skala będzie znacznie większa niż gdyby doszło do wycieku z serwera pojedynczej szkoły.

W Stanach Zjednoczonych, gdzie branża edukacyjno-informatyczna rozwija się najprężniej, jedynie 7 procent dystryktów (najmniejszych jednostek terytorialnych w systemie edukacji, które odpowiadają za szkoły publiczne) mających umowy z różnymi dostawcami edukacyjnych usług sieciowych (tzw. chmura) ogranicza możliwość sprzedaży i komercyjnego wykorzystania przetwarzanych przez firmy danych. Oznacza to, że większość szkół i lokalnych władz nie zadało sobie pytania o to, do kogo będą należeć dane uczniów zbierane przez usługi, za które płacą. Podobnych pytań zwykle nie zadają też sobie nauczyciele, którzy do codziennych zadań w szkole wykorzystują popularne narzędzia i portale społecznościowe.

Jeśli chcemy, aby edukacja pozwalała ludziom przekraczać bariery, a nie wzmacniała stereotypy; aby kreatywność rozwijana była w wolny, a nie zaplanowany i zaprogramowany sposób, musimy zacząć stawiać trudne pytania o rolę technologii w edukacji. Danych w procesie edukacji mogą być sensownie wykorzystywane, ale tylko pod warunkiem zadbania o odpowiednie organicznie ich zakresu, zasad udostępniania i możliwości wykorzystania – również w samym procesie nauczania. Nie bez znaczenia pozostaje również to, kto takie dane będzie posiadał: czy pozostaną pod kontrolą uczniów i instytucji edukacyjnej, czy trafią w ręce instytucji, które będą je wykorzystywać komercyjnie.

Autorstwo: Kamil Śliwowski, Katarzyna Szymielewicz

Źródło: [Fundacja Panoptikon](#)

POSTSCRIPTUM

Edukacja w poszczególnych stanach USA bardzo różni się od siebie – również na poziomie skali wdrażanych technologii i zasad, na jakich wpuszcza się do szkół komercyjne przedsiębiorstwa. W niektórych miejscach prowadzi to do radykalnych i eksperymentalnych projektów, które potem zyskują popularność, również poza granicami USA. Ciekawym tego, jak głęboko szkoły i firmy potrafią ingerować w prywatność uczniów, kiedy nie ogranicza ich prawo (aktualne przepisy chroniące dane o uczniach i studentach w USA pochodzą z lat 1970.).