edukacja medialna

Prywatność współcześnie

WIEDZA W PIGUŁCE

Prywatność wiąże się z określoną kulturą, zależy od miejsca i czasu. Trudno ją zdefiniować, jesteśmy jednak świadomi tego, że ją mamy — czujemy to zwłaszcza wówczas, gdy zostanie naruszona. Choć bywa utożsamiana z intymnością, ma znacznie szerszy zakres. Możemy wyróżnić jej cztery sfery: (1) ciała, (2) przestrzeni (pokój, plecak), (3) informacji (ochrona danych osobowych, ochrona wizerunku) oraz (4) komunikacji (poufność komunikacji). W przypadku korzystania z Internetu i nowych technologii mamy najczęściej do czynienia z ingerencją w dwa ostatnie aspekty prywatności.

Problemy związane z ingerencją w prywatność dotyczą nie tylko odległych reżimów. Spotykamy się z nimi codziennie. Rozwój technologii pociąga za sobą coraz to nowe wyzwania: dzisiaj różne podmioty nie tylko gromadzą informacje na nasz temat, ale także zajmują się ich wymienianiem i kojarzeniem. Informacje o obywatelkach i obywatelach są integrowane w centralnych bazach danych prowadzonych przez państwo (m. in. w ramach Systemu Informacji Oświatowej). Na każdym kroku pozostawiasz ślady: poruszając się po sieci, korzystając z karty płatniczej, kart lojalnościowych, karty miejskiej. Twoje rozmowy telefoniczne z przedstawicielami firm są nagrywane.

W przestrzeni publicznej — w banku, w urzędzie, w szkole, a czasem nawet w przebieralni (!) na basenie — otaczają Cię kamery monitoringu wizyjnego (CCTV). W szkołach obok monitoringu pojawiają się karty umożliwiające wejście do budynku, a nawet identyfikatory z chipem RFID. Współcześnie rodzice mogą łatwo zlokalizować swoje dzieci (np. poprzez telefonię komórkową). Choć niektórzy ludzie dzięki tym narzędziom czują się bezpieczniej, nie sposób nie zauważyć, że wyraźnie ingerują one w prywatność.

Istnieją sytuacje, w których ograniczenie prywatności bywa konieczne — możemy do nich zaliczyć na przykład podejrzenie o popełnienie przestępstwa (kontrola korespondencji) czy ochronę zdrowia (obowiązkowe szczepienia). Rozwój nowych technologii sprawia jednak, że ingerencje w prywatność stają się łatwiejsze i częstsze. Niestety, nie zawsze są one uzasadnione. Coraz powszechniejsze wykorzystywanie technologii do nadzoru tłumaczone bywa działaniami na rzecz walki z terroryzmem, naszej wygody czy cudzego prawa do informacji. Warto krytycznie patrzeć na te działania i zwracać uwagę, czy rzeczywiście służą one realizacji założonych celów, a nie na przykład zyskowi prywatnych firm czy zdobyciu popularności wśród wyborców.

Nowe technologie sprawiają również, że ingerencje w prywatność stają się mniej zauważalne i dokuczliwe. To pewnie dlatego czasami nie dostrzegasz w ich wykorzystaniu niczego niewłaściwego. Zastanów się jednak: czy gdyby zamiast kamery CCTV w autobusie komunikacji miejskiej znajdował się obcy człowiek nagrywający Cię przez cały czas trwania podróży, czuł(a)byś się równie komfortowo? Zapewne nie. W czym zatem tkwi różnica? W wykorzystywanym narzędziu.

Prywatność to wartość sama w sobie. Jej naruszenie może oznaczać krzywdę niezależnie od tego, czy wiąże się z realną szkodą, czy też nie, oraz czy zostało dokonane za pośrednictwem nowoczesnych technologii, czy też bez ich wykorzystania. Nie chcemy, by ktoś postronny czytał nasze papierowe listy, e-maile czy SMS-y — nawet wówczas, gdyby miał nikomu nie zdradzić ich treści.

ZADANIA SPRAWDZAJĄCE

Zadanie 1.

Oznacz zdania jako prawdziwe lub fałszywe.

1. Śledzenie aktywności użytkowników w sieci to przykład ingerencji w prywatność z użyciem nowych technologii. [Prawda/Fałsz]
2. Prywatności w sieci nie da się naruszyć, bo w sieci jesteśmy anonimowi. [Prawda/Fałsz]
3. Podejrzenie popełnienia przestępstwa to sytuacja uzasadniająca ingerencję w czyjąś prywatność. [Prawda/Fałsz]
4. Aktywność użytkowników e-booków jest śledzona przez producentów. [Prawda/Fałsz]
5. Walka z terroryzmem to częsty argument, który pada w dyskusji na temat ingerencji w prywatność. [Prawda/Fałsz]

SŁOWNICZEK

- **monitoring wizyjny**: (CCTV), system służący do zdalnego przekazywania obrazu, obejmujący jedną bądź wiele kamer. Wykorzystywany jest przez instytucje publiczne i podmioty prywatne do różnych celów (np. ochrony mienia czy walki z przestępczością). W niektórych krajach budzi spore kontrowersje ze względu na ingerencję w prywatność obserwowanych osób.
- **System Informacji Oświatowej**: (SIO), system baz danych, w których zbierane są informacje na temat uczennic i uczniów, nauczycielek i nauczycieli, szkół i placówek oświatowych oraz innych jednostek wykonujących zadania z zakresu oświaty. Na poziomie ministerstwa gromadzone są dane identyfikacyjne uczniów i uczennic, takie jak PESEL czy miejsce zamieszkania, oraz długa lista innych danych, zbieranych przez całą ścieżkę edukacyjną: od przedszkola do liceum.
- **geolokalizacja**: określenie fizycznego położenia geograficznego osoby i urządzenia telekomunikacyjnego za pomocą systemu GPS lub adresu IP.
- **dane osobowe**: wszelkie informacje dotyczące określonej osoby fizycznej (czyli zidentyfikowanej lub możliwej do zidentyfikowania). Nie mamy do czynienia z danymi osobowymi wówczas, gdy informacja dotyczy instytucji (np. firmy), grupy osób, osoby fikcyjnej (np. postaci literackiej) czy takiej, której nie jesteśmy w stanie rozpoznać. Dane osobowe podlegają ochronie i nie mogą być zbierane bez odpowiedniej podstawy prawnej (np. zgody osoby, której dotyczą).
- **prywatność**: sfera życia człowieka, w którą nie należy wkraczać bez pozwolenia. Ma ona swój aspekt cielesny, terytorialny, informacyjny i komunikacyjny. Prywatność jest chroniona przez prawo (m.in. przez Konstytucję RP i akty prawa międzynarodowego). Ograniczenie prawa do prywatności możliwe jest tylko w określonych sytuacjach (na przykład ze względu na bezpieczeństwo publiczne czy ochronę zdrowia).
- **cyfrowy ślad**: informacje na temat aktywności konkretnych osób w sieci, magazynowane na serwerach dostawców internetu i właścicieli stron. Tworzą go m.in. zdjęcia, informacje o kupionych produktach, nicki, wpisy na blogach, ale również dane, które zostawiamy w sieci mimowolnie, np. adres IP czy informacja o systemie operacyjnym, z którego korzystamy.
- **media społecznościowe**: różnorodne narzędzia umożliwiające użytkownikom internetu rozbudowaną interakcję. W zależności od charakteru tej interakcji wyróżniamy wśród nich fora, czaty, blogi, portale społecznościowe, społeczności gier sieciowych, serwisy crowdfundingowe i wiele innych.

- **ochrona wizerunku**: wizerunek każdej osoby (czyli jej podobizna utrwalona na przykład na zdjęciu bądź filmie) podlega ochronie. Oznacza to, że nie może on być rozpowszechniany bez zgody danej osoby. Są jednak wyjątki. Rozpowszechnianie wizerunku bez zgody jest możliwe na przykład w przypadku: (1) osób powszechnie znanych, jeżeli wizerunek wykonano w związku z pełnieniem przez nie funkcji publicznych, (2) osób stanowiących jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza, (3) osób, które otrzymały zapłatę za pozowanie, chyba że wyraźnie zastrzegły inaczej, (4) osób ściganych listem gończym.
- **RFID**: (ang. Radio-frequency identification), technika, która wykorzystuje fale radiowe do przesyłania danych na odległość. Używana jest w różnego rodzaju narzędziach działających bezstykowo (np. kartach PayPass).

Tekst: Urszula Dobrzańska, scenariusz: Weronika Paszewska, konsultacja merytoryczna: Wojciech Budzisz, Michał "rysiek" Woźniak, Małgorzata Szumańska. Materiał pochodzi z serwisu edukacjamedialna.edu.pl prowadzonego przez Fundację Nowoczesna Polska.

Źródło: http://edukacjamedialna.edu.pl/lekcje/prywatnosc-wspolczesnie/.

Publikacja zrealizowana w ramach projektu „Świadomie i bezpiecznie w świecie mediów i informacji".

Podstawa programowa:

Wiedza o społeczeństwie, IV poziom edukacyjny
Cele kształcenia
IV. Znajomość zasad i procedur demokracji.
VI. Znajomość praw człowieka i sposobów ich ochrony.
VI. Dostrzeganie współzależności we współczesnym świecie.
Treści nauczania
Ochrona praw i wolności.
Socjalizacja i kontrola społeczna.