

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 przebiegalni (!) 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 zdołaniu 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.

POMYŚL NA LEKCJĘ

Zajęcia wprowadzają uczestników i uczestniczki w temat prywatności, ze szczególnym uwzględnieniem ingerencji w prywatność za pośrednictwem nowych technologii. Uczestnicy i uczestniczki zastanowią się, w jakich sytuacjach ograniczenia prywatności są uzasadnione, a w jakich niedopuszczalne.

Cele operacyjne:

Uczestnicy i uczestniczki:

- potrafią wymienić zachowania, które ingerują w ich prywatność;
- potrafią podać przykłady naruszania prywatności z użyciem nowych technologii;
- wiedzą, w jakich sytuacjach ingerencja w prywatność jest uzasadniona;
- rozumieją, dlaczego nowe technologie są wyzwaniem dla prywatności;
- rozumieją, że prywatność powinna być chroniona, nawet jeśli konsekwencje jej naruszenia nie są od razu widoczne;
- potrafią podać przykłady naruszania prywatności poprzez działania różnych instytucji.

Przebieg zajęć

1.

Czas: 10 min
Forma: praca indywidualna
Pomoce: długopisy, **karta pracy**
„Ingerencje w prywatność”

Powiedz, że dzisiaj będziecie zajmować się tematem prywatności. Rozdaj każdej osobie **kartę pracy „Ingerencje w prywatność”**. Poproś o zapoznanie się z instrukcją i wykonanie zadania.

2.

Czas: 10 min
Forma: rozmowa
Pomoce: tablica, kreda, wyniki pracy
z ćwiczenia 1

Zapytaj uczestników, które zachowania uznali za najbardziej ingerujące w ich prywatność. Możesz zapisać je na tablicy. Rozpocznij rozmowę na temat ograniczeń prywatności związanych z wykorzystywaniem nowych technologii.

Pytania, które możesz zadać grupie:

1. Z jakiego powodu te zachowania najbardziej ingerują w Waszą prywatność?
2. Czy można ingerować w naszą prywatność, nawet jeśli nie pociąga to za sobą żadnych konsekwencji? Możesz podać przykład podglądania dla samego podglądania, przeczytania intymnego listu i nie zrobienia nic z tymi informacjami etc. Zwróć uwagę, że prywatność jest wartością, która jest chroniona bez względu na to, czy jej naruszenie ma jakieś skutki.

3. Czy zdarza się, że nie zauważamy ingerencji w prywatność za pomocą nowych technologii? Dlaczego tak się dzieje?
4. W jakich sytuacjach ingerencje w prywatność są dopuszczalne?

3.

Czas: 10 min
Forma: praca w grupach
Pomoce: **materiał pomocniczy**
„Wyzwania dla prywatności”

Podziel uczestników i uczestniczki na 3 grupy (w przypadku dużej liczby uczestników – na 6). Każdej grupie rozdaj tekst z **materiału pomocniczego dla grup „Wyzwania prywatności”**.

Poproś grupy o zapoznanie się tekstami i zastanowienie się nad odpowiedzią na następujące pytania:

- Jakie osoby i instytucje były opisane w tekście?
- Do jakich ograniczeń prywatności odnosi się tekst?
- Jakich argumentów mogą używać podmioty dążące do ingerencji w prywatność? Które z nich są przekonujące, a które nie?
- W jakich sytuacjach ograniczanie prywatności jest uzasadnione, a w jakich niedopuszczalne?

Pytania zapisz na tablicy. Zwróć uwagę, że zadaniem grup będzie później przygotowanie 2–4-minutowej prezentacji.

4.

Czas: 15 min
Forma: prezentacja
Pomoce: wyniki pracy z ćwiczenia 3

Poproś każdą grupę o przedstawienie odpowiedzi na pytania. Każda z grup ma na to 2–4 minuty (w zależności od liczby grup).

Podsumuj, zwracając uwagę na to:

- w jakich sytuacjach ograniczanie czyjejs prywatności jest uzasadnione (podejrzanie popełnienia przestępstwa, bezpieczeństwo narodowe);
- że argument dotyczący bezpieczeństwa bywa nadużywany w dyskusji o ograniczeniach prywatności;
- że w niektórych sytuacjach prywatność jest ceną za wygodę i że od nas zależy wybór między jednym a drugim.

Ewaluacja

Czy uczestniczki i uczestnicy po przeprowadzonych zajęciach:

- potrafią wymienić zachowania, które naruszają ich prywatność?
- potrafią podać przykłady naruszania prywatności z użyciem nowych technologii?
- wiedzą, w jakich sytuacjach ingerencja w prywatność jest uzasadniona?

- rozumieją, dlaczego nowe technologie stanowią wyzwanie dla prywatności?
- rozumieją, że prywatność powinna być chroniona, nawet jeśli od razu nie widać konsekwencji jej naruszenia?
- potrafią podać przykłady naruszania prywatności poprzez działania różnych instytucji?

Opcje dodatkowe

Jeśli masz więcej czasu, ćwiczenie 3 możesz zmodyfikować poprzez rozdanie każdej grupie wszystkich 3 tekstów.

MATERIAŁY

Karta pracy „Ingerencje w prywatność”

Materiał pomocniczy dla grup „Wyzwania prywatności”

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. [rozwiązanie: prawda] [Prawda/Fałsz]
2. Prywatności w sieci nie da się naruszyć, bo w sieci jesteśmy anonimowi. [rozwiązanie: fałsz] [Prawda/Fałsz]
3. Podejrzenie popełnienia przestępstwa to sytuacja uzasadniająca ingerencję w czyjąś prywatność. [rozwiązanie: prawda] [Prawda/Fałsz]
4. Aktywność użytkowników e-booków jest śledzona przez producentów. [rozwiązanie: prawda] [Prawda/Fałsz]
5. Walka z terroryzmem to częsty argument, który pada w dyskusji na temat ingerencji w prywatność. [rozwiązanie: prawda] [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 uczniów 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).

CZYTELNIA

- „Surveillance Camera Man 2”, YouTube [dostęp: 23.06.2013]: <https://www.youtube.com/watch?v=ym7x7twSoqc>.
- Katarzyna Jędruszczak, „Prywatność w różnych kulturach” [dostęp: 23.06.2013]: <http://www.psychologia.net.pl/artykul.php?level=90>.
- Małgorzata Szumańska, Dorota Głowacka, „Nadzór 2011. Próba podsumowania”, Fundacja Panoptikon — Wprowadzenie, s. 3–10 [dostęp: 23.06.2013]: http://www.panoptikon.org/sites/panoptikon.org/files/nadzor2011_raport.pdf.
- David Murakami Wood (red.), „Raport o społeczeństwie nadzorowanym” — Wprowadzenie do społeczeństwa nadzorowanego, s. 5–15 [dostęp: 23.06.2013]: <http://panoptikon.org/sites/panoptikon.org/files/raport-o-spoleszenstwie-nadzorowanym.pdf>.
- David Lyon, „Statystycznie podobny do Breivika”, Gazeta Wyborcza [dostęp: 23.06.2013]: http://wyborcza.pl/1,97738,10030938,Statystycznie_podobny_do_Breivika.html.

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.

Udostępniono na licencji [Creative Commons Uznanie autorstwa - Na tych samych warunkach 3.0](https://creativecommons.org/licenses/by/3.0/).

Źródło: <http://edukacjamedialna.edu.pl/lekcje/ Prywatność-współczesnie/>.

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.

Nowa podstawa programowa:

Etyka, liceum i technikum

Treści nauczania

zna różne kryteria moralnego wartościowania i posługuje się nimi przy wyznaczaniu moralnej wartości czynów.

wykorzystuje pojęcia dyskursu etycznego do analizowania przeżyć, działań i postaw bohaterów powieści, opowiadań, filmów, spektakli teatralnych, gier komputerowych.

wyjaśnia, dlaczego człowiekowi należy okazywać szacunek; kształtuje postawę szacunku wobec każdego człowieka.

podaje przykłady właściwego i niewłaściwego wykorzystywania nowych technologii, w szczególności technologii informatycznych.

identyfikuje i analizuje wybrane problemy moralne związane z postępem naukowo-technicznym (np. problem ochrony prywatności, ochrony praw autorskich, cyberprzemocy, rozwój sztucznej inteligencji, transhumanizm).