**Logo

Description automatically generated**

**­­**

**CSI-COP MOOC: *Twoje prawo do prywatności w Internecie\_v2***

**Obywatelscy Naukowcy badający pliki cookie i zgodność aplikacji z RODO**

**Treść**

**CSI-COP MOOC – kurs edukacji nieformalnej Strona 2**

**Szczegóły kursu Strona 3**

**Krok 1: Prywatność Strona 4**

**Krok 2: Dane Strona 8**

**Krok 3: Śledzenie online Strona 13**

**Krok 4: Prawo do ochrony danych i prywatności Strona 19**

**Krok 5: Narzędzia do ochrony danych i prywatności Strona 23**

**Twoja opinia na temat kursu Strona 27**

**Ocena nauki Strona 28**

**Zostań obywatelskim naukowcem CSI-COP Strona 29**

**Ankieta Strona 30**

### MOOC

Bezpłatny krótki kurs edukacji nieformalnej CSI-COP (masowy otwarty kurs online - MOOC), w którym można wziąć udział poprzez uczestnictwo w warsztatach online, hybrydowych lub osobistych (patrz strona internetowa: https://csi-cop.eu/ w celu uzyskania informacji) lub pracując nad tym dokumentem we własnym zakresie. Ukończenie pięcioetapowego kursu "Twoje prawo do prywatności w Internecie" powinno zająć od 2 1/2 do 3 godzin.

MOOC dotyczy **Twoich danych i Twojego prawa do prywatności w Internecie***.*  Dane w Internecie są gromadzone za pomocą technologii cyfrowych na stronach internetowych i w aplikacjach (programy na urządzenia mobilne). Technologie te obejmują pliki cookie, małe pliki tekstowe umieszczane na komputerach stacjonarnych, laptopach lub urządzeniach inteligentnych (tabletach, telefonach komórkowych) podczas odwiedzania strony w Internecie. Pliki cookie mogą obejmować cyfrowe moduły śledzące, takie jak śledzenie dokładnej lokalizacji urządzenia. Ustawienia aplikacji mogą mieć uprawnienia dostępu do kontaktów, kamery, wiadomości, mikrofonu i innych danych na urządzeniach mobilnych. Lokalizacja urządzenia może osobiście zidentyfikować osobę, która korzysta z urządzenia lub jest jego właścicielem, więc jego śledzenie ma wpływ na ochronę danych i prywatność.

Głównym celem projektu finansowanego ze [środków CSI-COP EU Horizon2020](https://csi-cop.eu/) jest nieformalna edukacja społeczeństwa na temat technologii śledzenia online i sposobów ich odrzucania. Może to prowadzić do tego, że ogół społeczeństwa staje się “naukowcami obywatelskimi". Naukowiec obywatelski (CS) jest członkiem społeczeństwa zaangażowanym w gromadzenie i analizę danych w ramach wspólnego projektu z profesjonalnymi naukowcami. Celem CSI-COP jest zaangażowanie naukowców obywatelskich do przyłączenia się **do zespołu projektowego CSI-COP** w celu zbadania zakresu, w jakim śledzenie jest *domyślnie*w całym Internecie. Ogólne rozporządzenie o ochronie danych (RODO) z 2018 r. zawiera listę kontrolną , na podstawie, której można ocenić zgodność. Zespół CSI-COP uważa, że obywatelskie naukowe podejście jest niezbędne do nawiązania współpracy między obywatelami a naukowcami oraz do zbadania, w jakim stopniu nasze dane są śledzone online za pośrednictwem odwiedzanych przez nas stron internetowych i aplikacji, z których korzystamy.

Dla kogo przeznaczony jest ten kurs?

Ten kurs jest odpowiedni dla każdej osoby w wieku powyżej 18 lat lub uczniów prowadzonych przez nauczyciela, który jest zainteresowany zrozumieniem, w jaki sposób nasze dane są gromadzone w Internecie i za pośrednictwem aplikacji, z których korzystamy. Kurs jest również odpowiedni dla każdej osoby, która chce dowiedzieć się , jak chronić swoją prywatność w Internecie.

Co jest potrzebne do ukończenia tego kursu

Korzystanie ze smartfona, tabletu, laptopa lub komputera z dostępem do Internetu. Możesz również uzyskać dostęp do bezpłatnego Wi-Fi, jeśli jesteś na uniwersytecie lub korzystasz z lokalnej biblioteki. Należy jednak pamiętać, że korzyści płynące z bezpłatnego publicznego Wi-Fi wiążą się z ryzykiem uzyskania przez hakerów dostępu do Twoich danych. Zapoznaj się z informacjami [Kaspersky](https://www.kaspersky.co.uk/resource-center/preemptive-safety/public-wifi-risks) na temat tego, jak uniknąć ryzyka związanego z publiczną siecią Wi-Fi tutaj: <https://bit.ly/3v6thff>

Jeśli korzystasz z Twittera

Zasugerowaliśmy krótki tweet na końcu każdego kroku , który możesz wysłać innym, informując ich, że bierzesz udział w nieformalnym kursie edukacyjnym CSI-COP. Możesz oznaczyć CSI-COP za pomocą [@cop\_csi](https://twitter.com/cop_csi?lang=en) .

**Sprawdź szczegóły** **kursu** **na stronie 3, a następnie wykonaj kroki 1, 2, 3, 4 i 5 ze strony 4.**

Przy każdym z kroków efekty nauki i treść zostaną krótko przedstawione na samym początku. Aby można było uzyskać więcej informacji, nazwiska osób będą podlinkowane do artykułów w Internecie, w każdym kroku kursu. Więcej szczegółów można znaleźć na końcu każdego kroku w sekcji "Dodatkowa lektura".

Aby poprawić swoją naukę i zrozumienie, zwróć uwagę na ***duże pytanie*** w każdym kroku. Spowoduje to, że rozważysz pytanie dotyczące tematu, zanim się o nim dowiesz. Możesz omówić "duże" i inne pytania z rodziną i przyjaciółmi lub porozmawiać z innymi na  [forum](https://csi-cop.eu/forum/) na stronie CSI-COP, jednak musisz najpierw zarejestrować się pod tym linkiem:

<https://csi-cop.eu/citizenscientistlogin/>

Będziesz miał okazję podsumować to czego się nauczyłeś po każdym z kroków poprzez zadania, które Ci w tym pomogą.

Po ostatnim kroku znajdziesz podsumowanie umożliwiające powtórkę całego kursu. Na końcu, po kroku 5, znajdą się również informacje na temat tego, jak dołączyć do zespołu CSI-COP, aby stać się obywatelskim naukowcem badającymi prywatność w Internecie i być mistrzem **prywatności**.

Powodzenia!

**SZCZEGÓŁY KURSU**

|  |  |
| --- | --- |
| **CSI-COP MOOC: kurs samokształcenia w zakresie edukacji nieformalnej** | *Twoje prawo do prywatności w Internecie* |
| **Cele MOOC** | Bezpłatny kurs online CSI-COP został zaprojektowany w **pięciu krokach.**  Ukończenie każdego kroku zapewni Ci wiedzę do podejmowania świadomych decyzji dotyczących Twojego prawa do prywatności w Internecie. Zdobędziesz również umiejętności, które pomogą Ci sprawdzić i zablokować technologie śledzenia w Internecie i aplikacjach na urządzeniach z Androidem (np. Telefon komórkowy lub tablet). Po wykonaniu wszystkich pięciu kroków możesz poprosić o certyfikat edukacji nieformalnej CSI-COP. Następnie możesz przejść od nieformalnego ucznia do zostania obywatelskim naukowcem wolontariuszem, dołączając do zespołu CSI-COP, aby badać zakres, w jakim Twoje dane są śledzone w Internecie (patrz krok 5).  Strona CSI-COP UE: [**https://cordis.europa.eu/project/id/873169**](https://cordis.europa.eu/project/id/873169) |
| **Czego się nauczysz** (*cele nauczania*) | 1. Zdobędziesz wiedzę na temat prywatności przyznanej na mocy kart praw człowieka 2. Zdobędziesz praktyczne umiejętności (*know-how)* potrzebne do odkrywania technologie śledzenia online osadzone w witrynach internetowych i aplikacjach na Androida 3. Odkryjesz, jak zostać obywatelskim naukowcem i jak dołączyć do zespołu CSI-COP, aby zbadać zakres śledzenia online za pomocą cyfrowych technologii śledzenia |
| **Czas trwania kursu** | Ten kurs jest przeznaczony do ukończenia w następujący sposób:   * Wszystkie pięć kroków w jednej sesji, w tym nieformalne uczenie się i zajęcia, w **2 1/2 -3 godziny** * We własnym tempie. |
| **Szczegóły nieformalnej edukacji** | |
| **Tytuł** | *Ochrona Twoich danych* |
| **Cele i podsumowanie** | Warsztaty te są przeznaczone do ukończenia w pół dnia. Możesz jednak rozłożyć naukę poszczególnych kroków czasie, aby dopasować je do swojej dostępności.  W tym warsztacie online uzyskasz kompleksowe zrozumienie różnych aspektów prywatności oraz tego, w jaki sposób odnosi się to do sposobu, w jaki Twoje dane osobowe mogą być wykorzystywane przez strony trzecie w interakcjach online na stronach internetowych i przy użyciu aplikacji. Dowiesz się, jak podejmować świadome decyzje dotyczące swoich danych osobowych i jak sprawdzić przejrzystość w sposobie gromadzenia danych o Tobie. |
| **Czego się nauczysz** - (*efekty nauki*) | **Zamierzone efekty nauki**   1. Opisuję i dyskutuję o różnych aspektach prywatności. 2. Określam i oceniam sposób, w jaki dane osobowe są gromadzone podczas poruszania się po Internecie i korzystania z aplikacji na inteligentnych urządzeniach. 3. Rozumiem prawa do prywatności w celu ochrony naszych danych |
| **Treść kursu** | * Prywatność i jej różne aspekty * Co to są dane osobowe? * W jaki sposób gromadzone są dane osobowe podczas korzystania z Internetu? * Prawo do prywatności (ONZ; UE; RODO) * Ochrona danych w Internecie. |

### Krok 1

|  |  |
| --- | --- |
| Krok 1 Tytuł: | Różne aspekty prywatności |
| Wiedza zdobyta po kroku 1 | Opisz i przedyskutuj różne aspekty prywatności. |
| Temat | Prywatność i jej różne aspekty |
| Wielkie pytanie | *Czy prywatność jest przywilejem czy prawem człowieka?*  Zapytaj Twoją rodzinę i przyjaciół, co myślą o **prywatności**. Możesz zamieścić swoje poglądy na forum CSI-COP tutaj: <https://csi-cop.eu/forum/> - musisz zarejestrować się na stronie przed opublikowaniem na forum, tworząc login tutaj: <https://csi-cop.eu/citizenscientistlogin/> |
| Krótkie podsumowanie | Jan Holvast (2009): "Dyskusja na temat kwestii prywatności jest tak stara jak ludzkość".  [Patrz dalsza sekcja lektury dodatkowej na końcu kroku 1] |
|  |  |
| Treści edukacyjne | **Krótka historia "prywatności"**  Według Jana Holvasta (2009) "Dyskusja na temat kwestii prywatności jest tak stara jak ludzkość. Zaczynając od **ochrony ciała i domu**, wkrótce **ewoluowała** w **kierunku kontrolowania swoich danych osobowych**. "  Obraz zawierający tekst, zrzut ekranu, elektronikę, komputer  Opis generowany automatycznie  W 1890 roku Warren & Brandeis napisali: "To, że jednostka powinna mieć pełną ochronę osobistą i własnością, jest zasadą tak starą jak prawo zwyczajowe", a "w bardzo wczesnych czasach prawo dawało lekarstwo tylko na fizyczną ingerencję w życie i własność". Dodali, że "teraz [w 1890 r.] prawo do życia zaczęło oznaczać [...] prawo do bycia pozostawionym samemu sobie", a "termin "własność" rozrósł się do każdej formy posiadania – zarówno niematerialnego, jak i materialnego".  W 2011 roku Nissenbaum poinformował, że "Rok 2010 był wielkim rokiem dla prywatności w Internecie. Doniesienia o gafach prywatności, takich jak te związane z Google Buzz i kapryśną polityką prywatności Facebooka, zdobiły pierwsze strony znanych mediów informacyjnych. W swojej serii "**On What They Know**" The Wall Street Journal skupił się na szalejącym śledzeniu osób z powodu reklamy behawioralnej i innych powodów.  Jeśli chodzi o *etykę prywatności*, Marijn Sax (2018) "koncentruje się na pytaniach takich jak: "**Jaka jest wartość prywatności?** " oraz ***"*Jakie normy prywatności powinny być przestrzegane przez jednostki (w tym nas samych), społeczeństwo i państwo?** "  10 kwietnia 2022 r. brytyjski komik John Oliver w swoim programie HBO "Last Week Tonight" zwrócił "uwagę na szkody wyrządzane przez 'brokerów danych', którzy przechwytują i łączą nasze internetowe 'cyfrowe okruchy danych', aby nas zdeanonimizować i sprzedawać nasze dane stronom trzecim" (Guardian, 11 kwietnia 2022 r.). Oliver poinformował, że brokerzy danych są "częścią wielomiliardowego przemysłu", który "zbiera Twoje dane osobowe, a następnie odsprzedaje je lub udostępnia innym" za pomocą "głównych narzędzi jakimi są pliki cookie, które umożliwiają stronom internetowym zapamiętanie Ciebie i ewoluowały tak, aby uwzględnić pliki cookie stron trzecich, które śledzą, co jeszcze robisz w Internecie". (Guardian). Powrócimy do plików cookie w kroku 3.  **Google Chrome**  Niektórzy z Was mogą korzystać z trybu ***incognito*** przeglądarki Google Chrome, aby zachować swoją prywatność. Wygląda jednak na to, że Google "potajemnie zbiera mnóstwo danych internetowych, nawet jeśli użytkownicy przeglądają w trybie "Incognito", aby zachować prywatność swojej aktywności wyszukiwania. (Nayak i Rosenblatt, 2021). Artykuł prasowy Bloomberg 2021 donosi, że "Konsumenci złożyli sprawę jako "pozew zbiorowy", twierdząc, że "nawet gdy wyłączają gromadzenie danych w Chrome, inne narzędzia Google używane przez strony internetowe gromadzą ich dane osobowe" (Nayak i Rosenblatt, 2021). Możesz dowiedzieć się więcej o tej sprawie na nowej stronie Bloomberga tutaj: <https://bloom.bg/3gFt4vV>  **Naruszenie prywatności danych 533 milionów użytkowników Facebooka**  Być może słyszałeś ostatnie wiadomości, że bez względu na to, jak bardzo staramy się zachować naszą informację w pewnym stopniu prywatną, jeśli korzystamy z mediów społecznościowych, jesteśmy do dyspozycji właściciela platformy i jego kompetencji zabezpieczania naszej prywatności. Dane **osobowe ponad 530 milionów użytkowników Facebooka zostały znalezione na hakerskiej stronie internetowej w kwietniu 2021** r. (Holroyd, 2021 r.). Dane osobowe 533 milionów obejmują użytkowników Facebooka w następujących krajach:   * Ponad 35 milionów we Włoszech * Ponad 32 miliony w USA * Prawie 20 milionów kont we Francji * 11 milionów użytkowników w Wielkiej Brytanii oraz * 6 milionów użytkowników w Indiach.   Lomas (2021) informuje, że zrzut informacji, które użytkownicy Facebooka udostępnili na tej platformie, obejmuje:   * Identyfikatory Facebooka * Imiona i nazwiska * Numery telefonów * Lokalizacje * Daty urodzenia * Niektóre adresy e-mail   Możesz przeczytać więcej na [TechCrunch](https://techcrunch.com/2021/04/06/answers-being-sought-from-facebook-over-latest-data-breach/?guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAMUOIlLG_dSDm7w74IG-14xWYBlW6py7Mv17hgb8XiPn2uZ7Dkrhgu4A0krDDh0ttvoqMkev6D_h7Man-RtR7mMGNmk5i1_oayagVtIi3W8g3McHb1cTXnWDGzLr9fUa3u1DIYa3yMFn1UCx2zMqgcF9J0G_2nP_mU6aSU41mLXG&guccounter=2).  Jeśli jesteś użytkownikiem Facebooka i chcesz dowiedzieć się, czy Twoje informacje są zawarte w tym naruszeniu danych, możesz to sprawdzić za pomocą poczty e-mail lub za pomocą naszego identyfikatora Facebooka lub numeru telefonu na tych stronach:   * [Czy zostałem pwned?](https://haveibeenpwned.com/)  Tutaj: <https://haveibeenpwned.com/> * [Czy zostałem zucked?](https://haveibeenzucked.com/)  Tutaj: <https://haveibeenzucked.com/>   Możesz także śledzić tweety [The Real Facebook Oversight Board](https://twitter.com/FBoversight) "odpowiedzialność Facebooka" na Twitterze tutaj: <https://twitter.com/FBoversight>  Być może słyszałeś nazwisko Frances Haugen. Jest analityczką danych i byłą pracowniczką Facebooka. Haugen zeznawała przed Senatem USA 5 października 2021 r., przed brytyjskim parlamentem 25 października 2021 r. i przed Parlamentem Europejskim w dniu 8 listopada 2021 r. Haugen ujawniła przewagę strategii zysku nad dobrem użytkowników Facebooka (przeczytaj więcej o propagowaniu Frances Haugen na rzecz "odpowiedzialności i przejrzystości w mediach społecznościowych" na jej stronie internetowej: https://www.franceshaugen.com/).  Irlandzka Komisja Ochrony Danych "nałożyła grzywnę w wysokości 17 milionów euro na Meta Platforms Ireland Limited za serię naruszeń danych w okresie od 7 czerwca 2018 r. do 4 grudnia 2018 r." (https://bit.ly/3MmUIKN ).  Christopher Wylie, były analityk danych w Cambridge Analytica i autor książki z 2019 r. "MindF\*ck: Inside Cambridge Analytica's Plot to Break the World" stwierdza: Facebook ma zbyt dużą niekontrolowaną moc" (strona 225).  W 2021 Roku Sąd Okręgowy USA Southern District of New York wytoczył powództwo cywilne: Google Digital Advertising Antitrust. Paragraf 175 na stronie 64 dokumentu sądu amerykańskiego stanowi:  "Google prezentuje publiczny wizerunek troski o prywatność, ale za kulisami ściśle koordynuje działania z dużymi firmami technologicznymi, aby lobbować rząd w celu opóźnienia lub zniszczenia środków, które faktycznie chroniłyby prywatność użytkowników" (Civil Action no.: 1:21-md-03010-PKC dokument dostępny na courtlistener.com).  Carissa Veliz, autorka książki "Prywatność to potęga" z 2020 roku, ostrzega:   * + Internet jest finansowany przede wszystkim przez gromadzenie, analizę i handel danymi ... gospodarka oparta na danych" (str. 1)   + "Wiele z tych danych to dane osobowe – dane o Tobie" (strona 1)   + " ... inteligentny telefon .... Nagrywanie swojej podróży i tego, jak długo zostałeś..." (strona 2)   + "Gospodarka danych i wszechobecna inwigilacja, którą się zasila, zaskoczyła nas" (strona 2)     Czego możesz się spodziewać w kolejnych krokach  W następnym kroku zaczniemy szukać *danych* i *danych osobowych*.  W kroku 3 przyjrzymy się *, w jaki sposób śledzone są nasze dane*.  W kroku 4 przyjrzymy się, jakie *mamy prawa do naszej prywatności*  W ostatnim kroku tego kursu, kroku 5, dowiemy się o *narzędziach online*, których możemy użyć, aby lepiej zabezpieczyć *naszą prywatność i chronić nasze dane*.  Zbadaj swoją wiedzę  Podsumuj to, czego nauczyłeś się w kroku 1, z pomocą pytania oraz zadań poniżej. |
| Podsumuj wiedzę | Co to jest *prywatność* ? |
| Zadanie | **Zadanie 1**  Czy poniższe stwierdzenie jest prawdziwe czy fałszywe?  "Dyskusja na temat prywatności jest nowa od czasu wynalezienia Facebooka".  **Zadanie 2:**  Omów koncepcję prywatności z rodziną, przyjaciółmi, sąsiadami lub współpracownikami.  Czego dowiedziałeś się o swoim własnym rozumieniu prywatności i spojrzeniu innych ludzi na prywatność?  Przypomnienie: możesz zamieścić swoje poglądy na forum csI-COP tutaj: <https://csi-cop.eu/forum/> - musisz zarejestrować się na stronie przed opublikowaniem na forum, tworząc login tutaj: <https://csi-cop.eu/citizenscientistlogin/> |
| Cel zadania | Zdobądź wiedzę na temat różnych *aspektów prywatności*. |
| Krótki tweet | Czy wygoda powinna mieć większe znaczenie niż prywatność w dobie mobilnego dostępu do Internetu? |

|  |  |
| --- | --- |
| Dodatkowa lektura | Linki do dalszej lektury wymienione w kroku 1 można znaleźć, wybierając podkreślony tekst poniżej:  **Zalecane**  Lomas, N. (2021). *Odpowiedzi poszukiwane od Facebooka w związku z najnowszym naruszeniem danych*. TechCrunch Dostępny stąd: <https://tcrn.ch/3xfrTsE>  Nayak, M. i Rosenblatt, J. (2021).  *Google musi zmierzyć się z podsłuchiwaniem przeglądania "incognito"*  Technologia Bloomberg. Dostępne stąd: <https://bloom.bg/3gFt4vV>  Konto Real Facebook Oversight Board na Twitterze @FBoversight dostępne tutaj: <https://twitter.com/FBoversight>  **Dodatkowo**  Holroyd, M. (2021). Irlandia wszczyna dochodzenie w sprawie ochrony danych w sprawie włamania na Facebooka. *Euronews – Irlandia*. Dostępne stąd <https://bit.ly/3mOfIOM>  Holvast, J. (2009). Historia prywatności. W: V. Matyáš et al. (Eds.): *The Future of Identity*, IFIP AICT 298, s. 13–42, 2009. Międzynarodowa Federacja Przetwarzania Informacji IFIP 2009. Dostępne z ResearchGate: <https://www.researchgate.net/publication/225802214_History_of_Privacy>  Nissenbaum, H. (2011 r.). Kontekstowe podejście do prywatności w Internecie. *Dædalus*, *Journal of the American Academy of Arts & Sciences*, Vol 140, No. 4 (jesień 2011), s. 32-48. Dostępne stąd: <https://www.amacad.org/publication/contextual-approach-privacy-online>  Guardian (2022). John Oliver o Data Brokers: To, co mogą kupić, jest dość niepokojące. Guardian Culture. 11 kwietnia 2022 r.: <https://bit.ly/3wzX0j3>  Sax, M. (2018 r.). Prywatność z etycznego punktu widzenia. Rozdział w B. Van der Sloot & A. De Groot (red.), *The Handbook of Privacy Studies: An Interdisciplinary Introduction* (str. 143-173). Amsterdam: Amsterdam University Press. Dostępne z tego linku: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3299047>  Warren, S.D. & Brandeis, L.D. (1890). Prawo do prywatności*.*  *Harvard Law Review*, vol. 4, no. 5. (15 grudnia 1890), s. 193-220. Dostępne od: [Prawo do prywatności na JSTOR](https://www.jstor.org/stable/1321160?origin=crossref&seq=1#metadata_info_tab_contents) |

### Krok 2

|  |  |
| --- | --- |
| Krok 2 Tytuł: | Data i dane osobowe |
| Wiedza zdobyta po kroku 2 | Opisz i przedyskutuj różne aspekty prywatności. |
| Temat | Co to są dane osobowe? |
| Wielkie pytanie | *Dlaczego miałbym się przejmować tym, kto ma dostęp do moich danych, nie mam nic do ukrycia?*  Zapytaj rodzinę i przyjaciół, co sądzą o swoich danych. Swoje poglądy na [forum](https://csi-cop.eu/forum/) CSI-COP możesz zamieszczać tutaj: <https://csi-cop.eu/forum/> - musisz zarejestrować się na stronie przed opublikowaniem na forum, tworząc login tutaj: <https://csi-cop.eu/citizenscientistlogin/> |
| Krótkie podsumowanie | Andreas Weigend (2017): "Za każdym razem, gdy coś wygooglujemy, Facebook kogoś, Uber gdzieś, a nawet po prostu włączamy światło, tworzymy dane, które zbierają firmy".  [Patrz dalsza sekcja lektury dodatkowej na końcu kroku 2] |
|  |  |
| Treści edukacyjne | **Co to są dane?**  Podsumowanie: w kroku 1 zostaliśmy wprowadzeni w pojęcie "prywatności"  W kroku 2 nieformalnego kursu edukacyjnego CSI-COP zrozumiesz, "czym są dane” i "jakie dane o Tobie” są zaangażowane w różne aspekty Twojego życia online: od zakupów online po wysyłanie wiadomości do znajomych, po wyszukiwanie informacji.  Pojedynczą formą "danych" jest datum:   * pojedynczy kawałek *jakości* lub *ilości* o czymś   Dane to liczba mnoga (więcej niż pojedynczy element):   * Punkty informacyjne, na przykład *dane o Tobie,* takie jak   1. Jeśli jesteś studentem, niezależnie od tego, czy jesteś studentem "home" , czy studentem zagranicznym   Data urodzenia  Kwalifikacje do uzyskania miejsca na uniwersytecie  Stały adres, adres czasowy  Numer kontaktowy  Dane są wszędzie i są przechowywane w wielu formach:   * *Nieustrukturyzowane*:   1. Rozważ filmy z YouTube   2. Sprawdź zdjęcia na Instagramie   3. Czytanie wiadomości e-mail   4. Zdjęcia satelitarne   5. Dane pogodowe * Strukturalne:   1. Numer legitymacji studenta/pracownika – ciąg cyfr   2. Numer NHS lub ubezpieczenia społecznego   3. Rezerwacje linii lotniczych   dane ustrukturyzowane a dane nieustrukturyzowane  Źródło: <https://bit.ly/2PhkKHa>  Z Irwin (2021): "W pewnych okolicznościach za dane osobowe można uznać dowolne z poniższych *danych:*":   * 1. Imię i nazwisko   2. Adres domowy   3. Adres e-mail   4. Numer dowodu osobistego   5. Dane o lokalizacji   6. Adres ip (Internet Protocol)   7. Identyfikator reklamowy telefonu   **Dane osobowe to dane, które identyfikują "naturalną" (żyjącą) osobę.**    Pat Walshe z "**Privacy Matters"** mówi: "Używamy naszych smartfonów i komputerów jak nigdy dotąd, aby wykonywać połączenia, wysyłać osobiste SMS-y i zdjęcia, wysyłać wiadomości do ludzi za pośrednictwem usług WhatsApp lub Snapchat, robić zakupy online w poszukiwaniu żywności lub leków, dzielić się osobistymi fragmentami naszego życia w mediach społecznościowych, wyszukiwać informacje na temat zdrowia psychicznego lub fizycznego, polityki, religii lub miejsc do odwiedzenia, przeglądać strony internetowe, wystawiać opinie i wskazywać nasze upodobania i antypatie. Bycie cyfrowym tworzy bogactwo danych o nas, często osobistych i wrażliwych. Dane, które mogą pozwolić innym poznać nas lepiej niż my znamy siebie" ([Privacy Matters](https://twitter.com/privacymatters?lang=en)).  Możemy **dobrowolnie przekazywać dane**, gdy składamy zamówienie online lub rezerwujemy wizytę zdrowotną. Dane o nas i naszych urządzeniach oraz naszym zachowaniu online mogą być **przechwytywane i obserwowane** (takie jak odwiedzane przez nas strony internetowe, piosenki, których słuchamy lub filmy, które oglądamy, rodzaj urządzenia, z którego korzystamy, nasze lokalizacje - niezależnie od tego, czy zdajemy sobie z tego sprawę, czy nie). Dane można uzyskać z profilowania i analizowania informacji o nas (takich jak nazwa użytkownika, która słuchała utworu lub oglądała film online, kategoria utworu lub filmu, w którym momencie osoba wstrzymała utwór lub film, wraz z datą i godziną, kiedy wstrzymała i ponownie uruchomiła lub zrezygnowała z słuchania lub oglądania, lokalizacja, w której się znajdowali (przynajmniej kraj) - dane, które są czymś w rodzaju cyfrowego cienia działań online ([Privacy Matters](https://twitter.com/privacymatters?lang=en)).  Oprócz danych osobowych. Istnieją również **wrażliwe dane osobowe**. Zgodnie z ogólnym rozporządzeniem o ochronie danych (RODO), o którym dowiemy się więcej w kroku 4, **wrażliwe dane osobowe** w ramach RODO mogą obejmować dane, które ujawniają:   * pochodzenie rasowe lub etniczne * wierzenia religijne * poglądy polityczne * członkostwo w związkach zawodowych.   Wrażliwe dane osobowe obejmują również dane dotyczące zdrowia danej osoby (na przykład psychicznego lub fizycznego); dane dotyczące życia seksualnego lub orientacji seksualnej danej osoby; dane genetyczne; dane biometryczne (wykorzystywane do jednoznacznej identyfikacji osoby) oraz dane dotyczące wyroków skazujących i przestępstw ([Privacy Matters](https://twitter.com/privacymatters?lang=en)).  Brodkin (2021) poinformował w kwietniu 2021 roku, że T-Mobile:   1. "... rozpocznie nowy program, który wykorzystuje niektóre dane, które mamy o Tobie" 2. "*w tym informacje, których uczymy się z danych o korzystaniu z Internetu i urządzenia* (takich jak aplikacje zainstalowane na urządzeniu)" 3. "oraz interakcje z naszymi produktami i usługami dla naszych własnych i 3stron reklamowych, chyba że powiesz nam, że tego nie robimy".   Jak się czujesz, jeśli Twój operator telefonii komórkowej poinformował Cię , że będzie działał jak T-Mobile? A jeśli korzystasz z T-Mobile, w jaki sposób ich oświadczenie sprawia, że czujesz się z gromadzeniem i wykorzystywaniem Twoich danych?    Czego możesz się spodziewać w kolejnych krokach  W następnym kroku (Krok 3) zaczniemy sprawdzać *, w jaki sposób śledzone są nasze dane.*  W kroku 4 przyjrzymy się, jakie *mamy prawa do naszej prywatności*  W ostatnim kroku tego kursu, kroku 5, dowiemy się o *narzędziach online*, których możemy użyć, aby lepiej zabezpieczyć *naszą prywatność i chronić nasze dane*.  Zbadaj swoją wiedzę  Podsumuj to, czego nauczyłeś się w kroku 2, z pomocą pytania oraz zadań poniżej. |
| Podsumuj wiedzę | Co to są *dane osobowe*? |
| Zadanie | **Ćwiczenie 1: krótki test**  Które z poniższych nazw odnoszą się do danych osobowych?   * Leonardo da Vinci * Prezydent Joe Biden * Freddie Mercury * Królowa Elżbieta II * Alan Turing * Meghan Markle * Albert Einstein * Papież * Kim Kardashian   Odpowiedź na Krok 2 Działanie 1 zostanie udzielona w Kroku 3.  **Działalność 2**  Wyszukaj i obejrzyj wykłady TED, na przykład, Tech-socjolog, **Zeynap Tufekci's** TED Global NYC talk, wrzesień 2017:  "**Budujemy dystopię tylko po to, aby ludzie klikali reklamy**".  Przypomnienie: możesz opublikować swoje poglądy na forum CSI-COP tutaj: <https://csi-cop.eu/forum/> - musisz zarejestrować się na stronie przed opublikowaniem na forum, tworząc login tutaj: <https://csi-cop.eu/citizenscientistlogin/> |
| Cel zadania | Dowiedz się *, czym są dane osobowe.* |
| Krótki tweet | Stwierdzenie: "Nie mam nic do ukrycia, więc nie obchodzi mnie, kto ma dostęp do moich danych" jest błędne |

|  |  |
| --- | --- |
| Dodatkowa Lektura | Linki do dalszej lektury wymienione w kroku 2 można znaleźć, wybierając podkreślony tekst poniżej:  **Zalecane**  Brodkin, J. (2021).  *T-Mobile sprzeda Twoje dane dotyczące korzystania z Internetu reklamodawcom, chyba że wyrazisz na to zgodę*.  arsTECHNICA. Dostępne stąd: <https://bit.ly/3sUdkaQ>  Irwin, L. (2021). *Dane osobowe a dane wrażliwe: jaka jest różnica?* Zarządzanie IT. Dostępne stąd: <https://bit.ly/3vhoRlX>  Privacy Matters na Twitterze: @PrivacyMatters:<https://twitter.com/privacymatters?lang=en>  Książka, którą być może znajdziesz w lokalnej bibliotece  Weigend, A. (2017). *Dane dla ludzi: jak sprawić, by nasza ekonomia post-prywatności działała dla Ciebie*. Podstawowe książki: Nowy Jork |

### Krok 3

|  |  |
| --- | --- |
| Krok 3 Tytuł: | Technologie śledzenia online |
| Wiedza zdobyta po kroku 3 | 1: Zapisz i omów różne aspekty prywatności.  2. Określam i oceniam sposób, w jaki dane osobowe są gromadzone podczas nawigacji po Internecie i korzystania z aplikacji na inteligentnych urządzeniach |
| Temat | W jaki sposób gromadzone są dane osobowe podczas korzystania z Internetu? |
| Wielkie pytanie | *Jakie szkody mogą wyrządzić technologie śledzenia online?*  Zapytaj rodzinę i przyjaciół, co sądzą o swoich danych. Swoje poglądy na [forum](https://csi-cop.eu/forum/) CSI-COP możesz zamieszczać tutaj: <https://csi-cop.eu/forum/> - musisz zarejestrować się na stronie przed opublikowaniem na forum, tworząc login tutaj: <https://csi-cop.eu/citizenscientistlogin/> |
| Krótkie podsumowanie | Nigel Warburton (2020): "Bez twojej zgody ... Firmy technologiczne zbierają twoje dane – twoją lokalizację, twoje upodobania, twoje nawyki, twoje lęki, twoje choroby, twoją politykę – i dzielą się nimi między sobą.  [Patrz dalsza sekcja lektury dodatkowej na końcu kroku 3] |
|  |  |
| Treści edukacyjne | **W jaki sposób informacje o Tobie są gromadzone w Internecie**  Podsumowanie tego, czego nauczyliśmy się w poprzednich dwóch krokach:   * W kroku 1 zostaliśmy wprowadzeni w pojęcie "prywatności" * W kroku 2 dowiedzieliśmy się, że "dane osobowe" odnoszą się do osoby fizycznej (żyjącej)   W tym kroku dowiemy się o różnych narzędziach online, które zbierają dane podczas korzystania z Internetu.  Menedżer produktu, Eliza Crawford (2020) informuje nas, że **powodem, dla którego dane o Tobie są gromadzone** w Internecie, jest **nauczenie się, jak się zachowujesz podczas odwiedzania strony internetowej**. Ma to na celu "**uzyskanie wglądu w to, jak [...] klienci korzystają ze stron internetowych "w celu zapewnienia spersonalizowanego doświadczenia online i zarabiania na użytkowniku poprzez wyświetlanie im ukierunkowanych reklam**. "  Wyjaśniając, dlaczego występuje śledzenie online, Crawford (2020) mówi:   * "Kiedy szukasz restauracji w Google, a usługa zapewnia listę restauracji w Twojej okolicy, to dlatego, że wyszukiwarka wie, gdzie się znajdujesz. " * "Kiedy sklep e-commerce pokazuje listę polecanych produktów, wie, co lubisz, ponieważ śledził przedmioty, które oglądałeś lub kupiłeś wcześniej. "   Pat Walshe (Privacy Matters) przypomina nam, że **dane behawioralne** mogą obejmować:   * Twoje dane **przeglądania stron** internetowych - odwiedzane strony internetowe, data i godzina wizyty, kraj, z którego odwiedziłeś (wywnioskowane z Twojego adresu IP - unikalny ciąg znaków, który identyfikuje każde urządzenie łączące się z Internetem i który jest automatycznie wysyłany podczas odwiedzania strony internetowej). Weź również pod uwagę, że kiedy opuścisz witrynę, będą w stanie powiedzieć, którą witrynę odwiedzasz jako następną, a następna odwiedzana witryna może być w stanie powiedzieć, z której witryny pochodzisz. Wszystko to byłoby uważane za dane behawioralne przeglądania stron internetowych. * **zachowanie w strumieniu kliknięć** – dane o interakcjach danej osoby na stronie internetowej, które mogą obejmować to, co klikają, przewijają i dotykają na ekranie dotykowym * **wyszukiwarki** , takie jak Google, które mogą gromadzić i wykorzystywać informacje o tym, czego szukasz, jakie wyniki klikasz, Twój adres IP i które mogą używać unikalnego identyfikatora pliku cookie do śledzenia Ciebie. * **lokalizacja** – lokalizacja i rodzaj odwiedzanego miejsca (supermarket, kasyno, miejsce kultu, szpital) lub miejsce, w którym korzystałeś z aplikacji, daty i godziny, przebyta trasa, częstotliwość wizyty lub trasy, które podróżujesz. Dane o lokalizacji mogą być bardzo [odkrywcze](https://www.fastcompany.com/3068846/how-your-location-data-identifies-you-gilad-lotan-privacy) i behawioralne. * **historia** **zakupów** – może to obejmować rodzaje subskrypcji (członkostwo w związkach zawodowych, siłownia, gazety itp.), Rezerwacje hoteli lub restauracji, które mogły zostać dokonane w ramach [wyszukiwania, map, inteligentnych asystentów](https://myaccount.google.com/purchases?pli=1) lub bezpośrednio od sprzedawców detalicznych lub usług stron trzecich itp. * **dane** **dotyczące płatności lub** "[transakcyjne"](https://medium.com/the-capital/what-you-dont-know-about-transactional-privacy-but-you-should-d0072941d050) – płatności, które ujawniają, komu/jakiej organizacji zapłaciłeś (które mogą ujawnić rodzaj organizacji - klinikę medyczną, aptekę, dostawcę alkoholu; sprzedawcę żywności, księgarza itp.) oraz ile, kiedy i jak często. Dobrym przykładem są płatności kartą typu "dotknij i idź" – pomyśl o kawie, którą kupujesz na początku podróży, miejscu, dacie i godzinie, w której za nią zapłaciłeś, a następnie o płatnościach dokonywanych później w ciągu dnia tą samą kartą. * **media strumieniowe** – "[jesteś tym, co streamujesz](http://assets.ctfassets.net/ziwa9xqm84y1/CFPSdMWTrtrhdD8iVHIcy/b136bd5e622c52675ec7e0b7dbde4625/Spotify_Media_Kit_2018_-_CA.pdf)" i "[Oni wiedzą, co oglądałeś wczoraj wieczorem](https://www.nytimes.com/2019/10/25/business/media/streaming-data-collection-privacy.html)". Media strumieniowe generują **wiele** danych behawioralnych na temat:   + data i godzina uzyskania dostępu do usługi strumieniowego przesyłania muzyki, dźwięku lub telewizji/filmu oraz nieprecyzyjna lokalizacja (poziom kraju lub regionu), z której uzyskano do niej dostęp   + jaki profil uzyskał dostęp do usługi i z niej korzystał (nazwa + kategoria np. dziecko)   + kategoria muzyka, audiobook, telewizja/film (np. horror polityczny, dorosły)   + wyszukuje treści   + czy wstrzymano utwór lub film i na jak długo (w tym datę (daty i godziny)   + czy pominąłeś/porzuciłeś utwór lub ścieżkę dźwiękową z filmu z odcinka telewizyjnego   + czy udostępniasz treści i z kim oraz jakie są Twoje interakcje z innymi osobami w ramach usługi   + czy oceniłeś utwór, program TV lub film   + playlisty lub listy obserwowanych, które tworzysz   + urządzenie używane do uzyskania dostępu do usługi oraz adres IP i identyfikatory urządzeń * **Dane dotyczące aktywności/zdrowia** – dane dotyczące korzystania z aplikacji aktywności, takich jak jazda na rowerze, bieganie, chodzenie lub dane dotyczące zdrowia, takie jak dane uzyskane za pośrednictwem aplikacji dietetycznych lub aplikacji na płodność. Dane te mogą być bardzo odkrywcze i często mogą być powiązane na przykład z Twoją lokalizacją. * **Wykres mediów społecznościowych –** dane ujawniające powiązane ze sobą relacje społeczne między ludźmi i ich naturą oraz wzorce komunikacji   Badanie przeprowadzone przez Ghostery (2017) "ujawniło, że trackery, które zbierają dane na temat zachowań użytkowników Internetu w Internecie, są obecne na co najmniej 79 procentach stron internetowych (unikalnych domen) na całym świecie. Śledzenie w sieci stało się tak wszechobecne, że około dziesięciu procent stron internetowych wysyła zebrane dane do dziesięciu lub więcej różnych firm (unikalne domeny trackerów). Jeśli chodzi o ruch w sieci, 15 procent wszystkich wczytywania stron w Internecie jest monitorowanych przez dziesięć lub więcej trackerów. Według badania najbardziej rozpowszechnione są skrypty śledzące z Google (60,3 procent wczytywania stron) i Facebooka (27,1 procent).  **Obraz zawierający ciemny  Opis generowany automatycznie**  To śledzenie odbywa się za pomocą narzędzi cyfrowych:   1. O plikach cookie usłyszeliśmy w kroku 1, z show HBO Johna Olivera z 10 kwietnia 2022 r. "Last Week Tonight" ujawniającego data brokerów. 2. **Pliki cookie**: Pliki cookie to małe fragmenty danych, które strony internetowe przechowują na urządzeniu użytkownika. Witryny często **używają plików cookie do zapamiętywania preferencji użytkownika** i **dostarczania spersonalizowanych doświadczeń, a także do uzyskiwania informacji do celów reklamowych**. Gdy strona internetowa upuści plik cookie na komputerze użytkownika, dostawca plików cookie może nadal uzyskiwać do niego dostęp. W ten sposób witryny mogą używać plików cookie do śledzenia użytkowników od strony do strony lub od witryny do witryny. To, jak długo plik cookie może śledzić użytkownika, zależy od rodzaju pliku cookie. Na przykład Sessional, Persistent, First-party; Strona trzecia (Crawford, 2020). 3. **Fingerprinting**: Odciski palców to forma śledzenia strony internetowej, która **wykorzystuje atrybuty urządzenia lub przeglądarki użytkownika do zbudowania profilu użytkownika**. Informacje, z których korzystają odciski palców , obejmują urządzenie, system operacyjny urządzenia, rozdzielczość ekranu, przeglądarkę i wersję przeglądarki, język i strefę czasową. Crawford (2020) stwierdza: "Sama informacja nie jest tak cenna. Jednakże, gdy wszystko jest połączone, zapewnia niezwykle dokładny sposób identyfikacji użytkowników.  **Electronic Frontier Foundation** ([EFF](https://www.eff.org/)) prowadzi stronę "[zacieraj ślady](https://coveryourtracks.eff.org/)", która testuje przeglądarkę, aby pokazać, jak unikalny jest twój odcisk palca w stosunku do innych, które strona śledziła. " 4. **Śledzenie wiadomości** e-mail: oprogramowanie do śledzenia wiadomości e-mail **umieszcza w wiadomościach e-mail niewidoczny piksel obrazu, który może wykryć dokładną godzinę i datę otwarcia wiadomości e-mail**. Powodem śledzenia wiadomości e-mail jest to, że firmy / sprzedawcy detaliczni itp. oszczędzają czas i uczą się, czy pierwszy e-mail firmy był wystarczająco interesujący, abyś go otworzył. Jeśli nie, może być mało prawdopodobne, że otworzysz przyszłe wiadomości e-mail. Zapobiegając niepotrzebnym wiadomościom e-mail, śledzenie wiadomości e-mail oszczędza czas zarówno przedstawiciela handlowego, jak i odbiorcy wiadomości e-mail. Podobnie, jeśli firma zauważy, że kontakt klika wysłane linki i przegląda list motywacyjny lub załączoną propozycję , firma wie, że jesteś obecnie na szczycie ich umysłów. Dotarcie do Ciebie w tym momencie, kiedy myślisz o ofercie firmy, np. Chcesz kupić odzież sprawia, że rozmowa jest znacznie bardziej istotna i aktualna dla firmy / sprzedawcy.   Badanie Sivan-Sevilla i in. (2020) wykazało, że "firmy, o których być może nigdy nie słyszeliśmy, zbierają punkty danych na temat każdego aspektu naszego życia - naszych zainteresowań, zakupów, stanu zdrowia, lokalizacji i innych". IAB (2019, cytowany w Sivan-Sevilla et al., 2020) "Te punkty danych są następnie łączone w wyjątkowo odkrywcze profile behawioralne, ujawniając intymne części naszej tożsamości i napędzając wielomiliardowy przemysł reklamowy, który twierdzi, że przewiduje, co prawdopodobnie zużyjemy, aby kierować do nas reklamy".  Sivan-Sevilla et al.’s (2020) donoszą ponadto, że gdy reklamodawcy przekraczają informacje o problemach zdrowotnych użytkowników, zainteresowaniach edukacyjnych i nawykach związanych z konsumpcją wiadomości, są w stanie lepiej przewidzieć, kiedy użytkownik może zostać przekształcony w konsumenta i podejmować decyzje zakupowe, których reklamodawcy nie byliby w stanie przewidzieć w inny sposób. Badania wykazały, w jaki sposób dane z różnych stron internetowych są agregowane i wykorzystywane do wnioskowania o demografii i zainteresowaniach użytkowników, narażając ich na praktyki manipulacyjne, które próbują zmusić ich do kliknięcia "właściwej" (spersonalizowanej) reklamy we "właściwym" (spersonalizowanym) czasie ... Branża reklamowa zdefiniowała te momenty jako "**momenty największej wrażliwości konsumentów"** ... w którym użytkownicy są "wyjątkowo otwarci" ...".  Srinivasan (2020) oświeca, że: "Wzrost elektronicznego handlu reklamami, powszechnie znanego dziś jako "reklama programowa", zbiegł się z rozwojem handlu elektronicznego w różnych sektorach gospodarki. wczesna firma zajmująca się technologią reklamową **Right Media** uruchomiła "giełdę reklamową” RMX, **pierwszy w historii elektroniczny system handlu reklamami**. ..... Dziś jedna firma, **Google**, jednocześnie prowadzi wiodącą giełdę, a także wiodących pośredników, z których wydawcy i reklamodawcy muszą korzystać w handlu ... Google nie tylko sprzedaje przestrzeń reklamową należącą do stron internetowych osób trzecich, ale sprzedaje przestrzeń reklamową pojawiającą się na własnych stronach, wyszukiwarce Google i YouTube.  Srinivasan (2020) donosi, że "Biznes reklamowy zmienił się drastycznie w ciągu ostatnich dwóch dekad. Dziś największa kategoria reklamy, reklama internetowa, rzadko jest negocjowana przez ludzi. Postęp technologiczny pozwala na kupowanie i sprzedawanie przestrzeni reklamowej drogą elektroniczną za pośrednictwem scentralizowanych systemów obrotu z dużą prędkością, bez konieczności spotykania się twarzą w twarz. Gdy użytkownik odwiedza witrynę, przestrzeń reklamowa na stronie jest natychmiast kierowana do jednego lub więcej z tych miejsc. Tam przestrzeń jest licytowana w czasie rzeczywistym do licytanta, który zaoferował najwyższą cenę. Po zakończeniu tych aukcji reklamy reklamodawców wracają i wyświetlają się użytkownikowi na czas, aby strona mogła się załadować i zanim użytkownik zauważył, że coś się wydarzyło. Użytkownik widzi tylko reklamy skierowane do niego, na przykład banku Barclays. "  Możesz teraz rozumieć, że wiele danych jest coraz częściej przechwytywanych, obserwowanych i wnioskowanych przez osoby, z którymi masz bezpośredni związek, nie tylko w celu świadczenia podstawowych usług, o które prosisz, ale coraz częściej w celu "personalizacji doświadczeń", niezależnie od tego, czy o nie poprosisz, czy nie, i / lub w celu kierowania reklam na ich stronach internetowych i poza nimi, aplikacjach i usługach. Jednak Twoje dane są nie tylko przechwytywane, obserwowane i wnioskowane przez osoby, z którymi masz bezpośredni związek, ale także przez podmioty zewnętrzne w ekosystemie reklamowym, które mogą być osadzone w odwiedzanych witrynach lub aplikacjach, z których korzystasz, na przykład w celu kierowania do Ciebie [reklam behawioralnych](https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf). Twoje dane mogą być wykorzystywane do obserwowania Cię w Internecie i aplikacjach mobilnych do celów targetowania behawioralnego, takich jak określanie [stawek w czasie rzeczywistym](https://www.outbrain.com/blog/programmatic-advertising/) , które umożliwia reklamodawcom automatyczne ustalanie stawek w czasie rzeczywistym w celu kierowania reklam do osób na podstawie określonych kryteriów – na przykład określonego przedziału wiekowego i płci lub typu urządzenia mobilnego lub lokalizacji.  Tak więc dane o TOBIE mogą być bardzo osobiste, rzeczywiście ujawniając intymne aspekty twojego życia. Może wpływać w sposób, którego nigdy nie brałeś pod uwagę i który narusza Twoje oczekiwania dotyczące prywatności, nie szanując i nie chroniąc Twojej prywatności. Na przykład [stwierdzono, że](https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdfhttps:/fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf) aplikacja Grindr udostępnia informacje "dużej *liczbie stron trzecich*" zaangażowanych w profilowanie i reklamę. Udostępnione dane "*obejmowały adres IP, identyfikator wyświetlania reklam, lokalizację GPS, wiek i płeć*". Doprowadziło to do dochodzenia przeprowadzonego przez norweski organ ochrony danych, który [ukarał](https://www.theguardian.com/technology/2021/jan/26/grindr-fined-norway-sharing-personal-information) Grindr grzywną w wysokości 8,6 miliona funtów (100 milionów koron norweskich).  Wszystkie rodzaje danych omówione powyżej są danymi osobowymi chronionymi przez przepisy o ochronie danych, takie jak RODO i unijne prawo dotyczące prywatności elektronicznej ([dyrektywa o prywatności i łączności elektronicznej](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02002L0058-20091219) "ePD"), które omówimy w następnym kroku 4 nieformalnego kursu CSI-COP. Przepisy te nakładają obowiązki na organizacje sektora prywatnego i publicznego, które przechwytują, obserwują i wnioskują o Tobie dane oraz dają prawa do tego wykorzystania. Ponownie zostanie to omówione w sekcji 4 kursu.  Ale poświęć chwilę i zastanów się, co twoje dane mówią o TOBIE i INNYCH, z którymi jesteś połączony.  Pamiętaj również, że jeśli korzystasz z "darmowego" Wi-Fi, musisz podać informacje o sobie, aby uzyskać dostęp do Internetu. Zobacz obrazek poniżej na temat tego, co jest zbierane.    Czego możesz się spodziewać w kolejnych krokach  W następnym kroku (Krok 4) przyjrzymy się, jakie *mamy prawa do naszej prywatności*  W ostatnim kroku tego kursu, kroku 5, dowiemy się o *narzędziach online*, których możemy użyć, aby lepiej zabezpieczyć *naszą prywatność i chronić nasze dane*.  Zbadaj swoją wiedzę  Podsumuj to, czego nauczyłeś się w kroku 3, z pomocą pytania oraz zadań poniżej. |
| Podsumuj wiedzę | Jakie są różne typy plików cookie?  Co to jest digital fingerprinting?  Jak działa śledzenie poczty e-mail? |
| Zadanie | **Ćwiczenie 1**  W działaniu 1 w kroku 2 poproszono o zidentyfikowanie danych osobowych z listy nazwisk. Ponieważ dane osobowe odnoszą się wyłącznie do osób naturalnych (żyjących). W przypadku osób na liście, które już nie żyją, ich nazwiska nie są danymi osobowymi. Zgadłeś, że słusznie? Sprawdź poniżej:   * Leonardo da Vinci – nie są danymi osobowymi * Prezydent Joe Biden * Freddie Mercury – nie są danymi osobowymi * Królowa Elżbieta II * Alan Turing – nie są danymi osobowymi * Meghan Markle * Albert Einstein – nie są danymi osobowymi * Papież * Kim Kardashian     "Papież" jest interesujący: jeśli wybrałeś to, ponieważ czułeś, że odnosi się to do obecnego żyjącego papieża, to masz rację.  **Zadanie 1**   * 1. Wyszukaj w Internecie różne rodzaje plików cookie, które mogą być osadzone na stronach internetowych   2. Jaka jest różnica między fingerprinting a śledzeniem wiadomości e-mail?   **Zadanie 2**  Rodzina, przyjaciele, sąsiedzi lub współpracownicy zastanawiają się, co rozumiesz przez "***profilowanie zachowań online***" i jak jest ono obsługiwane w Internecie.  **Ćwiczenie 3**  Wypróbuj tę darmową grę online to znajdź, jeśli możesz uniknąć plików cookie:  <https://cookieconsentspeed.run/>    Przypomnienie: możesz opublikować swoje poglądy na forum CSI-COP tutaj: <https://csi-cop.eu/forum/> - musisz zarejestrować się na stronie przed opublikowaniem na forum, tworząc login tutaj: <https://csi-cop.eu/citizenscientistlogin/> |
| Cel dania | Dowiedz się więcej o profilowaniu zachowań online. |
| Krótki tweet | Technologie śledzenia |

|  |  |
| --- | --- |
| Dodatkowa Lektura | Linki do dalszej lektury wymienione w kroku 3 można znaleźć, wybierając podkreślony tekst poniżej:  **Zalecane**  Crawford, E. (2020). Śledzenie witryny: Dlaczego i jak strony internetowe Cię śledzą? Blog CookiePro: Zgodność plików cookie. Dostępne stąd: <https://www.cookiepro.com/blog/website-tracking/>  EFR (brak daty). Fundacja Electronic Frontier. Wiodąca organizacja non-profit broniąca cyfrowej prywatności, wolności słowa i innowacji działająca [od 30 lat!](od%2030%20lat!) Dostępne stąd: <https://www.eff.org/>  Ghostery (2017). 79 procent stron internetowych na całym świecie potajemnie śledzi Twoje dane osobowe. Ghostery. Dostępne stąd: <https://www.ghostery.com/press/ghostery-global-tracking-study/>  Privacy Matters na Twitterze: @PrivacyMatters:<https://twitter.com/privacymatters?lang=en>  **Linki zewnętrzne**  Sivan-Sevilla, I., Chu, W., Liang, X. i Nissenbaum, H. (2020). Nierozliczone naruszenie prywatności: analiza porównawcza trwałej identyfikacji użytkowników w różnych kontekstach społecznościowych. Federalna Komisja Handlu (FTC) PrivacyCon 2020. Papier dostępny on-line za pośrednictwem tego linku: <https://news.cornell.edu/stories/2020/06/study-online-trackers-follow-health-site-visitors>  Srinivasan, D. (2020). Dlaczego Google dominuje na rynkach reklamowych Polityka konkurencji może opierać się na zasadach regulacji rynku finansowego. 24 STAN. TECH. LAW REV. Dostępne stąd: <https://law.stanford.edu/publications/why-google-dominates-advertising-markets/>  Warburton, N. (2020) wewnętrzna okładka książki Véliz, C. (2020). Prywatność to potęga: Dlaczego i jak powinieneś odzyskać kontrolę nad swoimi danymi. Pingwin w twardej oprawie. |

Krok 4

|  |  |
| --- | --- |
| Krok 4 Tytuł: | Twoje prawa do prywatności |
| Wiedza zdobyta po kroku 4 | 1: Opisuję i omawiam różne aspekty prywatności.  2. Określam i oceniam sposób gromadzenia danych osobowych podczas poruszania się po Internecie i korzystania z aplikacji na urządzeniach inteligentnych.  3. Rozumiem prawa do prywatności wynikające z kart w celu ochrony naszych danych. |
| Temat | Prawo do prywatności: Karta praw człowieka ONZ; Karta praw człowieka UE; Ogólne rozporządzenie o ochronie danych |
| Wielkie pytanie | *Jakie mam prawa do prywatności?*  Zapytaj rodzinę i przyjaciół, co sądzą o swoich prawach do prywatności. Swoje poglądy na forum CSI-COP możesz zamieszczać tutaj: <https://csi-cop.eu/forum/> - musisz zarejestrować się na stronie przed opublikowaniem na forum, tworząc login tutaj: <https://csi-cop.eu/citizenscientistlogin/> |
| Krótkie podsumowanie | Karty i przepisy, które obejmują prawa człowieka w odniesieniu do prywatności. |
| Treści edukacyjne | **Prawo człowieka do prywatności**  Podsumowując to, czego nauczyliśmy się do tej pory:   * W kroku 1 zostaliśmy wprowadzeni w pojęcie "prywatności" * W kroku 2 dowiedzieliśmy się, że "dane osobowe" odnoszą się do żywej osoby * W kroku 3 dowiedzieliśmy się o niektórych sposobach przechwytywania naszych danych online (np. za pomocą plików cookie)   Na tym etapie zajmiemy się "prawami człowieka".  Pat Walshe z [Privacy Matters](https://twitter.com/PrivacyMatters) przypomina nam, że "prawa człowieka od dawna mają znaczenie. Na przykład już w [1689](https://www.webarchive.org.uk/wayback/archive/20131031165954/http:/www.bl.uk/onlinegallery/takingliberties/staritemshumanrights.html) roku w Wielkiej Brytanii prawa człowieka były uważane za coś istotnego dla bycia człowiekiem, dla naszej godności i ochrony podstawowych praw i wolności (British Library, 2013). Prawa i wolności, które dziś kształtują różne wymiary naszego życia – offline i online. Od prawa do wyrażania opinii, przez prawo do swobodnego zrzeszania się z innymi i do wolności zgromadzeń, do wolności wyznania, do prawa do edukacji, do prawa do rzetelnego procesu sądowego, do prawa do zawarcia małżeństwa i do **prawa do prywatności**, na przykład. Prawa człowieka mają znaczenie. Codziennie. Offline i online. Pozwalają nam rozkwitać jako istoty ludzkie. "  Prawa człowieka w bardziej współczesnych czasach nabrały globalnego znaczenia w **1948 roku**. W odpowiedzi na okrucieństwa popełnione podczas drugiej wojny światowej, Zgromadzenie Ogólne Narodów Zjednoczonych przyjęło Powszechną Deklarację [Praw Człowieka](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.un.org%2Fen%2Fabout-us%2Funiversal-declaration-of-human-rights&data=04%7C01%7Cab7778%40coventry.ac.uk%7Ccb9af077aa24412296d008d8f1357e72%7C4b18ab9a37654abeac7c0e0d398afd4f%7C0%7C0%7C637524559344161263%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=uA%2B1stRDQLrowoxPVHRcaPjHo%2B0BT4CK0n60J364GWA%3D&reserved=0) (**PDPC**) w celu ochrony podstawowych praw człowieka, które wszyscy ludzie powinni mieć. Obejmuje to ochronę przed arbitralną ingerencją w **prywatność**, **rodzinę**, **dom** lub **korespondencję** danej osoby zgodnie z art. 12 PDPC.  W 1949 r. wiele krajów europejskich utworzyło [Radę Europy](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.coe.int%2Fen%2Fweb%2Fyerevan%2Fthe-coe%2Fabout-coe%2Foverview&data=04%7C01%7Cab7778%40coventry.ac.uk%7Ccb9af077aa24412296d008d8f1357e72%7C4b18ab9a37654abeac7c0e0d398afd4f%7C0%7C0%7C637524559344161263%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=JYIiQpLG0k8JcNGCurBcULLRd2iAd9iwASOg9yPWVOg%3D&reserved=0) (**RE**), która obecnie jednoczy 47 europejskich państw członkowskich.  W **1950** roku Rada Europy przyjęła Europejską Konwencję [Praw Człowieka](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.echr.coe.int%2FPages%2Fhome.aspx%3Fp%3Dbasictexts%26c%3D&data=04%7C01%7Cab7778%40coventry.ac.uk%7Ccb9af077aa24412296d008d8f1357e72%7C4b18ab9a37654abeac7c0e0d398afd4f%7C0%7C0%7C637524559344171219%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=iickwfKhNhJyIxTdU3hZDPYgAeUvGbj0RG1KkT7fPBE%3D&reserved=0) (EKPC), aby chronić nas w przyszłości przed okrucieństwami, takimi jak te popełnione podczas drugiej wojny światowej.  EKPC obejmuje kluczowe prawa zawarte w PDPC i weszła w życie w **1953 r.**  EKPC jest pierwszym **prawnie wiążącym międzynarodowym** instrumentem ochrony praw człowieka. Warto zauważyć, że wszystkie państwa członkowskie Unii Europejskiej (UE) [przystąpiły](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.europarl.europa.eu%2Ffactsheets%2Fen%2Fsheet%2F146%2FEuropean-Union-Charter&data=04%7C01%7Cab7778%40coventry.ac.uk%7Ccb9af077aa24412296d008d8f1357e72%7C4b18ab9a37654abeac7c0e0d398afd4f%7C0%7C0%7C637524559344171219%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=SSGYaHq2HZqUFPSYw%2FxwiNv5P40SeiL0jSwvhBgrIgU%3D&reserved=0) do EKPC.  Artykuł 8 EKPC stanowi, że każdy ma prawo do poszanowania swojego **życia prywatnego i rodzinnego**, **domu** i **korespondencji**. Łatwo zrozumieć, w jaki sposób takie prawo ma chronić intymne aspekty życia danej osoby. Aspekty, które są łatwe do zaobserwowania w Internecie.  Podczas gdy art. 8 EKPC chroni prawo do prywatności, obejmuje również prawo do ochrony danych, biorąc pod uwagę, że wykorzystanie danych osobowych o ludziach wpływa nie tylko na ich prywatność, ale także na inne prawa i wolności, będziemy o tym wspominać w kursie. Aby pomóc w ochronie osób fizycznych oraz ich praw i wolności, a w szczególności prawa do prywatności, w 1981 r. **RE** przyjęła zbiór zasad i przepisów mających zastosowanie do przetwarzania danych osobowych osób fizycznych. Zasady i reguły znane są jako Konwencja 108. Konwencja została niedawno zmodernizowana w celu odzwierciedlenia zmian w technologii i wykorzystaniu danych, które mogą negatywnie wpłynąć na prawa ludzi. Obecnie jest znana jako [Konwencja 108+](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.coe.int%2Fen%2Fweb%2Fdata-protection%2Fconvention108%2Fmodernised&data=04%7C01%7Cab7778%40coventry.ac.uk%7Ccb9af077aa24412296d008d8f1357e72%7C4b18ab9a37654abeac7c0e0d398afd4f%7C0%7C0%7C637524559344181176%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=4%2FyHZ6SiuxCw1AEWj0hVH0gYqGJA%2FbRQxow2%2F1Fazw0%3D&reserved=0)  W **2000** r. UE ustanowiła [Kartę praw podstawowych Unii Europejskiej](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Ffra.europa.eu%2Fen%2Feu-charter&data=04%7C01%7Cab7778%40coventry.ac.uk%7Ccb9af077aa24412296d008d8f1357e72%7C4b18ab9a37654abeac7c0e0d398afd4f%7C0%7C0%7C637524559344181176%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=EWVDDZrcKGqL9KAMEwfgIVTWdQXjtz5dIRfobjVTtkk%3D&reserved=0). Karta stała się prawnie wiążąca dla państw członkowskich UE w 2009 roku. Podobnie jak EKPC, Karta praw podstawowych Unii Europejskiej (**WSO**) stanowi, że każdy ma prawo do poszanowania swojego życia **prywatnego** i **rodzinnego**, **domu** i **komunikowania się** (art. 7). Ponadto Unijna **WSO** stanowi również, że każdy ma prawo do ochrony swoich danych osobowych (art. 8).  Odpowiednio art. 7 i 8 WSO UE przewidują prawo do prywatności i ochrony danych jako dwa odrębne prawa.  Prawa te są wprowadzane w życie przez **instrument o prywatności i łączności elektronicznej** znany jako unijna [dyrektywa o prywatności i łączności elektronicznej](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Feur-lex.europa.eu%2FLexUriServ%2FLexUriServ.do%3Furi%3DOJ%3AL%3A2009%3A337%3A0011%3A0036%3Aen%3APDF&data=04%7C01%7Cab7778%40coventry.ac.uk%7Ccb9af077aa24412296d008d8f1357e72%7C4b18ab9a37654abeac7c0e0d398afd4f%7C0%7C0%7C637524559344181176%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=4Vp99U43lyhjPuhTxYvnTnt81EYIefMk6pnaMHYdfEE%3D&reserved=0) (który ma zastosowanie do plików cookie i innych technik śledzenia online) oraz przez instrument ochrony danych, [ogólne rozporządzenie o ochronie danych](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Feur-lex.europa.eu%2Flegal-content%2FEN%2FTXT%2F%3Furi%3DCELEX%253A02016R0679-20160504%26qid%3D1532348683434&data=04%7C01%7Cab7778%40coventry.ac.uk%7Ccb9af077aa24412296d008d8f1357e72%7C4b18ab9a37654abeac7c0e0d398afd4f%7C0%7C0%7C637524559344191125%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=7C%2FTUWAp1ZxSTjmU2iVp1YX%2FPgDRUVzbcGrR4s2Bg6A%3D&reserved=0) UE (**RODO**). Unijne [przepisy o ochronie danych](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fec.europa.eu%2Finfo%2Flaw%2Flaw-topic%2Fdata-protection%2Feu-data-protection-rules_en&data=04%7C01%7Cab7778%40coventry.ac.uk%7Ccb9af077aa24412296d008d8f1357e72%7C4b18ab9a37654abeac7c0e0d398afd4f%7C0%7C0%7C637524559344191125%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=rR73YvtoWbmgl7AbuGa3PBQSGq43G4KIic1IymmNfSU%3D&reserved=0) i przepisy **RE** zostały wdrożone do prawa państw członkowskich i zostały wzmocnione w celu odzwierciedlenia zmian w technologii i zmian w wykorzystaniu danych. Dzisiaj, gdy ludzie korzystają z telefonów komórkowych lub laptopów itp., Dane o ludziach mogą być gromadzone w czasie rzeczywistym i udostępniane na przykład setkom reklamodawców zewnętrznych, często w sposób, w jaki ludzie nie są naprawdę świadomi lub mają jakiekolwiek znaczący wybór. Dane, które mogą ujawnić aspekty życia prywatnego danej osoby, takie jak jej lokalizacje, nawyki zakupowe, odwiedzane strony internetowe, kim są ich kontakty i ich powiązania społecznościowe.  Brytyjskie Biuro Komisarza ds. Informacji (ICO): "Ogólne rozporządzenie o ochronie danych (RODO) z 2018 **r. zapewnia osobom fizycznym prawo do informacji o gromadzeniu i wykorzystywaniu ich danych osobowych**. **Jest to kluczowy wymóg przejrzystości**" – wyjaśniono na stronie internetowej [ICO](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/) tutaj:<https://bit.ly/2QxmZH1>  Pat Walshe z Privacy Matters stwierdza: "Prawo do prywatności i ochrony danych jest ważniejsze niż kiedykolwiek, ponieważ nasze dane cyfrowe ujawniają głęboko osobiste i intymne aspekty nas samych i tych, z którymi jesteśmy połączeni. "  Tekst, tablica  Opis generowany automatycznie  Czego możesz się spodziewać w kolejnych krokach  W ostatnim kroku tego kursu, kroku 5, dowiemy się o *narzędziach online*, których możemy użyć, aby lepiej zabezpieczyć *naszą prywatność i chronić nasze dane*.  Zbadaj swoją wiedzę  Podsumuj to, czego nauczyłeś się w kroku 4, z pomocą pytania oraz zadań poniżej. |
| Podsumuj wiedzę | **1948r. Powszechna Deklaracja Praw Człowieka (PDPC**): **Artykuł 12**: "Nikt nie może być podmiotem arbitralnej ingerencji w swoją prywatność [...] [lub] korespondencji".  **Karta praw podstawowych Unii Europejskiej z 2000 r.: Artykuł 1**: "Godność ludzka jest nienaruszalna. Musi być szanowana i chroniona".  **Ogólne rozporządzenie o ochronie danych (RODO) z 2018 r. "ustanawia wysoki standard zgody**": Ta ***świadoma*** zgoda obejmuje:   * "oferowanie jednostkom prawdziwego wyboru i kontroli" * "prawdziwa zgoda powinna stawiać jednostki na czele, budować zaufanie i zaangażowanie". |
| Zadania | **Mini quiz** z różnych przepisów.  Czy poniższe stwierdzenia są prawdziwe czy fałszywe?   * UNHR to nowe rozporządzenie przyznające świadomą zgodę. * Dyrektywa o prywatności i łączności elektronicznej dotyczy plików cookie * RODO nie dotyczy przejrzystości.   Przedyskutuj swoje odpowiedzi z rodziną, przyjaciółmi, sąsiadami lub współpracownikami.  Przypomnienie: możesz opublikować swoje poglądy na temat swojej nauki na forum csI-COP tutaj: <https://csi-cop.eu/forum/> - musisz zarejestrować się na stronie przed opublikowaniem na forum, tworząc login tutaj: <https://csi-cop.eu/citizenscientistlogin/> |
| Cel zadania | Porozmawiaj ze swoimi przyjaciółmi, rodziną i sąsiadami o oświadczeniu z 1999 roku od dyrektora generalnego i współzałożyciela Sun Microsystems, Scotta McNealy'ego:  "***I tak masz zerową prywatność .... Pogódź się z tym*** !"  Cytat w Wired:  <https://www.wired.com/1999/01/sun-on-privacy-get-over-it/> |
| Krótki tweet | Prywatność w Internecie nie jest luksusem |

|  |  |
| --- | --- |
| Dodatkowa Lektura | Linki do dalszej lektury wymienione w kroku 3 można znaleźć, wybierając podkreślony tekst poniżej:  **Zalecana lektura**  Biblioteka Brytyjska (2013). Taking Liberties: Walka o wolności i prawa Wielkiej Brytanii. Taking Liberties – Star Items Index – Prawa człowieka. Dostępne stąd: <https://bit.ly/2QU4bSa>  ICO (brak daty). Przewodnik po ogólnym rozporządzeniu o ochronie danych (RODO): Prawo do informacji. Brytyjskie Biuro Komisarza ds. Informacji (ICO). Dostępne stąd: <https://bit.ly/3erd79K>  **Linki zewnętrzne**  EHCR (bez daty). Europejska Konwencja Praw Człowieka. Dostępne stąd: <https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c=> Dyrektywa o prywatności i łączności elektronicznej (2002 r.). 32002L0058 **Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej).**  **Dostępna w języku angielskim stąd:** <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058&from=EN> RODO (2016). ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). Dostępne w języku angielskim stąd:  <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN>  ONZ (brak daty). Deklaracja Praw Człowieka ONZ. Dostępne stąd[: https://www.un.org/en/about-us/universal-declaration-of-human-rights](https://www.un.org/en/about-us/universal-declaration-of-human-rights) |

### Krok 5

|  |  |
| --- | --- |
| Krok 5 Tytuł: | Jak chronić swoje dane w Internecie |
| Wiedza zdobyta po kroku 5 | 1: Opisz i omów różne aspekty prywatności.  2. Określam i oceniam sposób gromadzenia danych osobowych podczas poruszania się po Internecie i korzystania z aplikacji na urządzeniach inteligentnych.  3. Rozumiem prawa do prywatności wynikające z kart w celu ochrony naszych danych. |
| Temat | Narzędzia do ochrony danych online. |
| Wielkie pytanie | *Jak zmienić ustawienia przeglądania aplikacji i stron internetowych , aby zatrzymać śledzenie online?*  W dniu, w którym je poznasz, opowiedz swojej rodzinie i przyjaciołom o narzędziach, które mogą pomóc im chronić swoje dane online . Możesz zamieścić swoje poglądy na forum CSI-COP tutaj: <https://csi-cop.eu/forum/> - musisz zarejestrować się na stronie przed opublikowaniem na forum, tworząc login tutaj: <https://csi-cop.eu/citizenscientistlogin/> |
| Krótkie podsumowanie | **Aplikacje**: sprawdzanie uprawnień w "Ustawieniach" dla istniejących aplikacji na urządzeniach mobilnych. Przed pobraniem aplikacji sprawdź, o jakie uprawnienia prosi aplikacja – czy są one niezbędne, aby aplikacja działała? Na przykład aplikacja transportowa będzie potrzebować dostępu do Twojej lokalizacji, aby zapewnić dokładne informacje o tym , kiedy transport jest należny w pobliżu.  **Strony internetowe**: Użyj przeglądarki dostosowanej do ochrony prywatności lub zaktualizuj ustawienia przeglądarki, aby Cię nie śledziła i ogranicz reklamowe i marketingowe pliki cookie stron trzecich. |
|  |  |
| Treści edukacyjne | **Narzędzia online, które mogą pomóc w ochronie danych i prywatności**  Podsumowując to, czego nauczyliśmy się do tej pory:   * W kroku 1 zostaliśmy wprowadzeni w pojęcie "prywatności" * W kroku 2 dowiedzieliśmy się, że "dane osobowe" odnoszą się do żywej osoby * W kroku 3 dowiedzieliśmy się o niektórych sposobach przechwytywania naszych danych online (np. poprzez śledzące pliki cookie) * W kroku 4 dowiedzieliśmy się o różnych kartach i przepisach, które dają Ci prawo do prywatności   W tym kroku dowiemy się, jakie bezpłatne narzędzia są dostępne online, aby chronić nasze dane i naszą prywatność.  Myśląc o korzystaniu z Internetu, czy czujesz, że prowadzisz coraz więcej i więcej Twojego życia online niż kiedykolwiek wcześniej?  Pat Walshe ([Privacy Matters](https://twitter.com/PrivacyMatters)) zauważa, że przechodzimy online aby: robić zakupy, łączyć się poprzez wideo, wysyłać wiadomości do siebie, dzielić się naszymi doświadczeniami, myślami i uczuciami poprzez social media. Rezerwujemy również wizyty zdrowotne, wyszukujemy informacji na temat problemów zdrowotnych. Poruszamy się również online, aby znaleźć ze wskazówki odnośnie transportu - w przypadku podróży komunikacją miejską, samochodem, rowerem lub pieszo. Słuchamy również muzyki lub audio i oglądamy filmy lub TV w Internecie.  Znaczna część naszego życia stała się cyfrowa. Ale stawanie się coraz bardziej cyfrowym tworzy i pozostawia cyfrowe ślady, cyfrowe dane, które można zbierać i wykorzystywać do profilowania nas, poznawania nas, wpływania na nas w sposób, którego możemy nie być świadomi. Każda odwiedzana strona internetowa; każde kliknięcie i dotknięcie; każde połączenie lub wiadomość, którą wykonujesz lub otrzymujesz; każdy post w mediach społecznościowych, który publikujesz; miejsca, które odwiedzasz lub "tagujesz"; każde "polubienie"; utwory, których słuchasz lub filmy, które oglądasz (oraz szczegóły dotyczące tego, kiedy to zrobiłeś czy wstrzymałeś, szybko przewinąłeś do przodu lub pominąłeś utwór lub film) tworzy dane. Są to dane, które ujawniają aspekty Twojego zachowania, aspekty CIEBIE, często intymne. Na przykład aplikacje płodności, które znają Cię intymnie. Zobacz ten artykuł z magazynu Wired z 2018 r. "**Zanim zaczniesz korzystać z aplikacji antykoncepcyjnych, rozważ swoją prywatność"**: [https://bit.ly/3ajCyZz](https://bit.ly/3ajCyZz%20)  Organizacja charytatywna zajmująca się prywatnością zgłosiła w artykule Guardian z 2020 r., że "aplikacje menstruacyjne przechowują nadmierne informacje". Możesz o tym przeczytać tutaj:  [https://bit.ly/3aj7IQH](https://bit.ly/3aj7IQH )  Są też aplikacje, które dzielą się intymnymi aspektami seksualności, religii lub lokalizacji danej osoby na przykład (dane "lokalizacji" mogą sugerować bardzo wiele - niezależnie od tego, czy lokalizacja jest miejscem określonego rodzaju kultu, czy kliniką zdrowia o określonym charakterze).. Zobacz raport konsumencki 2020 na temat takich aplikacji tutaj: <https://bit.ly/3ggUw2x>  Istnieją również aplikacje skierowane do dzieci i nastolatków / młodych dorosłych, które przechwytują dane, być może bez wiedzy dziecka lub nastolatka, który pobrał aplikację, lub wiedzy rodzica (rodziców), którzy mogli kupić aplikację do użytku dziecka na inteligentnym urządzeniu. Yubo to "aplikacja społecznościowa" skierowana do dzieci, aby pomóc im znaleźć przyjaciół. Brytyjska gazeta Sunday Times poinformowała o problemach z ochroną aplikacji w wydaniu z 20 lutego 2022 r. Możesz przeczytać część tego raportu Sunday Times na poniższym obrazku:  Obraz zawierający tekst, gazetę  Opis generowany automatycznie  W dalszej części kroku 5 dowiemy się o bezpłatnych narzędziach online, które dostają się pod powierzchnię aplikacji takich jak Yubo , aby dowiedzieć się, czy w tej lub innych aplikacjach skierowanych do dzieci występują jakiekolwiek problemy z prywatnością danych.  Dane ujawniają nie tylko aspekty CIEBIE, ale także aspekty INNYCH. O tych, z którymi się komunikujesz i dzielisz informacjami, o swoich relacjach i wzorcach komunikacji. Na przykład aplikacja może poprosić o przesłanie lub udzielenie dostępu do "kontaktów" przechowywanych na komputerze lub smartfonie. Ale co jest w kontakcie? Kontakt może zawierać imię i nazwisko osoby, zdjęcie, numer telefonu komórkowego, adres e-mail, adres pocztowy, nazwę w mediach społecznościowych, datę rocznicy. Bycie cyfrowym online może wymagać od nas nie tylko myślenia o własnej prywatności, ale także o prywatności innych.  Jak omówiono w kroku 4, w UE i Wielkiej Brytanii prawo do prywatności w **Internecie** jest chronione przez szczególne przepisy dotyczące prywatności i łączności elektronicznej oraz ogólne rozporządzenie o ochronie danych (**RODO**). Ale prawa i ich egzekwowanie mają ograniczone działanie. Są jednak rzeczy, które możesz zrobić Ty, aby chronić swoją prywatność w Internecie.  Dowiedzieliśmy się o tym, że ludzie są śledzeni **przez Internet** w kroku 3. Obejmuje to technologię reklam (ad tech), takie jak pliki cookie, śledzenie po stronie serwera. Ale co możesz zrobić, aby to kontrolować i chronić swoją prywatność w Internecie? [[samodzielne zarządzanie prywatnością](https://policyreview.info/pdf/policyreview-2020-4-1537.pdf) jest trudne]. Możesz dowiedzieć się więcej o tym, że ludzie są [śledzeni](https://privacyinternational.org/case-study/4404/mobile-app-monetisation-covert-trackers-your-pocket) **za pośrednictwem aplikacji mobilnych** (zestawy programistyczne - SDK), czytając artykuł Binns et al. (2018): "Third Party Tracking in the Mobile Ecosystem" dostępny stąd:<https://arxiv.org/pdf/1804.03603.pdf> .  **Narzędzia do wykrywania śledzenia i kontrolowania go.**  **Narzędzia przejrzystości - web:**  Dostępnych jest wiele narzędzi, które pomogą Ci zrozumieć śledzenie, które ma miejsce na odwiedzanych stronach internetowych. Wiele śledzenia ma na celu skierowanie reklam lub "spersonalizowanie" Twojego doświadczenia. Często obejmuje to udostępnianie danych zewnętrznym firmom reklamowym, czasami setkom firm.  **Niektóre z narzędzi przezroczystości sieci obejmują:**  **Webbkoll** to narzędzie, które symuluje to, co dzieje się, gdy użytkownik odwiedza stronę internetową za pomocą typowej przeglądarki. Pokaże, jakie własne i zewnętrzne pliki cookie mogą być obecne na odwiedzanej stronie, a także jakie śledzenie ma miejsce, które nie opiera się na plikach cookie, takich jak żądania wysyłane przez serwery <https://webbkoll.dataskydd.net/en>  **Blacklight** skanuje stronę internetową i ujawnia kluczowe technologie śledzenia na stronie. <https://themarkup.org/blacklight>  **Pagexray** to narzędzie analityczne, które pokazuje wszystkie reklamy i moduły śledzące załadowane na stronę internetową i przedstawia wyniki w postaci wykresu drzewa. Wyniki można pobrać jako archiwum HTTP (.har.json) lub szczegółowe wyniki (.json) <https://pagexray.fouanalytics.com/>  **Request Map generator** pomaga określić, jakie strony trzecie znajdują się na stronie internetowej i gdzie przesyłane są dane. Wyniki można pobrać do pliku CSV. <https://requestmap.webperf.tools>  **Cover Your Tracks** to narzędzie do testowania, jak dobrze twoja przeglądarka chroni przed śledzeniem i odciskami palców <https://coveryourtracks.eff.org>  **Narzędzia transparentności – aplikacje mobilne:** Badanie aplikacji mobilnych nie jest łatwe. Kiedy korzystasz z aplikacji w telefonie, [O'Flaherty](https://www.forbes.com/sites/kateoflahertyuk/2021/01/31/apples-stunning-ios-14-privacy-move-a-game-changer-for-all-iphone-users/), dziennikarz zajmujący się cyber bezpieczeństwem, stwierdza, że aplikacje "mogą śledzić Cię w innych aplikacjach i witrynach internetowych, aby kierować reklamy. Obecnie odbywa się to za pomocą czegoś, co nazywa się identyfikatorem dla reklamodawców (**IDFA**), który śledzi bez ujawniania twoich danych osobowych. Istnieją pewne narzędzia, które pomagają rzucić światło na istnienie "trackerów" osadzonych w aplikacjach na Androida.  Kluczowym narzędziem dla Androida jest **Exodus Privacy**:  <https://exodus-privacy.eu.org/en/>  <https://developer.android.com/studio> Android Studio  Pat Walshe (Privacy Matters) informuje, że tutaj nie ma obecnie równoważnego narzędzia dla aplikacji Apple na iOS. Jednak Apple wprowadził nowe zasady przejrzystości dla swojego sklepu oraz dla programistów, które wymagają od nich używania predefiniowanych etykiet prywatności w celu ujawnienia, jakich danych używają i dlaczego. Nowy iOS [14.5](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.apple.com%2Fnewsroom%2F2021%2F04%2Fios-14-5-offers-unlock-iphone-with-apple-watch-diverse-siri-voices-and-more%2F&data=04%7C01%7Cab7778%40coventry.ac.uk%7C0961dc6c3373461cef5308d9096cf9ba%7C4b18ab9a37654abeac7c0e0d398afd4f%7C0%7C0%7C637551185936139952%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=yZzrdJ2Qdo3qBjKRGUWHNO5wjKePxo4%2BYYrWf3M4sHM%3D&reserved=0) firmy Apple wymaga również od programistów "*uzyskania zgody użytkownika przed śledzeniem jego danych w aplikacjach lub witrynach należących do innych firm w celach reklamowych lub udostępniania danych brokerom danych.* "  Zgodnie z Apple, jego nowa funkcja prywatności pozwala właścicielom telefonów Apple z tym systemem operacyjnym "dotknąć przycisku Raport prywatności, aby lepiej zrozumieć, w jaki sposób strony internetowe traktują Twoją prywatność. " ([Apple, 2021](https://www.apple.com/uk/ios/ios-14/)). Według Apple, jego funkcja przejrzystości śledzenia aplikacji (ATT) będzie "wymagać od wszystkich aplikacji prośby o wyraźne pozwolenie na śledzenie" i "W ustawieniach użytkownicy będą mogli zobaczyć, które aplikacje poprosiły o pozwolenie na śledzenie i wprowadzać zmiany według własnego uznania". ([O'Flaherty, 2021](https://www.forbes.com/sites/kateoflahertyuk/2021/01/31/apples-stunning-ios-14-privacy-move-a-game-changer-for-all-iphone-users/)).  W systemie Mac OS ("Big Sur") Apple zapewnia narzędzie do raportowania prywatności, które pojawia się jako ikona w przeglądarce Safari. Dzięki temu użytkownicy zobaczą, jakie moduły śledzące znajdują się na stronie internetowej i są blokowane. Przeglądarka Safari firmy Apple "daje więcej sposobów na ochronę prywatności" ([Apple, 2021](https://www.apple.com/uk/ios/ios-14/)). Kierunek firmy Apple w stronę ochrony prywatności ma ogromny wpływ na rynek według [O'Flaherty, 2021](https://www.forbes.com/sites/kateoflahertyuk/2021/01/31/apples-stunning-ios-14-privacy-move-a-game-changer-for-all-iphone-users/).  Wraz z "umieraniem plików cookie stron trzecich" ([Cyphers, 2021](https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea)), obywatelscy naukowcy mogą być siłą falową, która uniemożliwia jakiekolwiek zastąpienie śledzenia nas w Internecie, takie jak "nowy pakiet technologii Google do kierowania reklam w Internecie", przybliżający nas do przeglądania prywatności.  **Podsumowanie: Co możesz zrobić, aby chronić swoją prywatność?**  Używaj przeglądarek, które chronią Twoją prywatność  Korzystaj z blokerów reklam  Korzystaj z ustawień prywatności – systemów operacyjnych, przeglądarek, aplikacji.  Graficzny interfejs użytkownika, aplikacja  Opis generowany automatycznie |
| Przejrzyj swoją wiedzę | Zapoznaj się z tym, czego nauczyłeś się w kroku 5. Pamiętaj, że istnieją sposoby ochrony Twoich danych i prywatności, gdy jesteś online. |
| Zadania | Uczenie się przez doświadczenie: dowiedz się poprzez przeglądanie odwiedzanych witryn i aplikacji, z których korzystasz, jakie cyfrowe moduły śledzące, jeśli w ogóle, znajdują się w witrynach i aplikacjach.  **Zadanie 1:**  Użyj jednego z narzędzi, o których dowiedziałeś się w tym kroku, takiego jak [webbkoll](https://webbkoll.dataskydd.net/), aby zbadać często odwiedzaną witrynę. Sprawdź stronę internetową, aby zapoznać się z jej a) polityką prywatności i b) informacją o plikach cookie.  Pytania  -Jak łatwo było zrozumieć politykę prywatności?  -Czy informacja o plikach cookie informowała o obecnych plikach cookie i ich liczbie?  -Jakie osadzone *pliki cookie stron trzecich* zostały podane do wiadomości w informacji o plikach cookie?  **Zadanie 2**  Jeśli jesteś rodzicem i pozwalasz swoim dzieciom korzystać ze smartfona z aplikacjami, sprawdź uprawnienia aplikacji, zwłaszcza aplikacji przeznaczonej dla dzieci. Na przykład aplikacja do gier lub aplikacja do nawiązywania przyjaźni skierowana do młodych ludzi. Przejdź do "Ustawień" i wybierz dowolną aplikację, a następnie sprawdź jej uprawnienia.  Pytania  - Jakie uprawnienia zostały przyznane sprawdzonej aplikacji?  - Czy wiedziałeś o tych uprawnieniach dla aplikacji podczas jej pobierania?  Przypomnienie: możesz opublikować swoje poglądy na temat swojej nauki na forum csI-COP tutaj: <https://csi-cop.eu/forum/> - musisz zarejestrować się na stronie przed opublikowaniem na forum, tworząc login tutaj: <https://csi-cop.eu/citizenscientistlogin/> |
| Cel zadania | Przejście od nieformalnego ucznia do zostania obywatelskim naukowcem CSI-COP.  Przedyskutuj swoją opinię na temat tego warsztatu z rodziną i przyjaciółmi:   * Czy uważasz, że zyskałeś na podjęciu nauki z nieformalnym kursem CSI-COP? * Czy chciałbyś dołączyć do zespołu CSI-COP i zostać obywatelskim naukowcem, aby zbadać śledzenie online? * Czy byłbyś zainteresowany dalszą edukacją na temat ochrony danych, prywatności, tworzenia stron internetowych i aplikacji oraz powiązanych tematów? |
| Krótki tweet | Chronię swoje dane za pomocą narzędzi internetowych. |
| Dodatkowa Lektura | Zalecane:  Cyphers, B. (2021). Google FLoC (Federated Learning of Cohorts) to okropny pomysł. **Fundacja Electronic Frontier**. Dostępne stąd: <https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea>  O'Flaherty, K. (2021). Oszałamiający ruch prywatności Apple iOS14: przełom dla wszystkich użytkowników iPhone'a. **Forbes**. Dostępne stąd: <https://bit.ly/3vpOq4v/> |

Twoja opinia

|  |  |
| --- | --- |
| Twoja opinia na temat nieformalnego kursu edukacyjnego CSI-COP "Twoje prawo do prywatności w Internecie" | Pomogłoby to zespołowi CSI-COP dowiedzieć się, jak przydatny był ten kurs. Proszę wybierz jedną z poniższej opcji:  5. Bardzo przydatne  4. Przydatne  3. Nie mam zdania  2. Nieprzydatne  1. Zdecydowanie nieprzydatne  Zachęcamy do przekazania komentarzy lub sugestii dotyczących tego kursu: |

Oceń swoją naukę

Aby ocenić swoją naukę i uzyskać certyfikat CSI-COP, odpowiedz na pytania i napisz do Huma lub Jaimz na poniższe e-maile. Jeśli zdobędziesz 8/10 to otrzymasz certyfikat edukacji nieformalnej CSI-COP. Możesz wysłać swoje odpowiedzi do zespołu CSI-COP na Coventry University:

Huma na [ab7778@coventry.ac.uk](mailto:ab7778@coventry.ac.uk) lub

Jaimz w dniu [ad5956@coventry.ac.uk](mailto:ad5956@coventry.ac.uk)

**Pytania**

* 1. Czy to stwierdzenie jest prawdziwe czy fałszywe: Prywatność stała się problemem dopiero od czasów Facebooka?
  2. Czy to stwierdzenie jest prawdziwe czy fałszywe: przeglądarka incognito Google Chrome umożliwia wyszukiwanie w pełnej prywatności?
  3. Czy to stwierdzenie jest prawdziwe czy fałszywe: korzystanie z publicznej sieci Wi-Fi może udostępniać dane o Lokalizacji?
  4. Czy to stwierdzenie jest prawdziwe czy fałszywe: Wrażliwe dane osobowe odnoszą się do Twojego imienia i nazwiska?
  5. Czy to stwierdzenie jest prawdziwe czy fałszywe: Odciski palców to forma śledzenia witryny, która wykorzystuje atrybuty twojego urządzenia lub przeglądarki do zbudowania twojego profilu?
  6. Jakie klasy jako dane behawioralne – wybierz z poniższych:
     1. Twoje interakcje na stronie internetowej
     2. Twoje dane przeglądania stron internetowych
     3. Historia zakupów online
     4. Podczas korzystania z mapy online
     5. Korzystanie z aplikacji, na przykład do monitorowania stanu zdrowia
  7. Czy to stwierdzenie jest prawdziwe czy fałszywe: prawa człowieka były uważane za coś istotnego dla naszej godności i ochrony podstawowych praw i wolności?
  8. Czy to stwierdzenie jest prawdziwe czy fałszywe: Twoje prawa wynikające z Deklaracji Praw Człowieka (PDPC) obejmują "ochronę przed arbitralną ingerencją w prywatność, rodzinę, dom lub korespondencję danej osoby"?
  9. Czy to stwierdzenie jest prawdziwe czy fałszywe: Zgodnie z europejską konwencją praw człowieka (EKPC): w dzisiejszych czasach nie mamy prawa oczekiwać życia prywatnego i rodzinnego w naszym domu i naszej korespondencji?
  10. Zgodnie z ogólnym rozporządzeniem o ochronie danych (RODO) wybierz wszystkie, które mają zastosowanie:
      1. Prawo do informacji
      2. Prawo do przejrzystości
      3. Prawo do ochrony danych
      4. Prawo do niefilmowania przez sprzęt fotograficzny innych osób

Jak zostać naukowcem obywatelskim

|  |  |
| --- | --- |
| **Jak zostać obywatelskim naukowcem CSI-COP** | Po ukończeniu pięciu kroków w kursie edukacji nieformalnej CSI-COP i otrzymaniu certyfikatu, zapraszamy do dołączenia do zespołu CSI-COP i pomocy w zbadaniu zakresu śledzenia online.  Możesz dołączyć do zespołu CSI-COP i zgłosić się na ochotnika jako obywatelski naukowiec w projekcie.  Pełne informacje zostaną Państwu przekazane na żądanie, w tym:   * Arkusz informacyjny uczestników: na temat celu i roli obywatelskiego naukowca * Arkusz świadomej zgody zgodny z ogólnym rozporządzeniem o ochronie danych (RODO) * Informacje o tym, jak rozpocząć badanie stron internetowych i aplikacji pod kątem plików cookie.   Możesz dowiedzieć się więcej teraz, przechodząc do strony ["Informacje"](https://csi-cop.eu/about/) csi-COP tutaj: <https://csi-cop.eu/about/>.  Możesz również sprawdzić stronę często zadawanych pytań (FAQ) https://csi-cop.eu/faq/  Jeśli jeszcze tego nie zrobiłeś, możesz [zarejestrować](https://csi-cop.eu/citizenscientistlogin/) swoje zainteresowanie, zakładając konto na stronie CSI-COP tutaj: <https://csi-cop.eu/citizenscientistlogin/>  Forum internetowe CSI-COP do dyskusji z innymi naukowcami obywatelskimi w tym projekcie można znaleźć tutaj:  <https://csi-cop.eu/forum/>  Dziękuję bardzo za dotarcie tak daleko. Mamy jeszcze jedno zadanie, w którym chcielibyśmy, abyście nam pomogli: dowiedzieć się*, kim są* obywatelscy naukowcy. Poniżej znajdziesz ankietę. Zauważ, że nie zadajemy pytań, które mogą zidentyfikować Cię jako osobę. Naprawdę doceniamy Twój poświęcony czas. Z niecierpliwością czekamy na dołączenie do CSI-COP jako obywatelski naukowiec i przyszły mistrz prywatności.  Huma i Jaimz |

**Badanie CSI-COP1**

|  |  |
| --- | --- |
| **Przedział wiekowy: proszę zakreślić jeden z zakresu** | 18-39; 40-65; 66+; Wolę nie mówić |
| **Płeć: proszę wybrać jedną** | Kobieta; Mężczyzna; Interseksualność; Parasol Trans; Pozostałe; Wolę nie mówić |
| **Lokalizacja: proszę wybrać jedną** | Miasta i miasteczka  Wieś – wsie (poniżej 2000 mieszkańców)  Wolę nie mówić |
| **Języki:**   1. Jaki jest twój dominujący lub ojczysty język? 2. Czy mówisz płynnie w więcej niż jednym języku?   **Możesz woleć nie mówić.** | **1.**  **2.**  Wolę nie mówić |
| **Dostępność:**  Czy uważasz, że masz jakieś problemy z dostępnością; na przykład używanie oprogramowania do zamiany tekstu na mowę z powodu upośledzenia wzroku? | TAK  NIE  Wolę nie mówić |
| **Praca:** | Poziom studenta: proszę wybrać  Licencjackich  Studia podyplomowe  Doktoranckie  Osoba niebędąca studentem: wybierz kategorię, która najlepiej opisuje Twój status zatrudnienia:  Zatrudniony, pracujący 36,5 lub więcej godzin tygodniowo  Zatrudniony, pracujący 1-36 godzin tygodniowo  Niezatrudniony, poszukujący pracy  Niezatrudniony, nie szukający pracy  Uchodźca ubiegający się o azyl  Emerytowany  Problemy z dostępnością, niemożność pracy  Wolę nie mówić |
| **Dostęp do Internetu:** | Mieć dostęp do własnego połączenia internetowego (domowe lub służbowe szerokopasmowe /mobilne)  Korzystanie z dostępu publicznego podczas korzystania z Internetu  Wolę nie mówić |
| **Korzystanie z Internetu:**  Jak często korzystasz z Internetu? Proszę wybrać: | Codziennie  2-3 razy w tygodniu  Raz w tygodniu  Rzadziej niż raz w tygodniu  Nigdy  Wolę nie mówić |
| **Cel korzystania z Internetu:** | Korzystanie z Internetu w ramach codziennej pracy  Korzystanie z Internetu w celach rekreacyjnych, ale nie w ramach pracy  Korzystanie z Internetu do pracy i wypoczynku  Korzystanie z Internetu w ograniczony sposób, na przykład za pomocą komputera w bibliotece publicznej.  Wolę nie mówić |
| **Użycie aplikacji: komputery stacjonarne i laptopy** | Regularnie korzystam z aplikacji, na przykład do uwierzytelniania dostępu do narzędzi roboczych (np. Zoom, MS Teams). Jeśli tak, podaj nazwy niektórych aplikacji, z których korzystasz oraz ich przeznaczenie:  Narzędzia pracy (np. Microsoft Office itp.)  Granie w gry (np. STEAM).  Aplikacje edukacyjne  Styl życia (sport, fitness, zdrowie)  Wiadomości  Rozrywka (np. aplikacje do przesyłania strumieniowego, takie jak Netflix)  Inny  Wolę nie mówić  Rzadko używam aplikacji na komputerach stacjonarnych i laptopach  Nie używam aplikacji na komputerach stacjonarnych i laptopach  Wolę nie mówić |
| **Korzystanie z aplikacji: Urządzenia mobilne** | Regularnie korzystam z aplikacji, na przykład aplikacji transportowych, aby dowiedzieć się o czasie następnego pociągu, autobusu itp. Jeśli tak, podaj nazwy niektórych aplikacji, z których korzystasz oraz ich przeznaczenie:  Granie w gry  Aplikacje edukacyjne  Styl życia (sport, fitness, zdrowie):  Wiadomości  Rozrywka (np. aplikacje do przesyłania strumieniowego – Amazon Prime):  Inny  Wolę nie mówić  Rzadko używam aplikacji na telefon komórkowy lub tablet  Nie używam aplikacji  Wolę nie mówić |
| **Jak dowiedziałeś się o projekcie CSI-COP?** | Ze strony CSI-COP  Z uniwersytetu  Od członkostwa do stowarzyszenia (np. Kobiety w technologii)  Na przykład z obywatelskiej platformy naukowej   * SciStarter * Zooniverse * EU-Citizen.Nauka * Inna obywatelska platforma naukowa   Surfowanie po Internecie  Poprzedni wolontariat  W mediach społecznościowych powiedz, która platforma  Poczta pantoflowa  Inny |
| **Czy ukończyłeś bezpłatne warsztaty nieformalnej edukacji online CSI-COP?** | Tak  Jeszcze nie, ale zamierzam  Nie, wolę poczekać na przyszłe warsztaty twarzą w twarz, jeśli odbędą się w pobliżu miejsca, w którym mieszkam |
| **Jeśli ukończyłeś warsztaty, czy zamierzasz dołączyć do zespołu CSI-COP jako wolontariusz obywatelski naukowiec?** | Tak  Może  Potrzebuję więcej informacji  Nie |
| **Aby wysłać wypełnione pytania "Oceń swoją naukę", ankietę i wszelkie inne pytania, skontaktuj się z zespołem CSI-COP** **Uniwersytetu Coventry** | Prosimy o odesłanie tego wypełnionego dokumentu do członków zespołu CSI-COP Uniwersytetu Coventry:  Huma na [ab7778@coventry.ac.uk](mailto:ab7778@coventry.ac.uk) lub Jaimz na [ad5956@coventry.ac.uk](mailto:ad5956@coventry.ac.uk) |
| **Dziękujemy za poświęcony czas na ukończenie nieformalnego kursu edukacyjnego CSI-COP i ankiety**  **Ten dokument będzie wkrótce dostępny w innych językach.**  **Proszę sprawdzić stronę CSI-COP tutaj:** [**https://csi-cop.eu/**](https://csi-cop.eu/) | |