2025

JESTEŚ W CIĄŻY? NIE BĄDŹ TARGETEM – CHROŃ PRYWATNOŚĆ

FEDERA

FUNDACJA PANOPTYKON

Pisząc o dziewczynach i kobietach, mamy na myśli osoby, których płeć przy urodzeniu została określona jako żeńska.

FEDERA

FUNDACJA PANOPTYKON

JESTEŚ W CIĄŻY? NIE BĄDŹ TARGETEM – CHROŃ PRYWATNOŚĆ

Czy szukając w sieci informacji o ciąży – także o aborcji – da się zachować kontrolę nad tym, kto i co wie na twój temat? Dlaczego warto zadbać o prywatność?

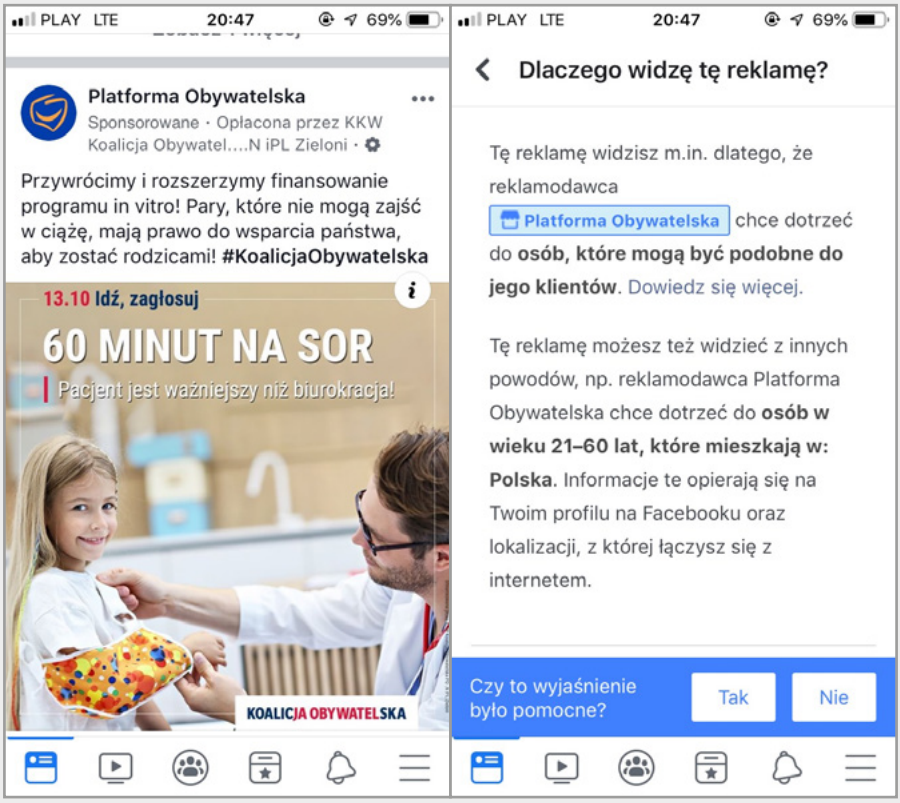
Każdego roku około pół miliona kobiet w Polsce zachodzi w ciążę. Rodzi się niecałe 300 tys. dzieci. Część ciąż kończy się samoistnym poronieniem. Szacunkowo co trzecia ciąża kończy się aborcją [**Guttmacher Institute**]. Kilkaset zabiegów rocznie przeprowadzanych jest w szpitalach [**Federa**, **PAP**], a pozostałe to samodzielne aborcje domowe – z wykorzystaniem tabletek zamówionych przez Internet. To gigantyczna grupa osób, która szuka w Internecie informacji o reprodukcji.

W Internecie? Tak, tam, gdzie na każdym kroku zostawiasz ślady, po których mogą do ciebie dotrzeć reklamodawcy (z reklamą przysłowiowych pieluch), przeciwnicy aborcji (którzy będą chcieli cię emocjonalnie zmanipulować) lub policja czy prokuratura.

Przede wszystkim przerwanie własnej ciąży nie jest w Polsce zabronione i nie grozi ci za to kara. Przy poszukiwaniu informacji czy zamawianiu tabletek warto jednak zadbać o bezpieczeństwo i prywatność – po to, żeby o twojej ciąży, aborcji, poronieniu lub porodzie wiedziały tylko te osoby, które chcesz o tym poinformować. A także po to, by uniknąć stania się „targetem” reklamowym.

W tym poradniku znajdziesz podpowiedzi, jak ochronić swoją prywatność i bezpieczeństwo. Nie masz czasu czytać go w całości? Zwróć uwagę na różowe ramki z symbolem maski, w których podajemy konkretne narzędzia i wskazówki, które ci pomogą.

Kobiety, zwłaszcza „potencjalne młode matki", to dziś jedna z ulubionych grup docelowych branży reklamowej. Można im sprzedać suplementy diety dla ciężarnych, akcesoria dla niemowląt, usługi banków komórek macierzystych czy warsztaty dla rodziców. Reklamują się nie tylko producenci i dostawcy usług, ale też politycy – na przykład partie czy kandydatki – obiecujący rozszerzenie dostępności darmowych badań prenatalnych.



W Polsce tematy dotyczące reprodukcji – ciąża, in vitro, aborcja – pozostają tematem jednego z ważnych publicznych sporów. I jak z każdym tematem, który porusza emocje wielu osób, tam, gdzie tylko się pojawia, wkracza też dezinformacja. Dzieje się tak zwłaszcza w komercyjnych mediach społecznościowych i na innych platformach internetowych, gdzie specjalne algorytmy dobierają treści w taki sposób, żeby jak najdłużej zaangażować czytelniczki. A to dlatego, że treści kontrowersyjne (sensacyjne, emocjonalne, polaryzujące) angażują skuteczniej niż te rzetelne i wyważone.

Dzisiejszy Internet to przede wszystkim usługi szyte na miarę. Do twoich indywidualnych „zainteresowań" dobierane są treści w portalach newsowych, wyniki wyszukiwania, posty w komercyjnych mediach społecznościowych. Informacja o ciąży jest w tym kontekście niezmiernie cenna – i „przyczepia się" do ciebie na długo, niezależnie od twojego stosunku do tego stanu. Czy czekałaś na ciążę latami, czy chcesz ją przerwać, pewne jest jedno: to temat, który cię „interesuje".

Do pewnego stopnia możesz kontrolować to, jak informacje na twój temat rozchodzą się w sieci, i postarać się, żeby o twojej ciąży wiedziały tylko te osoby, które chcesz o niej poinformować. Możesz się też chronić przed niechcianymi reklamami i innymi treściami podsuwanymi przez różne podmioty działające w sieci – wybierając usługi, które nie zarabiają na twojej uwadze, oraz korzystając z ustawień prywatności (dostępnych nawet w pozornie darmowych usługach).

JAK ZROBIĆ (SAMODZIELNIE) ABORCJĘ W POLSCE – BEZPIECZNIE W KONTEKŚCIE PRAWNYM I CYFROWYM

Załóżmy, że dowiedziałaś się, że jesteś w ciąży, i podjęłaś decyzję, że chcesz ją (samodzielnie) przerwać. Możesz to zrobić bezpiecznie, a przy tym ograniczyć ślady zostawiane w sieci. Tłumaczymy wszystko krok po kroku.

1. Oszacuj, w którym tygodniu ciąży jesteś

Jeśli nie jesteś pewna, jak liczyć, to w Internecie z łatwością znajdziesz kalkulatory długości trwania ciąży. Powyżej 12. tygodnia nadal można wywołać poronienie tabletkami, ale możliwe, że będziesz potrzebowała większej dawki leków.

2. Zamów tabletki

Najlepiej ze strony organizacji Women on Web (WOW) lub Women Help Women (WHW) – to dwa zaufane źródła, w których pracują lekarki i które nigdy nie oszukały żadnej kobiety. Za pozostałe źródła nie odpowiadamy. Na każdej ze stron najpierw wypełniasz formularz z podstawowymi informacjami zdrowotnymi, a po złożeniu zamówienia otrzymujesz e-mail z danymi do przelewu.

Pamiętaj, żeby zamówić tabletki ze swojego adresu e-mailowego i na swoje nazwisko, a zamówienie opłacić ze swojego konta!
Ty nie podlegasz odpowiedzialności karnej za przerwanie ciąży, ale twoi bliscy mogą odpowiadać za pomoc finansową lub logistyczną.

UWAGA – jeżeli minął już 12. tydzień ciąży, skontaktuj się z organizacją bezpośrednio, nie wypełniaj formularza.

3. Przyjmij tabletki zgodnie z instrukcją przedstawioną w **broszurze *Aborcja farmakologiczna w pytaniach i odpowiedziach*** [PDF]

W broszurze znajdziesz informacje o przygotowaniu do aborcji, o jej przebiegu i o tym, czego spodziewać się po fakcie.

Jeżeli nie zaobserwujesz u siebie niepokojących objawów, np. upławów w dziwnym kolorze lub o nietypowym zapachu, utrzymującego się bólu czy kłucia w podbrzuszu, podwyższonej temperatury ciała – nie musisz udawać się do lekarza.

Jeśli jednak cokolwiek cię niepokoi, udaj się do lekarza. Jeżeli zdecydujesz się opowiedzieć o swojej aborcji, to nic ci nie grozi. Jednak aborcja tabletkami to tak naprawdę wywołanie poronienia, które jest nie do odróżnienia od samoistnego (naturalnego). Jeśli więc nie chcesz mówić lekarzowi o swojej aborcji – nie musisz tego robić.

Więcej informacji o organizowaniu dostępu do aborcji (także w sytuacji, gdy płód rozwija się nieprawidłowo, gdy ciąża zagraża twojemu życiu lub zdrowiu bądź gdy jest ona wynikiem czynu zabronionego) znajdziesz na **stronie internetowej FEDERY**.

WARTO CHRONIĆ PRYWATNOŚĆ

Prywatność to obszar, w który nie wolno wkraczać bez przyzwolenia. Obejmuje sferę cielesną (nikt nie może cię dotykać, jeśli sobie tego nie życzysz), terytorialną (nie można wejść do czyjegoś domu bez pozwolenia), informacyjną (nie można bez pozwolenia zaglądać ci do poczty i udostępniać informacji o twoim zdrowiu) i komunikacyjną (nie można bez powodu podsłuchiwać czyichś rozmów).

Informacje, które zostawiasz na każdym kroku, są gromadzone. Następnie mogą być monetyzowane, np. poprzez reklamy personalizowane na podstawie twojej aktywności w sieci czy takie zestawienie treści w feedzie, które żerując na twojej wrażliwości, ma na dłużej zatrzymać cię na platformie. Nie można też wykluczyć, że twoją aktywnością zainteresują się służby, bo w Polsce nie ma nad nimi należytej kontroli.

Dobra wiadomość: do pewnego stopnia możesz kontrolować, jak bardzo różne podmioty aktywne w Internecie ingerują w twoją prywatność – np. ograniczając zostawiane przez siebie ślady, wybierając szanujące prywatność usługi czy korzystając z ustawień dostępnych w tych usługach.

ŚLADY ZOSTAWIANE W SIECI A INTERNETOWE KORPORACJE

Ciągle widzisz reklamy pieluch nowej generacji. Dlaczego?

Firmy nie wiedzą, czy planujesz aborcję, czy nie. Jednak samo to, że szukasz w sieci informacji związanych z ciążą, sprawia, że reklamodawcy wychodzą z założenia, że potrzebujesz różnych produktów i usług. Żeby nie przepalać budżetów na wyświetlanie reklam osobom, które na pewno w nie nie klikną, zawężają grupę docelową kampanii. Odpowiednie kryterium („wyświetlaj osobom zainteresowanym ciążą") mogą zadać np. w panelu reklamowym na Facebooku.

Platformy internetowe profilują nie tylko reklamy, ale też inne treści. W zależności od tego, na czym polega rdzeń biznesu danej platformy, będą to wyróżnione oferty (Allegro, Zalando), newsy (Onet), rolki czy profile (Facebook). Poznasz je po opisie: „może cię zainteresować", „proponowane dla ciebie", „oferta rekomendowana", „rekomendowane dla ciebie", „wybrane dla ciebie" (na potrzeby tego poradnika nazwijmy je treściami rekomendowanymi).

Decyzje, jakie treści rekomendowane komu wyświetli platforma, są wynikiem działania algorytmów, które analizują dane na temat twojej wcześniejszej aktywności w Internecie – a także aktywności wszystkich innych użytkowniczek i użytkowników. Szukanie informacji o aborcji to jedna z takich informacji.

*Mechanizm profilowania reklam wykorzystały działające w USA organizacje anti-choice (antyaborcyjne). Osobom szukającym informacji o aborcji wyszukiwarka Google wyświetlała sponsorowane wyniki „ośrodków zdrowia reprodukcyjnego", za którymi w rzeczywistości kryły się organizacje mające na celu odwiedzenie kobiet od decyzji o aborcji. Reklamy wyświetlały się po wpisaniu do wyszukiwarki na 15 tys. różnych haseł związanych z aborcją, np. abortion pill, abortion clinic, abortion clinic near me czy planned parenthood. W ciągu dwóch lat organizacje antyaborcyjne wydały na reklamę w Google ponad 10 milionów dolarów [**Center for Countering Digital Hate, 2023**].*

*Znane są też przykłady osób, które przeszły poronienie, a algorytmy profilujące wciąż podrzucają im reklamy produktów dla niemowląt [**The Washington Post, 2018**].*

ZMAGASZ SIĘ Z NIEPŁODNOŚCIĄ?

Zajrzyj na **stronę Stowarzyszenia „Nasz Bocian"** – to polska organizacja społeczna specjalizująca się w poradnictwie, edukacji i rzecznictwie w tym obszarze.

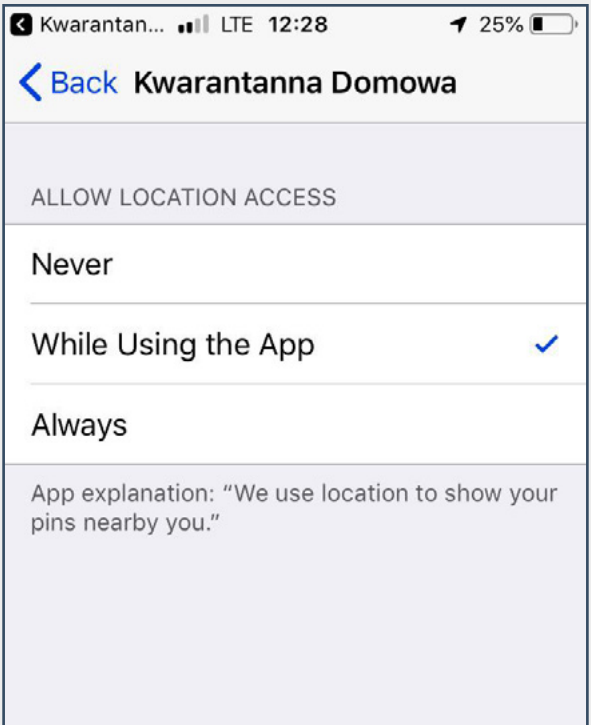
Możesz ograniczyć poziom zbierania danych i przesyłania ich w celu personalizacji, **kontrolując** poprzez **ustawienia prywatności w usługach i urządzeniach**, jakie informacje gromadzą o tobie platformy.

OGRANICZ DOSTĘP APLIKACJI DO DANYCH

W ustawieniach aplikacji w telefonie możesz określić, która aplikacja ma dostęp do lokalizacji, kontaktów, aparatu etc. („zawsze”, „nigdy”, „podczas korzystania z aplikacji”).

Bez lokalizacji ciężko korzystać z nawigacji w telefonie, ale wystarczy, gdy aplikacja ma do niej dostęp tylko wtedy, gdy jest aktywna. Inne aplikacje do prawidłowego działania nie potrzebują wszystkich uprawnień, które chciałyby mieć (np. Canva chce mieć dostęp do lokalizacji, ale jeśli nie przyznasz jej tego uprawnienia, nie wpłynie to na jej efektywność).

Warto dokładnie czytać treść wyskakujących okienek – wiele zgód jest opcjonalnych.



WYŁĄCZ PERSONALIZACJĘ REKLAM W TELEFONIE

Jeśli nie chcesz, żeby firmy dostarczały ci personalizowane reklamy, wyłącz identyfikator reklamowy. Opcję „włącz/wyłącz identyfikator reklamowy" znajdziesz w ustawieniach telefonu (Android) lub ustawieniach prywatności (iPhone).

System Android podpowiada, że dzięki włączonemu identyfikatorowi reklamowemu uzyskasz „bardziej dopasowane reklamy".
Jeśli czytasz ten poradnik, to być może wcale nie chcesz umożliwiać reklamodawcom powiązania danych o lokalizacji, historii wyszukiwania i historii przeglądanych stron, a co za tym

idzie – wyświetlania „bardziej dopasowanych reklam". Wyłączenie identyfikatora ograniczy możliwość śledzenia i dopasowywanie reklam do twojej aktywności.

WYŁĄCZ PERSONALIZOWANE REKLAMY W USŁUGACH (GOOGLE, FACEBOOK, INSTAGRAM, TIKTOK)

Możesz wyłączyć personalizowanie reklam w wyszukiwarce Google czy na YouTubie (działa, jeśli jesteś zalogowana na koncie Google). Na stronie pomocy znajdziesz **instrukcje**, jak wyłączyć reklamy spersonalizowane w usługach tej korporacji. Zaloguj się do swojego konta, wejdź w zakładkę „Dane i prywatność", następnie znajdź ramkę „Reklamy spersonalizowane" i wyłącz je.

W ustawieniach Facebooka lub Instagrama można zmienić „Preferencje reklamowe". Powinno to wpłynąć na zawartość reklam, które wyświetlą ci te portale (chociaż badania wskazują, że niestety nie zawsze działa to zgodnie z oczekiwaniami, z braku innych narzędzi warto próbować).

Jak oglądać wideo w sieci bez śledzenia? Materiały z YouTube'a odtworzysz przez interfejs **Invidious** w przeglądarce (np. w serwisie **yewtu.be**) lub przez aplikację **NewPipe** na Androidzie. Invidious i NewPipe nie zbierają danych o tym, co oglądasz, i nie wyświetlają reklam.

Od 2023 r. Meta oferuje opcję płatną swoich flagowych serwisów – bez klasycznych reklam. Firma jednak wciąż śledzi i analizuje twoją aktywność, a zamiast reklam zobaczysz więcej treści „proponowanych dla ciebie".

KTO ŚLEDZI W SIECI

Google i Facebook to nie jedyne firmy, które chcą wiedzieć, czego szukasz w sieci, i wystawić ci reklamę. Każdy twój ruch monitorują setki firm. Te, których nazwy na pewno kiedyś słyszałaś (np. TikTok, Amazon, Yahoo, Criteo, Adobe, Gemius), i takie, których nazwa prawdopodobnie nie budzi żadnych szczególnych skojarzeń (Human, Blue, Bababam). Do tego operator komórkowy, dostawca Internetu, każda (zwłaszcza komercyjna) aplikacja z dostępem do lokalizacji. W jakich celach te podmioty wykorzystują pozyskane informacje? Głównie reklamowych, ale dostęp do nich mogą mieć również służby. W Polsce ich działalność nie jest w sposób demokratyczny kontrolowana,

przez co dostęp do danych – potrzebny służbom w celu ścigania i zapobiegania przestępczości – może być nadużywany.

ROZWAŻ PRZEJŚCIE NA NIEKOMERCYJNE MEDIA SPOŁECZNOŚCIOWE

Na Mastodonie nie ma reklam, a treści, które widzisz, zależą od twoich decyzji, np. zaobserwowania konkretnych kont. Feed nie bazuje na nakarmionych twoimi danymi algorytmach.

Odwiedź **Profil Kobiety w Sieci na Mastodonie**

Polecamy poradnik Fundacji Panoptykon:
Zapraszamy do Fediwersu! [poradnik]

KORZYSTAJ Z PRZEGLĄDARKI INTERNETOWEJ SZANUJĄCEJ PRYWATNOŚĆ

Na telefonie korzystaj z przeglądarki **Firefox Focus** (zamiast z aplikacji domyślnych, np. Safari lub Chrome).

Przeglądarka z liskiem w logo nie przechowuje historii przeglądania, blokuje śledzenie przez tzw. strony trzecie (np. brokerów danych) za pomocą ciastek i skryptów. Nie sprzedaje też twoich danych.

PRYWATNOŚĆ W PRZEGLĄDARCE, CZYLI ZAINSTALUJ WTYCZKI I ZMIEŃ USTAWIENIA CIASTECZEK

Na komputerze korzystaj z przeglądarki Firefox. Zainstaluj w niej dodatki (nazywane też wtyczkami lub rozszerzeniami) chroniące prywatność. Polecamy wtyczki blokujące skrypty (np. **NoScript**)

i reklamy (np. **uBlock Origin** – nie zablokuje ona śledzenia, ale przynajmniej zmniejszy liczbę wyświetlanych niechcianych reklam). Wtyczki dostępne są też na przeglądarkę Chrome.

W ustawieniach przeglądarki wybierz opcję „kasuj ciastka przy zamykaniu przeglądarki" albo domyślnie używaj trybu prywatnego (incognito).

UWAGA! Tryb incognito nie zapewnia anonimowości, chroni jedynie przed zapisaniem informacji o twojej aktywności na danym urządzeniu. Po zamknięciu przeglądarki na urządzeniu nie zapisze się historia przeglądania ani ciastka.

Jesteś jednak cały czas widoczna dla administratorów stron, które odwiedzasz, czy dostawcy sieci. W sekcji „Dane w twoim telefonie" znajdziesz informacje, jak skutecznie zamaskować aktywność w przeglądarce.

KORZYSTAJ Z WYSZUKIWARKI SZANUJĄCEJ PRYWATNOŚĆ
Wyszukiwarka **DuckDuckGo** nie zapisuje danych wyszukiwania i nie zbiera żadnych informacji o tobie. DuckDuckGo nie sprzedaje też danych reklamodawcom.

Komercyjne wyszukiwarki Google i Bing (od Microsoftu) zapisują wszystkie twoje wyszukiwania i przechowują je na twoim koncie i swoich serwerach. Na szczęście na rynku jest wiele niesledzących wyszukiwarek, które także pozwalają na korzystanie z narzędzi zawężania wyszukiwania znanych z popularnych usług.

O ZAUFANIU

„W sieci nikt nie wie, że jesteś psem" – i odwrotnie: w Internecie nie wiesz, czy rozmawiasz z psem. Osoba, która w USA wyszukuje w Google hasło „aborcja w mojej okolicy", może natknąć się na reklamy organizacji „pro life", które podszywają się pod kliniki.

Również w Polsce może się zdarzyć, że ktoś będzie próbował zdobyć jak najwięcej wrażliwych informacji o osobie poszukującej informacji o aborcji. Nie każda osoba deklarująca wirtualne wsparcie naprawdę chce ci pomóc. Jeśli masz wątpliwości, czy możesz komuś zaufać, zweryfikuj to z administratorkami grupy pomocowej lub zadzwoń do organizacji wspierających kobiety, np. do FEDERY.

Jeśli rozmawiasz na publicznych grupach, minimalizuj liczbę informacji. Używaj anonimowych kont, nie udostępniaj informacji o osobach z twojej rodziny.

DANE W TWOIM TELEFONIE

Ile można wyczytać z analizy użytkowania telefonu?

Pewnego dnia, wcześnie rano, Ewa (imię zmienione) odbyła ze swoją siostrą długą rozmowę telefoniczną. Dwa dni później kilkakrotnie dzwoniła do pobliskiej poradni dla kobiet (Planned Parenthood). Dwa tygodnie później powtórzyła ten schemat – i jeszcze raz po miesiącu.

Ewa była jedną z ochotniczek biorących udział w badaniu przeprowadzonym w 2016 r. przez grupę naukowców z Uniwersytetu Stanforda. Chcieli oni sprawdzić, co da się wyczytać z metadanych telekomunikacyjnych. W przypadku Ewy informacje

*o wykonanych połączeniach pozwoliły bez większego wysiłku wyczytać, że kobieta dowiedziała się o swojej ciąży [**PBS**, **PNAS**].*

Metadane telekomunikacyjne, czyli „dane o danych", to informacje o tym, w jaki sposób korzystasz z sieci. Odkładają się one w logach operatora sieci (Orange, T-Mobile itp.). Zapisują się m.in. numery telefonów, pod które dzwonisz i SMS-ujesz, lokalizacja twojego urządzenia, adresy IP stron w sieci, które odwiedzasz.

Metadane telekomunikacyjne to ważne narzędzie pracy policji i innych służb. Zgodnie z obowiązującymi w Polsce przepisami operatorzy telekomunikacyjni mają obowiązek przechowywać metadane przez rok. To znaczy, że policja może sprawdzić bilingi do 12 miesięcy wstecz – oczywiście musi mieć ku temu powód (na przykład podejrzewać przestępstwo). Żeby ściągnąć metadane, nie potrzebuje zgody sądu.

W Polsce karane jest tzw. pomocnictwo w aborcji, co oznacza, że w teorii możliwy jest scenariusz, w którym policja sięgnie po billingi kobiety, aby ścigać na przykład partnera, który pomógł jej w przerwaniu ciąży. Do pewnego stopnia można ograniczyć zasób informacji, jaki trafia do dostawcy Internetu lub operatora sieci komórkowej. Najłatwiej ochronić treść wiadomości i historię odwiedzanych stron, ale można chronić także metadane.

KORZYSTAJ Z SZYFROWANYCH KOMUNIKATORÓW

Kiedy wysyłasz SMS-y, operator komórkowy zachowuje ich metadane, czyli czas wysłania wiadomości i numer, pod który

ją wysyłasz. Wie zatem, z kim się kontaktujesz i jak często. Ma obowiązek przechowywać te dane przez rok i udostępniać służbom na żądanie.

Żeby tego uniknąć, korzystaj z komunikatora, który szyfruje wszystkie wiadomości od końca do końca (z ang. *end-to-end*). **Signal** nie ma dostępu do treści wiadomości i nie przechowuje metadanych wiadomości.

Signal zapisuje jedynie informację o tym, kiedy konto zostało założone i kiedy nastąpiła ostatnia aktywność. Nie zapisuje, z jakimi numerami i kiedy osoba się kontaktuje (ta informacja zostaje na twoim urządzeniu – zajrzyj do sekcji ***Utrata kontroli nad sprzętem***).

Uważaj na komunikatory, które udają szyfrowane, choć wcale takie nie są (np. dostawca może odszyfrować treść wiadomości lub funkcja szyfrowania nie jest domyślnie włączona – takie komunikatory to na przykład Telegram i Messenger od Mety).

W Europie toczy się debata polityczna o ograniczeniu szyfrowania pod pretekstem ochrony dzieci. Kiedy piszemy ten poradnik, politycy nie zdecydowali się na ten krok – ale też nie zaufali argumentom, że ograniczenie szyfrowania wpłynie negatywnie także na dzieci, które chcą chronić, pozbawiając je możliwości bezpiecznej komunikacji w sieci.

KORZYSTAJ Z TORA I VPN-A

Możesz ograniczyć zostawianie śladów swojej aktywności w Internecie, korzystając z **sieci Tor** lub takiego VPN-a (wirtualnej sieci prywatnej), który nie zapisuje danych o tym, co za jego pomocą robisz.

Przeglądarka Tor jest bezpieczna i darmowa. Szyfruje twój ruch internetowy i prowadzi go przez liczne inne komputery. W ten sposób operator „nie widzi", jakie strony odwiedzasz. W Torze nie kupisz wprawdzie biletów PKP, ale sieć doskonale nadaje się do poszukiwania informacji. Znajdziesz w niej wiele zasobów, np. stron internetowych, które dostępne są też w sieci WWW.

VPN można porównać do tunelu, który chroni twoją aktywność w sieci przed zewnętrznymi „oczami", np. twojego dostawcy Internetu. „Tunelem" zarządza dostawca wybranego przez ciebie VPN-a. Wybierz VPN, który nie śledzi tego, co robisz (nie zapisuje metadanych), np. **Mullvad**. Możesz też przetestować za darmo **ProtonVPN** („Załóż darmowe konto") oraz **Tunnelbear** („Try for free").

Czym różni się Tor od VPN-a? VPN-y są płatne, z Tora skorzystasz za darmo. W przypadku VPN-a musisz zaufać jego operatorowi (dlatego polecamy konkretnych sprawdzonych operatorów), w przypadku Tora prywatność użytkownika jest chroniona przez samą konstrukcję tej sieci.

Jakich informacji nie zapisują operatorzy, a jakie zapisują? Jeśli korzystasz z szyfrowanego protokołu HTTPS (obecnie działa on na większości stron w sieci), w logach nie zapisuje się, co robisz na tych stronach, np. jakie słowa wpisujesz do formularza w sklepie internetowym (zapisują się one w bazie tego sklepu) ani jakie podstrony na danej stronie odwiedzasz. Operator internetowy będzie miał jednak dostęp do informacji, że odwiedziłaś konkretną witrynę internetową.

Operatorzy komórkowi nie przechowują treści SMS-ów. Dostęp do treści twoich SMS-ów mogą uzyskać służby, ale pod warunkiem, że otrzymają zgodę sądu na prowadzenie kontroli operacyjnej. W takim przypadku uzyskają dostęp wyłącznie do wiadomości przesyłanych od momentu zarządzenia kontroli, a nie do wcześniej wysłanych. Same wiadomości zostają też na urządzeniu (o tym w kolejnej sekcji).

REJESTR CIĄŻ

W 2023 r. Ministerstwo Zdrowia wydało rozporządzenie, które nakładało na lekarzy obowiązek umieszczania w centralnej bazie informacji medycznych – także o tym, że pacjentka jest w ciąży. Tak zwany „rejestr ciąż" miał chronić kobiety (np. przed podaniem im leków zagrażających ciąży w sytuacji utraty przytomności), ale wywołał głośną krytykę (m.in. ze strony Fundacji Panoptykon)

w związku z napiętą społecznie atmosferą wokół aborcji i ograniczeń w dostępie do niej. Do dziś wiele osób dzwoniących do FEDERY z pytaniem o to, jak bezpiecznie przerwać ciążę w warunkach domowych, obawia się, że „rejestr" w jakiś sposób im zagraża.

Uspokajamy – przede wszystkim przerwanie własnej ciąży nie jest zabronione ani karane. Nawet jeśli w rejestrze zapisana została informacja, że jesteś w ciąży, to w przypadku poronienia lub aborcji rejestr nie jest zagrożeniem. Przerywając ciążę przed 22. tygodniem, nie popełniasz przestępstwa. Więcej dowiesz się ze strony ***federa.org.pl****.*

Co więcej, Ministerstwo Zdrowia zdecydowało, że informacja o ciąży będzie umieszczana w rejestrze jedynie za zgodą pacjentki. Zmiana weszła w życie we wrześniu 2024 r. Od tej pory to ty decydujesz, czy informacja o ciąży zostanie wpisana do systemu, czy nie.

POUFNA KOMUNIKACJA W INTERNECIE

Kto widzi twoje SMS-y (oraz e-maile i wiadomości z komunikatorów)

Treść pocztówki wysłanej z wakacji łatwo mogą odczytać osoby trzecie, nie zostawiając śladów. Włożoną do zaklejonej koperty – bez jej naruszania – odczytać trudniej. Podobnie jest z komunikacją elektroniczną. Tradycyjny SMS, połączenie telefoniczne czy niezaszyfrowany e-mail są jak odkryta pocztówka – łatwo podejrzeć ich treść. Do tego w bazie operatora zostają metadane (o których piszemy wyżej).

Po metadane chętnie sięgają policja i inne służby (nie potrzebują na to zgody sądu). Listę połączeń i numerów, na które wysłano SMS-y, może też podejrzeć osoba, która płaci rachunek za telefon (rodzic, partner, pracodawca). Po samą treść SMS-ów, rozmów telefonicznych czy e-maili mogą sięgać służby, ale muszą najpierw wystąpić do sądu o zgodę na kontrolę operacyjną – i ją otrzymać. Jeśli ją dostaną, będą mogły podejrzeć rozmowy i treść SMS-ów **w przód**, czyli od momentu wyrażenia zgody przez sąd. Operatorzy tych materiałów nie przechowują.

Do komunikacji poufnej **wybierz szyfrowany komunikator**, np. Signal (piszemy o nim wyżej). Wiadomości i historia połączeń zostają w telefonie. Nie ma do nich dostępu operator sieci komórkowej ani dostawca usługi komunikatora. Do zaszyfrowanych wiadomości nie mają dostępu żadne inne osoby ani podmioty (pomijamy sytuację zainfekowania urządzenia oprogramowaniem szpiegującym).

Niepotrzebne już wiadomości i historię połączeń warto skasować. W Signalu możesz skorzystać z opcji „znikających wiadomości", które skasują się automatycznie po określonym czasie (np. po dniu, tygodniu, 4 tygodniach).

Uwaga: za pośrednictwem Signala możesz komunikować się tylko z osobami, które również mają zainstalowaną tę aplikację.

NAJPOPULARNIEJSZY KOMUNIKATOR – NIEKONIECZNIE NAJLEPSZY

W Polsce wciąż najpopularniejszym komunikatorem jest Messenger od Mety. Od niedawna oferuje on opcję szyfrowania wiadomości pod warunkiem ustawienia 6-cyfrowego PIN-u. Domyślnie komunikacja nie jest szyfrowana – rekomendujemy wybór komunikatora, w którym wszystkie czaty są domyślnie szyfrowane.

UTRATA KONTROLI NAD SPRZĘTEM

Co jeśli ktoś przechwyci kontrolę nad twoim telefonem

Jeśli zostawisz telefon w taksówce, w toalecie na lotnisku, jeśli ktoś ukradnie ci go z plecaka czy też skonfiskują go służby (np. Straż Graniczna) – stracisz nad nim kontrolę. Kontrola nad urządzeniem jest również ograniczona, jeśli współdzielisz je z innymi osobami – wszystkie one mają dostęp do informacji na nim zapisanych.

W każdym przypadku możesz utrudnić osobom niepowołanym wydobycie ze smartfonu informacji na twój temat.

WSPARCIE W SYTUACJI PRZEMOCY

Gdy ktoś, np. partner(-ka) czy rodzic, domaga się dostępu do twojego telefonu, grozi ci, jeżeli nie pokażesz mu wiadomości, albo żąda od ciebie podania haseł, jest to forma przemocy. Jeśli dotknęła cię przemoc, możesz się zwrócić o wsparcie.

Telefony pomocowe dla kobiet z doświadczeniem przemocy prowadzone przez Fundację Feminoteka (**feminoteka.pl**):

- **PL 888 88 33 88** czynny od poniedziałku do piątku w godzinach 11:00–19:00
- **UA 888 88 79 88** czynny od poniedziałku do piątku w godzinach 14:00–19:00

PRZEGLĄDAJ INTERNET W OKNIE INCOGNITO LUB CZYŚĆ HISTORIĘ PRZEGLĄDANIA

Na telefonie możesz skorzystać z przeglądarki **Firefox Focus**, która kasuje historię przeglądania przy zamknięciu aplikacji (patrz wyżej). Ręcznie czyść historię przeglądania w przeglądarkach **Safari**, **Chrome** czy **Firefox**. Możesz skasować całą historię, a w Chrome i Firefox wybrać konkretne adresy do usunięcia.

USTAW MOCNY PIN ALBO HASŁO

iPhone'y i nowsze Androidy zostają automatycznie zaszyfrowane, gdy chronisz je kodem PIN (ustaw co najmniej 6-cyfrowy PIN) lub hasłem.

Możesz też przeglądać strony w trybie incognito (prywatnym), w którym historia przeglądania nie zapisuje się na urządzeniu. Taką opcję oferują **Safari**, **Chrome** czy **Firefox**. Pamiętaj jednak, że tryb incognito chroni cię tylko przed innymi osobami, które chcą zajrzeć do twojego urządzenia. Nie chroni przed dostępem służb do danych internetowych – zgodnie z obowiązującym w Polsce prawem te mogą sprawdzić, jakie strony odwiedzono z twojego urządzenia/adresu IP (jeśli dane te są przechowywane w logach odwiedzanej strony lub dostawcy Internetu).

KASUJ ZBĘDNE KONWERSACJE W KOMUNIKATORACH I SMS-Y

W niektórych komunikatorach możesz włączyć znikające wiadomości (np. w Signalu) – wtedy będą kasowane automatycznie. Wtedy nawet fizyczne przejęcie urządzenia i wpisanie hasła nie pozwoli po nie sięgnąć.

Pamiętaj, że czas znikania wiadomości możesz zmieniać na bieżąco – na przykład ustawić na 4 tygodnie w grupie znajomych, a później zmienić ten czas na 1 dzień.

SPRÓBUJ ZDALNIE ZABLOKOWAĆ TELEFON
Opcje zablokowania telefonu z innego urządzenia są już standardem. Rozwiązanie „logowania awaryjnego" oferują praktycznie wszyscy producenci (nie tylko Apple).

To ty decydujesz, komu powiesz o swojej ciąży lub aborcji. Podane w tym poradniku wskazówki mogą pomóc wszystkim osobom, które chcą zadbać o swoją prywatność.

Poradnik powstał na bazie materiału Digital Defense Fund
Keep Your Abortion Private & Secure

Opracowanie:
Fundacja Panoptykon
Fundacja na Rzecz Kobiet i Planowania Rodziny FEDERA

Konsultacja techniczna: Michał „rysiek" Woźniak

Ilustracje: Hazel Mead

Projekt graficzny, projekt okładki: Jakub Sudra [sudragrafika.com]

Korekta: Urszula Dobrzańska

POMÓŻ NAM WSPIERAĆ KOBIETY, WOLNOŚĆ I PRYWATNOŚĆ!

FUNDACJA PANOPTYKON

Fundacja Panoptykon walczy o wolność i prywatność w cyfrowym świecie. Patrzy na ręce państwu i firmom, a przede wszystkim sprawdza, jak wykorzystują informacje o ludziach.

Przekaż 1,5% podatku (KRS: 0000327613)
Wpłać darowiznę: panoptykon.org/wspieraj-nas
Nr konta: PL 43 1440 1101 0000 0000 1044 6058

FEDERA

FEDERA walczy o prawo do decydowania o swoim ciele oraz o zdrowie seksualne i reprodukcyjne każdej osoby. Zapewnia dostęp do informacji i usług związanych z antykoncepcją, aborcją, badaniami prenatalnymi i prewencją raka szyjki macicy.

Prowadzi też w Warszawie Centrum Zdrowia FEDERA – miejsce, gdzie każda osoba może spokojnie i bezpiecznie uzyskać pomoc ginekologiczną, psychiatryczną i psychologiczną, a także za darmo przebadać się w kierunku chorób i infekcji przenoszonych drogą płciową.

Wpłać darowiznę: federa.org.pl/wesprzyj-nas
Nr konta: PL 19 1020 1013 0000 0002 0462 5002