

Odzyskaj prywatność

Poradnik dla zwykłych ludzi

Wersja 1.1. Aktualizacje będą dostępne na stronie <https://github.com/azsdaja/OdzyskajPrywatnosc>.

Poniższa lista przedstawia działania, jakie można podjąć, aby ograniczyć zbieranie naszych danych przez internetowe firmy. Poszczególne kroki są uszeregowane w kolejności od tych **najprostszych** technicznie, **najmniej ingerujących** w naszą wygodę i **najmocniej ograniczających** zbieranie informacji o nas.

Opis działania i poniższa legenda mogą pomóc w podjęciu decyzji, czy chcemy się na dany krok zdecydować.

Wymagana wiedza techniczna: 😊 duża, 😊😊 średnia, 😊😊😊 mała.










Wygoda użytkowania: ☂ mała, ☂☂ średnia, ☂☂☂ duża.



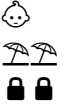
Ograniczenie zbieranych o nas danych: 🛡 małe, 🛡🛡 średnie, 🛡🛡🛡 duże.




Krok	Zmiana	Szczegóły	Jak to zrobić
PRZEGLĄDARKA Zmień przeglądarkę w komputerze 😊😊😊 ☂☂☂ 🛡🛡🛡	Chrome ↓ Firefox	W interesie Google jest zbieranie danych użytkowników, a Chrome to wspomaga. Firefox stawia na prywatność. Nie ustępuje Chrome'owi funkcjonalnością.	<ol style="list-style-type: none">1. Zainstaluj Firefoksa.2. Jeśli chcesz, zaimportuj dane z Chrome: https://support.mozilla.org/pl/kb/jak-przejsc-z-chrome-na-firefoksa3. Wejdź w <i>Opcje</i> → <i>Prywatność i bezpieczeństwo</i>:<ol style="list-style-type: none">a. Na samym dole włącz <i>Tryb używania wyłącznie protokołu HTTPS we wszystkich oknach</i> (zwiększy to bezpieczeństwo).b. Jeśli chcesz, wyłącz przesyłanie danych technicznych do Mozilli nieco wyżej w sekcji <i>Dane zbierane przez program Firefox</i>.
PRZEGLĄDARKA Zmień przeglądarkę w telefonie 😊😊😊 ☂☂☂ 🛡🛡🛡	Chrome ↓ Firefox	Jak wyżej.	<ol style="list-style-type: none">1. Zainstaluj w telefonie Firefoksa.2. Jeśli chcesz zaimportować dane z Chrome, możesz najpierw dokonać importu w przeglądarce komputerowej (patrz: wyżej), a potem zsynchronizować dane z Firefoksem na komputerze przez Firefox Sync. <p>Podobnymi i też zorientowanymi na prywatność przeglądarkami są DuckDuckGo i Brave.</p>
PRZEGLĄDARKA Zmień wyszukiwarkę 😊😊😊 ☂☂ 🛡🛡🛡	Google ↓ DuckDuckGo	DuckDuckGo oferuje anonimowe wyszukiwanie. Funkcjonalnością jest podobne do Google. Jakość wyników jest jednak gorsza (szczególnie map), dlatego warto pozostawić sobie furtkę do wygodnego korzystania z Google.	<ol style="list-style-type: none">1. W Firefoksie wybierz <i>Opcje</i> → <i>Wyszukiwanie</i> → <i>Domyślna wyszukiwarka</i> i wybierz DuckDuckGo.2. Na tym samym ekranie wejdź w <i>Skróty wyszukiwania</i> i utwórz skrót dla Google, np. „g”. Od tej pory jeśli zaczniesz wyszukiwanie od tej litery, np. „g trójmiasto”, to dostaniesz wynik dla zapytania „trójmiasto” w Google, a nie w DuckDuckGo. Warto z tego korzystać, gdy zależy nam na jakości danych, a nasze wyszukiwanie nie ujawnia żadnych informacji, które chcielibyśmy zachować dla siebie.3. Jeśli zamiast preferujesz Google jako domyślną wyszukiwarkę, ustaw skrót „d” dla DuckDuckGo.


<p>KOMUNIKACJA Zmień komunikator</p>   	<p>Messenger, WhatsApp ↓ Signal</p>	<p>Messenger dostarcza Facebookowi masy danych, w tym treści naszych rozmów. WhatsApp nie ma dostępu do treści wiadomości i rozmów oraz wysyłanych mediów, jednak w dalszym ciągu daje Facebookowi informacje, z kim się komunikujemy i jak często. Jego kod jest zamknięty (niepubliczny), a więc potencjalna „niespodzianka” umieszczona przez twórców jest trudniejsza do wykrycia. Signal jest bardzo podobny w działaniu, ale informacje o naszych kontaktach i komunikacji z nimi nie trafiają do nikogo. Ma otwarty kod.</p>	<ol style="list-style-type: none"> 1. Zainstaluj Signal w telefonie. 2. Jeśli potrzebujesz wygody, zainstaluj też wersję na komputer. Wymaga to jedynie sparowania na samym początku z telefonem przez skanowanie kodu z ekranu. 3. Chcąc się skontaktować z osobą nieposiadającą Signala, proponuj jego zainstalowanie zanim zdecydujesz się na inny komunikator.
<p>PRZEGLĄDARKA Włącz wtyczki dbające o prywatność</p>   	<p>—</p>	<p>Podane wtyczki do Firefoksa częściowo przeciwdziałają różnym formom śledzenia cię w internecie:</p> <ul style="list-style-type: none"> • Ciasteczkom śledzącym, co robimy i na jakie strony się przemieszczamy, • Serwerom CDN dostarczającym pewnych składowych wielu witryn i przy okazji odczytujących, na jakiej jesteśmy stronie, • Pikselom śledzącym, • Linkom zawierającym śledzące fragmenty. 	<ol style="list-style-type: none"> 1. W menu Firefoksa wejdź w <i>Dodatki</i> i zainstaluj poniższe wtyczki: 2. uBlock Origin (blokowanie skryptów i ciasteczek śledzących). 3. Decentraleyes (ograniczenie wglądu stron trzecich do adresów stron, na jakie wchodzimy). 4. Facebook Container (ograniczenie śledzenia przez Facebooka). 5. ClearURLs (ograniczenie śledzenia bazującego na zmodyfikowanych linkach). 6. Opcjonalnie: <ol style="list-style-type: none"> a. AdNauseam (robienie sztucznego ruchu klikając „w tle” reklamy na stronach, aby stworzyć nasz fałszywy profil konsumencki). b. Terms of Service; Didn't Read (wyświetlanie oceny polityki prywatności strony) <p>Taki zestaw wtyczek ma znikomy wpływ na wydajność przeglądarki.</p>
<p>KOMUNIKACJA Zmień narzędzie do wideokonferencji</p>   	<p>Zoom ↓ Jitsi</p>	<p>Zoom w wątpliwy sposób dba o prywatność naszych danych (zaliczył kilka wpadek), a jego twórcy mają dostęp do rozmów. Jitsi oferuje funkcjonalność podobną do Zooma, jego twórcy nie mogą podejrzewać rozmów, a jego kod jest otwarty.</p>	<ol style="list-style-type: none"> 1. W telefonie zainstaluj aplikację Jitsi Meet. 2. Na komputerze korzystaj z Jitsi w przeglądarce (https://meet.jit.si).
<p>PRZEGLĄDARKA Ogranicz śledzenie przez Google</p>   	<p>„Akceptuj wszystko” ↓ Wyłączenie czego się da</p>	<p>Zwykle kliknięcie „Akceptuj”, aby pozbyć się nieznosnego okienka przy pierwszym użyciu jakiejś usługi Google, włącza śledzenie naszej aktywności w internecie, w aplikacjach oraz śledzenie lokalizacji. Wbrew przepisom RODO, odwołanie zgody nie jest takie proste jak jej wyrażenie.</p>	<p>W telefonie i w komputerze:</p> <ol style="list-style-type: none"> 1. Wejdź w <i>Zarządzanie aktywnością</i> konta Google (https://myactivity.google.com/activitycontrols) i powyłączaj, co się da. 2. Wejdź w <i>Personalizację reklam</i> (https://adssettings.google.com) i powyłączaj, co się da.

<p>TELEFON</p> <p>Ogranicz dostęp aplikacji w telefonie do internetu</p> <p>👤👤 ☂️☂️ 🔒🔒</p>	<p>Brak ograniczeń ↓ NetGuard</p>	<p>Wszystkie aplikacje w Androidzie mają dostęp do internetu, mogą więc wysyłać różne dane na serwery ich twórców.</p> <p>Dzięki NetGuard możemy zablokować dostęp do internetu tym aplikacjom, które de facto go nie potrzebują, a mogłyby potencjalnie wysyłać nasze dane (choćby zdjęcia) na obce serwery.</p> <p>Dodatkowy plus: mniejsze zużycie danych i odcięcie od serwisów wyświetlających reklamy.</p>	<ol style="list-style-type: none"> 1. Zainstaluj i uruchom NetGuard. 2. Włącz blokowanie: <div data-bbox="1193 143 1474 322" data-label="Image"> </div> 3. Jeśli czujesz się pewny technicznie: <ol style="list-style-type: none"> a. Wejdź w <i>Ustawienia</i> → <i>Domyślne</i> i włącz blokowanie Wi-Fi i danych komórkowych. b. Ustaw zgodę dla aplikacji, dla których internet jest niezbędny. Niektóre aplikacje systemowe, np. Usługi Google Play, wymagają dostępu do internetu. 4. W przeciwnym razie: wyłącz zgodę dla aplikacji, którym chcesz zablokować internet (poprzez dotknięcie przy nich ikonki sieci WiFi i komórkowej). W razie wątpliwości, co dana aplikacja robi, lepiej zostawić zgodę. 5. Niezależnie od domyślnego ustawienia blokowania pamiętaj, żeby instalując nową aplikację podjąć świadomą decyzję: pozostawić czy zablokować jej internet.
<p>TELEFON</p> <p>Zmień klawiaturę</p> <p>👤👤 ☂️☂️ 🔒🔒</p>	<p>Wbudowana klawiatura, GBoard ↓ AnySoft Keyboard</p>	<p>Klawiatury wbudowane czy GBoard mogą wysyłać do swoich twórców wpisywane przez nas treści. Ze sposobu pisania (tempo itd.) też można wywieść pewne informacje.</p> <p>AnySoftKeyboard to niespiegująca klawiatura z otwartym kodem i dużą ilością układów i opcji.</p> <p>Jej obsługa pisania gestami ustępuje jakością powyższym klawiaturom.</p> <p>W razie nieznamości angielskiego lepszą opcją będzie prostsza OpenBoard.</p>	<ol style="list-style-type: none"> 1. Zainstaluj AnySoftKeyboard. 2. Zainstaluj Polish for AnySoftKeyboard. 3. Wejdź w systemie w <i>Ustawienia</i> → <i>Zarządzanie ogólne</i> → <i>Język i wprowadzanie</i> → <i>Klawiatura domyślna</i> i wybierz <i>polski – AnySoftKeyboard</i>. 4. W razie potrzeby uruchom aplikację AnySoftKeyboard i skonfiguruj ją po swojemu.
<p>MAPY</p> <p>Zmień aplikację do nawigacji w telefonie</p> <p>👤👤👤 ☂️☂️ 🔒🔒</p>	<p>Mapy Google ↓ Maps.Me</p>	<p>Mapy Google śledzą nasze wyszukiwania i działania.</p> <p>Maps.me to otwarta aplikacja korzystająca z publicznej bazy OpenStreetMaps (patrz: następny punkt).</p> <p>Jakość danych geograficznych jest na podobnym poziomie co w Mapach Google, a ich prezentacja jest może nawet lepsza. Posiada jednak mniej domyślną wyszukiwarke, gorsze uwzględnianie ruchu na trasie i często mniej aktualne informacje o firmach i usługach.</p>	<ol style="list-style-type: none"> 1. Zainstaluj Maps.Me. 2. W aplikacji pobierz mapy szczegółowe dla interesujących Cię regionów (Maps.me nie pobiera map na żywo). <p>Jeśli interesuje Cię korzystanie w telefonie z map satelitarnych, z odpowiednika Google Street View, z nawigacji z punktami pośrednimi lub po prostu większa konfigurowalność, wypróbuj aplikację OsmAnd (w darmowej wersji można pobrać do 7 regionów, np. województw; płatna kosztuje 20-40 zł).</p>

<p>MAPY</p> <p>Zmień mapy w przeglądarce</p>   	<p>Mapy Google ↓ OpenStreet Map</p>	<p>Mapy Google śledzą nasze wyszukiwania i działania (oczywiście nie zawsze ma to znaczenie w przypadku oglądania map). OpenStreetMap (OSM) to duży, otwarty projekt pozwalający na przeglądanie map z poszanowaniem prywatności. Jakość danych geograficznych jest na podobnym poziomie co w Mapach Google, a wygląd samej mapy w OSM jest nawet lepszy. Posiada jednak mniej domyślną wyszukiwarkę, gorsze uwzględnianie ruchu na trasie i często mniej aktualne informacje o firmach i usługach.</p>	<ol style="list-style-type: none"> Wejdź na www.openstreetmap.org. Możesz skonfigurować skrót wyszukiwania w Firefoksie dla OSM, aby łatwo móc przejść do tych właśnie map: <ol style="list-style-type: none"> Na stronie www.openstreetmap.org kliknij prawym klawiszem na pole wyszukiwania i wybierz „Utwórz słowo kluczowe dla tej wyszukiwarki...” Podłącz jako słowo kluczowe jakąś literę, na przykład „m”. Przetestuj rozwiązanie wpisując w nowej karcie np. „m Kartuzi” — zostaniesz przeniesiony do widoku miasta <p>Lista podobnych serwisów używających tej samej bazy znajduje się tutaj: https://wiki.openstreetmap.org/wiki/List_of_OSM-based_services</p>
<p>TELEFON</p> <p>Zmień sklep i aplikacje w telefonie</p>    <p>* – zależnie od konkretnej aplikacji</p>	<p>Sklep Google Play ↓ F-Droid</p>	<p>F-Droid to alternatywa dla Sklepu Google Play, która zapewnia, że aplikacje tam dostępne są darmowym oprogramowaniem o otwartym kodzie. Warto domyślnie szukać aplikacji przede wszystkim w F-Droidzie, a dopiero w razie niepowodzenia zajrzeć do Sklepu Google Play.</p>	<ol style="list-style-type: none"> Zainstaluj na telefonie F-Droid z https://f-droid.org/pl (trzeba będzie wyrazić zgodę na „instalowanie aplikacji z nieznanego źródła”). Zainstaluj przez F-Droid któreś z interesujących cię aplikacji: <ol style="list-style-type: none"> NewPipe Legacy — świetny odtwarzacz filmów z YouTube. Pozwala dodatkowo na pobieranie filmów i odtwarzanie ich przy wygaszonym ekranie. Simple Calendar Pro — prosty, przyjemny w użyciu kalendarz z możliwością definiowania przypomnień i z wygodnym widżetem. FitoTrack — pozwala rejestrować treningi i przebyte trasy. Jeśli wcześniej przegapiłeś: komunikator Signal, mapy Maps.me, wideokonferencje Jitsi.
<p>SYSTEM</p> <p>Ogranicz śledzenie przez Windows</p>   	<p>— ↓ WPD</p>	<p>Produkty Microsoftu, a zwłaszcza Windows 10, zbierają bardzo dużo naszych danych. WPD pozwala łatwo wyłączyć różne interesujące się nami funkcje systemu (z których większość jest nieprzydatna).</p>	<ol style="list-style-type: none"> Pobierz WPD z https://wpd.app i uruchom. W menu <i>Privacy</i>: <ol style="list-style-type: none"> Wyłącz wszystko, czego nie używasz. W razie wątpliwości co do danej usługi, lepiej ją pozostawić. Jeśli używasz nocnego wyświetlania, zachowaj włączoną opcję <i>Usługa użytkownika platformy podłączonych urządzeń</i> albo po prostu zainstaluj program Flux oferujący tę samą funkcjonalność co nocne wyświetlanie. W menu <i>Blocker</i>: <ol style="list-style-type: none"> Zablokuj <i>Telemetry</i>. Jeśli nie potrzebujesz, aby programy wymienione w <i>Extra</i> miały dostęp do internetu, zablokuj tę opcję. Nie blokuj opcji Update. Aktualizacje są ważne choćby ze względów bezpieczeństwa.

<p>LOKALIZACJA</p> <p>Ogranicz lokalizację w telefonie</p> 	<p>Wspomaganie ↓ Bez wspomagania (tylko GPS)</p>	<p>Android oferuje wspomaganie lokalizacji satelitarnej przez wykorzystanie sieci GSM i WiFi. Można to wyłączyć, aby zmniejszyć nieco zużycie baterii i dać Google trochę mniej informacji o naszej lokalizacji. Zysk jest jednak niewielki, a telefon może sobie gorzej radzić z wykryciem naszej pozycji.</p>	<ol style="list-style-type: none"> 1. Wejdź na Androidzie w <i>Ustawienia</i> → <i>Połączenia</i> → <i>Lokalizacja</i> <ol style="list-style-type: none"> a. <i>Metoda lokalizowania</i> → wybierz Tylko telefon b. <i>Zwiększ dokładność</i> → wyłącz dostępne opcje
<p>WSPÓŁDZIELENIE</p> <p>Współdziel dokumenty i pliki w CryptPadzie</p> 	<p>Google Docs, Office 365, Google Drive, OneDrive, Dropbox ↓ CryptPad</p>	<p>Dokumenty Google, Office 365 i inne powszechnie używane narzędzia do współdzielenia plików czy współtworzenia dokumentów dają ich twórcom dostęp do ich zawartości. Jeśli są tam dane, których nie chcielibyśmy im udzielać, warto sprawdzić CryptPad. Jest on uboższy pod kątem funkcjonalności, ale w dalszym ciągu pozwala na płynną współpracę nad m.in. plikami DOC, XLS i na dzielenie się dowolnymi plikami.</p>	<ol style="list-style-type: none"> 1. Wejdź na www.cryptpad.fr i załóż konto. <p>Darmowe konto daje 1 GB na pliki. Płatne konto kosztuje ok. 250 zł rocznie.</p> <p>Jeśli potrzebujesz wygodnego odpowiednika Formularzy Google, to warto sprawdzić Framaforms.org (niestety obecnie dostępne jedynie w języku francuskim).</p>
<p>WSPÓŁDZIELENIE</p> <p>Współdziel pliki przez folder w SyncThing</p> 	<p>DropBox, GoogleDrive ↓ SyncThing</p>	<p>SyncThing pozwala na prostą synchronizację plików między urządzeniami za pomocą zwykłego folderu (tak jak w Dropboksie). Pliki nie przechodzą przez żaden serwer, a jedynie przez nasze urządzenia, a transfer jest bardzo szybki. Dobrze nadaje się to współdzielenia plików między własnymi urządzeniami, w rodzinie czy w ramach tworzenia kopii zapasowej danych. Konfiguracja nie jest najprostsza, ale po jej wykonaniu wystarczy po prostu korzystać z wybranego folderu.</p>	<ol style="list-style-type: none"> 1. Zainstaluj SyncThing na telefonie i SyncTrayzor na komputerze. 2. Skonfiguruj wg instrukcji: https://websetnet.net/pl/synctrayzor-to-klient-synchronizacji-typu-open-source-dla-platformy-windows/

<p>ANTYWIRUS</p> <p>Zmień lub ogranicz antywirusa</p> 	<p>Windows Defender, AVG, Avast</p> <p>↓</p> <p>Windows Defender (z ewentualnymi ograniczeniami)</p>	<p>Wszystkie komercyjne i bezpłatne antywirusy mogą wysyłać nasze pliki na serwery swoich twórców ze względu na potrzebę ich analizy. Mogą one sprzedawać pewne nasze dane. Szczególnie te darmowe (np. AVG, Avast) robią to jawnie i legalnie. Potencjalnie antywirus może też pomóc służbom podsłuchiwać naszą szyfrowaną komunikację. Źródło</p> <p>Jedynym pełnoprawnym antywirusem celującym w zbieranie tylko koniecznych danych jest Emsisoft (kosztuje ok. 40-75 zł rocznie).</p> <p>Jeśli nie chcemy płacić, zaleca się wybrać mniejsze zło i polegać na wbudowanym w system antywirusie Windows Defenderze.</p>	<ol style="list-style-type: none"> 1. Usuń innego antywirusa, włącz Windows Defender (po wpisaniu w Menu Start „Ochrona przed wirusami”). 2. Opcjonalnie — jeśli chcesz wysyłać mniej danych Microsoftowi: <ol style="list-style-type: none"> a. Wejdź w <i>Ochrona przed wirusami i zagrożeniami</i> → <i>Zarządzaj ustawieniami</i> b. Wyłącz opcję <i>Ochrona dostarczana z chmury</i>, aby nie polegać na chmurze Microsoft (wykrywalność zagrożeń spada z 99% do 90%). c. Wyłącz opcję <i>Automatyczne przesyłanie próbek</i>, aby uniknąć w większości przypadków przesyłania Twoich plików do Microsoftu (może to doprowadzić do zablokowania podejrzanego pliku).
<p>POCZTA</p> <p>Załącz drugą skrzynkę</p> 	<p>Gmail, Outlook itd.</p> <p>↓</p> <p>Tutanota</p>	<p>Prawie każdy dostawca poczty ma dostęp do treści maili, jakie są przez niego wysyłane i odbierane. Poczta Tutanota szyfruje maile i kontakty w taki sposób, że jej twórcy nie mogą ich zobaczyć. Jeśli jednak wysyłamy maila na adres inny niż należący do Tutanota (np. Gmail), serwer odbiorcy będzie mógł go odczytać, dlatego korzyść co do ochrony danych jest ograniczona.</p> <p>Inne podobne rozwiązania to Protonmail oraz FastMail.</p>	<ol style="list-style-type: none"> 1. Załóż konto na https://tutanota.com/pl/ <p>Wersja darmowa daje 1 GB miejsca oraz pozwala na przeszukiwanie maili po tekście do 4 tygodni wstecz.</p> <p>Wersja płatna kosztuje (zależnie od potrzeb) od 50 zł rocznie wwyż.</p>
<p>PRZEGLĄDARKA</p> <p>Włącz czyszczenie ciasteczek przy zamknięciu przeglądarki</p> 	<p>—</p>	<p>Czyszczenie ciasteczek przy zamknięciu przeglądarki sprawia, że po ponownym jej uruchomieniu trudniej nas rozpoznać mechanizmom śledzącym (choć dalej jest to możliwe przez metody takie jak <i>fingerprinting</i>). Wiąże się to z koniecznością ponownego logowania w serwisach oraz ponownego konfigurowania ustawień prywatności na stronach.</p>	<ol style="list-style-type: none"> 1. W <i>Opcjach</i> Firefoksa wejdź w <i>Prywatność i bezpieczeństwo</i>. Zaznacz opcję <i>Usuwanie ciasteczek i danych stron podczas zamykania przeglądarki Firefox</i>. 2. Jeśli chcesz, ustaw wyjątki, tj. strony, których ta opcja nie będzie dotyczyć. 3. Wskazówka: korzystanie z menedżera haseł takiego jak KeePass pozwoli ci się szybciej logować.

<p>SYSTEM</p> <p>Zmień system w telefonie</p> 	<p>Android od Google ↓ LineageOS, /e/, GrapheneOS, SailfishOS</p>	<p>Nie da się w pełni odciąć od szpiegowania przez Google bez zmiany systemu. Jednym z powodów jest zależność od Usług Google Play, które są niezbędne do działania wielu aplikacji (ze względu na dawanie dostępu do lokalizacji, powiadomień itd.).</p> <p>Istnieje kilka alternatyw dla oficjalnego Androida. Zmiana systemu wymaga sporej wiedzy technicznej i poświęcenia czasu, a przesiadka może się wiązać z pewnymi niewygodami (zależność od projektów rozwijanych bez wielkiego budżetu). Mimo to wspomniane alternatywy mogą być wygodne i przyjemne w użyciu.</p>	<p>Zapoznaj się z alternatywami dla Androida:</p> <ul style="list-style-type: none"> • LineageOS: https://lineageos.org/ (wspierane telefony: https://download.lineageos.org/) • /e/: https://e.foundation/ (wspierane telefony: https://doc.e.foundation/devices/; szczególnie dobrze obsługuje sprzedawane przez nich zmodyfikowane Fairphone'y i Samsungi Galaxy) • GrapheneOS: https://grapheneos.org/ (wspierane telefony: kilka modeli Pixela) • SailfishOS: https://sailfishos.org/ (płatny ok. 50€; wspierane telefony: kilka modeli Sony Xperia)
<p>SYSTEM</p> <p>Zmień system w komputerze</p> 	<p>Windows ↓ Linux (Ubuntu, Mint, Manjaro, Elementary OS)</p>	<p>Zmiana systemu na Linuksa pozwala odciąć się od mechanizmów śledzących wspieranych przez Windowsa.</p> <p>Linuksy są darmowe i mają otwarty kod. Istnieją dystrybucje podobne wizualnie do Windowsa (Mint, Manjaro) czy iOS-a (Elementary OS), pozwalające na łagodniejsze wejście w świat tego systemu.</p>	<p>Przed podjęciem decyzji upewnij się, czy możesz zrezygnować z oprogramowania, którego nie uruchomisz na Linuksie (jest tego coraz mniej), albo dla którego nie ma sensownych alternatyw.</p> <p>Warto rozważyć instalację Linuksa obok Windowsa, aby móc korzystać z obydwu systemów.</p>

Źródła: <https://privacytools.io/>, <https://www.reddit.com/r/privacytoolsIO/>, <https://panoptikon.org/>, <https://restoreprivacy.com/>

Autor: Paweł Ślusarczyk. Na licencji [MIT](#).