DAVEIL


PORADNIK PRYWATNOŚCI

# Twój cień w sieci.

Jak Twoje dane osobowe trafiają do internetu, jak można Cię namierzyć i śledzić, i jak skutecznie zniknąć z radaru. Świadomość, narzędzia i Twoje prawa w jednym przewodniku.

Materiał edukacyjny · Wydanie rozszerzone 2026 · Część I & II

DAVEIL

CZĘŚĆ I · TWÓJ CIEŃ W SIECI

# 01 Zanim ktoś Cię znajdzie.

Każdego dnia zostawiasz w internecie ślady: wpisy, zdjęcia, numer telefonu na ogłoszeniu, adres e-mail przy zakupach. Pojedynczo wyglądają niewinnie. Złożone razem tworzą Twój pełny profil, dostępny dla każdego, kto wie, gdzie patrzeć.

Techniki, które to umożliwiają, noszą nazwę **OSINT** (Open-Source Intelligence, czyli biały wywiad). Posługują się nimi śledczy, dziennikarze i analitycy bezpieczeństwa. Tymi samymi metodami posługują się jednak również oszuści, stalkerzy, naciągacze „na wnuczka" oraz firmy handlujące danymi. Różnica leży wyłącznie w intencji.

CO TO JEST OSINT

### Wywiad z informacji jawnych

To zbieranie i łączenie informacji wyłącznie z publicznie dostępnych źródeł: wyszukiwarek, mediów społecznościowych, rejestrów, wycieków danych. Bez włamań i bez łamania zabezpieczeń. Cała siła tej metody tkwi w **łączeniu** drobnych okruchów w jeden obraz.

## Co znajdziesz w tym poradniku

- **Część I:** skąd biorą się Twoje dane, jak z jednego okrucha buduje się profil, jak działa śledzenie online i jak sprawdzić własną ekspozycję.
- **Część II:** filozofia prywatności w warstwach, cztery filary, zabezpieczenie urządzeń i haseł, Twoje prawa z RODO i gotowy plan działania.
- Wszystko dostosowane do **polskich realiów**: PESEL, BIK, RODO, UODO.

# 02 Skąd biorą się Twoje dane

Twój profil nie powstaje w jednym miejscu. Składa się z okruchów rozsianych po sześciu typach źródeł. Każde dokłada kolejny element układanki.

### 01 Wyszukiwarki

Indeksują wszystko, co publiczne: profile, komentarze, listy uczestników, PDF-y z Twoim nazwiskiem. To zwykle pierwszy przystanek każdego, kto Cię szuka.

### 02 Media społecznościowe

Zdjęcia, miejsca, znajomi, praca, plan dnia. Nawet prywatny profil zdradza wiele przez znajomych, oznaczenia i stare, zapomniane wpisy.

### 03 Brokerzy danych i strony „people-search"

Firmy, które agregują i odsprzedają gotowe profile: imię i nazwisko, adresy, telefony, wiek, krewni. Zwykle bez Twojej wiedzy i zgody.

### 04 Wycieki i bazy z włamań

Po każdym wycieku Twój e-mail, hasło i dane lądują w bazach krążących w sieci. Jedno stare hasło potrafi otworzyć kolejne konta.

### 05 Rejestry publiczne i firmowe

KRS, CEIDG, księgi wieczyste, ogłoszenia, sprawozdania. Legalne i jawne, a mimo to ujawniają adresy, powiązania i majątek.

### 06 Śledzenie i zdjęcia

Trackery łączą Twoją aktywność między stronami, a plik zdjęcia może nieść ukryte dane EXIF: współrzędne GPS i model telefonu.

Im więcej źródeł, tym dokładniejszy obraz. Dlatego ochrony prywatności nie załatwia jedno kliknięcie. Polega ona na **systematycznym ograniczaniu śladów** w każdym z tych miejsc.

# 03 Jeden trop wystarczy

Podstawowa zasada białego wywiadu: z jednego drobnego elementu można rozwinąć całą resztę. To tak zwany „pivoting", czyli przeskakiwanie od jednej informacji do następnej.

| | |
|---|---|
| **Adres e-mail**<br>PUNKT WEJŚCIA | Sprawdzany w bazach wycieków i przy odzyskiwaniu kont. Często prowadzi do nicku, powiązanych serwisów i starych haseł. |
| **Numer telefonu**<br>PUNKT WEJŚCIA | Ujawnia profil w komunikatorach i ogłoszeniach, a przez funkcję „odzyskaj konto" także częściowo zamaskowane dane właściciela. |
| **Nazwa użytkownika**<br>PUNKT WEJŚCIA | Ten sam nick na wielu platformach to prosty sposób na połączenie kont, które wydawały się anonimowe. |
| **Imię i nazwisko**<br>PUNKT WEJŚCIA | W połączeniu z miastem prowadzi do stron people-search, rejestrów i profili społecznościowych. Zawęża wynik do jednej osoby. |
| **Zdjęcie / twarz**<br>PUNKT WEJŚCIA | Wyszukiwanie wsteczne i rozpoznawanie twarzy potrafią odnaleźć inne miejsca, w których pojawia się ta sama fotografia. |

DLACZEGO TO WAŻNE

## Liczy się połączenie tropów

Osobno te dane wyglądają nieszkodliwie. Połączone pozwalają ustalić, kim jesteś, gdzie mieszkasz, z kim się znasz i kiedy nie ma Cię w domu. Gdy ograniczysz choćby kilka tropów, rozbijasz cały łańcuch.

# 04 Jak Cię śledzą, nawet bez cookies

Nie trzeba Cię „wyszukiwać" ręcznie. Sieć śledzi Cię automatycznie: między stronami, między aplikacjami, często bez jednego pliku cookie. Oto jak to działa.

| | |
|---|---|
| **Cookies**<br>STARY SPOSÓB | Pliki zapisane w przeglądarce, które rozpoznają Cię przy powrocie. Można je skasować, więc trackery sięgnęły po coś trwalszego. |
| **Fingerprinting**<br>ODCISK PRZEGLĄDARKI | Strony składają dziesiątki cech Twojego sprzętu i przeglądarki (wersja, język, strefa czasowa, czcionki, sposób rysowania grafiki) w niemal unikalny „odcisk". Nie da się go skasować, bo wynika z konfiguracji urządzenia. |
| **Odcisk karty graficznej**<br>BADANIE „DRAWNAPART" | Naukowcy pokazali, że nawet dwa identyczne modele urządzeń da się odróżnić po mikroskopijnych, fabrycznych różnicach GPU, a potem śledzić dłużej niż samym odciskiem przeglądarki. Działa też na telefonie, bez żadnych uprawnień. |
| **Telefon „dzwoni do domu"**<br>ANDROID | Nawet bezczynny telefon z Androidem wysyła dane do producenta i Google (oraz firm trzecich), często **bez możliwości rezygnacji**. Reset identyfikatora reklamowego niewiele daje, bo idzie on w parze ze stałym numerem sprzętu. |

TRZY MITY, KTÓRE WARTO OBALIĆ

## Incognito i brak cookies to nie ochrona

**„Tryb incognito mnie ukrywa".** Nieprawda. Incognito kasuje tylko cookies i historię; Twój odcisk pozostaje identyczny. **„Bez cookies nie da się mnie śledzić".** Da się, bo fingerprinting nie zapisuje niczego na urządzeniu. **„Reset ID reklamowego wystarcza".** To półśrodek; trwałe identyfikatory natychmiast łączą stare dane z nowym ID.

# 05 Sprawdź swoją ekspozycję

Zacznij od spojrzenia na siebie oczami osoby, która Cię szuka. Poniższy mini-audyt zajmie kilkanaście minut i pokaże, co naprawdę jest o Tobie dostępne.

- **Wygoogluj siebie.** Wpisz imię i nazwisko w cudzysłowie, dodaj miasto, pracodawcę, a potem numer telefonu i e-mail. Sprawdź też grafiki.
- **Sprawdź wycieki.** Wpisz swój adres e-mail na *haveibeenpwned.com*, by zobaczyć, w ilu wyciekach się pojawił.
- **Zobacz, kto Cię śledzi.** Wklej dowolną stronę na *themarkup.org/blacklight*. Pokaże trackery i skrypty działające w tle.
- **Przejrzyj ustawienia prywatności** głównych kont: kto widzi Twoje wpisy, znajomych, numer i datę urodzenia.
- **Poszukaj swojego nicku** i sprawdź zdjęcie wstecznie: które „anonimowe" konta da się ze sobą powiązać.

## Sygnały ostrzegawcze

Jeśli zauważasz któreś z poniższych, Twoje dane prawdopodobnie już krążą w sieci:

### Nieoczekiwane kody i resety

SMS-y lub maile z kodami logowania, o które nie prosiłeś.

### Telefony „z banku"

Rozmówca zna Twoje dane i buduje na nich zaufanie.

### Twój profil na people-search

Adres i krewni widoczni na stronie, której nie zakładałeś.

### Spersonalizowany spam

Wiadomości odwołujące się do Twoich zakupów lub lokalizacji.


CZĘŚĆ II

# Zniknij z radaru.

Wiesz już, jak łatwo Cię odnaleźć i śledzić. Teraz przechodzimy do działania: filozofia warstw, cztery filary, zabezpieczenie urządzeń i haseł, Twoje prawa z RODO i gotowy plan.

# 06 Nie musisz znikać.

Pierwsza część pokazała, jak łatwo Cię odnaleźć. Druga to działanie. I dobra wiadomość: nie musisz znikać z internetu, żeby odzyskać prywatność. Wystarczy świadomie dokładać warstwy ochrony, a każda utrudnia złożenie Twojego profilu w całość.

## Trzy zasady, na których oprzesz wszystko

| | |
|---|---|
| **Minimalizacja**<br>ZASADA 1 | Podawaj wyłącznie dane naprawdę wymagane. Każde puste pole w formularzu to o jeden trop mniej, który ktoś mógłby później wykorzystać. |
| **Kompartmentalizacja**<br>ZASADA 2 | Oddzielaj tożsamości: inny e-mail i login do banku, inny do zakupów, inny do forów. Wyciek w jednym miejscu nie odsłania wtedy całej reszty Twojego życia. |
| **Ograniczanie śladu**<br>ZASADA 3 | Tam, gdzie dane nie są wymagane prawnie (newsletter, program lojalnościowy), nie musisz podawać prawdziwej daty urodzenia czy adresu. Mniej prawdziwych okruchów to trudniejsze profilowanie. |

ZMIANA MYŚLENIA

### Prywatność budujesz warstwami

Całkowite zniknięcie jest nierealne i niepotrzebne. Chodzi o coś innego: żebyś przestał być **łatwym celem**. Każda dodana warstwa podnosi koszt i wysiłek potrzebny, by Cię namierzyć.

# 07 Cztery filary prywatności

Najwięcej zyskasz, pilnując czterech obszarów, z których najczęściej wyciekają Twoje dane. To one tworzą trzon ochrony; reszta to szczegóły.

### 01 Adres

Używaj skrytki pocztowej, paczkomatu lub adresu do korespondencji zamiast domowego. Adres zamieszkania podawaj tylko tam, gdzie naprawdę wymaga tego prawo (bank, urząd).

### 02 Telefon

Załóż drugi numer (eSIM lub VoIP) do ogłoszeń, rejestracji i sklepów. Prawdziwy numer zachowaj dla rodziny i banku, a do rozmów używaj szyfrowanych komunikatorów.

### 03 Płatności

Do subskrypcji i mniej zaufanych sklepów korzystaj z kart wirtualnych lub jednorazowych. Mniej transakcji powiązanych z Twoim nazwiskiem to mniej danych do skupienia.

### 04 Tożsamość online

Osobne aliasy e-mail i unikalne loginy do każdej usługi, przechowywane w menedżerze haseł. Jeden e-mail i nick wszędzie to gotowa mapa Twojego życia.

Nie musisz wdrożyć wszystkiego naraz. Wybierz filar, który dziś najbardziej Cię odsłania, i zacznij od niego. **Każda warstwa działa od razu**.

# 08 Zabezpiecz urządzenia i hasła

Zanim usuniesz dane z sieci, zabezpiecz to, co masz pod ręką: telefon, laptop i hasła. To pierwsza linia obrony i najtańsza w czasie.

- **Blokada ekranu i mocny kod.** PIN min. 6 cyfr (4-cyfrowy łamie się w minuty), auto-blokada po chwili, opcja „wymaż dane po 10 błędnych próbach".
- **Nie wyłączaj szyfrowania.** Współczesne telefony i laptopy szyfrują dane domyślnie. Sprawdź, że jest aktywne, i nigdy tego nie wyłączaj.
- **Wyłączony telefon = najlepiej chroniony.** Po restarcie klucze nie siedzą w pamięci. Gdy oddajesz urządzenie z rąk lub obawiasz się przejęcia, wyłącz je całkowicie.
- **Aktualizuj system.** Sprzęt bez wsparcia producenta traci ochronę przed znanymi atakami i jest najłatwiejszym celem.
- **Szyfruj dysk laptopa:** BitLocker (Windows) lub FileVault (Mac) wbudowane, albo darmowe **VeraCrypt** (Windows/Mac/Linux). Klucz odzyskiwania zapisz w bezpiecznym miejscu.
- **Szyfruj pliki ZANIM trafią do chmury.** Dane w Drive/iCloud/Dropbox dostawca zwykle może odczytać. Zaszyfruj je lokalnie (**Cryptomator**, **7-Zip** z hasłem AES) przed wysłaniem.
- **Menedżer haseł + 2FA.** Długie, unikalne hasło do każdego konta (np. **Bitwarden**, **KeePassXC**); weryfikacja dwuetapowa aplikacją lub kluczem sprzętowym, **nie SMS-em**.

ZANIM ZASZYFRUJESZ

## Utrata hasła = utrata danych

Przy każdym szyfrowaniu obowiązuje jedna żelazna zasada: jeśli zapomnisz hasła lub zgubisz klucz odzyskiwania, odzyskanie plików będzie **praktycznie niemożliwe**. Zapisz hasło i klucz w menedżerze haseł albo fizycznie, w bezpiecznym miejscu.

# 09 Twoje prawa z RODO

RODO daje Ci konkretne i zwykle **darmowe** narzędzia. Możesz ich użyć wobec każdej firmy, także wobec stron, które zebrały Twoje dane bez pytania.

| | |
|---|---|
| **Dostęp**<br>ART. 15 | Żądaj kopii danych, które firma o Tobie ma, wraz z informacją, skąd je wzięła, po co i komu je udostępnia. |
| **Usunięcie**<br>ART. 17 · „BYCIE ZAPOMNIANYM" | Żądaj skasowania danych, np. gdy nie są już potrzebne, cofnąłeś zgodę lub przetwarzano je bezprawnie. |
| **Sprzeciw**<br>ART. 21 | Sprzeciw wobec przetwarzania „w uzasadnionym interesie". Wobec **marketingu bezpośredniego sprzeciw jest bezwzględny**: muszą natychmiast przestać. |
| **Sprostowanie, ograniczenie, przeniesienie**<br>ART. 16 · 18 · 20 | Popraw błędne dane, „zamroź" ich użycie na czas sporu albo odbierz je w formacie do przeniesienia do innego dostawcy. |

## Co warto wiedzieć w praktyce

- **Administrator ma miesiąc na odpowiedź** (do 3 miesięcy przy żądaniach złożonych) i zwykle musi to zrobić bezpłatnie.
- **Brokerzy i strony people-search to też administratorzy.** Możesz wysłać im żądanie usunięcia, nawet jeśli nigdy się nie rejestrowałeś.
- **„Prawo do bycia zapomnianym" w Google** usuwa link z wyników na Twoje nazwisko, ale **nie** kasuje strony źródłowej. To dwie różne rzeczy.
- **Spór zgłosisz do UODO** (Prezes Urzędu Ochrony Danych Osobowych), a w razie kradzieży tożsamości także na policję.

# 10 Plan ochrony: od czego zacząć

Oto konkretne pierwsze kroki, dostosowane do polskich realiów. Zacznij od góry. Każdy z nich realnie zmniejsza Twoją widoczność.

**01** **Zastrzeż swoją tożsamość** POLSKA

Zastrzeż numer PESEL w aplikacji mObywatel oraz załóż zastrzeżenie kredytowe w BIK. To blokuje wzięcie kredytu czy karty na Twoje dane.

**02** **Zabezpiecz urządzenia i hasła**

Mocny kod, włączone szyfrowanie, menedżer haseł i 2FA aplikacją. Zaszyfruj dysk laptopa i wrażliwe pliki przed wysłaniem do chmury.

**03** **Ogranicz śledzenie w przeglądarce i telefonie**

uBlock Origin, prywatna wyszukiwarka, ścisła ochrona przed śledzeniem oraz higiena uprawnień aplikacji.

**04** **Usuń dane od brokerów i ze stron people-search**

Złóż wnioski o usunięcie (opt-out lub żądanie z art. 17 RODO). To żmudne i trzeba je powtarzać. Można też zlecić to wyspecjalizowanej usłudze.

**05** **Ogranicz ślad w mediach społecznościowych**

Ustaw profile jako prywatne, usuń stare i nieużywane konta, zdejmij publiczny numer i adres, przejrzyj dawne wpisy.

**06** **Korzystaj z praw RODO** UE

Żądaj dostępu (art. 15), usunięcia (art. 17) i wnoś sprzeciw (art. 21). Administrator musi odpowiedzieć; spór zgłosisz do UODO.

# 11 Jak pomaga DAVEIL

Samodzielne usuwanie danych jest możliwe, ale czasochłonne i trzeba je powtarzać, bo dane wracają. DAVEIL robi to za Ciebie i pilnuje, by zostały usunięte.

01

### Skanujemy

Przeszukujemy ponad 100 źródeł danych, by odnaleźć Twoje dane osobowe w całym internecie.

02

### Usuwamy

Składamy żądania usunięcia i pilnujemy ich aż do skutku, sami albo przekazując Ci gotowe pisma.

03

### Monitorujemy

Stale monitorujemy sieć i wykrywamy nowe wycieki Twoich danych, zanim się rozprzestrzenią.

ODZYSKAJ SWOJE DANE

## Prywatność to *Twoje* prawo.

Zacznij od bezpłatnego skanu i zobacz, gdzie w sieci znajdują się Twoje dane.

**Zacznij się chronić →**

daveil.pl · kontakt@daveil.pl

**Zastrzeżenie:** Ten dokument ma charakter wyłącznie edukacyjny i nie stanowi porady prawnej. Opis praw RODO jest uproszczony: przepisy mają wyjątki i warunki. Pełne brzmienie znajdziesz w Rozporządzeniu (UE) 2016/679 oraz na **uodo.gov.pl**. Opisane techniki przedstawiono w celu podniesienia świadomości i ochrony własnych danych. Wykorzystuj je odpowiedzialnie i zgodnie z prawem.

**Źródło i inspiracja:** opracowanie własne na podstawie ogólnodostępnej metodyki białego wywiadu i ochrony prywatności (m.in. „OSINT Techniques" oraz „Extreme Privacy" autorstwa M. Bazzella), badań nad śledzeniem i odciskiem przeglądarki/urządzenia oraz bezpieczeństwem urządzeń mobilnych, a także przepisów RODO, w wersji skróconej, przetworzonej i dostosowanej do polskich realiów. Nazwy własne należą do ich właścicieli.