

Inwigilacja na kółkach

1 czerwca 2025

Tvoja codzienna jazda do pracy staje się wynikiem punktacji behawioralnej, a twój samochód nawet nie pyta o pozwolenie.



Gratulacje. Kupiłeś samochód. Może nawet wybrałeś wersję premium – z obsługą głosową, synchronizacją z chmurą i podgrzewanymi uchwytemi na kubki, które znają temperaturę twojego latte, zanim ty ją poznasz. Siadasz za kierownicą i czujesz się panem swojego małego świata. Fotel się dopasowuje, drzwi zamykają się z satysfakcjonującym kliknięciem, a ty znikasz w świętej prywatności fotela kierowcy.

Tylko że... nie kupiłeś samochodu. Wydzierżawiłeś kapsułę inwigilacyjną.

Brak telefonu, brak prywatności?

Tu wkraczają paranoiczni minimaliści. Chwalą się: „Nie podłączam telefonu. Nawet nie używam Bluetootha. Mój samochód to po prostu samochód”. Ale w nowoczesnych pojazdach telefon to tylko przystawka. Menu inwigilacyjne ciągnie się dalej – z twoją zgodą lub bez niej.

Czujniki szpiegowskie

Dzisiejszy samochód zawiera ponad 100 czujników. To, co kiedyś było siedzeniem i kierownicą, jest teraz toczącym się laboratorium biomedycznym z krzemowymi szpiegami.

Twój samochód zbiera:

- dane GPS z każdej trasy;**
- styl jazdy: hamowanie, przyspieszanie, omijanie przeszkód;**
- obrazy z kamer: z zewnątrz i wewnątrz (w tym rozpoznawanie twarzy);**
- nagrania z mikrofonu: „Sterowanie głosowe” to nagrywanie non stop;**

- dane biometryczne: waga, postawa, kierunek spojrzenia;
- aktywność w kabinie: ilu pasażerów, jak się poruszają.

Po co? „Dla bezpieczeństwa”. W rzeczywistości: dla zysku. Ubezpieczyciele wykorzystują dane z jazdy do ustalania składek. Reklamodawcy śledzą twoje trasy. Policja żąda dostępu do lokalizacji lub nagrań audio. Pośrednicy danych zbierają, „anonimizują” i sprzedają informacje. W przeciwieństwie do danych finansowych czy zdrowotnych, dane z pojazdów są prawie niechronione prawnie. Nie ma obowiązku ujawniania, brak jasnych regulacji. Tylko PR-owy bełkot.

Zawsze włączone

Czy możesz to wszystko wyłączyć? Najczęściej nie. Przynajmniej nie bez młotka. Nawet przy wyłączonych usługach niektóre auta nadal wysyłają dane przez wbudowane karty SIM.

Niektóre systemy oferują „Connected Services” czy „Remote Diagnostics”. Brzmi niewinnie. Ale są to legalne furtki dla monitoringu w czasie rzeczywistym. Nawet gdy ustawisz „wyłączone”, często aktywna pozostaje jakaś ścieżka danych. Brak ostrzeżeń, brak kontrolek, brak zielonego światełka jak w telefonie, gdy działa mikrofon. Kamera w samochodzie? Nie ma opcji „Proszę, nie filmuj mojej twarzy”.

Teraz robi się naprawdę niepokojąco: twój samochód nie interesuje się tylko trasą – interesują go twoje emocje.

Przykłady:

- śledzenie wzroku (eye tracking): mierzy uwagę, kierunek spojrzenia;**
- rozpoznawanie ruchu: analizuje nastrój;**
- tętno: odczytywane przez kierownicę;**
- rozpoznawanie pasażerów: czujniki wykrywają pozycję, napięcie pasów, szacują wiek.**

Co dzieje się z tymi profilami? Kto je przechowuje? Kto jest ich właścicielem? Odpowiedź: nie

wiadomo. I to jest celowe.

**Wielu ludzi wzrusza ramionami.
„Smart” dziś znaczy: „szpieg”.**

Nowa normalność?

**OnStar – usługa General Motors –
przez lata potajemnie zbierała
dane: sposób hamowania, prędkość,
godziny jazdy, wybór muzyki. I
sprzedawała je pośrednikom danych.
Kierowcy dowiedzieli się o tym
dopiero przez pozwy sądowe. Teksas
pozwał GM: ponad 14 milionów
pojazdów stało się bez zgody
kierowców odkurzaczami danych.**

**2024 rok: wyciek danych w VW, Audi,
Skodzie i Seacie. Dane
lokalizacyjne, e-maile, numery**

telefonów – publicznie dostępne.
Luka bezpieczeństwa trwała
miesiącami.

2023 rok: sygnaliści ujawnili, że
pracownicy Tesli mieli dostęp do
nagrań z kamer klientów i dzielili
się nimi wewnątrz – np. filmami
z nagimi osobami biegającymi po
garażach. Brak ochrony, brak zasad,
brak przejrzystości.

Kia zbierała dane o stylu jazdy –
hamowanie, nocne przejazdy, krótkie
trasy – i przekazywała je
ubezpieczycielom bez zgody
klientów. Efekt: podwyżki składek
bez ostrzeżenia.

Mozilla w 2024 r. przeanalizowała
praktyki ochrony danych w branży
motoryzacyjnej:

- 84% dzieli się danymi z podmiotami trzecimi;**
- 76% sprzedaje dane dalej;**
- 0% spełnia podstawowe wymagania prywatności;**
- tylko Renault i Dacia oferują prawo do usunięcia danych.**

Wniosek: według Mozilli samochody to „najgorsza kategoria produktów” pod względem prywatności – gorsza niż smart TV, opaski fitness czy smartfony.

Po połączeniu z danymi zewnętrznymi (np. numery telefonów, historia kredytowa, użycie streamingu) powstają niezwykle precyzyjne profile behawioralne:

- Miejsce zamieszkania, zwyczaje zakupowe, stany emocjonalne;**
- GPS + mikrofon = psychologiczny profil ryzyka;**
- analiza głosu wykrywa kłótnie – rekomendacja: podwyżka ubezpieczenia.**

Jak się bronić?

- Nigdy nie podłączaj telefonu bezpośrednio. Używaj Bluetooth w trybie audio lub osobnego urządzenia bez danych osobistych.**
- Wyłącz dostęp do danych pojazdu. Szukaj w ustawieniach systemowych opcji typu „Connected Services”, „Telematics”, „Remote Access” – i dezaktywuj.**

– Przed sprzedażą lub oddaniem usuń dane. Przywróć ustawienia fabryczne, rozłącz urządzenia, wyłoguj konta.

– Używaj „burnerów”. Tanie urządzenia do muzyki i map – bez kontaktów, wiadomości czy logowania.

– Wymagaj przejrzystości. Pytaj sprzedawcę. Czytaj politykę prywatności. Wspieraj przepisy o ochronie danych. Wywieraj presję w sieciach i na forach.

Twój samochód nie jest już neutralną maszyną. To toczący się system inwigilacji. Nie możesz go całkiem zatrzymać. Ale możesz go spowolnić. I zmusić producentów, żeby przestali szpiegować w

**ukryciu. To twoje dane. Powinny
jechać razem z tobą. Nie być
sprzedawane.**

Autorstwo: Christina Maas

Ilustracja: WolneMedia.net (CC0)

Źródło zagraniczne:

[ReclaimTheNet.org](https://reclaimthenet.org)

Źródło polskie: WolneMedia.net