

# Gdy obywatele walczą

2 lutego 2017

Słynny niemiecki prawnik Rudolf von Jhering twierdził, że dobre prawo powstaje, gdy zdeterminowane jednostki chcą walczyć o swoje interesy i znajdują się sędziowie oraz instytucje, które pragną tych interesów chronić. Dynamiczny rozwój nowych technologii sprawia, że bardzo często przepisy nie nadążają za postępem. W takich sytuacjach mogą pojawić się poważne ryzyka dla praw obywatelskich – w tym prawa do prywatności. Potrzebni są więc odważni obywatele gotowi zawalczyć o swoje prawa, którzy pomogą sądom w „docieraniu” standardów ich ochrony.

Prezentujemy 5 spraw, które przysłużyły się lepszej ochronie prywatności. Może zainspirują one innych do sięgnięcia po swoje prawa. Pierwszym krokiem może być złożenie skargi do Generalnego Inspektora Ochrony Danych Osobowych.

## 1. MAX SCHREMS I JEGO SPORY Z „FACEBOOKIEM”

Max Schrems jest austriackim aktywistą, który zyskał niemałą sławę w związku ze swoimi sporami z „Facebookiem”. Austriak w 2012 r. skierował do irlandzkiego komisarza ds. ochrony danych 22 skargi dotyczące polityki prywatności Facebooka i... zaczął odnosić pierwsze sukcesy w starciu z internetowym gigantem. Najgłośniejsza ze spraw zainicjowanych przez Schremsa dotyczyła programu Safe Harbour, który umożliwiał amerykańskim firmom przekazywanie danych Europejczyków na drugą stronę Atlantyku. Schrems zakwestionował legalność transferu swoich danych zamieszczonych na Facebooku na serwery, które ta firma posiada w Stanach Zjednoczonych. Schrems zwrócił się do irlandzkiego organu ochrony danych osobowych (którego jurysdykcji podlega europejski oddział amerykańskiego giganta), by ten wydał decyzję zakazującą Facebookowi takich praktyk. Organ jednak stwierdził, że jest związany wspomnianą decyzją Komisji Europejskiej z 2000 r., i odmówił rozpatrzenia

sprawy. Schrems nie poddał się, a sprawa trafiła do irlandzkiego sądu najwyższego, który uznał, że ten spór powinien rozstrzygnąć Trybunał Sprawiedliwości Unii Europejskiej. W konsekwencji unijny Trybunał zawiesił obowiązywanie programu Safe Harbour, a Bruksela i Waszyngton musiały ponownie usiąść do stołu negocjacyjnego.

## **2. O HISZPANIE, KTÓRY CHCIAŁ ZNIKNAĆ Z GOOGLE**

Mario Costeja González po wpisaniu swojego nazwiska do wyszukiwarki Google odnalazł link do strony internetowej gazety ze wzmianką o licytacji nieruchomości zajętej ze względu na niespłacone przez niego należności na rzecz zakładu ubezpieczeń społecznych. Zajęcie nieruchomości było już zakończone, a sprawa niespłaconych należności nieaktualna. Zwrócił się więc do Google Spain, żądając usunięcia tych informacji. Firma odrzuciła jego żądanie, powołując się na model biznesowy wyszukiwarki, która nie modyfikuje, a jedynie indeksuje dostępne w Internecie treści. Tak zawiązał się spór, który swój finał znalazł przed Trybunałem Sprawiedliwości Unii Europejskiej. Sędziowie orzekli, że operator wyszukiwarki przetwarza dane osobowe, jest więc odpowiedzialny za wyniki wyszukiwania. Oznacza to, że osoba, której dane (np. imię i nazwisko) wyświetlają się na liście wyników wyszukiwania, może zwrócić się bezpośrednio do operatora o usunięcie linku z listy wyników wyszukiwania. Trybunał uznał przy tym, że europejskie przepisy mogą być stosowane również wobec Google – firmy z siedzibą w USA, ponieważ prowadzi ona działalność gospodarczą (np. w postaci sprzedaży reklam) również w Unii Europejskiej.

## **3. IRLANDCZYCY PRZECIWKO RETENCJI**

Digital Rights Ireland to mała irlandzka organizacja, która zajmuje się sprawami cyfrowymi. W 2012 r. wniosła przed Irlandzki Sąd Najwyższy sprawę przeciwko przepisom antyterrorystycznym, które dotyczyły obligatoryjnego gromadzenia danych telekomunikacyjnych. Sprawa ta znalazła

swój finał w Luksemburgu dwa lata później. Trybunał Sprawiedliwości Unii Europejskiej uznał, że przepisy, które zobligowały państwa członkowskie do nałożenia na operatorów telekomunikacyjnych obowiązku przechowywania danych telekomunikacyjnych, np. billingów, na „wszelki wypadek”, w nieproporcjonalny sposób ingerują w prywatność Europejczyków. Tym samym Trybunał potwierdził zastrzeżenia, jakie zgłaszano od lat: prewencyjne gromadzenie danych o wszystkich połączeniach telekomunikacyjnych i ich udostępnianie organom ścigania bez kontroli sądu stanowi nieproporcjonalne naruszenie praw i wolności obywatelskich.

#### **4. BO IP TO TEŻ DANE OSOBOWE**

Niemiecki polityk z Partii Piratów Patrick Breyer sprzeciwiał się gromadzeniu przez niemieckie służby adresów IP osób, które odwiedziły ich strony. Sprawa przeszła przez niemieckie instancje sądowe i ostatecznie wylądowała w Luksemburgu. W sprawie pojawiły się dwa pytania: czy adres IP można uznać za dane osobowe oraz czy instytucje prowadzące strony mogą przetwarzać tego typu informacje. Na oba te pytania luksemburski Trybunał odpowiedział twierdząco: adres IP, nawet ten dynamiczny, jest daną osobową. Samo orzeczenie nie jest rewolucyjne i raczej potwierdza znane już poglądy. Może mieć natomiast istotne znaczenie dla praktyki administratorów stron internetowych. Obecnie adresy IP gromadzi się często „domyślnie”. Wyrok w sprawie Brejera być może wymusi na właścicielach witryn więcej refleksji w tej kwestii.

#### **5. WĘGRZY KONTRA INWIGILACJA SŁUŻB**

Dwoje węgierskich działaczy społecznych, Mate Szabo i Beatrix Vissy, zakwestionowało ustawę o policji, która według nich naruszyła ich prawo do prywatności. Po zmianach wprowadzonych w 2011 r. ustawa pozwala specjalnym oddziałom antyterrorystycznym na niejawnie przeprowadzanie przeszukań domów, instalowanie podsłuchów, otwieranie listów i przesyłek, a także na niekontrolowane przeglądanie i rejestrowanie

korrespondencji elektronicznej. Sprawą zajął się Europejski Trybunał Praw Człowieka, który uznał, że kwestionowane przepisy mogą dotknąć każdą osobę przebywającą na terenie tego kraju i każdą położoną tam nieruchomość, a obywatele nie dysponują żadnym środkiem weryfikacji, czy byli poddani nadzorowi. Wprowadzenie specjalnych uprawnień służb na potrzeby walki z terroryzmem jest zdaniem Trybunału uzasadnione, jednak Węgry powinny jednocześnie zagwarantować dostateczną ochronę praw swoich mieszkańców. Przepisy prawa powinny wskazywać, że podsłuchiwanie i przechwytywanie komunikacji jest możliwe jedynie wobec osób, co do których istnieje uzasadnione podejrzenie o działalność terrorystyczną. Podjęte środki powinny zaś podlegać zewnętrznej, najlepiej sądowej, kontroli (choćby następczej). Gdy tylko będzie to możliwe bez narażania na szwank prowadzonego postępowania, należy poinformować sprawdzaną osobę o podjętych wobec niej działaniach.

Źródło: [Panoptykon.org](https://panoptykon.org)

## **BIBLIOGRAFIA**

1.  
<https://panoptykon.org/wiadomosc/czy-dzialania-studenta-prawa-z-austrii-doprowadza-do-zamknienia-programu-safe-harbour>
2.  
<https://panoptykon.org/wiadomosc/wyjscie-z-bezpiecznej-przystani-musi-bolec>
3.  
<https://panoptykon.org/wiadomosc/wyrok-tsue-w-sprawie-google-konieczny-choc-zgnily-kompromis>
4.  
<https://panoptykon.org/wiadomosc/dyrektywa-retencyjna-jest-nie-wazna>
- 5.

<https://panoptykon.org/wiadomosc/trybunal-w-luksemburgu-ip-dane-osobowe>

6 .

<https://panoptykon.org/wiadomosc/etpc-prawo-musi-przewidywac-gwarancje-dla-prywatnosci>