

---

## Telefony pod specjalnym nadzorem

Unijne przepisy określają, że dane o abonentach powinny być gromadzone maksymalnie na dwa lata, ale może być to krótszy okres. Polska postanowiła wybrać wariant najdłuższy. Dlatego operatorzy telekomunikacyjni przez 24 miesiące przechowują informacje o naszych billingach telefonicznych, lokalizacji telefonów komórkowych, a nawet nieudanych połą-

czeniuach. Muszą je udostępnić na potrzeby policji, sądów, prokuratury czy Agencji Bezpieczeństwa Wewnętrznego. Tak szeroki zakres informacji, w dodatku przechowywanych przez tak długi czas, jest nie tylko niepotrzebny, ale też niebezpieczny – uważają uczestnicy debaty, która odbyła się w redakcji „DGP”.

[lukasz.kuligowski@infoc.pl](mailto:lukasz.kuligowski@infoc.pl)

B10 | PRAWO

# Zbieramy dużo da

- **DEBATA „DGP”** Dane o połączeniach abonentów przechowywane są za długo
- *Bilingi telefoniczne są wykorzystywane nawet w sprawach rozwodowych*
- *Polska nie przewidziała skutków szerokiego dostępu do danych abonentów*

**W redakcji „Dziennika Gazety Prawnej” odbyła się debata na temat przechowywania danych telefonicznych i internetowych obywateli. Zaproszeni goście dyskutowali m.in. o konsekwencjach implementacji do polskiego prawa tzw. dyrektywy retencyjnej, która zawiera zasady przechowywania i zbierania danych dotyczących abonentów.**

## Implementacja dyrektywy retencyjnej

**WOJCIECH RAFAŁ WIEWIÓROWSKI**  
Polska wdrożyła dyrektywę retencyjną w sposób niezgodny z założeniami unijnych projektodawców. Dyrektywa ta miała bowiem ułatwić ściganie poważnych przestępstw. Tymczasem ze względu na drobne błędy, które nasz kraj popełnił

Ustawodawca skupił się na implementacji tylko w odniesieniu do danych telekomunikacyjnych. Zapominał o zwiększeniu pewnych gwarancji dla obywateli w momencie, kiedy wprowadza się bardzo inwazyjny środek inwigilacji społecznej. Dane retencyjne to nowy typ inwigilacji polegający na tym, że dane są gromadzone przez podmiot prowadzący działalność gospodarczą, ale mogą być i są wykorzystywane operacyjnie przez służby specjalne czy policję. Gromadzone dane telekomunikacyjne pozwalają określić lokalizację obywatela. Z tym że na przykład w Portugalii dostęp do takich danych jest możliwy w sytuacji przestępstwa związanego np. z zabójstwem. W Polsce dostęp taki jest możliwy w przypadku niemal każdego przestępstwa.

**KAZIMIERZ MORDASZEWSKI**  
Celem dyrektywy było wykorzystanie danych retencyj-

na. Prawo telekomunikacyjne mówi ogólnie o obowiązku retencji danych, natomiast w kwestii określenia zasad dostępu do danych retencyjnych odsyła do innych ustaw. To z poszczególnych ustaw regulujących uprawnienia służb wynika, jak w przypadku ABW czy CBA, że służby te mogą wykorzystywać dane retencyjne w celu realizacji swoich ogólnych zadań. Katalog tych zadań jest dość szeroki. Dlatego też nie mamy prawnych gwarancji, że dane retencyjne nie są wykorzystywane w nieodpowiedni sposób.

**WOJCIECH RAFAŁ WIEWIÓROWSKI**  
Są sytuacje, które dowodzą, że osoby chcące zapewnić szeroki zakres retencji danych nie przewidziały, jak zostaną one wykorzystane w Polsce. Z pewnością nie po to zostały wprowadzone przepisy o retencji danych, by były wykorzystywane w spra-

w maksymalnym wymiarze. W maksymalnym na skalę europejską. Zbierane są one w zakresie przewidzianym dyrektywą retencyjną. Zbierane są także dane dotyczące trasowania połączenia, co oznacza, że zatrzymywane są dane o lokalizacji urządzenia końcowego w sieci telefonii ruchomej wyłącznie w trakcie trwania połączenia telekomunikacyjnego. Takie rozwiązanie niekoniecznie wprost wynika z dyrektywy. Co do tego istnieją różne interpretacje prawne, a o ile wiem, Komisja Europejska nigdy nie odpowiedziała wprost, czy jest to interpretacja właściwa.

**MIROSLAW MAJ**  
Tworzymy regulację przeciwko terrorystom. Tymczasem oni użyją takich technik informatycznych, że nawet przy retencji danych wynoszącej 20 lat nic to nie pomoże w walce z terroryzmem. Natomiast ryzyko wykorzystania dostępu do



**dr Wojciech Rafał Wiewiórowski**  
generał inspektor ochrony danych osobowych



**prof. Andrzej Adamski**  
Wydział Prawa i Administracji Uniwersytetu Mikołaja Kopernika w Toruniu



**Kazimierz Mordaszewski**  
dyrektor biura prawnego w Agencji Bezpieczeństwa Wewnętrznego



**Katarzyna Szymielewicz**  
członek zarządu i założycielka Fundacji Panoptikon zajmującej się ochroną praw człowieka

przy jej implementacji do polskiego porządku prawnego, uprawnione jest wykorzystanie danych retencyjnych w postępowaniach dotyczących bardzo szerokiej gamy zdarzeń, w tym w postępowaniu cywilnym. Błąd polega na tym, że stwarzając sądom możliwość występowania o dane retencyjne, nie ograniczono tego uprawnienia wyłącznie do sądów karnych. W konsekwencji dane te są wykorzystywane w postępowaniach cywilnych, np. w sprawach rozwodowych. Zatem nie dość, że przedsiębiorcy świadczący usługi telekomunikacyjne są zobowiązani do gromadzenia i przechowywania przez 2 lata danych o połączeniach, które umożliwiają ustalenie, z kim i kiedy się kontaktowali, jak długo trwała rozmowa oraz z jakiego miejsca ją wykonywali, to jeszcze muszą udostępniać te dane na żądanie zbyt dużej liczby podmiotów.

**ANDRZEJ ADAMSKI**  
W przypadku implementacji dyrektywy prawo zostało naruszone w dwóch miejscach.

nych w sprawach poważnych przestępstw, a w szczególności do zwalczania terroryzmu. Dyrektywa powstała na fali zamachów terrorystycznych i wówczas głosy w tej sprawie były jak najbardziej pozytywne. Obowiązek przechowywania danych telekomunikacyjnych uznano za niezwykle potrzebny w zwalczaniu poważnych przestępstw. Na temat wprowadzenia retencji danych do prawa telekomunikacyjnych toczyła się w Sejmie dyskusja, podczas której pojawiały się propozycje, by okres przechowywania danych przez operatorów telekomunikacyjnych trwał nie 24 miesiące, a nawet pięć lat. Dobrze, że pozostał okres 24 miesięcy, na który wskazuje dyrektywa, bowiem w przypadku wydłużonego okresu narazilibyśmy się na zarzut naruszenia dyrektywy. Takie dane są istotne, np. by można było zapobiegać zamachom terrorystycznym.

**KATARZYNA SZYMIELEWICZ**  
Polska implementacja dyrektywy retencyjnej jest specyficz-

wach cywilnych. Należy podkreślić również, że dyrektywa retencyjna nie jest wdrożona w zakresie świadczenia usług drogą elektroniczną.

**MIROSLAW MAJ**  
Po atakach terrorystycznych 11 września 2001 roku oraz zamachach w Londynie i Madrycie wzrosła aktywność legislacyjna w obszarze dotyczącym retencji danych telekomunikacyjnych. W przypadku Madrytu organy ścigania sięgnęły po dane z grudnia 2003 roku. Zamach był w marcu 2004 roku. Wystarczyło sięgnąć po dane sprzed czterech miesięcy do znalezienia potrzebnych informacji. Tak jest w większości przypadków. W dodatku wystarczyły same dane billingowe. Nie ma dowodów na to, że tak głęboka i szeroka retencja danych jak w Polsce jest potrzebna.

**MAREK JURKIEWICZ**  
W Polsce z woli ustawodawcy zatrzymywane i przechowywane są dane telekomunikacyjne

danych zwykłych obywateli istnieją. Zbieramy zbyt wiele informacji o zwykłych ludziach, co jest dużym ryzykiem.

## Konsekwencje szerokiego dostępu do danych

**ANDRZEJ ADAMSKI**  
Z badań, które były przeprowadzone w odniesieniu do przestępstwa drobnego, jakim jest posiadanie narkotyku, wynika, że w takich sprawach rutynową praktyką polskich prokuratorów jest żądanie danych billingowych i zlecenie ekspertyz biegłym, po to by poszerzyć materiał dowodowy o listę interakcji telekomunikacyjnych między podejrzanym a osobami, które się z nim kontaktowały. Skutkuje to tym, że osoby, które widnieją w wykazie połączeń, są wzywane do prokuratury i przesłuchiwane w charakterze świadków. W ten sposób rozszerza się zarzuty z posiadania narkotyku na zaangażowanie po-



# nych o abonentach

dejrzanego w handel narkotykami. To jest przykład wskazujący na to, że środek, który miał służyć do walki z poważną przestępczością, w praktyce przybiera zupełnie nieoczekiwaną postać i służy do inwigilowania zwykłych obywateli w błahych sprawach.

**KATARZYNA SZYMIELEWICZ**

Nie mamy wiarygodnych danych na temat użycia danych retencyjnych w Polsce. Służby najprawdopodobniej same takich statystyk nie tworzą, a jeśli tworzą, odmawiają nam prawa do tej informacji ze względu na klauzulę tajemnicy. Mamy jednak dostęp do bardzo pouczających wyników badań z Niemiec. Badacze z Max Planck Institute ustalili, że konieczność użycia danych retencyjnych – czyli danych przechowywanych specjalnie na potrzeby organów egzekwowania prawa o wiele więcej, niż dane telekomunikacyjne standardowo trzymane przez operatorów na ich własne potrzeby – występuje niezwykle rzadko. Okazało się, że były one użyteczne tylko w 0,01 proc. spraw karnych.



**Mirosław Maj**

prezes Fundacji Bezpieczna Cybprzestrzeń zajmującej się bezpieczeństwem teleinformatycznym

**ANDRZEJ ADAMSKI**

W 2009 roku było 1 mln zapytań o dane retencyjne od służb. Przepisy o retencji danych zaczęły obowiązywać 1 stycznia 2010 roku. Dlatego nasuwa się pytanie, czy implementacja nie poluzowała namiastki mechanizmów kontrolnych obowiązujących w poprzednim prawie. W ustawie o policji nie ma już mechanizmu kontrolnego, który polegał na tym, że gdy oficer policji ustnie zgłaszał się o udostępnienie danych do operatora, to ten mógł o tym zawiadomić komendanta wojewódzkiego. Przepis ten zniknął, gdyż policja ma bezpośredni dostęp do takich danych i nikogo o nic nie musi pytać. To jest nie do przyjęcia w państwie prawnym.

**KAZIMIERZ MORDASZEWSKI**

Ustawa o policji rzeczywiście nie zawiera zamkniętego katalogu określającego dostęp do danych przechowywanych przez operatorów telekomunikacyjnych. Natomiast w ustawie o ABW sam zakres zadań mówi o poważnych przestępstwach. W ustawie o CBA też

jest mowa o poważnych przestępstwach, choć w tym przypadku można mieć wątpliwość co do postępowań kontrolnych. Zakres dostępu danych jest więc wyszczególniony. W przypadku policji sprawa jest dyskusyjna. Jednak możliwość łączności z danymi w sieciach telekomunikacyjnych pokazuje, czy do systemu łączy się uprawniony policjant. Jest możliwość sprawdzenia, kto, kiedy i po co się zalogował. Przełożeni mogą to sprawdzić bez problemu.

**WOJCIECH RAFAŁ WIEWIÓROWSKI**

Większość zapytań o udostępnienie danych przechowywanych przez operatorów nie dotyczy samych billingów. Są to zapytania dotyczące rozpoznania abonenta, czyli sprawdzenia, kto jest właścicielem danego numeru telefonu. Nie jest to zapytanie o to, w jaki sposób dana osoba łączyła się z siecią. Dziwi jednak brak protestów operatorów, którzy są przymuszani przez prawo do działań związanych z przechowywaniem danych. Zastanawiam się, czy dyrektywa nie jest dla nich o tyle wygodna, że dzięki temu



**Marek Jurkiewicz**

zastępca dyrektora departamentu spraw obronnych w Urzędzie Komunikacji Elektronicznej

**MAREK JURKIEWICZ**

przerzucają na abonentów koszty dotyczące bezpieczeństwa ich systemów, które musieli by ponieść, nawet gdyby nie było takich obowiązków. W rozwinięciu polskim to przedsiębiorcy telekomunikacyjni ponoszą koszt procesu zatrzymywania i przechowywania danych. Są państwa, gdzie jest identycznie jak w Polsce. W niektórych krajach UE ciężar ten spoczywa w całości lub częściowo na państwie. UE zwraca na to uwagę w dyrektywie, zalecając rozważenie ewentualnego zwrotu kosztów ponoszonych przez operatorów. Wola polskiego ustawodawcy jest jednak taka, jak to wpisano w przepisy prawa. Te koszty to koszty ujęcia danych ich przechowywania, zabezpieczenia. Czasem to także koszty odfizjowania danych, jakiegoś rodzaju wydruków, jakie muszą przygotować, gdy dostaną zapytanie o dane ze strony uprawnionych podmiotów, sądów lub prokuratury. Dyrektywa wskazuje, że dane trzeba zatrzymywać, o ile są one dostępne. Dotyczy to nie-

stety nie tylko informacji potrzebnych przedsiębiorcy telekomunikacyjnemu, ale także informacji pojawiających się w sieci czy przetwarzanych przez przedsiębiorców. Przykładem może tu być zatrzymywanie danych o połączeniach nieudanych, zbędnych dla przedsiębiorcy, a objętych obowiązkiem.

## Koszty finansowe będą ponosić abonenci

**KATARZYNA SZYMIELEWICZ**

Operatorzy przyznają, że ponoszą duże nakłady finansowe na zbieranie i przechowywanie tych danych. Bardzo szeroki jest także zakres gromadzonych informacji – zbierane są nawet dane o nieudanych połączeniach i o lokalizacji rozmówcy. Co prawda Komisja Europejska twierdzi, że celem dyrektywy nie miało być zbieranie większej ilości danych niż standardowo gromadzone przez operatorów, a jedynie wydłużenie okresu ich zatrzymywania. Tak jednak nie jest. Ostatecznie dyrektywa retencyjna wymusza na operatorach wdrożenie dedykowanych systemów zbierania i przechowywania danych właśnie pod kątem wymogów związanych z retencją danych. Telekomunikacja Polska w odpowiedzi przesłanej Komisji Europejskiej twierdzi, że na samo wdrożenie takiego systemu wydała ok. 200 mln zł. Jednocześnie operatorzy przyznają, że te koszty nie mają wpływu na ich konkurencyjność na rynku europejskim. Być może gromadzone dane o abonentach przydają się więc operatorom do innych celów? To, w jaki sposób mogą być wykorzystane dane o codziennej komunikacji obywateli, zaprezentowali badacze MIT (Massachusetts Institute of Technology). Z ich analizy wynika, że dzięki danym lokalizacyjnym i billingowym można w 90 proc. przypadków ustalić, gdzie będziemy w ciągu 12 godzin, z kim się spotkamy i co będziemy robić.

**MIROSLAW MAJ**

Jest wiele podobnych badań. Jedne z nich pokazują, że nie wiedząc nic o osobie, której dotyczy, a mając znaczącą ilość danych, jesteśmy w stanie ustalić, kim jest ta osoba. Nie musimy mieć żadnego przywiązania tych danych do konkretnej osoby. Nie jestem jednak przeciwny temu, by te dane były gromadzone. Powinny być i powinny być wykorzystywane. Praktyka pokazuje, że dotychczasowy sposób ich wykorzystania jest wystarczający.

**MAREK JURKIEWICZ**

W sytuacji gdy ktośkolwiek ponosi jakieś koszty i za bardzo nie protestuje, należy domniemywać, że ma z tego jakieś korzyści lub inny sposób na zbilansowanie wydatków. To jest prosty mechanizm rynkowy. Możemy pytać przedsiębiorców, jak to jest, ale wątpię, czy się doczeka-

my szczerzej odpowiedzi na tak postawione pytanie. Firmy telekomunikacyjne świadczące usługi mobilne mają w swojej ofercie usługi lokalizacyjne przeznaczone dla indywidualnego abonenta. Ważne jest jednak to, że dotyczy to aparatu telefonicznego, a raczej aktywnej karty SIM należącej do tego abonenta. Abonent, kupując usługę, wyraża zgodę na przetwarzanie tego rodzaju danych. Dane lokalizacyjne, technicznie rzecz biorąc, są przetwarzane przez przedsiębiorcę, są one bowiem niezbędne do świadczenia usługi. Upraszczając – sieć operatora musi wiedzieć, gdzie jest urządzenie końcowe, by być w gotowości do jego obsłużenia. Inną jednak sprawą jest dokładne wskazanie, gdzie się znajduje urządzenie końcowe, i to z dużą dokładnością. W końcu gdy abonent polskiego przedsiębiorcy znajdzie się za granicą, informacja lokalizacyjną dostępną przedsiębiorcy, całkowicie mu wystarczającą jest informacja, że jest np. w Niemczech. A więc nie wszystkie dane lokalizacyjne i nie zawsze bardzo dokładne są potrzebne operatorom.

**KAZIMIERZ MORDASZEWSKI**

Kwestia kosztów ponoszonych przez operatorów jest istotna, ale dotyczy tak naprawdę przyjętego w Polsce modelu. W Unii Europejskiej są różne modele finansowania działalności związane z retencją danych. Gdyby operator nie ponosił tych kosztów, to służby, sądy i prokuratury musiałyby być finansowane w tym zakresie z budżetu państwa. Placiliby więc wszyscy obywatele. W obecnym modelu placą tylko abonenci.

**ANDRZEJ ADAMSKI**

Istnieje obszar różnic, jeżeli chodzi o kategorię danych, jakie powinny być zatrzymywane według dyrektywy, a które z punktu widzenia biznesowego operatorom do niczego nie są potrzebne. Przykładem są informacje o nieudanych próbach połączeń. Są one gromadzone, mimo że operatorzy wystawiają rachunki za zrealizowane połączenia. Koszt zbudowania bazy danych o takich połączeniach w przypadku Telekomunikacji Polskiej wyniósł około 20 mln zł. Powstaje pytanie o wartość danych o nieudanych połączeniach. Tak naprawdę nieważne jest, czy połączenie było udane, czy nie. Nawet nieudane połączenie wskazuje na pewną interakcję, która sama w sobie może być interesująca. Nawiasem mówiąc, wstępny raport Komisji Europejskiej wskazuje, że średni okres retencji danych w Unii Europejskiej wynosi 12 miesięcy. Przez taki czas polscy operatorzy przechowują dane o połączeniach np. do celów rozliczeniowo-reklamacyjnych. Te same dane mogłyby więc również służyć organom ścigania. Rzecz w tym, że dyrektywa rozszerza katalog danych podlegających zatrzymaniu.

**DEBATĘ PROWADZIŁ  
ŁUKASZ KULIGOWSKI**