

Katarzyna Szymielewicz

Anna Mazgal

Współpraca: Dorota Głowacka, Józef Halbersztadt

INTERNET A PRAWA PODSTAWOWE

Ekspresowy przegląd problemów regulacyjnych



INTERNET A PRAWA PODSTAWOWE

Ekspresowy przegląd problemów regulacyjnych



Warszawa
sierpień 2011

Autorki

Katarzyna Szymielewicz
Anna Mazgal

Współpraca

Dorota Głowacka
Józef Halbersztadt

Raport stanowi podsumowanie informacji i opinii zawartych w licznych stanowiskach Fundacji Panoptykon i Internet Society Poland oraz w następujących opracowaniach:

1. Michał Małyszko, „Jak działa Internet i co z tego wynika dla jego regulacji?”
2. Tomasz Rychlicki, „Ograniczanie praw podstawowych w kontekście ochrony prawnoautorskiej w środowisku teleinformatycznym”
3. Krzysztof Siewicz, „Ponowne wykorzystanie informacji sektora publicznego”
4. Grzegorz Pacek, „Jak należy uregulować odpowiedzialność za treść w Internecie. Wybrane aspekty”
5. Andrzej Adamski, „Retention of telecommunication data in Poland: does the legal regulation pass the proportionality test?”
6. Wojciech Czarnecki, „Jak usunąć pornografię dziecięcą z Internetu?”
7. Dariusz Adamski, „Zasady wykorzystywania przez służby specjalne danych telekomunikacyjnych w aspekcie obowiązującego stanu prawnego oraz tendencji regulacyjnych w Polsce i Unii Europejskiej”

Wydawca

Fundacja Panoptykon / <http://panoptykon.org>

Projekt graficzny, skład i łamanie

CityLab / www.citylab.pl

Druk

Drukarnia Ghaj, ul. Przytorowa 19, 16-400 Suwałki

Wszystkie materiały są dostępne do pobrania na stronie internetowej <http://panoptykon.org>

Raport jest dostępny na licencji Creative Commons Uznanie autorstwa 3.0 Polska.

Raport powstał dzięki wsparciu Open Society Foundations.

WSTĘP OD AUTOREK

5 Walka o „wolny i otwarty internet” staje się strategicznym frontem walki o prawa podstawowe we współczesnym świecie. Walki, która nie może się zakończyć sformułowaniem - choćby najbardziej postępowej - „karty praw internetu”. Podobnie jak w przypadku podstawowych praw człowieka i obywatela, proces kształtowania standardów nigdy nie jest raz na zawsze zakończony i raz na zawsze wygrany.

W dyskusji o standardach dotyczących tego szczególnego obszaru trzeba jednak pamiętać o jednym: internet jest zgromadzeniem, mową, prasą i informacją. Każdy atak na sieć, to bezpośredni zamach na te wolności. Niektóre rządy i instytucje zrozumiały już doniosłość tego stwierdzenia. Finlandia i Estonia uznały dostęp do „społeczeństwa informacyjnego” za podstawowe prawo obywatelskie. W marcu 2009 r. internet został nawet nominowany do pokojowej Nagrody Nobla.

Równolegle obserwujemy jednak tendencję odwrotną: do demonizowania sieci i akcentowania zagrożeń wynikających z jej anarchistycznego potencjału. Na fali medialnych doniesień uciera się przekonanie, że nawet jeśli nie zaatakują nas haker, spamer, wirus komputerowy czy kryjący się w sieci przestępca seksualny, to co najmniej padniemy ofiarą kradzieży tożsamości.

Brak zaufania w stosunku do cyberprzestrzeni zwiększa prawdopodobieństwo nieprzemyślanych propozycji regulacyjnych, które nie rozwiązując realnych problemów społecznych mierzą w wartości, jakimi stoi internet. Próby kontrolowania i cenzurowania przepływu informacji w sieci, zastraszanie i aresztowanie blogerów, utajnianie obrad organów państwowych, angażowanie prywatnych firm do egzekwowania prawa w internecie - to tylko niektóre przejawy tej tendencji.

Minimum, o jakie musimy w tej sytuacji zadbać, to uczciwa debata publiczna na temat granic, jakich w internecie przekroczyć nie wolno: zarówno jego użytkownikom, jak i regulującemu sieć państwu.

Celem tego opracowania nie jest szczegółowe omówienie problemów regulacyjnych w obszarze internetu i praw podstawowych, ale jedynie ich nazwanie, uporządkowanie i zebranie w jednym miejscu. Przekazujemy Państwu rodzaj mapy, która

może pomóc w ukierunkowaniu poszukiwań i zdefiniowaniu problemów, natomiast w kwestiach szczegółowych odsyła do innych źródeł. Polecamy go szczególnie osobom, które - nie posiadając wiedzy eksperckiej - chcą rozpoznać podstawowe problemy i wyzwania w tym obszarze oraz zorientować się w możliwych kierunkach zmian regulacyjnych. Ekspertów zainteresowanych pogłębionymi opracowaniami odsyłamy na stronę <http://panoptykon.org>, gdzie pod hasłem „Sieć Panoptykon” publikujemy odrębne analizy, dotyczące każdego z poruszanych w raporcie wątków regulacyjnych.

W omawianiu poszczególnych tematów przyjęliśmy zasadę wyodrębnienia analogicznych elementów, aby w maksymalnie kompleksowy sposób opisać regulacyjny wymiar poruszanych problemów. Tymi elementami są:

- podstawowe dylematy, z jakimi musi się zmierzyć prawodawca oraz wartości (nie tylko te, zawarte w Konstytucji), które za nimi stoją;
- mapa aktorów, która w żadnej mierze nie wyczerpuje całej palety możliwych zależności i interesów, natomiast ilustruje najważniejsze dążenia i oczekiwania, które musi uwzględnić prawodawca;
- scenariusze regulacyjne, które - nie wyczerpując wszystkich możliwych kombinacji - odnoszą się do tych najbardziej racjonalnych i prawdopodobnych (lub już realizowanych);
- dobre kierunki, które w naszej opinii da się zrealizować w ramach - lub dzięki kombinacji - niektórych scenariuszy oraz rekomendacje, odpowiadające na bardziej złożone problemy, które wykraczają poza podstawowe scenariusze regulacyjne;
- dobre i złe praktyki, które ilustrują, w jaki sposób można wykorzystać szanse albo zmaterializować zagrożenia, związane z realizacją praw obywatelskich w danym obszarze.

Na końcu opracowania znajduje się aneks, zawierający skrótową prezentację obowiązującego prawa, najważniejszego orzecznictwa i polecanych źródeł.

Mamy nadzieję, że wędrówka po tej mapie problemów zachęci Państwa do głębszego zainteresowania się problematyką praw podstawowych i regulacji internetu.

INTERNET A PRAWA PODSTAWOWE

Ekspresowy przegląd problemów regulacyjnych

SPIIS TREŚCI

RETENCJA DANYCH TELEKOMUNIKACYJNYCH I ICH UDOSTĘPNIANIE NA POTRZEBY WALKI Z PRZESTĘPCZOŚCIĄ	6
ODPOWIEDZIALNOŚĆ POŚREDNIKÓW ZA TREŚĆ W INTERNECIE	16
BLOKOWANIE STRON INTERNETOWYCH	26
EGZEKWOWANIE PRAW AUTORSKICH W ŚRODOWISKU CYFROWYM	36
POWTÓRNE WYKORZYSTANIE INFORMACJI PUBLICZNEJ	46
ANEKS	57

RETENCJA DANYCH TELEKOMUNIKACYJNYCH

i ich udostępnianie na potrzeby walki z przestępczością

WPROWADZENIE

9 Obowiązkowa retencja danych to zatrzymywanie informacji o wszystkich rodzajach połączeń elektronicznych na potrzeby bezpieczeństwa publicznego. Zgodnie z ustawą Prawo telekomunikacyjne, operatorzy muszą przechowywać dane niezbędne do ustalenia kto, kiedy, gdzie, z kim i w jaki sposób się połączył lub próbował połączyć. Dane te są przedmiotem zainteresowania służb specjalnych, policji, prokuratury i sądów ponieważ mogą stanowić cenne źródło informacji i dowodów w sprawach prowadzonych przez te organy. Polskie prawo umożliwia wykorzystywanie tych danych nie tylko do wykrywania poważnych przestępstw, ale także w celach prewencyjnych. Wszystkie uprawnione służby mają dostęp do danych retencyjnych bez kontroli sądu i prokuratora. Stwarza to bardzo wysokie ryzyko nadużyć.

60

średnio tyle rodzajów śladów elektronicznych pozostawiają po sobie użytkownicy w różnych miejscach internetu.

W 2009 r. służby, policja i sądy sięgały do danych telekomunikacyjnych ponad milion razy. W 2010 r. ta liczba zwiększyła się o ponad 1/3. Jednocześnie, analiza przeprowadzona przez ministra ds. służb specjalnych na polecenie premiera Donalda Tuska pokazała, że w obecnym stanie prawa i praktyki nie można w pełni ustalić, jakiego rodzaju są to zapytania, ani kto je kieruje do operatorów. Ponad połowa (56%) dokonywanych sprawdzeń pozostaje niewiadomą, ponieważ policja, sądy i prokuratury nie przedstawiły żadnych szczegółowych danych na ich temat.

1 milion
tyle razy sięgano do naszych danych w 2009 r.

Dane na podstawie sprawozdań operatorów telekomunikacyjnych dla Urzędu Komunikacji Elektronicznej.

Nie ma potwierdzenia związku między skutecznością w tropieniu przestępstw a obowiązkiem zatrzymywania danych. Dla organów ścigania kluczowa jest dostępność danych, a ta nie jest ściśle zależna od obowiązku retencji. Na podstawie doświadczeń innych krajów okazuje się bowiem, że ilość danych przechowywanych przez dostawców usług telekomunikacyjnych w celach komercyjnych jest z zasady wystarczająca.

Koszt ograniczenia prawa do prywatności obywateli, jakim jest przetrzymywanie danych o ich komunikacji z innymi, jest ogromny. Jak pokazują badania przeprowadzone przez MIT, taki zestaw informacji nie tylko pozwala na ustalenie, z kim utrzymywaliśmy kontakty, gdzie byliśmy i jak się poruszaliśmy w przeszłości, ale także na profilowanie i przewidywanie naszych zachowań w przyszłości. W przypadku zawodów zaufania publicznego (dziennikarzy, lekarzy, prawników) retencja stwarza dodatkowe ryzyko: podważenie zasady poufności, zagrożenie dla tajemnicy zawodowej czy ochrony źródeł informacji dziennikarskich.

56%

to odsetek sprawdzeń, dla którego policja, prokuratura i sądy nie potrafią przedstawić szczegółowych danych.

Kluczowy problem tkwi w mechanizmie gromadzenia danych na wszelki wypadek, zgodnie z zasadą, że każdy obywatel jest „potencjalnie podejrzany”. Wątpliwe, czy takie podejście może być uzasadnione w demokratycznym państwie prawnym. Ile społeczeństwo jest w stanie poświęcić dla iluzorycznego poczucia bezpieczeństwa? Służby kierują się logiką: im więcej wiedzą o obywatelach, tym więcej są w stanie przewidzieć i tym większej ilości zagrożeń mogą zapobiec. Czy instytucjonalizacja tego myślenia nie prowadzi do nowego totalitaryzmu?

Obywatelskich, Generalny Inspektor Ochrony Danych Osobowych, Naczelna Rada Adwokacka, a nawet minister ds. służb specjalnych. Propozycja zmian, które rozwiązują zidentyfikowane problemy, musi opierać się na ich rzetelnej analizie i obiektywnych danych na temat działania nie tylko służb, ale także operatorów telekomunikacyjnych. Tej niezbędnej bazy w polskiej debacie publicznej wciąż brakuje.

Obecny reżim obowiązkowej retencji danych trzeba zmienić. Jest to nie tylko opinia organizacji pozarządowych; podobnego zdania jest Rzecznik Praw

10



Wygoda działania służb, a nie względy konieczności, decydują o ingerencji w konstytucyjną wolność i ochronę tajemnicy komunikowania się.

Rzecznik Praw Obywatelskich prof. Teresa Lipowicz, list RPO do Premiera Donalda Tuska w sprawie pozyskiwania przez służby informacji objętych tajemnicą komunikowania się
za: <http://www.sprawy-generalne.brpo.gov.pl/pdf/2010/12/662587/1540465.pdf>

DYLEMAT**1**

Ile informacji o obywatelach rzeczywiście potrzeba, żeby skutecznie wykrywać poważne przestępstwa?

Sprzeciw wobec obowiązkowej retencji danych telekomunikacyjnych nie powinien być utożsamiany ze sprzeciwem wobec umożliwienia policji i służbom dostępu do takich danych. Organy egzekwowania prawa powinny, w określonych okolicznościach, móc korzystać z danych gromadzonych przez operatorów i inne podmioty prywatne.

11

Czy przetrzymywanie szerokiego zakresu danych przez operatorów wyłącznie na potrzeby potencjalnych przyszłych postępowań jest niezbędne? A może jest po prostu wygodne, bo ułatwia uprawnionym organom dostęp do nich? Być może ten sam cel udałoby się osiągnąć na podstawie danych, jakie operatorzy przetwarzają w związku ze swoją bieżącą działalnością: na potrzeby rozliczeń, reklamacji, logistyki, itp. Wielu ekspertów twierdzi też, że w walce z przestępczością zorganizowaną drążenie danych (*data mining*) nie zastąpi tradycyjnych metod śledczych (informatorzy, infiltracja środowiska itp.).

DYLEMAT**2**

Jak umożliwić służbom skuteczne wykonywanie ich pracy, jednocześnie chroniąc obywateli przed skutkami niekontrolowanego dostępu do danych retencyjnych?

W Polsce dane retencyjne są udostępniane na każde żądanie upoważnionych do tego organów, bez kontroli sądu czy prokuratora. Prawo pozwala na ich wykorzystywanie przy wykrywaniu każdego rodzaju przestępstw, a nawet w ogólnie pojętych celach prewencyjnych. Skutkuje to rekordową liczbą sprawdzeń u operatorów. Tymczasem prowadzone w innych krajach badania nie wykazują związku między obowiązkiem zatrzymywania danych a wzrostem wykrywalności przestępstw.

Bez współpracy policji i służb nie sposób ustalić, czy taka zależność występuje w Polsce. Organy te nie chcą tłumaczyć społeczeństwu, z jakich metod korzystają w pracy operacyjnej.

Ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw.

”

DYLEMAT 3

Jak pogodzić potrzebę stworzenia precyzyjnych przepisów z nieprzewidywalnością spraw, w których dane telekomunikacyjne mogą okazać się przydatne?

Prawo powinno być tak skonstruowane, żeby wszyscy - obywatele, służby i operatorzy rozumieli, jakie mają prawa i obowiązki. Brak ustawowego ograniczenia katalogu spraw, w których można wykorzystywać dane retencyjne jest sprzeczny z tą zasadą i sprzyja arbitralności decyzji sądów, policji i służb.

Z drugiej strony prawo powinno elastycznie odpowiadać na rzeczywiste wyzwania. Można to osiągnąć np. w oparciu o orzecznictwo sądowe. Oparcie się na decyzjach sędziów w tej materii wymaga jednak kompetentnych w sprawach dochodzeniowych i nieprzeciążonych sądów.

WARTOŚCI

Zasada demokratycznego państwa prawnego

Decyzje podejmowane przez prawodawcę powinny być oparte na weryfikowalnych danych i przejrzystych argumentach. Jest to warunek niezbędny, żeby obywatele mogli sprawować realną kontrolę nad władzą ustawodawczą.

Prywatność i tajemnica korespondencji

Ilość, zakres i czas przechowywania danych telekomunikacyjnych w połączeniu z dość swobodną możliwością sięgnięcia do nich przez policję i służby, zagrażają tym prawom obywatelskim.

Swoboda działalności gospodarczej

Daje operatorom podstawę do sprzeciwu wobec praktyk zmierzających do nałożenia na nich dodatkowych obciążeń (np. obowiązku przechowywania zbędnych z biznesowego punktu widzenia danych) bez możliwości zwrotu kosztów.

Efektywność działania organów egzekwowania prawa

Jest często argumentem za ułatwieniem im dostępu do danych. Zmierzających do nałożenia na nich dodatkowych obciążeń (np. obowiązku przechowywania zbędnych z biznesowego punktu widzenia danych) bez możliwości zwrotu kosztów.

retencja danych

wynika z podstawowej potrzeby operatorów, jaką jest gromadzenie informacji potrzebnych w rozliczeniach i komunikacji z klientami. Ustawa Prawo telekomunikacyjne nakłada na operatorów dodatkowy obowiązek zatrzymywania (retencji) tych i innych danych, z uwagi na to, że mogą być przydatne organom ścigania. Ten pierwszy rodzaj retencji nie budzi sprzeciwu z punktu widzenia ochrony praw podstawowych. Natomiast prewencyjny aspekt obowiązkowej retencji danych godzi w domniemanie niewinności, jakie jest podstawą nowoczesnych systemów prawnych.

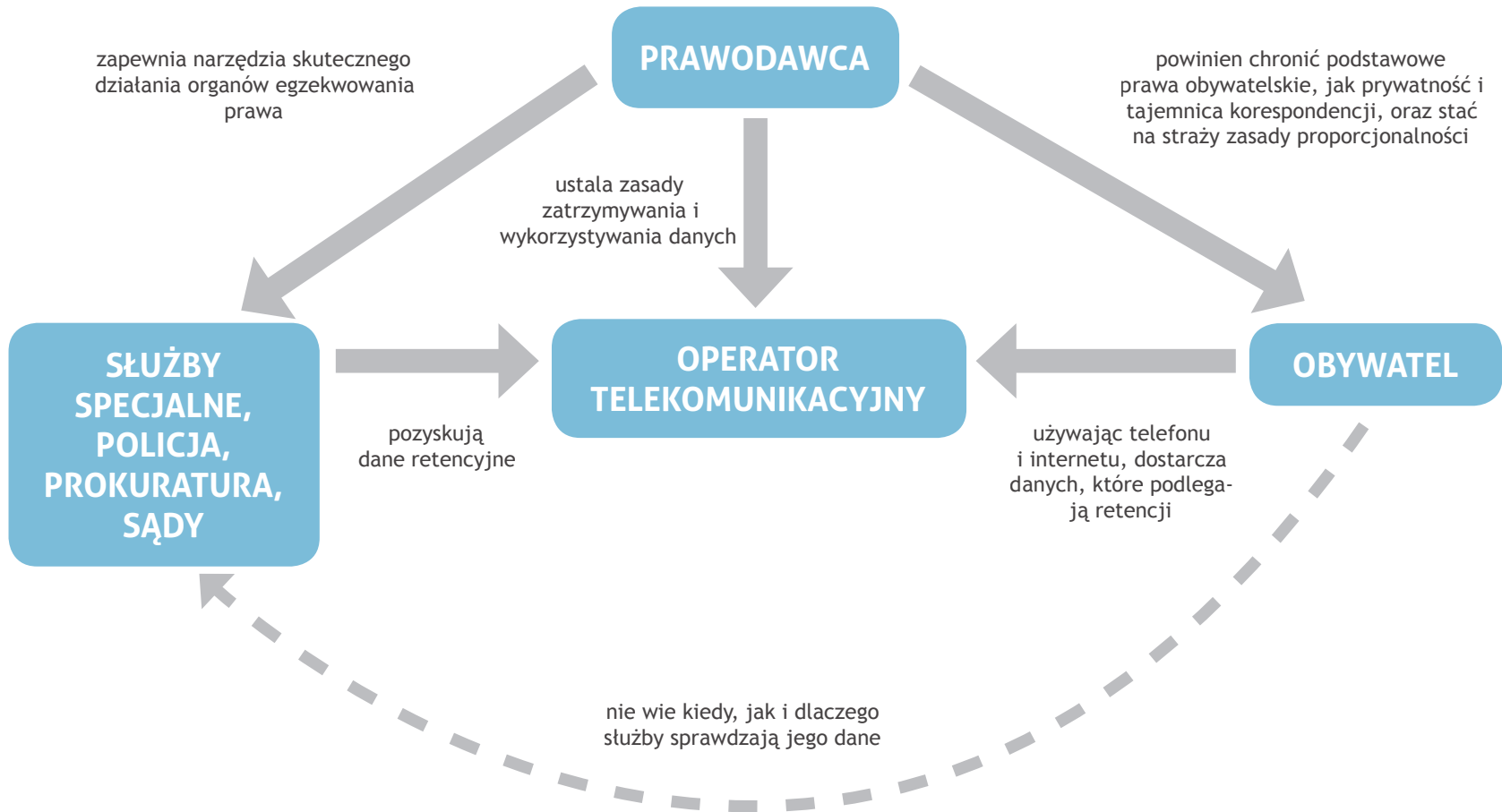
Bezpieczeństwo publiczne

Zwolennicy retencji danych twierdzą, że bez ustawowego obowiązku zatrzymywania danych telekomunikacyjnych na potrzeby potencjalnych postępowań karnych, organy ścigania byłyby pozbawione istotnego narzędzia.

Konieczność i proporcjonalność

Zgodnie z Konstytucją, ograniczenia praw i wolności obywatelskich są dopuszczalne tylko, jeśli są konieczne i proporcjonalne. Nie wystarczy zatem wykazanie „użyteczności” narzędzia takiego, jak retencja danych, które w ewidentny sposób ogranicza prawo do prywatności.

GŁÓWNI AKTORZY I DANE RETENCYJNE W OBECNYM STANIE PRAWNYM



Niektóre scenariusze zakładają jedynie uszczelnienie i doprecyzowanie przepisów (1 i 4); inne – stworzenie mechanizmów kontroli nad dostępem do danych (3). Jeszcze inne, jak scenariusz 2, przewidują zniesienie obowiązku retencji i korzystanie tylko z mechanizmu zamrażania danych. Można też rozważyć scenariusze pośrednie i łączyć zawarte w nich propozycje.

SCENARIUSZE ZMIANY OBOWIĄZUJĄCEGO PRAWA

SCENARIUSZ 1 - „Ucywilizowanie” przepisów

1. Ograniczenie dostępu do danych retencyjnych poprzez wprowadzenie wymogu uzyskiwania zgody sądu bądź prokuratora (zgoda następcza w nagłych przypadkach).
2. Stworzenie zamkniętego katalogu przestępstw i innych spraw (np. zaginięcia), w związku z którymi sądy, prokuratura, policja i służby mogłyby sięgać po dane retencyjne.
3. Skrócenie okresu przechowywania danych do 6 miesięcy, uznawanego za niezbędny w oparciu o obiektywne dane na temat wykrywania przestępstw.
4. Weryfikacja katalogu służb uprawnionych do korzystania z danych retencyjnych (zmiany w przepisach kompetencyjnych).
5. Wprowadzenie obowiązku zwrotu kosztów ponoszonych przez operatorów w związku z realizacją ich obowiązków w zakresie retencji danych.

SCENARIUSZ 2 - Zniesienie obowiązku retencji

Rezygnacja z obowiązkowej retencji danych, przy zachowaniu mechanizmu szybkiego zamrażania danych wraz z udoskonaleniem go.

SCENARIUSZ 3 - Stworzenie skutecznych mechanizmów nadzoru nad służbami

1. Wprowadzenie kontroli GIODO nad przetwarzaniem danych przez organy uprawnione do korzystania z danych retencyjnych.
2. Zobowiązanie policji i uprawnionych służb do statystycznej, ale szczegółowej, sprawozdawczości z wykorzystywania danych retencyjnych.
3. Zobowiązanie UKE do przeprowadzania przy wsparciu GIODO szczegółowej kontroli, jakie dane i jak długo przechowują operatorzy telekomunikacyjni.
4. Ulepszenie mechanizmów wewnętrznej kontroli nad

zamrażanie danych

to zatrzymywanie (przez operatora telekomunikacyjnego wskazanych danych na wniosek uprawnionej służby w związku z konkretnym, już toczącym się, postępowaniem. Zamrożenie dokonywane jest natychmiastowo, bez oczekiwania na decyzję sądu, co skutecznie zapobiega utracie cennych danych, które inaczej mogłyby zostać skasowane, jako zbędne dla operatora. Aby jednak uzyskać dostęp do zamrożonych danych potrzebna jest zgoda sądu.

przetwarzaniem danych telekomunikacyjnych w policji i innych służbach.

5. Zobowiązanie służb do informowania obywatela po zakończeniu postępowania o tym, że jego dane były przedmiotem ich zainteresowania.
6. Utworzenie niezależnego organu nadzorującego działanie służb, do którego obywatele mogliby kierować swoje skargi.

SCENARIUSZ 4 - Zmiana ogólnych zasad dostępu do danych telekomunikacyjnych

1. Zweryfikowanie zasad uzyskiwania przez policję i inne uprawnione służby dostępu do wszelkich danych telekomunikacyjnych - zarówno informacji o samych połączeniach, jak i o treści komunikacji.
2. Wprowadzenie - jako zasady - obowiązku uzyskiwania zgody sądu na dostęp do danych, w tym na dostęp do danych lokalizacyjnych z systemu GPS oraz treści wiadomości wysyłanych przez użytkowników portali społecznościowych lub poczty elektronicznej.

Tyle razy proszono w 2008 r. w krajach Unii Europejskiej o dane z sieci komórkowych starsze niż rok. O dane starsze niż 21 miesięcy wniosków było jedynie 40.

891

Dane na podstawie raportu Komisji Europejskiej z ewaluacji dyrektywy o retencji danych.

PODSUMOWANIE SCENARIUSZY – DOBRE KIERUNKI

1. Zastąpienie obowiązkowej retencji zamrażaniem danych

Uprawnione organy miałyby jedynie dostęp do danych, jakie operatorzy przetwarzają w związku ze swoją bieżącą działalnością: na potrzeby rozliczeń, reklamacji, logistyki, itp. Analizy doświadczeń innych krajów wskazują, że takie rozwiązanie pozwala na skuteczne wykrywanie przestępstw.

2. Precyzyjne określenie powodów uzasadniających możliwość korzystania z retencji

Gdyby zniesienie obowiązku retencji danych okazało się niemożliwe, należałoby stworzyć zamknięty katalog przestępstw i innych spraw (np. zaginięcia), w związku z którymi można by sięgać do danych retencyjnych.

3. Skrócenie okresu przechowywania danych do 6 miesięcy

4. Stworzenie skutecznych mechanizmów nadzoru nad służbami

Kompleksowa reforma zasad przetwarzania danych telekomunikacyjnych musi zakładać wprowadzenie skutecznych mechanizmów kontroli nad działaniami służb specjalnych, zgodnie z założeniami scenariusza 3.

5. Zaostrzenie ogólnych zasad dostępu do danych telekomunikacyjnych

Dostęp do wszelkich danych telekomunikacyjnych powinien być uregulowany analogicznie do zasad korzystania z podsłuchu: wymagana byłaby zgoda sądu, a w nagłych przypadkach zgoda następcza.

Dyskusja o utrzymaniu retencji powinna zostać oddzielona od dyskusji na temat zaostrzenia zasad dostępu do danych telekomunikacyjnych oraz zwiększenia kontroli nad działaniami operacyjnymi policji i służb. Kwestia pierwsza budzi wiele kontrowersji i wymaga dłuższej dyskusji. W kwestii drugiej panuje względna zgoda, zatem scenariusz 4 powinien być realizowany.

KWESTIE DO ROZSTRZYgniĘCIA - REKOMENDACJE

1. Tworzenie prawa w oparciu o dowody (zasada *evidence-based policy making*)

Prawodawca nie przedstawia szczegółowych statystyk, porównujących wykrywalność przestępstw z krajów, które wprowadziły obowiązek retencji oraz z takich, które radzą sobie innymi metodami. Nikt - ani obywatele, ani ich ustawowi reprezentanci - nie mogą zweryfikować, czy decyzje ograniczające ich prawa i wolności mają oparcie w dowodach. Jest to sprzeczne z zasadami nowoczesnego prawodawstwa. Przy zmianie przepisów należałoby zatem zadbać o zgromadzenie odpowiednich danych i opracowanie szczegółowych uzasadnień dla proponowanych rozwiązań.

2. Wprowadzenie kontroli sądów nad wykorzystywaniem danych retencyjnych

Należy rozważyć zwiększenie roli sądów w decydowaniu o tym, czy dane telekomunikacyjne mogą być wykorzystane w danej sprawie czy procesie dochodzenia. Obecnie sądy powszechne nie są odpowiednio przygotowane do podejmowania tego typu decyzji, skoro same żądają danych retencyjnych od operatorów nawet na potrzeby sporów cywilnych, np. spraw rozwodowych, czy o alimenty. Taka zmiana wymagałaby jednak kompleksowej reformy systemu sądownictwa.

3. Skuteczna kontrola nad praktykami retencyjnymi operatorów telekomunikacyjnych

W rzeczywistości wiadomo bardzo niewiele o tym, jakie dane, na jak długo i w jakich celach są gromadzone przez operatorów. Powoduje to, że trudno ustalić, z jakich danych rzeczywiście korzystają uprawnione organy. Nie wiadomo też, czy zasada przetrzymywania danych nie starszych niż 2 lata jest ściśle przestrzegana. Dlatego niezbędnym elementem reformy prawa powinien być wymóg audytu praktyk stosowanych przez operatorów.

16

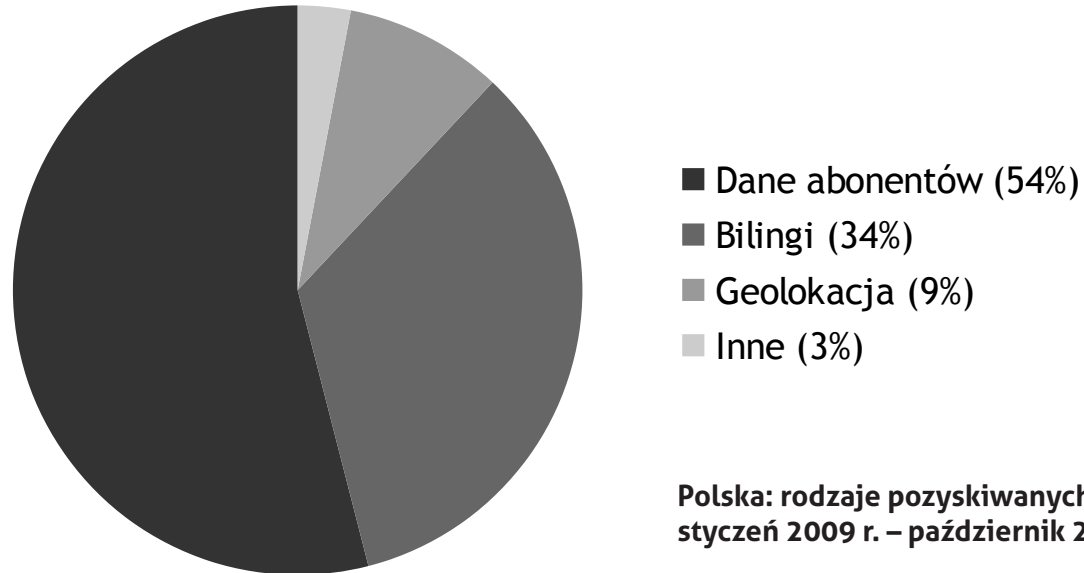


Uświadomiliście nam na nowo, jak ogromnym wyzwaniem jest internet; że nie można [go] traktować jak zwykłego narzędzia, gdzie decyzje administracyjne albo ograniczenia o charakterze prawnym czy ustawowym są bezkarne, albo których konsekwencje nie są szczególnie groźne.

Premier Donald Tusk w podsumowaniu cyklu rozmów poświęconych regulacji Internetu za: <http://www.panoptikon.org/wiadomosc/co-maja-wspolnego-prawa-podstawowe-i-internet-proba-podsumowania-rozmow-z-rzadem>

4. Uwzględnienie dostępu do danych innych niż telekomunikacyjne w debacie o retencji

Należy rozpocząć debatę nad zasadami dostępu służb do wszelkich danych generowanych przez użytkowników nowych technologii, tj. danych lokalizacyjnych z systemu GPS; danych klientów portali społecznościowych, wyszukiwarek czy dostawców poczty elektronicznej; danych klientów firm świadczących usługi drogą elektroniczną; danych z „inteligentnych” sieci przesyłowych; danych generowanych przez tzw. internet przedmiotów itd. Potencjalny zakres retencji jest o wiele większy niż informacje o połączeniach telefonicznych czy internetowych, a z czasem będzie się on tylko poszerzać.



Polska: rodzaje pozyskiwanych danych
styczeń 2009 r. – październik 2010 r.

17

DOBRA PRAKTYKA

Rumuński Trybunał Konstytucyjny (październik 2009 r.), Niemiecki Federalny Sąd Konstytucyjny (marzec 2010 r.) i Czeski Trybunał Konstytucyjny (marzec 2011 r.) **stwierdziły niekonstytucyjność przepisów wdrażających dyrektywę retencyjną do swoich systemów prawnych.**

ODPOWIEDZIALNOŚĆ POŚREDNIKÓW

za treść w internecie

WPROWADZENIE

19

Internet jako medium udostępniania treści odgrywa obecnie kluczową rolę. Możliwości, jakie na tym polu stwarzają narzędzia takie jak Twitter, portale społecznościowe, fora internetowe czy komunikatory są ogromne, zwłaszcza w połączeniu z terminalem w każdym telefonie. Dostęp do informacji staje się bardziej demokratyczny dzięki rosnącemu dostępowi do narzędzi, które umożliwiają publikowanie na masową skalę, po niewielkich lub wręcz zerowych kosztach. Dzięki usługom dostępnym w ramach Web 2.0 każdy może „wydawać gazetę” w formie bloga, czy „nadawać program telewizyjny”, publikując nagrania filmowe.

Ta rewolucja w dostępności treści generuje jednak konkretne problemy i wyzwania regulacyjne. Autor treści może się ukryć za pseudonimem lub pozostać w pełni anonimowy, podczas gdy informacje przez niego zamieszczane mogą zyskać globalny zasięg. Treści umieszczone w sieci rozpowszechniają się i wpływają na opinie innych użytkowników, bez względu na to, czy są zgodne z prawdą. Sam autor często nie ma wpływu na to, gdzie dociera umieszczona przez niego treść i jakie wywołuje skutki.

Jakie prawa ma osoba, która doświadczyła zniesławienia czy naruszenia prywatności lub innych dóbr osobistych w internecie? Wobec kogo może je egzekwować? Prawo w tym zakresie nie jest wystarczająco precyzyjne. Pokrzywdzony może zwrócić się z żądaniem zablokowania spornej treści do pośrednika - czyli firmy, która zarządza platformą, na której treść została opublikowana - jednak nie ma gwarancji, że wysłana przez niego „wiadomość” zostanie uznana za „wiarygodną”. Wreszcie, jeśli pokrzywdzony zdecyduje się pójść ze swoim problemem do sądu, poza długotrwałą i kosztowną procedurą, napotka fundamentalną barierę: obowiązek ustalenia tożsamości i adresu domniemanego naruszcyciela, bo bez tego nie można nawet wnieść sprawy do sądu. Dodatkowo, nie ma możliwości np. zablokowania treści, które są rozpowszechniane przez wyszukiwarki w formie zachowanych kopii stron WWW.

Zadanie, które stoi przed regulatorami na całym świecie, to pogodzenie interesów i wartości, jakie występują po obydwu stronach sporu. Jak zaprojektować skuteczny mechanizm eliminowania z sieci treści, które rzeczywiście naruszają prawa innych osób, nie ograniczając wolności słowa bardziej, niż to konieczne i zachowując zasady uczciwego procesu?

Złożoność tego wyzwania może generować poczucie „politycznej bezradności” i skłaniać do podejmowania radykalnych, a niekoniecznie sensowych kroków. Pomysły w rodzaju obowiązkowej weryfikacji tożsamości w internecie czy objęcia wszystkich blogerów obowiązkami przewidzianymi dla wydawców prasy elektronicznej to niebezpieczny, błędny kierunek. **Musimy szukać rozwiązania, które z jednej strony umożliwia pokrzywdzonym łatwe i szybkie dochodzenie roszczeń, a z drugiej zachowuje to, co jest siłą i esencją internetu: możliwość nieskrępowanej, także anonimowej, wymiany informacji i poglądów.**

W wielu krajach próbuje się osiągnąć ten cel poprzez przerzucenie częściowej (warunkowej) odpowiedzialności za publikowaną treść na pośredników (dostawców platform), np. administratorów portalu, którzy mają techniczną możliwość kontrolowania postów zamieszczanych przez użytkowników. Rozwiązanie to nie jest jednak doskonałe. Może ono doprowadzić dla groźnej w demokratycznym porządku prawnym sytuacji, kiedy to pośrednicy - z ostrożności - będą eliminować ze swoich platform wszelkie potencjalnie kontrowersyjne treści. Z drugiej strony, nie chcemy też pośredników bezkarnych, którzy nie muszą reagować na problemy zgłaszane im przez użytkowników. Dlatego odpowiednie ukształtowanie zasad odpowiedzialności pośredników za treść staje się kluczowym wyzwaniem regulacyjnym.

20



Ponieważ usługi internetowe są dostarczane przez prywatne firmy, sektor prywatny zyskał bezprecedensowy wpływ na prawa jednostki do wolności wypowiedzi i dostępu do informacji.

Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 20 kwietnia 2010 r., Organizacja Narodów Zjednoczonych, A/HRC/14/23

DYLEMAT 1

Jaki stopień kontroli treści przez pośredników da się pogodzić z zasadą wolności słowa?

W obecnym stanie prawnym pośrednik nie odpowiada za treść, jeżeli nie wie, że narusza ona prawo. Jeśli zostaje o tym urzędowo powiadomiony lub „uzyska wiarygodną wiadomość”, musi niezwłocznie zablokować sporną treść, by uniknąć odpowiedzialności za naruszenie.

Z jednej strony zwalnia to pośrednika z obowiązku prewencyjnej kontroli treści, co chroni wolność słowa. Z drugiej zaś, nakłada na niego ciężar oceny bezprawności opublikowanej treści i wiarygodności otrzymanej wiadomości. Stawia go to w roli prywatnego „egzekutora”, który sam wymierza sprawiedliwość i sam ją egzekwuje.

21

DYLEMAT 3

Jak chronić prawa autorów treści?

Prawa autora treści też nie są odpowiednio zabezpieczone. Obecnie przepisy nie przewidują procedury, w której autor niesłusznie posądzony o naruszenie mógłby dochodzić zadośćuczynienia. Co więcej, pośrednik nie ma też obowiązku informowania autora o blokadzie treści, a więc autor - jeśli zależy mu na zachowaniu postów umieszczonych w internecie - jest zmuszony do ciągłego monitorowania wszystkich platform publikacyjnych, z których korzysta.

DYLEMAT 2

Jak chronić prawa pokrzywdzonych użytkowników?

Nie ma wątpliwości, że należy chronić użytkowników internetu przed skutkami działań takich jak pomówienie czy rozpowszechnianie prywatnych informacji na ich temat. Nadużycie wolności słowa w internecie może mieć dotkliwe skutki, ze względu na specyfikę tego medium. Użytkownicy powinni mieć zatem skuteczny i szybki instrument dochodzenia swoich praw.

Oczywiste jest też, że ostateczną odpowiedzialność powinien ponosić sprawca naruszenia, nie zaś pośrednik, nieświadomie udostępniający forum do dokonania go. Zlokalizowanie autora internetowego wpisu może być jednak bardzo trudne, szczególnie jeśli podejmie on starania, żeby pozostać w ukryciu.

Cel w postaci eliminacji z internetu „nielegalnych” treści powinien być osiągnięty z poszanowaniem potrzeby praworządności, interesu osób, których prawa są naruszane oraz wartości fundamentalnych, takich jak wolność słowa.

WARTOŚCI

Wolność tworzenia, prawo do dostępu do dóbr kultury

Te wartości mogą być zagrożone, jeśli pośrednicy zostaną obciążeni odpowiedzialnością za umieszczane w sieci - przez ich użytkowników - utwory objęte prawami autorskimi. Taki niepokojący trend obserwujemy w USA i niektórych krajach Unii Europejskiej (Francja, Wielka Brytania).

Prywatność i inne „prawa osób trzecich”

Treść umieszczona w internecie - a zatem publicznie dostępna - może powodować naruszenie prawnie chronionych interesów innych osób. Przedmiotem takiego naruszenia mogą być np. prywatność, dane osobowe, dobre imię (reputacja) czy własność intelektualna.

Wolność słowa

Wolność słowa zapewniona w art. 54 Konstytucji jest fundamentem demokratycznego społeczeństwa i powinna być chroniona bez względu na rodzaj medium. Przerzucenie pełnej odpowiedzialności za treść na pośredników mogłoby doprowadzić do swoistej cenzury - eliminowania z sieci wszelkich treści kontrowersyjnych w obawie przed procesami.

Swoboda prowadzenia działalności gospodarczej

Obciążenie pośredników nadmierną odpowiedzialnością może również prowadzić do zahamowania rozwoju rynku usług internetowych i stłumienia innowacyjności na tym polu.

Wiarygodna wiadomość

nie jest zdefiniowana w ustawie o świadczeniu usług drogą elektroniczną. Nie ma też procedury, której ścisłe przestrzeganie gwarantowałoby, że wiadomość będzie uznana za wiarygodną. Powoduje to problemy dla wszystkich aktorów procesu, ponieważ nie chroni dostatecznie niczyich interesów: osoby dotkniętej naruszeniem (która nie wie, według jakich kryteriów jej zgłoszenie będzie oceniane); pośrednika (który nie wie, czym ma się kierować przy uznawaniu wiadomości za wiarygodną); ani autora spornych treści (którego prawo do wolności wypowiedzi może zostać ograniczone w oparciu o niejasne kryteria).

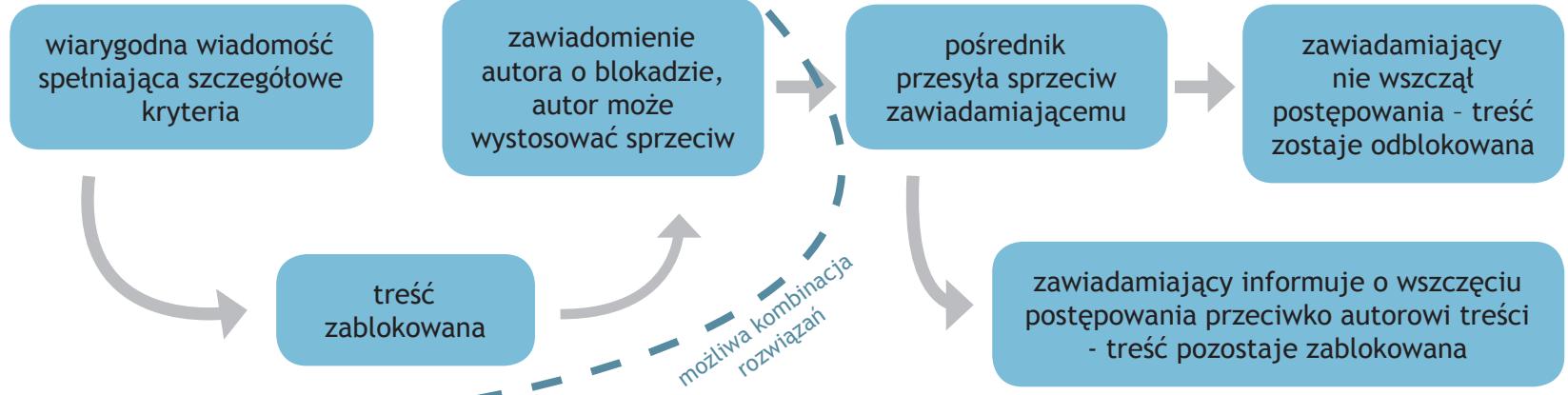
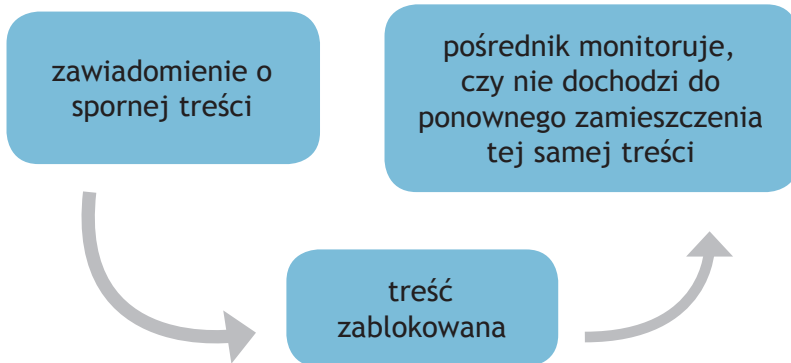
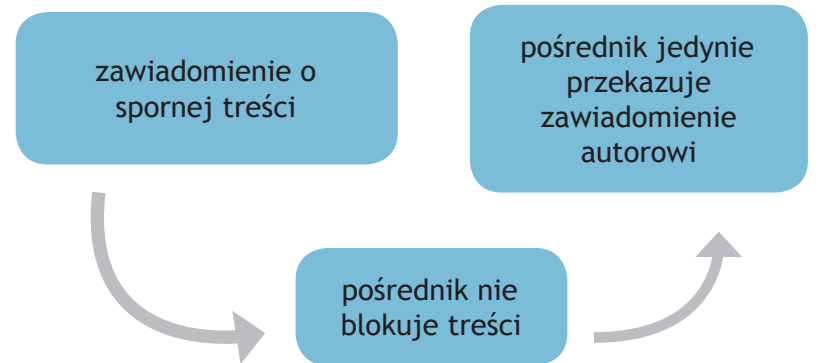
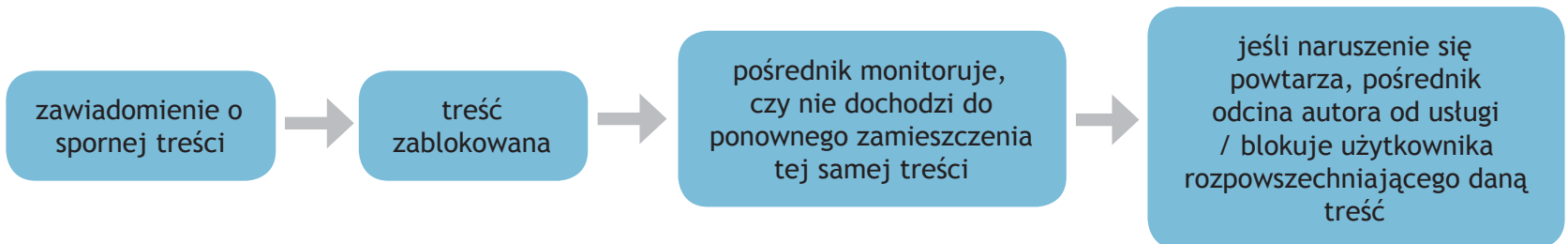
GŁÓWNI AKTORZY W SPORACH O LEGALNOŚĆ TREŚCI I FAKTYCZNE ZALEŻNOŚCI POMIĘDZY NIMI



Możliwe są różne warianty zmian w obecnie obowiązującej procedurze, które w różnym stopniu rozwiązują dylematy odpowiedzialności za treść. Niektóre ze scenariuszy nie wykluczają się wzajemnie i możliwe są ich połączenia lub kombinacje. Zakładają one też różne stopnie odpowiedzialności pośrednika: np. pośredniczenie w procesie dochodzenia praw przez użytkowników (1 i 3), co w pewnym stopniu zabezpiecza prawa zarówno pokrzywdzonego użytkownika jak i autora treści, a jednocześnie chroni wolność słowa. Możliwe jest też monitorowanie, czy naruszenie się nie powtarza (2 i 4) i w razie potrzeby odcięcie użytkownika winnego ponownemu wprowadzeniu nielegalnych treści do obrotu (4) – oba te scenariusze skupiają się na ochronie praw pokrzywdzonego użytkownika, podczas gdy inne wartości są brane pod uwagę w mniejszym stopniu. Dwa z nich już funkcjonują w innych krajach – scenariusz 1 w USA (w odniesieniu do utworów objętych prawem autorskim), scenariusz 3 w Kanadzie.

SCENARIUSZE ZMIANY PROCEDURY blokowania spornych treści

W przygotowywaniu propozycji nowych rozwiązań, ważne jest zbudowanie definicji, które jasno wytyczą zakres odpowiedzialności poszczególnych aktorów. Jednocześnie ich konstrukcja powinna być na tyle elastyczna, żeby uwzględniać dynamiczny rozwój rynku usług internetowych.

SCENARIUSZ 1 - notice and takedown**SCENARIUSZ 2 - notice and stay down****SCENARIUSZ 3 - notice only****SCENARIUSZ 4 - notice and disconnect**

PODSUMOWANIE SCENARIUSZY – DOBRE KIERUNKI

- 1. Określenie, jakie elementy powinna zawierać wiarygodna wiadomość.** Bez doprecyzowania prawa w tym zakresie rośnie ryzyko, że pośrednik zablokuje treść na podstawie fałszywej lub błędnej informacji, godząc tym samym w prawo autora do wolności wypowiedzi.
- 2. Stworzenie minimalnych gwarancji uczciwego procesu.** Można to osiągnąć poprzez obwarowane sankcjami zobowiązanie pośrednika do poinformowania autora kwestionowanej treści o jej zablokowaniu i jego prawie do zgłoszenia uzasadnionego sprzeciwu.

PROBLEMY DO ROZSTRZYgniĘCIA - REKOMENDACJE

1. Jak zapewnić transparentność i przewidywalność działań pośredników w stosunku do spornych treści?

Brak jasnych granic odpowiedzialności i kryteriów, według których treść może zostać zablokowana lub odblokowana, powoduje, że łatwo o ograniczenie wolności słowa czy dostępu do dóbr kultury. Z drugiej strony, nadmierny formalizm usztywnia postępowanie, zwiększa ryzyko nadużyć i może stanowić obciążenie hamujące swobodę prowadzenia działalności gospodarczej. Aby wyważyć te dwa podejścia, prawodawca powinien zaangażować możliwie wielu różnorodnych interesariuszy w proces zmiany prawa, by znaleźć rozwiązanie najlepiej godzące wskazane wartości.

2. Kim jest pośrednik?

W warunkach dynamicznego rozwoju usług internetowych nie mają sensu definicje odwołujące się do konkretnych typów usług, które szybko się dezaktualizują. Należy raczej tworzyć definicje, które odwołują się do funkcji, jaką pośrednik spełnia w dostarczaniu treści. Wyszukiwarki np. powinny być traktowane analogicznie do tradycyjnych host-providerów, jeśli przechowują i dostarczają treści, które zostały usunięte z macierzystych serwerów w związku z naruszeniem prawa.

3. Jak przyspieszyć procedurę sądową w sprawach o treści publikowane w internecie?

Decyzje pośredników nie powinny i nie mogą zastępować rozstrzygnięć sądów. Dlatego niezwykle ważne jest, aby strony sporu o treść mogły zawsze skorzystać ze sprawnej i szybkiej procedury sądowej. Przy czym nie powinna to być nowa procedura w ramach niesprawnego systemu. Specyficzny problem sporów o treść powinien zostać rozwiązany w ramach kompleksowej reformy systemu sądownictwa.

4. Jak zapewnić analogiczne prawa autorom anonimowych wpisów?

Autorzy anonimowych wpisów nie powinni być zupełnie pozbawieni prawa do „obrony” umieszczanych treści. Można rozważyć wprowadzenie „powszechnego prawa sprzeciwu”, zgodnie z którym każdy, kto uważa, że wartościowy, anonimowy post został przez pośrednika usunięty, mógłby zgłosić takie zastrzeżenie.

5. Jak zwiększyć wiedzę sędziów na temat specyfiki postępowania w sporach o treść w internecie?

Należy zastanowić się, czy poprzez szkolenia i inne sposoby popularyzacji wiedzy, nie udałoby się podnieść świadomości sędziów na temat specyfiki regulacji zawartych w ustawie o świadczeniu usług drogą elektroniczną i samych sporów dotyczących treści w internecie.

Hosting

to, zgodnie z dyrektywą o handlu elektronicznym (2000/31/WE), świadczenie usługi społeczeństwa informacyjnego polegającej na przechowywaniu informacji przekazanych przez usługobiorcę. Ustawodawca polski nie używa tego terminu, a jedynie odnosi się do „udostępniania zasobów systemu teleinformatycznego”. W praktyce, większość **host-providers** (świadczących hosting) nie tylko przechowuje dane ale i je udostępnia, przetwarza, itp. Dlatego też wielu komentatorów jest zdania, że definicja hostingu powinna zawierać w sobie również udostępnianie treści w taki sposób, aby dostęp do nich był możliwy w miejscu i czasie wybranym przez użytkownika.

27

DOBRA PRAKTYKA SĄDOWA

Standard K.U. przeciwko Finlandii

W wyroku K.U. przeciwko Finlandii Europejski Trybunał Praw Człowieka wskazał, iż na państwie ciąży „pozytywny obowiązek” zapewnienia skutecznych instrumentów dochodzenia roszczeń przez osoby, które doznały krzywdy na skutek nadużycia wolności słowa w internecie, w stosunku do sprawcy naruszenia (autora komentarza). Poszkodowani zwykle próbują dochodzić swoich roszczeń od pośredników ze względu na zdecydowanie większą łatwość ich zlokalizowania, niż w przypadku autora komentarza. ETPCz uznał jednak, że konieczne jest zagwarantowanie bezpośredniej odpowiedzialności sprawcy naruszenia. Zdaniem sądu, mechanizmy krajowe, pozwalające na pociągnięcie do odpowiedzialności zamiast niego – pośrednika, są niewystarczające i naruszają prawo do prywatności zawarte w art. 8 Europejskiej Konwencji Praw Człowieka.

Z orzeczenia tego wynika, że rozwojowi internetu oraz anonimowych form komunikacji powinien towarzyszyć rozwój skutecznych procedur pozwalających na identyfikację sprawców naruszeń.

ZŁA PRAKTYKA SĄDOWA

Sprawa A.J.

W 2010 r. Burmistrz Tarnowa wystąpił na drogę sądową po tym, jak poczuł się urażony obraźliwym wpisem anonimowego użytkownika, zamieszczonym pod jednym z artykułów blogera A.J. Sąd Okręgowy w Tarnowie (sygn. akt I Ns 162/10), orzekając w trybie wyborczym, uwzględnił rację powoda, pomimo że A.J. nie był autorem komentarza i niezwłocznie zablokował do niego dostęp. W uzasadnieniu sąd stwierdził:

Nie do przyjęcia jest stanowisko uczestnika, że nie ponosi za nie [komentarze, które pojawiły się na blogu] odpowiedzialności, skoro pochodziły od internautów korzystających ze swobody wypowiedzi. Właśnie prowadzenie blogu w sposób umożliwiający zamieszczenie w nim takich informacji uznać należy za działanie bezprawne jako sprzeczne porządkiem prawnym i zasadami współżycia społecznego. [pisownia oryginalna].

Sąd Apelacyjny w Krakowie utrzymał w mocy orzeczenie Sądu Okręgowego (sygn. akt Acz 1457/10). Wyrok - obowiązek publikacji przeprosin na blogu, nakaz zapłaty 5 tys. zł na cel społeczny oraz nakaz pokrycia kosztów procesu - został wykonany.

BLOKOWANIE

stron internetowych

WPROWADZENIE

29

Internet stwarza w zasadzie nieograniczone możliwości rozpowszechniania informacji, także tych szkodliwych. Mowa nienawiści, nakłanianie do przemo- cy na tle religijnym, etnicznym czy politycznym, rozpowszechnianie obra- zów seksualnego wykorzystywania dzieci, handel podrabianymi towarami i masowe naruszenia praw autorskich to tylko niektóre przykłady naruszeń prawa w internecie. W debacie publicznej pojawiają się więc pytania o to, jakimi metodami można walczyć z tego rodzaju złem.

W szukaniu odpowiedzi kluczowa jest kwestia proporcjonalności: regu- lacyjna reakcja na dany problem musi być adekwatna do jego powagi i skali. W de- mokratycznym państwie powinniśmy unikać rozwiązań radykalnych, które być może odpowiadają w jakimś stopniu na problem, ale przy okazji prowadzą do poważnych naruszeń praw podstawowych. Wprowadzenie obowiązku blokowania stron internet- owych, które zawierają nielegalne treści, jest odpowiedzią nieproporcjonalną i w swoich dalekosiężnych skutkach zmierzającą do zamknięcia internetu, który ze swej natury powinien zostać otwarty i neutralny.

Nielegalne treści należy skutecznie usuwać, a nie prowizorycznie blokować. Blo- kowanie działa jak „parawan”, za który może zajrzeć każdy, kto ma na to ochotę, nawet jeśli nie ma szczególnych technicznych kompetencji. Już dziś wystarczy do tego zainstalowanie odpowiedniej wersji przeglądarki stron internetowych.

Blokowanie treści z definicji jest niebezpieczne dla wolności słowa. Praktyka państw, które eksperymentowały z tym środ- kiem pokazuje, że ze względu na techniczne ograniczenia nie da się z chirurgiczną precyzją blokować tylko tego, co praw- dawca uzna za nielegalne. Przy okazji blokowane bywają także legalne treści. Co więcej, wymaga ono stworzenia specjalnej infrastruktury, która może być następnie wykorzystana do blokowania dowolnych treści.

2,36
dni to średni czas
usuwania strony z tzw.
pornografią dziecięcą.

Dane na podstawie raportu dr. Weixiao Wei, *Online Child Sexual Abuse Content: The Development of a Comprehensive, Transferable International Internet Notice and Takedown System.*

80%

o tyle od 2009 r. spadła liczba adresów zarejestrowanych przez największą sieć organizacji zwalczających treści pedofilskie. Przystępcy przenoszą się do internetowego podziemia, gdzie treści nie da się łatwo zablokować.

Dane na podstawie raportu dr. Weixiao Wei, *Online Child Sexual Abuse Content: The Development of a Comprehensive, Transferable International Internet Notice and Takedown System*.

Blokowanie stron internetowych w Polsce i Europie. Problem blokowania stron internetowych zaistniał w polskiej debacie publicznej w 2009 r., w związku z rządową propozycją stworzenia Rejestru Stron i Usług Niedozwolonych. Próbowano tym sposobem rozwiązać m.in. problemy nielicencjonowanego hazardu w internecie, mowy nienawiści oraz rozpowszechniania obrazów seksualnego wykorzystywania dzieci. Propozycja upadła w wyniku masowych protestów wszystkich środowisk związanych z internetem.

Już wówczas przewidywano jednak, że temat wróci, pod najlepszym politycznym pretekstem ochrony dzieci. W 2010 r. pojawił się projekt unijnej dyrektywy, zakładającej blokowanie stron jako metodę walki z rozpowszechnianiem obrazów seksualnego wykorzystywania dzieci. Istnieje jednak obawa, że na blokowaniu takich treści się nie skończy. Przemysł rozrywkowy już sygnalizuje chęć wykorzystania tego mechanizmu do wzmocnienia ochrony praw autorskich.

30

Blokowanie treści jest rozwiązaniem nieskutecznym i szkodliwym – zarówno dla samej walki z rozpowszechnianiem nielegalnych treści, jak i dla przyszłości wolnego internetu.



Propozycje ograniczania tych [obywatelskich] wolności muszą być poprzedzone procesem dowodowym, który pokaże, że albo nie ma innego wyjścia, żeby wyleczyć jakąś groźną chorobę społeczną – albo że negatywne skutki dla wolności nie są ważące.

Premier Donald Tusk na spotkaniu z organizacjami pozarządowymi, 13 lipca 2011 r.

DYLEMAT 1

Jak walczyć z cyberprzestępczością nie ograniczając wolności słowa?

Obywatele mają prawo oczekiwać, że państwo ochroni ich przed skrzywdzeniem w wyniku przestępstwa. Ofiary wykorzystywania seksualnego mają prawo do ochrony przed wtórną wiktyimizacją, jaką stanowi rozpowszechnienie obrazów ich krzywdy w internecie. Jednak nawet najlepsza intencja ochrony ofiary nie usprawiedliwia doboru metod, których stosowanie nie tylko ogranicza korzystanie z wolności obywatelskich, ale i nie chroni ofiar. Zablokowanie treści nie wyeliminuje żadnego z przejawów cyberprzestępczości. Dobra wiadomość jest taka, że można z nią walczyć innymi metodami, przede wszystkim poprzez usuwanie nielegalnych treści i eliminowanie ich źródeł.

WARTOŚCI

Proporcjonalność

Wolność słowa można i należy ograniczać, jeśli jest to konieczne do ochrony praw innych osób, np. ofiar wykorzystywania seksualnego. Blokowanie treści pozostaje jednak środkiem nieproporcjonalnym do realizowanego celu, ponieważ zbyt łatwo może zostać zastosowane do w pełni legalnych treści.

Wolność wypowiedzi

Blokowanie dostępu do treści, czyli rodzaj cenzury prewencyjnej - w dodatku egzekwowany bez wyroku sądu - stoi w sprzeczności z zasadami wolności słowa.

DYLEMAT 2

Jak przeciwdziałać rozpowszechnianiu treści naruszających prawa obywateli, znajdujących się na serwerach poza jurysdykcją ich kraju?

W internecie granice państwowe i geograficzne nie mają znaczenia. Każdy użytkownik może umieścić treść na serwerze po drugiej stronie globu. Komplikuje to pracę organów egzekwowania prawa, które nie mogą skutecznie działać poza granicami swojego państwa bez międzynarodowych porozumień i skomplikowanych procedur. Poczucie bezradności może sprawić, że prosty środek, jakim jest zablokowanie nielegalnych treści dla własnych obywateli, stanowi kuszące rozwiązanie. Treści te jednak pozostają dostępne dla wszystkich poza blokującym krajem, a i tam blokadę łatwo można ominąć. Jedynym skutecznym rozwiązaniem jest usprawnianie procedur i stworzenie ponadnarodowej sieci kontaktów operacyjnych dla organów ścigania.

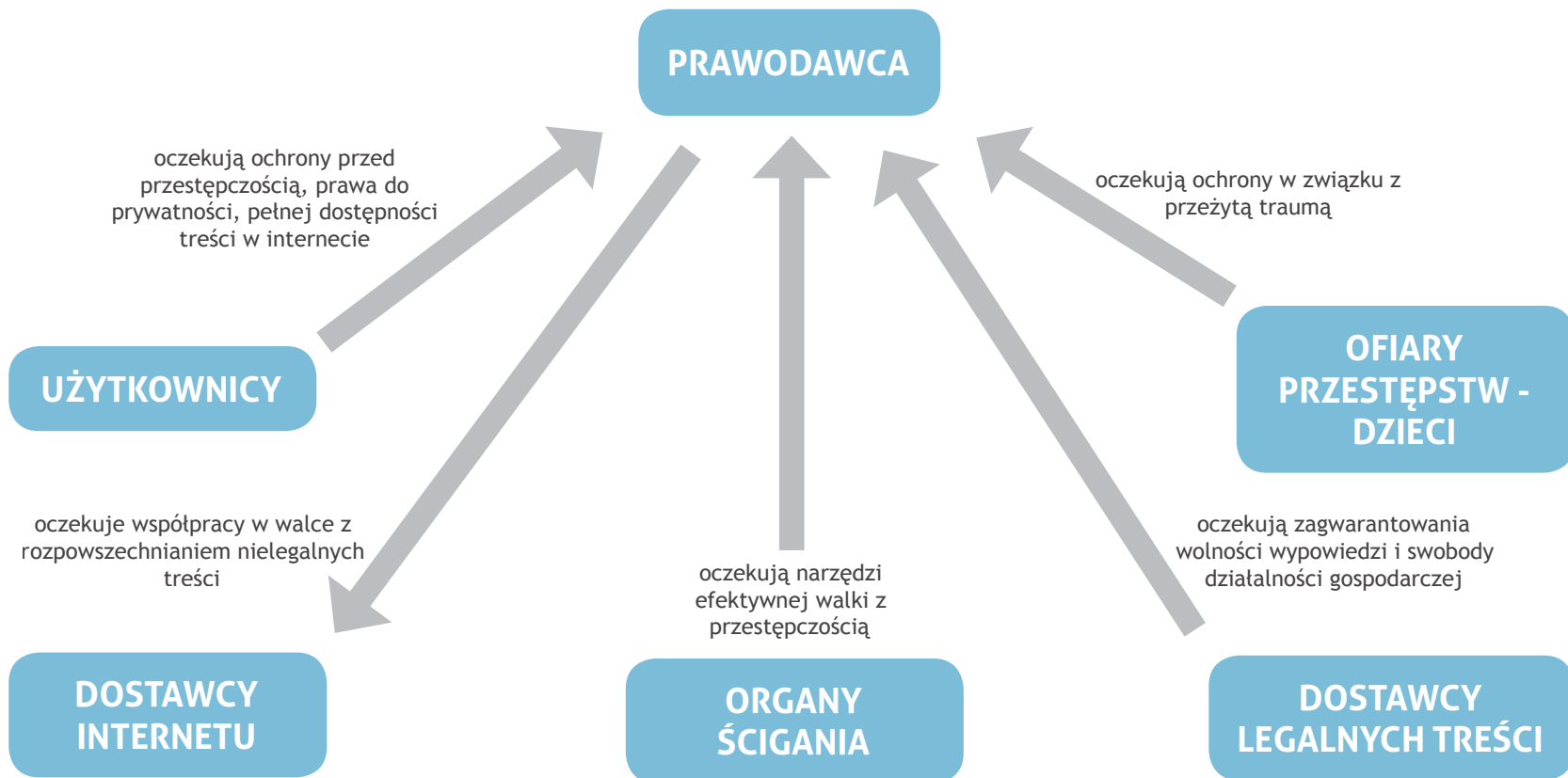
Bezpieczeństwo publiczne i „prawa osób trzecich”

Bezspornie państwo ma obowiązek chronić swoich obywateli przed krzywdą ze strony innych oraz zwalczać przestępczość, także w internecie. Zwolennicy blokowania upatrują w nim skuteczną metodę ochrony użytkowników internetu przed potencjalną krzywdą, na jaką może ich narazić kontakt z nielegalnymi treściami.

Prywatność

Z technicznego punktu widzenia, zablokowanie treści opiera się na uprzednim sprawdzeniu, jaka informacja znajduje się wewnątrz pakietu, który użytkownik wysyła bądź odbiera w internecie. W zależności od metody blokowania, będzie to albo nagłówek albo pełna zawartość. Ponieważ sprawdzanie ma charakter przesiewowy, w każdym przypadku dochodzi do naruszenia tajemnicy korespondencji.

GŁÓWNI AKTORZY KONFLIKTU WOKÓŁ NIELEGALNYCH TREŚCI W INTERNECIE I ICH OCZEKIWANIA



Mierząc się z problemem rozpowszechniania krzywdzących lub nielegalnych treści w internecie, trzeba szukać rozwiązań skutecznych i proporcjonalnych do realizowanego celu.

SCENARIUSZ 1 - Wprowadzenie obwarowań zapewniających poszanowanie praw człowieka

Propozycja taka pojawiła się toku prac legislacyjnych nad projektem dyrektywy o zwalczaniu seksualnego wykorzystania i seksualnej przemocy wobec dzieci oraz pornografii dziecięcej. Reguły te miałyby obowiązywać państwa, które chcą wprowadzić blokowanie stron internetowych. Zgodnie z tym projektem, wszelkie działania zmierzające do blokowania sieci powinny być zgodne z Europejską Konwencją Praw Człowieka i Kartą Praw Podstawowych Unii Europejskiej.

Ten wymóg oznacza o wiele wyższy poziom ochrony użytkowników internetu, niż stosowany w państwach Unii Europejskiej - obecnie w Szwecji czy w Danii blokowanie stron odbywa się bez jakichkolwiek podstaw prawnych.

33

SCENARIUSZ 2 - Usprawnianie procedur usuwania nielegalnych treści

Odpowiednie umowy i konwencje międzynarodowe już zapewniają podstawy prawne do takich działań. Głównym wyzwaniem jest poprawienie komunikacji i współpracy z organami ścigania z państw spoza Unii Europejskiej. Obecnie reakcja na zawiadomienie o nielegalnych treściach na zagranicznych serwerach jest niewystarczająco sprawna i szybka. Efektywność działań ma zatem związek z zacieśnieniem współpracy międzypaństwowej, w szczególności z Rosją, Ukrainą i USA. Taka współpraca mogłaby obejmować np. stworzenie sieci operacyjnych punktów kontaktowych dla organów egzekwowania prawa.

Stworzenie europejskiego systemu corocznego raportowania o postępach w usuwaniu nielegalnych treści z internetu wzmocniłoby współpracę międzypaństwową. Konsekwentne raportowanie umożliwiłoby instytucjom Unii Europejskiej ocenę sukcesów i porażek poszczególnych państw członkowskich, sprzyjałoby promowaniu najlepszych praktyk i maksymalizacji wysiłków na polu wykrywania przestępstw, ścigania sprawców i identyfikowania ofiar.

SCENARIUSZE ZMIANY PODEJŚCIA

Jest wiele metod poprawiających skuteczność walki z nielegalnymi treściami w internecie. Strony można usuwać, nie blokować (scenariusz 2). Blokowanie może odbywać się na poziomie filtra w komputerze (scenariusz 3), albo na podstawie zobowiązania dostawców internetu (scenariusz 4), jak ma to miejsce w Belgii, Szwecji, Finlandii, Danii i Wielkiej Brytanii. Można także narzucić państwom reguły ograniczające możliwość blokowania treści ze względu na ochronę praw człowieka (scenariusz 1).

SCENARIUSZ 3 - Blokowanie stron internetowych w ramach usługi komercyjnej

Blokowanie nielegalnych stron internetowych może się odbywać na życzenie, jeśli właściciel konkretnego komputera zamówi i uruchomi odpowiedni filtr. Jest to wówczas usługa komercyjna, działająca wyłącznie na komputerze, na którym została zainstalowana. Tym samym, nie wpływa na działanie internetu i dostępność blokowanych treści dla innych użytkowników sieci. Każdy użytkownik może zdecydować, czy chce tego typu ochrony dla siebie lub swojej rodziny. Na polskim rynku oferta usług komercyjnego blokowania jest dobrze rozwinięta.

SCENARIUSZ 4 - Obowiązkowe blokowanie treści przez dostawców internetu

Obowiązek ten może być wprowadzony w formie powszechnie obowiązującego prawa albo w formie tzw. samoregulacji dostawców internetu (jako środek dobrowolny, ale zalecany). W wariantcie pierwszym system filtrowania i blokowania projektuje i nadzoruje policja lub inny wyspecjalizowany organ, natomiast dostawcy internetu jedynie go stosują. W drugim wariantcie odpowiedni system tworzą dostawcy internetu we współpracy z policją.

PODSUMOWANIE SCENARIUSZY – DOBRE KIERUNKI

1. Regulacja na poziomie europejskim

Regulacje wspólnotowe powinny nakładać na państwa, które chcą wprowadzić mechanizmy blokowania, ograniczenia gwarantujące przejrzystość zasad i poszanowanie fundamentalnych praw: uczciwego procesu, proporcjonalności w ograniczaniu wolności słowa, odszkodowania za przypadkowe zablokowanie legalnych treści itp.

Ograniczenia wynikające z regulacji europejskich mogą być ważnym instrumentem wspierającym obywateli w walce o ich prawa. Bez nich, w przyszłości możliwe byłoby rozszerzanie zakresu blokowania na inne obszary: treści politycznych lub obrażających uczucia religijne czy serwisów umożliwiających naruszenia praw autorskich.

34

„czarna lista”

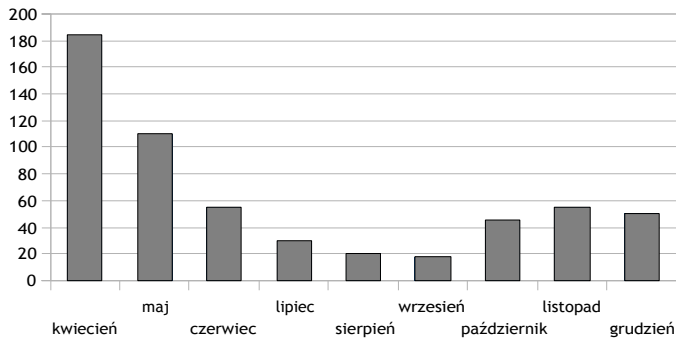
Wspólną cechą technicznych metod blokowania stron jest to, że blokowanie odbywa się na poziomie sieci: numeru IP, domeny, adresu URL. Taki system opiera się na „czarnych listach” – aktualizowanych wykazach adresów URL (lub innych parametrów technicznych), które podlegają obowiązkowemu blokowaniu. Zawartość „czarnych list” ustalają specjalnie do tego powołane organizacje lub policja, bez ingerencji czy kontroli sądu.

2. Usuwanie zamiast blokowania

Jedyną skuteczną i zgodną z demokratycznymi standardami metodą walki z nielegalnymi treściami w sieci jest ich usuwanie. Powinno się ono odbywać pod kontrolą sądu, z udziałem biegłych i po rzetelnym zbadaniu sprawy.

3. Blokowanie stron internetowych w ramach usługi komercyjnej

Tylko taka - w pełni uzależniona od indywidualnych decyzji obywateli - forma blokowania pozostaje w zgodzie z wartościami chronionymi w demokratycznym państwie prawa.



Liczba URL pozostająca na liście Internet Watch Foundation dłużej niż miesiąc

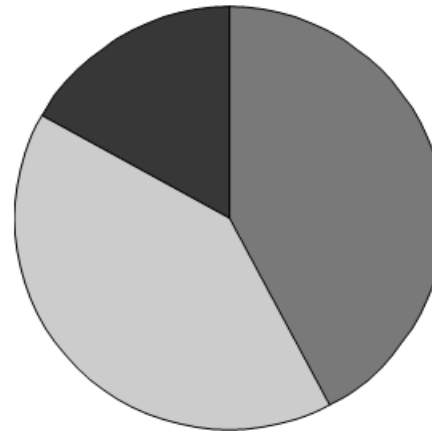
Dane na podstawie IWF Annual Report 2010 & IWF Research Report

Holandia

tu zlokalizowany był jeden z największych serwerów z pornografią dziecięcą, zlikwidowany w 2010 r.

84 000

tyle przypadkowych stron zablokowano (jednorazowo) w USA w ramach walki z tzw. pornografią dziecięcą.



Pochodzenie zablokowanych URL

Dane na podstawie Internet Watch Foundation Annual Report 2010

- Azja - 2839 (17%)
- Australia - 1 (0%)
- Europa (z Rosją) - 6829 (41%)
- Ameryka Pn - 7058 (42%)
- Ameryka Pd - 12 (0%)



Blokowanie to niepotrzebny i nieproporcjonalny środek do osiągnięcia celu, ponieważ często jest niewystarczająco ukierunkowane, a także uniemożliwia dostęp do treści w szerszym zakresie, niż ten uznany za nielegalny.

Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 20 kwietnia 2010 r., Organizacja Narodów Zjednoczonych, A/HRC/14/23

KWESTIE DO ROZSTRZYgniĘCIA – REKOMENDACJE

1. Blokowanie czy usuwanie?

Nielegalne treści należy usuwać u źródła, czyli eliminować z serwerów. Odpowiednie organy wiedzą, gdzie ich szukać: większość stron internetowych zawierających obrazy seksualnego wykorzystywania dzieci znajduje się w Europie Zachodniej (gł. Belgia i Niemcy). Kolejne kluczowe lokalizacje to Rosja, Ukraina i USA. Istnieją też stosowne narzędzia: według danych amerykańskiego Narodowego Centrum Zaginionych i Wykorzystywanych Dzieci, stosowana w USA procedura usuwania nielegalnych treści ma stuprocentową skuteczność. W Europie działania policji oraz organizacji pozarządowych (np. Internet Watch Foundation) na polu wykrywania i usuwania nielegalnych treści, w tym stron pedofilskich, również są bardzo skuteczne.

2. Jaki problem ma rozwiązywać regulacja?

Komisja Europejska, która uznała blokowanie stron internetowych za właściwy środek w walce z seksualnym wykorzystywaniem dzieci, nie przedstawiła analiz potwierdzających skalę zwalczanego zjawiska ani dowodów na skuteczność tego środka. Jednocześnie, dane gromadzone przez specjalizujące się w zwalczaniu pedofilii w internecie organizacje pokazują, że rozpowszechnianie obrazów seksualnego wykorzystywania dzieci na powszechnie dostępnych stronach WWW traci na znaczeniu.

Internetowe podziemie: tzw. TOR (głęboka sieć) i alternatywne sposoby komunikacji sieciowej, np. wymiana plików w trybie *peer-to-peer*, są efektywniejszymi i bezpieczniejszymi sposobami wymieniania nielegalnych treści. Ponieważ w wyścigu cyfrowych technologii blokowanie to broń zdecydowanie przestarzała, należy tworzyć ramy zwalczania przestępczości związanej z seksualnym wykorzystywaniem dzieci uwzględniając nowe metody rozpowszechniania tych treści.

3. Oblicza samoregulacji

Promowana w Unii Europejskiej samoregulacja dostawców internetu w celu stworzenia europejskiego systemu filtrowania i blokowania nielegalnych treści, narusza standardy ochrony praw człowieka. Blokowanie treści nieodzwrotnie łączy się z ograniczeniem wolności słowa, która nie może być ograniczona inaczej, jak ustawowo. Ponieważ porozumienie podmiotów komercyjnych nie podlega demokratycznej kontroli, nie może być samoistną podstawą ograniczania praw obywatelskich. Dlatego zachęcanie dostawców internetu do ustalania własnych reguł „czyszczenia sieci” jest niedopuszczalne.

Samoregulacja może natomiast pełnić pozytywną funkcję, jeśli nie zastępuje regulacji prawnych, ale służy ich wzmocnieniu. Ścisła współpraca dostawców internetu i administratorów sieci jest niezbędna, by prawo zakazujące rozpowszechniania pewnych typów treści było skutecznie i sprawnie egzekwowane.

36

W rozwiązywaniu problemu dostępności treści obrazujących seksualne wykorzystywanie dzieci trudno jest oddzielić społeczne emocje związane z powagą problemu od namysłu nad sensownością rozwiązań. Chęć szybkiego ukrócenia działalności przestępców może zepchnąć debatę nad znalezieniem skutecznego rozwiązania na dalszy plan.

ZŁA PRAKTYKA

internet jako sieć

internet jest siecią, której zakończenia – serwery – komunikują się poprzez skomplikowany układ połączeń. Każdy serwer ma swój unikatowy identyfikator, który pozwala ustalić jego lokalizację w sieci. Wystarczy odciąć zakończenie, na którym znajdują się nielegalne treści, żeby skutecznie uniemożliwić ich rozpowszechnianie. Ta metoda jest z powodzeniem wykorzystywana w walce ze spamem i stronami służącymi do wyłudzeń finansowych (phishing). Sukcesy w walce z tymi zjawiskami dowodzą, że współpraca międzynarodowa firm rejestrujących domeny internetowe i administratorów sieci może działać bardzo sprawnie.

Blokowanie stron internetowych zawierających obrazy seksualnego wykorzystywania dzieci (Belgia, Szwecja, Finlandia, Dania, Wielka Brytania, USA)

Blokowanie nie działa, ponieważ nie likwiduje dostępu do treści, które próbujemy wyeliminować. Zablockowane strony nie znikają z serwerów. Aby do nich dotrzeć, wystarczy wybrać inną ścieżkę przez internet. Taką podstawową umiejętnością jest w stanie opanować każdy użytkownik. Stanie się to jeszcze łatwiejsze wraz z postępującym rozwojem technologii. Odpowiedzią rynku na obowiązkowe blokowanie nielegalnych treści będzie niewątpliwie rozwój technik omijania blokad.

Blokowanie nie zmienia sytuacji ofiary utrwalonego w internecie obrazu wykorzystywania seksualnego, ponieważ treść nadal jest dostępna w sieci.

Blokowane strony są natychmiast przenoszone na inne serwery (nawet kilkadziesiąt razy w ciągu doby), co niweczy sens blokowania. Zweryfikowanie ujawnionej w Danii „czarnej listy” przez niemieckich aktywistów, potwierdziło obawy, że organy ścigania nie zawsze zajmują się dotarciem do sprawców i skutecznym usunięciem nielegalnych treści. Niektóre ze stron były na liście blokowanych adresów już ponad dwa lata. Wystarczyło zawiadomienie właścicieli serwerów, żeby zniknęły z internetu w ciągu 30 minut.

Blokowanie (jakichkolwiek) treści stanowi zagrożenie dla wolności słowa. Zablockowanie nawet kilku niechcianych stron oznacza, że musimy stworzyć infrastrukturę cenzurującą, która filtruje cały ruch w sieci i tym samym narusza tajemnicę korespondencji oraz prawo do prywatności. Co więcej, żadna ze znanych technik blokowania nie działa na zasadzie „chirurgicznego cięcia”, które wycina tylko niechciany obrazek. Z definicji blokowanie treści nielegalnych zagraża także tym legalnym, które przez przypadek znalazły się pod tym samym adresem URL czy numerem IP. Znany jest przypadek zablokowania 84 000 przypadkowych stron w USA, właśnie w ramach strategii walki z tzw. pornografią dziecięcą.

DOBRA PRAKTYKA

Kluczowym elementem w walce z rozpowszechnianiem obrazów seksualnego wykorzystywania dzieci jest wykrywanie i eliminowanie źródeł tego typu treści, czyli ściganie i osądzanie sprawców przestępstw.

Europol we współpracy z policjami państw członkowskich przeprowadza co roku kilka operacji przeciwko pedofilom, w których jednorazowo zatrzymywanych jest kilkaset osób.

EGZEKWCOWANIE PRAW AUTORSKICH

w środowisku cyfrowym

WPROWADZENIE

39

Technologie, które globalnie zmieniają oblicze dostępu do dóbr kultury, zagrażają tradycyjnym modelom ich produkcji i generowania zysku. Pojawiają się nowe modele tworzenia i dystrybucji treści, których niskie koszty znacząco obniżają próg wejścia na rynek masowej rozrywki i kultury. Dzięki internetowi i technologiom cyfrowym niszowy artysta może znaleźć swoją publiczność na drugim końcu świata.

Twórcy nie są największymi beneficjentami obecnego modelu biznesowego. Największe korzyści czerpią z niego producenci oraz różnego rodzaju pośrednicy. Nad alternatywnym podziałem zysków zastanawiają się liczni eksperci i aktywiści. Badania pokazują też, że konsumenci treści kulturalnych i rozrywkowych nie szukają „darmowego lunchu”, ale uczciwych warunków i ceny adekwatnej do wartości rynkowej produktu. Kiedy mają wybór, co do zasady płacą, jednak ich pieniądze coraz częściej nie przechodzą przez ręce tradycyjnych pośredników.

Model biznesowy, jakim posługują się tradycyjni producenci dóbr kultury i rozrywki, oparty jest na wielkich inwestycjach i równie olbrzymich marżach, które płacą końcowi odbiorcy. W świecie opartym na błyskawicznym przepływie informacji i globalnej podaży produktów rozrywkowych ten model przestaje się sprawdzać. Od lat 90. XX w. narasta konflikt pomiędzy wielkim przemysłem rozrywkowym, opartym na tradycyjnych kanałach dystrybucji, twórcami chcącymi zarabiać lepiej i użytkownikami, którzy szukają bezpośredniego i przez to tańszego dostępu do dóbr kultury i rozrywki.

Siła, z jaką lobby przemysłu rozrywkowego broni tradycyjnej konstrukcji praw autorskich, powoduje, że zasady ich egzekwowania usztywniają się. Dzieje się to wbrew trendom obserwowanym w społeczeństwie. Co więcej, wprowadzane są coraz bardziej represyjne metody egzekwowania tych zasad, zagrażające podstawowym prawom obywateli - użytkowników internetu. Pojawiają się nowe instrumenty, nie zawsze zgodne z demokratycznymi standardami, jak np. narzucanie roli „policji internetowej” prywatnym firmom świadczącym usługi dostępu do internetu.

Prawo własności intelektualnej może generować i wynagradzać kreatywność i innowacyjność. Te korzyści można jednak łatwo zniwelować poprzez represyjne regulacje ograniczające wolność tworzenia i upowszechniania dóbr kultury oraz inno-

wacji technicznych. Podobny skutek mają nadmierne ograniczenia praw podstawowych, takich jak prawo do prywatności czy swobody wypowiedzi.

W tej dyskusji możemy albo postawić na wartości, takie jak demokracja czy postęp technologiczny, albo stosować prawo autorskie w sposób całkowicie nieodpowiadający dzisiejszym realiom i potrzebom. Co niepokojące, strategia Komisji Europejskiej w zakresie ochrony prawa autorskiego i własności intelektualnej w ogóle wydaje się zmierzać ku tej drugiej opcji.

1%

taka w przybliżeniu część zysku z produktu końcowego – płyty z nagraniem – trafia do artysty w tradycyjnym modelu produkcyjnym.

DYLEMAT 1

Represyjne egzekwowanie czy głęboka reforma obowiązującego prawa?

Przy obecnym konflikcie interesów w kontekście prawa autorskiego, żadna grupa interesu nie chce zachowania status quo. Producenci i pośrednicy, w których interesie jest egzekwowanie obecnie obowiązującego prawa, pod presją zmniejszających się zysków, dążą do zaostrzania przepisów i metod ich egzekwowania. Twórcy, dotąd zdominowani pod presją potężnych producentów, chcą swobody artystycznej, większej dostępności swoich utworów i korzystniejszego dla nich podziału zysków. Odbiorcy rozrywki i kultury oczekują ciągłego poszerzania oferty i radykalnie niższych cen. W obecnej konstrukcji prawa autorskiego, potrzeby twórców i odbiorców często się rozmiągają.

DYLEMAT 2

Jak finansować produkcję treści dostępnych w internecie?

Twórcy mają prawo oczekiwać większego udziału w zyskach, jakie generuje ich twórczość. Jeśli te oczekiwania nie będą spełniane, a oni sami nie będą w stanie utrzymać się na rynku, powstanie mniej nowych utworów. Takie zubożenie oferty kulturalnej będzie niekorzystne z punktu widzenia interesu społecznego. Z drugiej strony, internet otworzył dostęp do milionów potencjalnych klientów i umożliwił nowe modele finansowania twórczości.

Dylemat sprowadza się do tego, w jakim modelu finansować tworzenie dóbr kultury? Czy przez regulację prawną powinien być wspierany model tradycyjny, oparty na kluczowej roli producentów i pośredników, czy nowy - zmierzający do radykalnego skrócenia łańcucha dystrybucji.

40



Kartezjusz zrobił krok w dobrym kierunku. (...) Jeśli ja spojrzę trochę dalej, to dlatego, że stanęłam na ramionach gigantów.

Isaac Newton, w liście do Roberta Hooke'a, 5 lutego 1676 r.

kultura remiksu

Prawo do korzystania z cudzych utworów w celu stworzenia nowej jakości ma podstawowe znaczenie w czasach, gdy coraz trudniej stworzyć coś, czego jeszcze nie było. Jednocześnie obszar potencjalnych innowacji, opartych o już istniejące pomysły, jest niezbadany. Próbkę tego potencjału daje fenomen wolnego oprogramowania (np. Linux) czy Wikipedii. Są to utwory rozwijane kolektywnie, w oparciu o pracę innych autorów, na zasadach niekomercyjnych. Innowacja jest zatem możliwa nie tylko dla zysku. Dlatego wolność przekształcania treści powinna być chroniona i poważnie uwzględniana w debacie publicznej.

Wolność w przekształcaniu treści

Zachowanie tej wartości ma fundamentalne znaczenie dla rozwoju kultury i innowacyjności, mimo, że nie gwarantuje jej konstytucja. (patrz: ramka - kultura remiksu).

Prywatność użytkowników i zasada neutralności sieci

Te fundamentalne wartości zostaną naruszone, jeśli dostawcy internetu będą zmuszeni do filtrowania pakietów i monitorowania przepływu treści w sieci, aby przeciwdziałać naruszeniom praw autorskich.

Prawo do udziału w kulturze i korzystania z jej dóbr

w bezpośredni sposób wiąże się z wolnym dostępem do twórczości kulturalnej i zasobów wiedzy. „Wolny” nie zawsze musi jednak oznaczać „darmowy”.

Swoboda działalności gospodarczej

Dostęp do treści generowanych przez miliony użytkowników w sieci oraz możliwość ich twórczego przekształcania służy przedsiębiorcom i innowacyjności; a także budowaniu gospodarki opartej na wiedzy.

WARTOŚCI

Wolność słowa

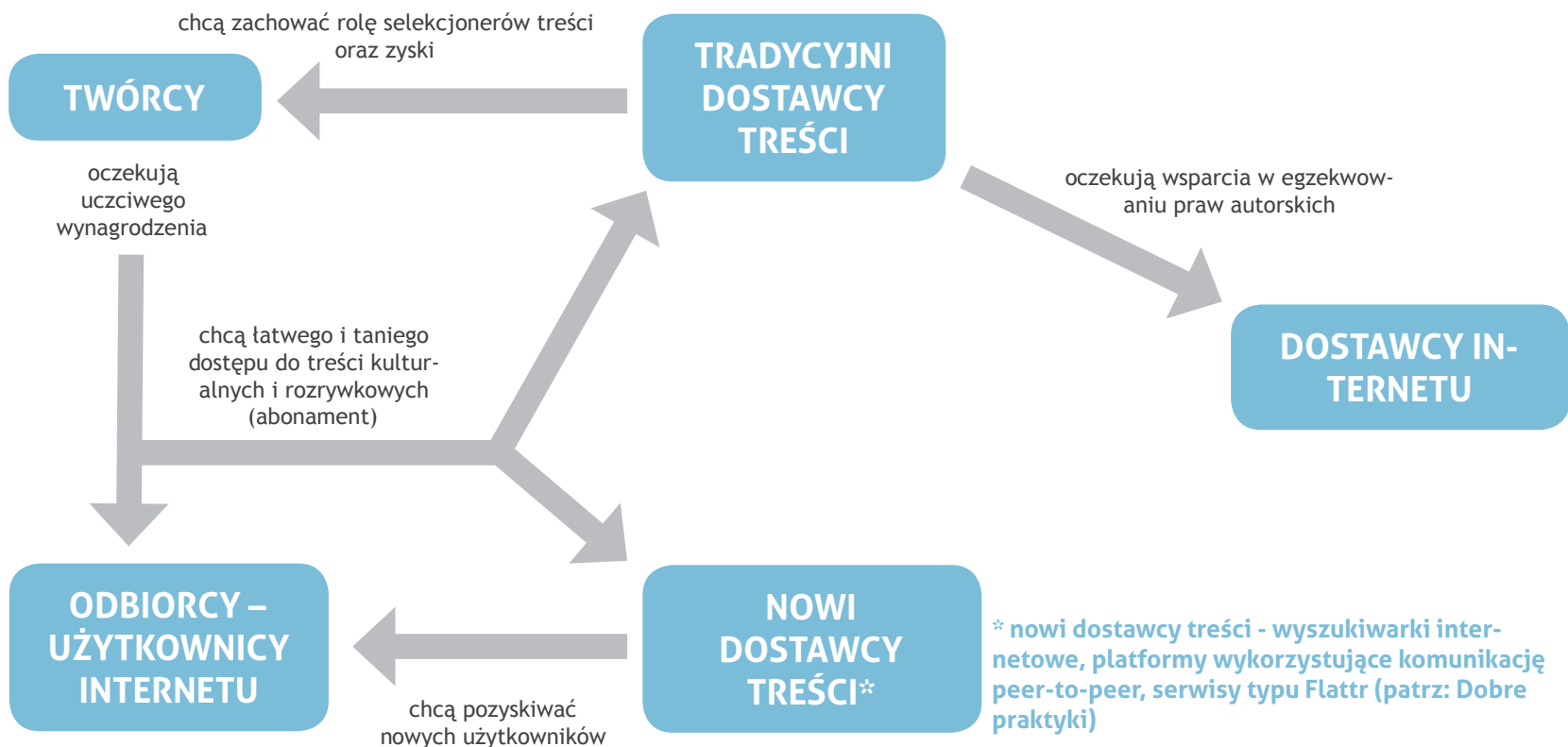
Obejmuje zarówno prawo tworzenia i rozpowszechniania własnych treści, jak i dostęp do informacji rozpowszechnianych przez innych. Oba aspekty ograniczane są coraz częściej na rzecz ochrony praw autorskich, np. poprzez blokowanie materiałów umieszczanych na portalach społecznościowych czy w serwisach umożliwiających dzielenie się plikami wideo.

Kultura posługuje się dziś rozłaczaniem pokus i rozstawianiem przynęt, kuszeniem i uwodzeniem, a nie normatywną regulacją; piarem raczej, niż policyjnym nadzorem; produkcją, rozsiewaniem i nasadzaniem nowych potrzeb, pożądań i pragnień raczej, niż przymusem.



Prof. Zygmunt Bauman

AKTORZY KONFLIKTU WOKÓŁ EGZEKWOWANIA PRAW AUTORSKICH W INTERNECIE



Mimo że dzięki internetowi świat stał się mniejszy niż kiedykolwiek, stwarzając twórcom możliwość niezwykle łatwego dotarcia do nieograniczonej liczby osób, prawo autorskie i przemysł rozrywkowy stoją im na drodze.

Komisarz Neelie Kroes, wiceprzewodnicząca Komisji Europejskiej, przemówienie na Forum Awiniońskim, grudzień 2010 r.

SCENARIUSZ 1 - Wzmocnienie egzekwowania prawa autorskiego

1. Wzmocnienie egzekwowania prawa autorskiego wspiera tradycyjny przemysł rozrywkowy, chroniąc przede wszystkim interesy tradycyjnych producentów i pośredników.

2. Kluczowym elementem tej strategii jest zaangażowanie dostawców internetu do wykrywania i ścigania naruszeń praw autorskich (poprzez filtrowanie i monitorowanie przesyłanych treści). W rezultacie musi dojść do naruszenia podstawowych praw użytkowników internetu.

43

3. Kolejny ważny instrument to ułatwienie prywatnym firmom - właścicielom praw autorskich, pozyskiwania danych osobowych użytkowników internetu, co ma duże znaczenie dla sprawności dochodzenia roszczeń.

4. Jeszcze dalej idące propozycje obejmują możliwość odcinania domniemych naruszcycieli praw autorskich od internetu (zasada trzech ostrzeżeń; patrz: Zła praktyka HADOPI).

SCENARIUSZ 2 - Dostosowanie zasad prawa autorskiego do nowych warunków

70 lat

tyle czasu po śmierci autora prawa autorskie uniemożliwiają swobodne korzystanie z jego dorobku. Film przynosi zyski mające znaczenie ekonomiczne dla producenta średnio przez kilka miesięcy od premiery.

1. Poszerzenie zakresu dozwolonego użytku: W dobie internetu każdy, kto ma do niego dostęp, może pobierać i wykorzystywać treści z obszaru szeroko rozumianej kultury. W tym kontekście nierealne i społecznie szkodliwe wydaje się egzekwowanie prawa, zgodnie z którym każdy publikujący materiały audiowizualne w sieci powinien móc wykazać swoje prawo do tych materiałów, nawet jeśli wykorzystuje je w celu niekomercyjnym. Prawo, które większość obywateli narusza nieświadomie, trzeba uznać za dysfunkcyjne.

2. Znaczne skrócenie okresu ochrony dzieła: Taka zmiana prawa odpowiadałaby uwarunkowaniom tzw. kultury remiksu (patrz: definicja) i radykalnemu skróceniu czasu komercyjnej eksploatacji dzieł. Przy obecnej dynamice rynku producent nie jest w stanie czerpać wymiernych zysków np. z filmu dłużej, niż przez kilka miesięcy od premiery. Podobnie wygląda sytuacja z innymi typami twórczości i produkcji kulturalnej. Mimo to, każdy utwór podlega ochronie prawnoautorskiej jeszcze przez 70 lat po śmierci autora, co skutecznie eliminuje go z puli materiałów dostępnych do twórczego przetwarzania i rozwijania.

SCENARIUSZE ZMIANY PODEJŚCIA

Przedstawione scenariusze dotyczące problematyki praw autorskich są wobec siebie alternatywne. Można albo zakładać wzmocnienie egzekwowania obecnych zasad prawa autorskiego, albo pracować nad ich nową konstrukcją, uwzględniającą rzeczywistość twórców i użytkowników kultury w XXI w.

PODSUMOWANIE SCENARIUSZY – DOBRE KIERUNKI

1. Dostosowanie zasad prawa autorskiego do nowych warunków

Aby zapewnić ochronę podstawowych praw obywateli, w tym wolności słowa, tworzenia i dostępu do dóbr kultury, należy realizować postulaty scenariusza 2. Debata publiczna nie powinna się koncentrować na tym, w jaki sposób lepiej egzekwować anachroniczne prawo autorskie, ale na tym, jak wprowadzić modele finansowania, które nie będą uderzały w ogół społeczeństwa. Nowe prawo powinno chronić obywateli przed represjami, jeśli w celach niekomercyjnych publikują i ściągają multimedia z internetu. Powinno też przyczyniać się do rozwoju kultury i innowacyjności.

2. Stwierdzanie naruszeń prawa autorskiego

Naruszenia prawa autorskiego może stwierdzać jedynie niezawisły sąd, zgodnie z prawem do rzetelnego procesu. Prywatne firmy nie posiadają ani prawnego umocowania, ani odpowiednich kompetencji, aby oceniać, czy doszło do naruszenia prawa i jaka jest skala ewentualnego przewinienia użytkownika. Podmioty prywatne nie powinny ani stwierdzać naruszeń prawa autorskiego, ani - tym bardziej - decydować o środkach zaradczych.

KWESTIE DO ROZSTRZYgniĘCIA – REKOMENDACJE

1. Tworzenie polityk opartych na dowodach

Analizy i badania* prowadzone przez środowiska obywatelskie, promujące alternatywne modele tworzenia i finansowania kultury, pokazują, że podrabianie i nielegalne kopiowanie utworów nie odbywa się na wielką skalę i nie zagraża zyskom producentów muzycznych czy audiowizualnych. Są to wnioski diametralnie inne, niż te przywoływane w uzasadnieniach zaostrenia reżimu egzekwowania prawa autorskiego w Unii Europejskiej. Stosowanie tych samych metod egzekwowania praw autorskich w stosunku do osób wymieniających się plikami i do fałszerzy towarów, jak planowała Komisja Europejska, nie ma zatem żadnego uzasadnienia.

*Źródło: European Digital Rights, *Raport na temat strategii Komisji Europejskiej w zakresie ochrony praw własności intelektualnej*; TNO Information and Communication technology, *Ups and downs Economic and cultural effects of file sharing on music, film and games* (patrz: aneks)

44



Żadna historycznie ugruntowana pozycja nie zagwarantuje pośrednikom przetrwania na rynku. Bez względu na to, czy im się to podoba czy nie, pośrednicy ryzykują marginalizację, jeśli nie dostosują się do potrzeb zarówno twórców, jak i konsumentów kultury.

Komisarz Neelie Kroes, Wiceprzewodnicząca Komisji Europejskiej, przemówienie na Forum Awiniońskim, grudzień 2010 r.

2. Harmonizacja prawa autorskiego

Rozdrobniony system praw autorskich stwarza wiele problemów twórcom i konsumentom kultury. Potencjalnym konsumentom często odmawia się dostępu do dzieł, które twórcy chcą zaoferować. Powstały deficyt wypełnia nielegalna wymiana treści, pozabawiająca twórców należnego wynagrodzenia. Dlatego niezbędna jest harmonizacja podstawowych zasad prawa autorskiego w ramach Unii Europejskiej, w szczególności wyjątków od ochrony prawnoautorskiej (np. zakresu dozwolonego użytku - patrz: definicja).

3. Proporcjonalność ograniczeń narzucanych przez prawo autorskie

Zgodnie z Konstytucją oraz wiążącymi Polskę międzynarodowymi standardami praw człowieka (Europejska Konwencja Praw Człowieka, Karta Praw Podstawowych UE), ograniczenie praw podstawowych - takich jak prawo do informacji, prawo do prywatności czy wolność wypowiedzi - jest dopuszczalne tylko o tyle, o ile jest ono konieczne i proporcjonalne ze względu na realizowany cel.

Ciężar wykazania, że dane ograniczenie spełnia ów standard proporcjonalności, spoczywa na tym, kto ograniczenie proponuje. Faworyzowanie interesu ekonomicznego wąskiej grupy społecznej kosztem praw podstawowych i ekonomicznych interesów ogółu społeczeństwa, wymaga zatem bezwzględniego uzasadnienia. W debacie publicznej w Polsce, jak i w Unii Europejskiej brakuje rzetelnego odniesienia się do dysproporcji między tymi interesami oraz przyczyn faworyzowania tradycyjnego przemysłu rozrywkowego.

Czy wymiana plików zniechęca do płacenia za kulturę i rozrywkę?

Zachowania konsumenckie nabywców w ciągu 12 miesięcy - wymieniający pliki i niewymieniający plików				
	Muzyka - liczba kupionych albumów	Filmy		Gry - liczba kupionych gier
		Kupione DVD	Wizyty w kinie	
wymieniający pliki	5,69	7,29	1,30	2,69
niewymieniający plików	5,49	11,97	1,28	4,21
średnio	5,61	7,97	1,30	3,04

Źródło: TNO Information and Communication Technology, *Ups and downs. Economic and cultural effects of file sharing on music, film and games* (2009 r.)

dozwolony użytek

Nie powinno być wymagane uzyskanie zgody autora na powielanie lub rozpowszechnianie dla celów edukacyjnych, naukowych, badawczych, informacyjnych, satyrycznych czy incydentalnych, utworów artystycznych, naukowych lub technologicznych, które już zostały udostępnione publicznie.

Za: *Charter for Innovation, Creativity and Access to Knowledge*

ACTA

W 2007 r. rozpoczęły się negocjacje ACTA (Anti-Counterfeiting Trade Agreement), międzynarodowego porozumienia dotyczącego walki z podrabianiem towarów i piractwem. Porozumienie ma objąć: USA, UE, Japonię, Australię, Kanadę, Koreę Południową, Nową Zelandię, Meksyk i kilka innych krajów. ACTA proponuje ochronę prawa autorskiego i patentowego ogromnym kosztem. Przede wszystkim otwiera drogę do naruszeń prywatności i innych praw podstawowych. Obywatele państw rozwijających się mogą też utracić dostęp do leków ratujących życie. Porozumienie było negocjowane w tajemnicy, z rażącym naruszeniem zasad przejrzystości. Brak szczegółowej wiedzy na temat przebiegu negocjacji i zawartości dokumentów roboczych sprawia, że trudno przewidzieć w jaki sposób poszczególne państwa podejną do interpretacji i egzekwowania porozumienia. Można przypuszczać, że postanowienia ACTA realizują interesy potężnych lobby przemysłowych, trudniejsze do przeforsowania w prawie krajowym, którego proces stanowienia jest z zasady bardziej przejrzysty.

Ustawa HADOPI - Francja

Od 1 stycznia 2001 we Francji obowiązuje tzw. ustawa Hadopi. Za domniemane naruszenia praw autorskich przez użytkowników internetu wymieniających się nielegalnie plikami w sieci, ustawa przewiduje odcięcie dostępu do internetu („prawo trzech ostrzeżeń”), karę pozbawienia wolności do 2 lat, a także grzywnę w wysokości do 300 tysięcy euro. O zastosowaniu konkretnej sankcji ma decydować sąd.

HADOPI była głośno krytykowana za nieproporcjonalne ograniczanie praw podstawowych. W celu przeciwdziałania naruszeniom interesów ekonomicznych jednego sektora przemysłu, dopuszcza się naruszenie tajemnicy korespondencji wszystkich użytkowników internetu poprzez monitorowanie ruchu w sieci. W przypadku odcięcia od internetu utrata dostępu do informacji i podstawowego narzędzia komunikacji dotyka wszystkich użytkowników, którzy korzystają z danego łącza. Takie rozwiązanie stoi w sprzeczności z przyjętą w demokratycznych państwach prawa zasadą indywidualnej odpowiedzialności.

46

DOBRA PRAKTYKA

Projekty technologiczne odpowiadające na potrzeby twórców i odbiorców treści

W odpowiedzi na zapotrzebowanie na nowe modele finansowania i dystrybucji treści kulturalnych i rozrywkowych w internecie, powstają już pierwsze interesujące projekty technologiczne, np. platforma Kickstarter (<http://www.kickstarter.com/>), która promuje niezależnych twórców i umożliwia im zbieranie środków na realizację zaplanowanych projektów. Dzieła, jakie powstają dzięki kolektywnemu modelowi finansowania, są udostępniane na otwartych licencjach. Inny pomysł na uruchomienie potencjału społecznego finansowania utworów, oferuje platforma Flattr (<https://flattr.com/>), umożliwiająca proste i szybkie przekazywanie drobnych kwot (mikropłatności) twórcom, których projekty lub utwory znajdują się w sieci. Po zarejestrowaniu, wystarczy jedno kliknięcie, żeby środki ze specjalnego konta użytkownika - odbiorcy zasiliły konto wybranego twórcy.

Swoistą odpowiedzią na przestarzały system prawa autorskiego jest też międzynarodowy projekt Creative Commons, oferujący darmowe rozwiązania prawne i inne narzędzia służące zarządzaniu przez twórców prawami autorskimi do swoich utworów. Creative Commons wspiera wolną kulturę: produkcję i wymianę utworów traktowanych jako dobro wspólne.

47

Jeżeli prawo wspólnotowe tworzone będzie na potrzeby restrykcyjnego podejścia do ochrony własności intelektualnej, Europie zagraża separacja sektora kultury i rozrywki od potrzeb obywateli. Dostawcy internetu zaczną filtrować oraz monitorować treści przesyłane w sieci, aby przeciwdziałać naruszeniom praw autorskich. Powszechny dostęp do wiedzy i kultury zostanie ograniczony, a wzrost gospodarczy i postęp osiągnięty do tej pory dzięki Internetowi - zahamowane.

PONOWNE WYKORZYSTANIE

informacji publicznej

WPROWADZENIE

49

Dostęp do informacji jest warunkiem skutecznej kontroli społeczeństwa nad sprawowaniem mandatu przez reprezentującą je władzę. Wymusza on większą transparentność poczynañ, ponieważ można przeświełać działania administracji nie tylko na podstawie jej komunikatów, ale także dzięki dostępowi do baz danych i analizie dokumentów źródłowych. Publiczne zasoby wiedzy w rękach prywatnych przedsiębiorców mogą stać się źródłem wymiernych zysków i kolejnym motorem rozwoju gospodarczego. Wreszcie, prawo do informacji stanowi jedno z zagwarantowanych konstytucyjnie praw i wolności człowieka.

W gospodarce opartej na wiedzy, dostęp do informacji z sektora publicznego ma fundamentalne znaczenie. Informacje zawarte w dokumentach generowanych przez organy sektora publicznego są przydatne nie tylko państwu. Możliwość ich ponownego wykorzystania ma dla obywateli i podmiotów prywatnych znaczenie nie mniejsze niż sam dostęp do informacji - kto ma informacje, ten ma władzę.

Prawo do informacji powinno być jak najpełniej realizowane poprzez system udostępniania informacji do ponownego wykorzystania. W Polsce bariery prawne i faktyczne przeszkadzają w realizacji tego postulatu. Administracja publiczna nie wydaje się gotowa do pełnej otwartości w udostępnianiu obywatelom tego, co wytwarza za publiczne pieniądze.

Istnienie niektórych barier jest uzasadnione interesami samych obywateli. Pełna otwartość oznacza nie tylko pełne prawo dostępu, ale także możliwość przetwarzania (np. łączenia z innymi informacjami) danych generowanych przez państwo, w tym danych o obywatelach z licznych rejestrów publicznych. Wartością, o której nie można w tym kontekście zapomnieć jest prywatność i ochrona danych osobowych.

27 mld
euro

tyle wart jest rynek ponownego wykorzystania informacji w Unii Europejskiej, według szacunków Komisji Europejskiej. Polski rynek jest wart przynajmniej kilkaset milionów euro.

Dane na podstawie badania „Measuring European Public Sector Information Resources” (MEPSIR).

Większa otwartość administracji w zakresie udostępniania informacji publicznej nie musi - i nie powinna - prowadzić do nieograniczonego przetwarzania wszelkich jawnych danych o obywatelach. Dobrze ilustrują ten dylemat kontrowersje wokół elektronicznego systemu ksiąg wieczystych, który przy odrobinie determinacji umożliwia np. ustalenie przez internet, jaki kredyt ma nasz sąsiad. Dane zgromadzone w rejestrach publicznych, w połączeniu z innymi informacjami np. śladami w internecie, stwarzają ogromne możliwości profilowania i przewidywania naszych zachowań.

DYLEMAT

1

Jak zdefiniować informację publiczną?

Obecnie definicja informacji publicznej odnosi się do niejasnego pojęcia „spraw publicznych”, co jest przyczyną sporów między obywatelami a instytucjami publicznymi o granice tego pojęcia. Rozstrzygają je sądy administracyjne, co wydłuża postępowanie w sprawach o odmowę udostępnienia informacji. Organ władzy publicznej zawsze może odmówić, powołując się na to, że dana informacja nie jest informacją publiczną. Wówczas pierwszy etap sprawy to ustalenie przez sąd, jaki status ma sporna informacja. Dopiero na drugim etapie, jeśli do niego dojdzie, sąd ustala, czy odmowa udostępnienia informacji publicznej była uzasadniona np. ze względu na tajemnicę prawnie chronioną.

Najczęstszą przyczyną sporów są informacje, które nie mają klauzuli tajności, ale udostępnia się je niechętnie, np. statystyki działań operacyjnych służb specjalnych. Im mniej precyzyjna definicja informacji publicznej, tym większa szara strefa informacji o niesprecyzowanym statusie, stanowiąca pole do nadużyć władzy.

DYLEMAT

2

Czy dostęp do informacji publicznej i prawo do jej ponownego wykorzystania powinny być tożsame?

Kwestia, czy na gruncie Konstytucji można utożsamiać prawo do informacji publicznej i prawo do jej ponownego wykorzystania, pozostaje sporna. Niezależnie od jej rozstrzygnięcia, prawodawca może te dwa reżimy prawne połączyć albo rozdzielić, tworząc przepisy wprost regulujące ten obszar.

50



To, co powstaje za publiczne pieniądze, jest własnością publiczną, a więc także tych, którzy chcą z tego korzystać w sposób wybrany przez siebie.

Premier Donald Tusk na spotkaniu z organizacjami pozarządowymi, 18 maja 2011

DYLEMAT 3

Jakie wyłączenia od prawa do ponownego wykorzystania informacji publicznej są dopuszczalne?

Ustalenie, jakie informacje nie powinny podlegać ponownemu wykorzystaniu jest kwestią kluczową. Czy powinny być to wyłącznie informacje objęte klauzulą tajności? Czy także niektóre rejestry publiczne, które mimo tego, że są jawne, nie powinny być w pełni otwarte - np. księgi wieczyste, ewidencja działalności gospodarczej lub Krajowy Rejestr Sądowy? To pytanie dotyczy też szczególnie cennych lub pracochłonnych w wytworzeniu zasobów wiedzy. W tej dyskusji prawo do informacji i dążenie do przejrzystości ścierają się z prawem do prywatności i ekonomicznymi interesami państwa.

51

Główne problemy w debacie o ponownym wykorzystaniu informacji z sektora publicznego to: które informacje generowane przez państwo będą dostępne dla obywateli i jaki użytek obywatele będą mogli z nich zrobić.

rejestr publiczny

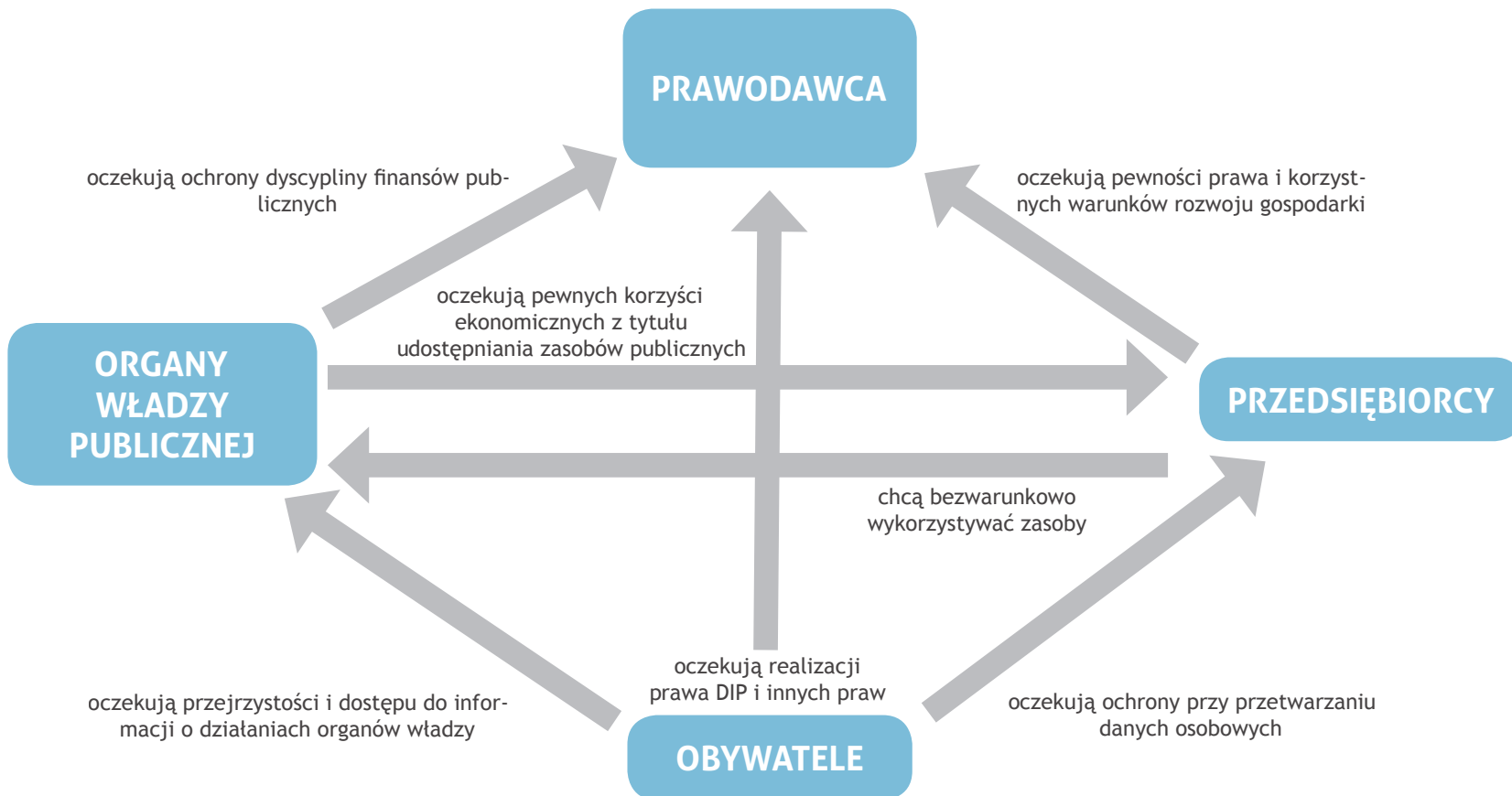
to rejestr, ewidencja, wykaz, lista, spis albo inna forma ewidencji, służąca do realizacji zadań publicznych, prowadzona przez podmiot publiczny na podstawie odrębnych przepisów ustawowych (na podstawie ustawy o informatyzacji podmiotów realizujących zadania publiczne z 17 lutego 2005 r. (Dz.U. Nr 64, poz. 565).

zwierzchnia władza narodu

Zgodnie z art. 4 ust. 1 Konstytucji, władza zwierzchnia w Rzeczypospolitej Polskiej należy do Narodu. Tym samym, obywatele mają prawo do tego, co zostało wytworzone za pieniądze z danin publicznych.



PODMIOTY ZAINTERESOWANE WYKORZYSTYWANIEM INFORMACJI PUBLICZNEJ I ICH INTERESY



udostępnienie informacji publicznej a ponowne wykorzystanie

Udostępnienie informacji oznacza samo wydanie dokumentu, żeby można było się z nim zapoznać. Zgoda na ponowne wykorzystanie informacji odnosi się do jej dalszego przetwarzania, np. łączenia z innymi danymi, wykorzystywania do oferowanych komercyjnie lub niekomercyjnie analiz i usług.

53

Wolność wypowiedzi

możliwość pozyskiwania i dowolnego wykorzystywania informacji publicznej jest jednym z filarów wolności wypowiedzi. Wykorzystują ją media i organizacje obywatelskie do formułowania i uzasadniania opinii na temat działań władzy.

Efektywność i subsydiarność

państwo powinno efektywnie zarządzać swoimi zasobami. Powinno również wspierać obywateli i przedsiębiorców, ale nie zastępować ich w tym, co mogą zrobić sprawniej lub taniej, np. w tworzeniu nowych usług czy zasobów informacyjnych w oparciu o dane, które wytwarza administracja publiczna.

Prywatność

warunkiem skutecznej kontroli obywateli nad tym, jakie informacje na ich temat gromadzi państwo i w jakich celach je wykorzystuje, jest możliwość dostępu do tych danych. Z drugiej strony, prawo do prywatności i ochrona danych osobowych muszą być uwzględniane przy ponownym wykorzystywaniu informacji z rejestrów publicznych.

Bezpieczeństwo publiczne

analiza danych publicznych przeprowadzana na masową skalę przez media i obywateli, polegająca także na łączeniu rozmaitych typów informacji, może się okazać jednym z najskuteczniejszych narzędzi wczesnego wykrywania zagrożeń dla bezpieczeństwa publicznego.

WARTOŚCI

Prawo do informacji publicznej

jest podstawowym prawem obywatelskim (art. 61 Konstytucji). Do jego realizacji niezbędne są mechanizmy i procedury umożliwiające obywatelom realny dostęp do dokumentów i zbiorów danych tworzonych przez administrację publiczną. Dostęp do informacji jest warunkiem skutecznej kontroli społeczeństwa nad sprawowaniem mandatu przez reprezentującą je władzę.

Scenariusze opisują różne możliwości uregulowania podstawowych aspektów reżimu udostępniania i wykorzystywania informacji, ale tylko niektóre z nich – 3 i 4 oraz 5 i 6 – są wobec siebie alternatywne. Dlatego też możliwe jest łączenie ich w całościowe koncepcje zmiany przepisów i praktyk wokół ponownego wykorzystywania informacji publicznej.

SCENARIUSZE ZMIANY PRAWA

SCENARIUSZ 1 - Doprecyzowanie definicji informacji publicznej

1. Przyjęcie, że każdy dokument wygenerowany przez instytucję publiczną oraz każda informacja o tym, jak taka instytucja działa, ma status informacji publicznej, uporządkowałoby dyskusję o tym, jakich informacji obywatele mają prawo domagać się od państwa.
2. Ograniczenia prawa do informacji publicznej powinny być kwestią odrębnie regulowaną poprzez zamknięty katalog, interpretowany w orzecznictwie niezawisłych sądów.
3. Katalog dopuszczalnych ograniczeń powinien zawierać jedynie to, co konieczne, ponieważ wpływa on na ograniczenie konstytucyjnych praw obywateli. Obecnie istniejące przesłanki ograniczenia prawa do informacji publicznej (art. 5 ustawy) są wystarczające również w przypadku jej ponownego wykorzystania. Wyczerpują też ograniczenia możliwe na gruncie Konstytucji.
4. Decyzje odmawiające udostępnienia określonych informacji lub dokumentów powinny być wydawane na podstawie konkretnych kryteriów wynikających z ustawy, a nie na podstawie arbitralnej oceny urzędnika, że dokument nie stanowi informacji publicznej.

SCENARIUSZ 2 - Pełna dostępność danych

1. Informacje publiczne powinny być dostępne dla wszystkich, co oznacza także osoby niepełnosprawne, zgodnie m.in. z Deklaracją Praw Osób Niepełnosprawnych i Kartą Praw Osób Niepełnosprawnych. Można to osiągnąć poprzez zapisywanie danych w odpowiednich, otwartych formatach.
2. Wykorzystywanie zamkniętych standardów informatycznych ogranicza prawo do informacji. Licencje na oprogramowanie wykorzystywane przy udostępnianiu informacji publicznych powinny umożliwiać stosowanie otwartych standardów, czyli takich, które nie wprowadzają dodatkowych ograniczeń prawnych związanych z zapisywaniem i przetwarzaniem informacji.
3. Organy sektora publicznego powinny nabywać od zewnętrznych autorów opracowań odpowiednie prawa lub licencje, aby móc ich opracowania udostępniać dalej bez ograniczeń prawnych. Zakres nabywanych praw powinien być wystarczający, aby zapewnić każdemu możliwość nieograniczonego, nieodpłatnego i niewyłączonego korzystania - oczywiście z zagwarantowaniem uznania autorstwa.

SCENARIUSZ 3 - Wprowadzenie dwóch odrębnych reżimów prawnych dla dostępu i ponownego wykorzystania informacji, z różnymi katalogami wyłączeń

To rozwiązanie daje możliwość innego ukształtowania zakresów obydwu praw i ustalenia, które informacje można od państwa pozyskiwać bez możliwości ich ponownego wykorzystania (np. poprzez łączenie z innymi danymi lub sprzedaż).

SCENARIUSZ 5 - Wprowadzenie zasady bezwarunkowego ponownego wykorzystania informacji publicznej

55

Zasada bezwarunkowego wykorzystania informacji publicznej oznacza, że informacja wytwarzana przez organy władzy publicznej ma być nie tylko dostępna, ale także możliwa do dalszego przetwarzania za pomocą dowolnych systemów technicznych i bez dodatkowych warunków. Na wykorzystującego informację można nakładać jedynie obowiązki wynikające z interesu społecznego, które nie mogą ograniczać jego własnej działalności (np. obowiązek podania źródła czy udostępniania innym zainteresowanym).

SCENARIUSZ 4 - Stworzenie jednego, spójnego reżimu, w którym te same zasady obowiązują dla udostępnienia informacji i jej ponownego wykorzystania

Każde udostępnienie informacji jest równoznaczne ze zgodą na jej dalsze wykorzystanie.

SCENARIUSZ 6 - Ustalanie warunków wykorzystywania informacji przez organy władzy publicznej

W tym scenariuszu ustawa określa jedynie ogólne ramy decyzji organów władzy publicznej co do tego, na jakich warunkach udostępnić informację publiczną do ponownego wykorzystania. Organy te mogłyby np. nakładać dodatkowe opłaty, nakazywać przetwarzanie informacji w określonym formacie, zakazywać łączenia udostępnianych informacji z innymi, czy ograniczać możliwe pola eksploatacji. Obywatel lub podmiot gospodarczy, który uważa te warunki za niezgodne z prawem, mógłby się odwoływać do sądu administracyjnego.



Z jednej strony informacja chce być droga, ponieważ jest tak cenna. Właściwa informacja w odpowiednim momencie może zmienić nasze życie. Z drugiej strony informacja chce być darmowa, bo koszt jej wydobywania ciągle się zmniejsza. Te dwie tendencje ścierają się ze sobą.

PODSUMOWANIE SCENARIUSZY – DOBRE KIERUNKI

1. Definicja informacji publicznej

Aby zapewnić efektywność ponownego wykorzystania informacji publicznej, jej definicja powinna zostać doprecyzowana zgodnie ze scenariuszem 1.

2. Zapewnienie pełnej dostępności danych

Zgodnie ze scenariuszem 2.

3. Zniesienie podziału na prawo do dostępu i prawo do ponownego wykorzystania informacji

Dostępność informacji publicznej powinna być tożsama z możliwością jej ponownego wykorzystania przez każdego i bez ograniczeń. Wszelkie wyjątki od tej zasady powinny być zgodne z art. 61 ust. 3 Konstytucji. Proponowany obecnie przez rząd odrębny tryb wnioskowania o udzielenie informacji publicznej i o jej ponowne wykorzystanie jest sprzeczny z tą zasadą.

4. Bezwarunkowe wykorzystywanie informacji publicznej

Przyjęcie zasady bezwarunkowego wykorzystywania informacji publicznej ma podstawowe znaczenie dla stworzenia dobrych fundamentów całego systemu. Ta zasada została wprowadzona do rządowego projektu ustawy o dostępie do informacji publicznej, w wyniku debaty publicznej oraz stosownej deklaracji premiera Donalda Tuska. Realizowany powinien być scenariusz 5.

56

PROBLEMY DO ROZSTRZYgniĘCIA – REKOMENDACJE

1. Stworzenie założeń stopniowej reformy systemu ponownego wykorzystania informacji publicznej

Skuteczna reforma systemu nie będzie możliwa, jeśli ograniczy się ją do jednej nowelizacji Ustawy o dostępie do informacji publicznej. Konieczna jest wielostopniowa strategia wprowadzania zmian, określająca cele i etapy dochodzenia do systemu realizującego postulat pełnej otwartości. Potrzebna jest m.in. kompleksowa ustawa o rejestrach publicznych, zastępująca skomplikowaną sieć ustaw branżowych.

2. Podmiotowy zakres obowiązku udzielania informacji publicznej do ponownego wykorzystywania

Katalog wyłączeń podmiotowych od zasady ponownego wykorzystania informacji musi mieć charakter minimalny. Nie powinien obejmować np. archiwów państwowych, publicznego radia i telewizji, instytucji kultury i nauki, uczelni czy jednostek organizacyjnych systemu oświaty. Zrozumiałe jest, że organy władzy publicznej muszą mieć czas na przygotowanie odpowiednich mechanizmów i procedur wewnętrznych, żeby udostępnianie informacji do jej ponownego wykorzystania stało się codziennością. Taki czas można jednak zagwarantować poprzez wprowadzenie odpowiednich przepisów przejściowych.

3. Zagwarantowanie praw obywateli wykorzystujących informację publiczną

Skomplikowane i długotrwałe postępowanie administracyjnie ogranicza prawa obywateli w zakresie dostępu do informacji publicznej i jej ponownego wykorzystania. Potrzebny jest np. skuteczny mechanizm egzekwowania prawa w sytuacji, gdy organ władzy publicznej nie wywiązuje się ze swoich zobowiązań. Prawodawca powinien zapewnić skuteczny, szybki i zrozumiały me-

chanizm zabezpieczający prawa starających się o pozyskanie lub wykorzystanie informacji publicznej.

4. Obowiązek raportowania / prowadzenia statystyk dotyczących ponownego wykorzystania

Należy rozważyć nałożenie na organy władzy publicznej obowiązku prowadzenia szczegółowych statystyk dotyczących ponownego wykorzystania informacji, którymi zarządzają. Statystyki te powinny być obowiązkowo publikowane, a raporty publicznie dostępne. Obowiązek ten służyłby przede wszystkim zwiększeniu przejrzystości w zarządzaniu informacją publiczną i zwiększeniu kontroli społecznej nad praktykami instytucji sektora publicznego.

5. Prawo nakładania opłat

Prawo powinno przeciwdziałać powstawaniu monopolu informacyjnego administracji publicznej. Organy władzy publicznej, jako powołane do działania w interesie społeczeństwa, nie mogą przypisywać sobie praw właścicielskich (praw autorskich do tworzonych dokumentów czy praw do baz danych). Zgodnie z tą logiką, organy władzy publicznej nie powinny mieć

też prawa pobierania opłat za ponowne wykorzystanie informacji. Opłaty mogą dotyczyć tylko etapu udostępnienia informacji, jeśli ta czynność generuje dodatkowe koszty (np. pracy urzędnika przygotowującego nietypowe zestawienie danych). W tym wypadku musi być jednak zagwarantowana ścieżka odwoławcza.

Wszystkie dane i dokumenty w posiadaniu organów sektora publicznego powinny być objęte prawem do informacji oraz do jej ponownego wykorzystania. Dopuszczalne są tylko ograniczenia uzasadnione na gruncie Konstytucji, np. ze względu na bezpieczeństwo państwa.

57

DOBRA PRAKTYKA

Domena publiczna w USA

W Stanach Zjednoczonych, informacje tworzone przez instytucje państwowe są z zasady dostępne dla każdego bez ograniczeń co do ich wykorzystania (czyli znajdują się w tzw. domenie publicznej). Informacje w formie surowych danych są gromadzone w centralnym repozytorium i tą drogą udostępniane w otwartym formacie wszystkim zainteresowanym.

Dzięki udostępnieniu zdjęć satelitarnych powierzchni ziemi wykonanych przez NASA, dziś możemy korzystać z dostępnego w internecie systemu Mapy Google. Bez wdrożenia zasady publicznej dostępności i możliwości wykorzystania informacji byłoby to niemożliwe. Dostępność takich informacji tworzy więc zupełnie nowe rynki i usługi, pozytywnie wpływa na innowacyjność gospodarki i buduje wartość przemysłów opartych o domenę publiczną.

Więcej: Gazeta Wyborcza, *Żeby publiczne było publiczne*

ZŁA PRAKTYKA

Spór na temat globalnego ocieplenia i wpływu człowieka na zmiany klimatu

Grupa naukowców została oskarżona o nierzetelność procesu naukowego. Oskarżeni nie mieli możliwości obrony wyników swoich badań, gdyż uniemożliwiano im dostęp do danych wejściowych przez ponad półtora roku. W lipcu 2011 w „New Scientist” ukazał się komunikat: „Zgoda, sceptycy, oto macie surowe dane klimatyczne, których chcieliście”. Z artykułu wynika, że naukowcom ujawniono zapisy temperatury z 5113 stacji pogody z całego świata, poza danymi z 19 polskich stacji meteorologicznych. Polska, jako jedyny kraj odmówiła zgody na ich publikację.

Materiały wspierające i dokumentujące proces decyzyjny w państwie - Polska

Kancelaria Prezydenta RP Bronisława Komorowskiego odmówiła dostępu do przedstawionych prezydentowi opinii prawnych na temat ustawy o reformie systemu emerytalnego uznając, że nie są one informacją publiczną. Sąd administracyjny uznał jednak inaczej i Kancelaria Prezydenta przegrała sprawę w pierwszej instancji.

Podobna sytuacja zaistniała w związku ze staraniami o uzyskanie informacji o tzw. tarczy antykorupcyjnej. W grudniu 2008 r. w prasie ukazały się informacje o powołaniu przez premiera narzędzia pod nazwą „tarcza antykorupcyjna”. Media, powołując się na materiały przekazane przez rząd oraz wystąpienia minister Julii Pitera, podały ogólnikowe informacje na ten temat. Koalicja organizacji pozarządowych wystąpiła do premiera o udostępnienie dokumentów wyjaśniających założenia tego projektu. Mimo trwającej trzy lata batalii i wyroku NSA, nakazującego udostępnienie informacji lub wydanie odmowy ich udostępnienia, premier nie podjął żadnych kroków.

Bez kompleksowych zmian w obowiązującym prawie, informacje wygenerowane za pieniądze obywateli w dalszym ciągu będą niedostępne lub wykorzystywane jedynie przez powiązane z instytucjami publicznymi grupy interesów.

ANEKS

RETENCJA DANYCH TELEKOMUNIKACYJNYCH I ICH UDOSTĘPNIANIE NA POTRZEBY WALKI Z PRZESTĘPCZOŚCIĄ

Prawo

Prawo krajowe

1. Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800).
2. Ustawy regulujące kompetencje policji i służb specjalnych w zakresie korzystania z danych telekomunikacyjnych, m.in. Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U. Nr 43, poz. 277 oraz Dz. U. Nr 57, poz. 390), Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. Nr 104, poz. 708), Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu z dnia 24 maja 2002 r. (Dz. U. Nr 74, poz. 676).

Prawo wspólnotowe

Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE (dyrektywa o retencji danych).

59

Plany legislacyjne

Prawo krajowe

Ujawnienie skali problemu, jakim jest w zasadzie niekontrolowany dostęp policji i służb specjalnych do danych retencyjnych, zapoczątkowało debatę publiczną na temat konieczności zmiany prawa. Rzecznik Praw Obywatelskich skierowała do Premiera

“

Przetrzymywanie danych komunikacyjnych i lokalizacyjnych osób znajdujących się na terenie Unii Europejskiej (...) ogranicza prawo do prywatności, jakie przysługuje wszystkim obywatelom. Niewątpliwie, dyrektywa [o retencji danych] jest najbardziej ingerującym w prywatność instrumentem, jaki kiedykolwiek przyjęto w Unii Europejskiej, zarówno jeśli chodzi o skalę, jak i o liczbę ludzi, których dotyka.

Peter Hustinx, European Data Protection Supervisor, *The moment of truth for the Data Retention Directive*, przemówienie na konferencji *Taking on the Data Retention Directive*, Bruksela, 3 grudnia 2010 r.

wystąpienie generalne, w którym wskazała rekomendowane kierunki zmian w przepisach kompetencyjnych służb. Minister ds. służb specjalnych, Jacek Cichocki podjął działania zmierzające do zbadania praktyki wykorzystywania danych retencyjnych w pracy operacyjnej służb i policji, a następnie opublikował raport z propozycjami kierunków zmian legislacyjnych. Rząd nie zamierza odstąpić od obowiązkowej retencji danych, ale planuje zasadnicze zmiany co do jej zakresu, celów i czasu przechowywania danych. Zapowiedziane zostało także wzmocnienie nadzoru nad działaniami operacyjnymi służb, w szczególności stworzenie niezależnego organu nadzorczego.

Prawo wspólnotowe

Komisja Europejska prowadzi obecnie proces rewizji dyrektywy o retencji danych (2006/24/WE). Zakończony został pierwszy etap, czyli proces ewaluacji implementacji dyrektywy w poszczególnych państwach członkowskich. Wnioski zawarte w raporcie z ewaluacji, przygotowanym przez Dyрекcję ds. wewnętrznych, są zdumiewające: żadne państwo członkowskie nie wdrożyło dyrektywy zgodnie z zamiarem twórców tego instrumentu. Rozbieżności w implementacji pomiędzy poszczególnymi państwami członkowskimi są tak daleko idące, że trudno w ogóle mówić o harmonizacji prawa. Dyrekcja ds. wewnętrznych pracuje obecnie nad propozycją rewizji dyrektywy. Kluczowym dokumentem, uzasadniającym proponowany kierunek zmian, będzie ocena skutków regulacji, spodziewana jeszcze w 2011 r.

Polecane źródła

1. Report From the Commission to the Council And The European Parliament: Evaluation report on the Data Retention Directive (COM(2011) 225 final)
2. Raport Ministra Jacka Cichockiego dotyczący retencji danych telekomunikacyjnych (http://bip.kprm.gov.pl/kprm/komunikaty/281_4067.html)

Wyroki sądów i skargi złożone w sprawie obowiązkowej retencji danych *

Niemcy

Wyrok niemieckiego Federalnego Sądu Konstytucyjnego z 11 marca 2010 r. (1 BvR 256/08)

Sąd nie wypowiedział się radykalnie przeciwko zasadzie prewencyjnego gromadzenia danych, ale stwierdził, że retencja danych telekomunikacyjnych stanowi poważne ograniczenie prawa do prywatności i dlatego powinna być dopuszczalna tylko w ściśle określonych okolicznościach. Sąd zasugerował również, że maksymalny dopuszczalny okres zatrzymywania danych to 6 miesięcy. Przepisy, które wdrażały dyrektywę retencyjną do prawa niemieckiego przestały obowiązywać.

Czechy

Wyrok Czeskiego Trybunału Konstytucyjnego z 22 marca 2011 r. (Akt nr 127/2005 i Dekret nr 485/2005)

Sąd nie podważył wprost zasady prewencyjnego gromadzenia danych o obywatelach, ale zakwestionował - i anulował - krajowe przepisy implementujące dyrektywę jako niedostatecznie jasne i precyzyjne. Wyraził także wątpliwość co do konieczności, sensowności i adekwatności gromadzenia danych o ruchu w sieciach telekomunikacyjnych w kontekście pojawiania się w świecie przestępczym nowych narzędzi, takich jak anonimowe karty SIM.

Rumunia

Decyzja rumuńskiego Sądu Konstytucyjnego nr 1258 z 8 października 2009 r.

Sąd wypowiedział się kategorycznie przeciwko zasadzie prewencyjnego gromadzenia danych o obywatelach. Uznał, że sama zasada retencji godzi w domniemanie niewinności oraz pozostaje w sprzeczności z prawem do prywatności i do wolności wypowiedzi z art. 8 Europejskiej Konwencji Praw Człowieka. W efekcie, przepisy, które wdrażały dyrektywę retencyjną do prawa rumuńskiego, przestały obowiązywać.

Bułgaria

Decyzja bułgarskiego Najwyższego Sądu Administracyjnego nr. 13627 z 11 grudnia 2008 r.

Sąd uznał za niekonstytucyjne przepisy, które implementowały dyrektywę retencyjną, ponieważ nie stwarzały wystarczających gwarancji ochrony praw obywatelskich. W wyniku tego wyroku Bułgaria ponownie implementowała dyrektywę do swojego porządku prawnego.

Węgry

Skarga do węgierskiego Trybunału Konstytucyjnego z 2 czerwca 2008 r. wniesiona przez Węgierską Unię Wolności Obywatelskich (sprawa C-189/09 oraz C-185/09)

Sprawa w toku. Skarga koncentruje się na niewłaściwej transpozycji dyrektywy retencyjnej do krajowego porządku prawnego (niezdefiniowanie celów przetwarzania danych).

**Polska**

Wniosek do Trybunału Konstytucyjnego z 28 stycznia 2011 r. wniesiony przez grupę posłów SLD

Sprawa w toku. Wniosek kwestionuje zarówno sposób implementacji dyrektywy retencyjnej do polskiego porządku prawnego (zasady wykorzystywania danych retencyjnych przez służby specjalne), jak i sam reżim prewencyjnego gromadzenia danych o obywatelach, jako niezgodny z zasadą demokratycznego państwa prawnego (wyrażoną w art. 51 ust. 2 Konstytucji).

Wniosek Rzecznika Praw Obywatelskich do Trybunału Konstytucyjnego z 1 sierpnia 2011 r. (RPO-662587-II-II/ST)

RPO nie kwestionuje samej idei retencji danych, ale bardzo swobodne zasady ich udostępniania wybranym organom, brak kontroli zewnętrznej oraz gwarancji niszczenia niepotrzebnych informacji, które uderzają w prawo do prywatności i tajemnicę komunikowania się obywateli.

* informacje na podstawie raportu Komisji Europejskiej w sprawie ewaluacji dyrektywy o retencji danych

ODPOWIEDZIALNOŚĆ POŚREDNIKÓW ZA TREŚĆ W INTERNECIE

Prawo

Prawo krajowe

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (UŚUDE), Rozdział III, art. 12-15 (Dz. U. Nr 144, poz. 1204). UŚUDE wdraża do polskiego porządku prawnego postanowienia dyrektywy o handlu elektronicznym.

Prawo wspólnotowe

Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym).

Plany legislacyjne

Prawo krajowe

W 2009 r. MSWiA podjęło próbę zreformowania UŚUDE, w tym zasad odpowiedzialności pośredników. W czerwcu 2011 r. rząd przyjął projekt założeń do nowelizacji, jednak nie powstał jak dotąd projekt nowelizacji ustawy.

Prawo wspólnotowe

Trwa proces ewaluacji dyrektywy o handlu elektronicznym, obejmującej także problematykę odpowiedzialności pośredników za treść. W okresie od sierpnia do listopada 2010 r. Komisja Europejska prowadziła konsultacje społeczne, a na wrzesień 2011 r. zapowiedziała publikację komunikatu dotyczącego przyszłości usług elektronicznych w UE.

Wybrane orzecznictwo

Europejski Trybunał Praw Człowieka

Times przeciwko Zjednoczonemu Królestwu
(skarga nr 3002/03
i 23676/03)

Wolność wypowiedzi, informacji i komunikowania się powinny być chronione jednakowo skutecznie w środowisku cyfrowym, jak i w rzeczywistości niewirtualnej.

Delfi przeciwko Estonii
(skarga nr 64569/09)

Sprawa w toku. Problem zakresu odpowiedzialności pośredników, w szczególności obowiązku prewencyjnego monitorowania treści umieszczanej przez użytkowników.

Autronic AG przeciwko Szwajcarii
(skarga nr 12726/87)

„Naruszenia wolności słowa należy badać nie tylko przez pryzmat ingerencji w treść; może ono polegać również na ingerencji w środki komunikacji bądź recepcji treści, niezależnie od bezprawnego charakteru samej treści, która może nie zasługiwać na ochronę gwarantowaną przez Europejską Konwencję Praw Człowieka”. Nadmierne sankcje stosowane nie tylko wobec autorów treści, ale także wobec pośredników internetowych mogą w bezpośredni sposób wpływać na korzystanie z prawa do rozpowszechniania oraz pozyskiwania informacji w internecie.

Trybunał Sprawiedliwości Unii Europejskiej

eBay przeciwko L'Oréal
(sygn. C-324/09)

Wyłączenie odpowiedzialności pośrednika ze względu na brak wiedzy o bezprawności treści umieszczanych przez użytkowników, nie obejmuje hostin-godawcy, który oprócz „czysto technicznego i automatycznego przetwarzania danych” odgrywa czynną rolę, polegającą w szczególności na „optymalizacji prezentacji konkretnych ofert sprzedaży lub ich promocji”. Przetwarzanie, klasyfikowanie czy jakakolwiek ingerencja w treści dodawane przez użytkowników jest równoznaczna z powzięciem „wiarygodnej wiadomości” o ich bezprawnym charakterze.

Sabam przeciwko Scarlet
(sygn. C-70/10)

Sprawa w toku. Ważna opinia Rzecznika Generalnego dotycząca roli pośredników w zapobieganiu naruszeniom praw autorskich w internecie. Rzecznik opowiedział się przeciwko metodzie automatycznego filtrowania stron internetowych: „wdrożenie tego systemu stanowiłoby ograniczenie prawa do poszanowania tajemnicy połączeń telekomunikacyjnych i prawa do ochrony danych osobowych chronionych Kartą Praw Podstawowych”.

Orzecznictwo krajowe

Sprawa Forum Akademickiego
(sygn. I ACa 544/10)

Sąd stwierdził, że zatrudnienie moderatora forum internetowego powoduje przejęcie obowiązku aktywnego monitorowania wszelkich treści dodawanych przez użytkowników.
Sprawa czeka na rozpoznanie przed Sądem Najwyższym.

Sprawa portalu GazetaBytowska.pl
(sygn. VI Ka 202/09)

Administrator portalu nie ponosi odpowiedzialności za treść umieszczonych na nim komentarzy na takiej zasadzie, jak redaktor naczelny za treść w tradycyjnej gazecie. Wpisy użytkowników nie są materiałem prasowym, dlatego w takich przypadkach zastosowanie powinno mieć nie Prawo prasowe, a UŚUDE.

Sprawa portalu NaszaKalwaria.pl
(sygn. akt IC 1532/09)

Redaktor portalu odmówił usunięcia niektórych komentarzy pod swoimi artykułami na żądanie burmistrza. Redaktor blokował jedynie komentarze wulgarne. Sąd oddalił powództwo o naruszenie dóbr osobistych, uznając, że odmowa usunięcia komentarzy była uzasadniona, ponieważ miały one charakter indywidualnych opinii użytkowników oraz dotyczyły oceny działań burmistrza związanych ze sprawowaną przez niego funkcją publiczną.

Sprawa portalu Nasza Klasa
(sygn. I A Ca 1202/09)

Sąd stwierdził naruszenie dóbr osobistych mężczyzny, który zwrócił się do Naszej Klasy (obecnie NK) o udostępnienie danych, umożliwiających identyfikację osoby, która w tym serwisie samowolnie wykorzystała jego wizerunek.

EGZEKOWANIE PRAW AUTORSKICH W ŚRODOWISKU CYFROWYM

Prawo

Prawo krajowe

Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. Nr 24 poz. 83).

Prawo wspólnotowe

Dyrektywa 2004/48/WE Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. w sprawie egzekwowania praw własności intelektualnej.

Plany legislacyjne

Prawo wspólnotowe

W maju 2011 Komisja Europejska ogłosiła strategię w zakresie ochrony praw własności intelektualnej. W związku z opublikowaną strategią spodziewana jest rewizja prawa wspólnotowego w tym zakresie, związana również ze spodziewanym przyjęciem porozumienia ACTA przez UE oraz, niezależnie, przez poszczególne państwa członkowskie.

Polecane źródła

- Raport EDRI na temat strategii Komisji Europejskiej w zakresie ochrony praw własności intelektualnej (http://www.edri.org/files/IPR_shadowreport_110523.pdf).
- Free Culture Forum, *Charter for Innovation, Creativity and Access to Knowledge* (<http://fcforum.net/en/charter>).
- Free Culture Forum, *Sustainable Models for Creativity in the Digital Age* (<http://fcforum.net/en/sustainable-models-for-creativity>).
- TNO Information and Communication technology, *Ups and downs Economic and cultural effects of file sharing on music, film and games* (http://www.ivir.nl/publicaties/vaneijk/Ups_And_Downs_authorized_translation.pdf).
- Institute for Information Law, University of Amsterdam, *The Recasting of Copyright & Related Rights for the Knowledge Economy* (http://ec.europa.eu/internal_market/copyright/docs/studies/etd2005imd195recast_report_2006.pdf)

PONOWNE WYKORZYSTANIE INFORMACJI PUBLICZNEJ

Prawo

Prawo krajowe

1. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. Nr 112, poz. 1198)

API (ang. Application Programming Interface)

to interfejs do programowania aplikacji (w postaci biblioteki procedur lub innej formy oprogramowania) umożliwiający realizację określonego zakresu zadań z pewnego języka programowania, np. dostępu do bazy danych, systemu operacyjnego, interfejsu graficznego.

Jest to kluczowa ustawa regulująca dostęp do informacji publicznej. Reżim ponownego wykorzystania informacji publicznej jak dotąd nie został uregulowany w sposób wyraźny. Zgodnie z zasadą „co nie jest zakazane, jest dozwolone”, nawet bez wyraźnej podstawy prawnej istnieje możliwość ponownego wykorzystywania informacji uzyskiwanych od organów administracji państwowej. Obywatele i podmioty gospodarcze napotykają jednak wiele barier już na etapie pozyskiwania informacji publicznej, podczas gdy dla jej ponownego wykorzystania fundamentalne znaczenie mają także takie parametry, jak format danych czy udostępnienie interfejsu API.

2. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2002 r. Nr 101, poz. 926)
Ustawa ma zastosowanie do przetwarzania (w tym ponownego wykorzystywania) wszelkiej informacji publicznej, która jednocześnie stanowi dane osobowe. Ochrona danych osobowych ma fundamentalne znaczenie przy przetwarzaniu danych z rejestrów publicznych.
3. Reżim prawny dotyczący informacji publicznej jest niezwykle złożony. Obejmuje ponad sto ustaw regulujących przetwarzanie danych przez rozmaite organy administracji państwowej, w tym w ramach rejestrów publicznych (m.in.: księgi wieczyste, ewidencja gruntów i budynków, Krajowy Rejestr Sądowy, Krajowy Rejestr Karny, Powszechny Elektroniczny System Ewidencji Ludności (PESEL), Centralna Ewidencja Pojazdów i Kierowców (CEPiK), Ogólnopolska Ewidencja Wydanych i Utraconych Dowodów Osobistych).

Prawo wspólnotowe

Dyrektywa 2003/98/WE Parlamentu Europejskiego i Rady z dnia 17 listopada 2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego.

Plany legislacyjne

Prawo krajowe

Polska wciąż jeszcze nie wdrożyła postanowień dyrektywy do krajowego porządku prawnego. W związku z tym Komisja Europejska zapowiada nałożenie na Polskę kar rzędu wielu milionów euro.

W lipcu 2011 r. rząd skierował do Sejmu pilny projekt nowelizacji ustawy o dostępie do informacji publicznej, wprowadzający szereg przepisów dotyczących jej ponownego wykorzystywania. Nowelizacja ma wprowadzić jasne zasady przetwarzania, łączenia i dalszego udostępniania, także w celach komercyjnych, informacji pochodzących z sektora publicznego. Jeśli projekt wejdzie w życie, najważniejszym osiągnięciem będzie wprowadzenie zasady bezwarunkowego wykorzystywania informacji publicznej.

Prawo wspólnotowe

W marcu 2011 Komisja Europejska opublikowała raport z zasięgnięcia opinii na temat funkcjonowania dyrektywy. Dyskusja nad dalszymi krokami trwa, jednak w niedalekiej przyszłości należy się spodziewać rewizji postanowień dyrektywy.

Polecane źródła

Centrum Cyfrowe Projekt: Polska, *Mapa drogowa otwartego rządu w Polsce* (<http://centrumcyfrowe.pl>).



**Warszawa
2011**