

## **UCHWAŁA nr 10 RADY do SPRAW CYFRYZACJI**

**z dnia 7 stycznia 2016 r.**

### **w sprawie projektu nowelizacji ustawy o Policji**

Na podstawie art. 17 ust. 2 ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne* (j.t. Dz.U. z 2014 r. poz. 1114) oraz § 5 Regulaminu Rady do Spraw Cyfryzacji stanowiącego załącznik do Zarządzenia nr 1 Ministra Administracji i Cyfryzacji z dnia 5 stycznia 2015 r. *w sprawie ustanowienia regulaminu prac Rady do Spraw Cyfryzacji* (Dz. Urz. z 2015 r. poz. 1), uchwała się, co następuje:

**W odniesieniu do poselskiego projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw z dnia 23 grudnia 2015 roku (Druk nr 154) oraz w nawiązaniu do uchwały nr 8 Rada do Spraw Cyfryzacji z zaniepokojeniem zauważa, że projekt ten procedowany jest niezgodnie z dobrymi praktykami stanowienia prawa w demokratycznym państwie, które wymagają przeprowadzenia konsultacji społecznych oraz przygotowania oceny skutków regulacji. Jednocześnie w opinii Rady przedstawiony projekt budzi wiele wątpliwości co do jego zgodności z Konstytucją RP i wymaga dalszych prac legislacyjnych, które dostosują go do wymogów wynikających z orzeczenia Trybunału Konstytucyjnego z dnia 30 lipca 2014 r. sygn. akt K23/11 (Dz.U. z 2014 r. poz. 1055) i prawa Unii Europejskiej.**

**Biorąc pod uwagę harmonogram prac mających na celu dostosowanie polskiego systemu prawa do ww. wyroku Trybunału Konstytucyjnego, Rada do Spraw Cyfryzacji rekomenduje:**

1. Wprowadzenie realnych mechanizmów kontroli zarówno uprzedniej jak i następczej nad wykorzystywaniem danych telekomunikacyjnych i internetowych, w którym konieczność uzyskania zgody sądu bądź innego niezależnego organu będzie zasadą, a nie wyjątkiem;
2. Uwzględnienie standardu wyznaczonego przez prawo Unii Europejskiej dotyczącego zakresu ustawy i gromadzonych na jej podstawie danych, kryteriów określenia najpoważniejszych przestępstw, które uzasadniałyby dostęp do danych, wymogów

odnoszących się do kontroli uprzedniej i gwarancji ochrony przed nadużyciami. Rada podziela stanowisko Rzecznika Praw Obywatelskich przedstawione w piśmie z dnia 29 grudnia 2015 r. (II.519.109.2015.KŁS). W projekcie ustawy nie dookreślono przestępstw uzasadniających stosowanie działań operacyjno-rozpoznawczych, nie określono także szczegółowo kategorii podmiotów, wobec których mogą być podejmowane czynności operacyjno-rozpoznawcze, nie wyznaczono szczegółowych zasad wykorzystywania zgromadzonych materiałów;

3. Doprecyzowanie projektowanych zapisów w taki sposób, by nie było wątpliwości, że sięganie przez uprawnione podmioty po dane internetowe zawierające treść przesłanego komunikatu będzie możliwe jedynie w ramach kontroli operacyjnej, tj. za uprzednią zgodą sądu;
4. Doprecyzowanie projektowanej regulacji w zakresie form kontroli operacyjnej, w taki sposób, by nie dochodziło do pogorszenia uprawnień procesowych jednostki przy jednoczesnym poszerzeniu zakresu kontroli operacyjnej;
5. Rozważenie wprowadzenia krótszego czasu retencji danych telekomunikacyjnych (do sześciu miesięcy);
6. Doprecyzowanie projektowanych przepisów w zakresie procedury niszczenia materiałów pochodzących z kontroli operacyjnej zawierających tajemnice zawodowe zgodnie ze standardem wyznaczonym przez Trybunał Konstytucyjny;
7. Wprowadzenie obowiązku przedstawienia przed Sejmem RP corocznego sprawozdania przez Prokuratora Generalnego w zakresie pobieranych danych telekomunikacyjnych i internetowych. Dane te powinny być przedstawione w podziale na rodzaje spraw oraz działania mechanizmu kontrolnego (ile razy sąd się zgodził – ile razy odmówił zgody, ile razy zgoda była uzyskiwana w trybie następczym – wyniki kontroli w trybie następczym). Obowiązek sprawozdawczy Prokuratora Generalnego powinien być realizowany w oparciu o dane przekazywane przez Policję i inne podmioty uprawnione do sięgania po dane telekomunikacyjne i internetowe. Dostęp parlamentu i opinii publicznej do informacji o skali i celach ingerencji w prawa jednostki zwiększa przejrzystość życia publicznego i stanowi formę kontroli nad działaniami służb. Równocześnie obowiązek sprawozdawczy Prokuratora Generalnego nie utrudnia prowadzenia działań, które są niezbędne ze względu na bezpieczeństwo Państwa;
8. Wprowadzenie zasady subsydiarności, która zapewni, że uprawnione podmioty będą

sięgać po dane wyłącznie w sytuacjach, w których inne środki okażą się niewystarczające lub nieprzydatne. W tym kontekście Rada zwraca uwagę na niebezpieczeństwa związane z zawieraniem ogólnych porozumień z operatorami telekomunikacyjnymi i podmiotami świadczącymi usługi drogą elektroniczną na bazie których uprawnione podmioty zyskają bezpośredni dostęp do serwerów zawierających dane telekomunikacyjne i internetowe. Zawieranie porozumień przy tak ogólnym kształcie przepisów stwarza ryzyko masowej inwigilacji i może w efekcie doprowadzić do naruszania zasady subsydiarności;

9. Wprowadzenia zasady odpłatności za dostęp do danych telekomunikacyjnych i internetowych. Proponowany zapis na mocy którego operatorzy i usługodawcy mają na własny koszt zapewnić warunki techniczne i organizacyjne utrwalania i przekazywania danych jest nieuzasadniony. Rozwiązanie to utrwała niekorzystną dla rozwoju gospodarczego praktykę przerzucania kosztów realizacji obowiązków Państwa na przedsiębiorców;
10. Wprowadzenie mechanizmu informowania osób, których dane zostały pobrane, o tym fakcie.

Jednocześnie Rada do Spraw Cyfryzacji pragnie przypomnieć, iż dane telekomunikacyjne stanowią integralny element tajemnicy komunikowania się. Potwierdził to m.in. Europejski Trybunał Praw Człowieka (ETPC) w wyrokach Malone przeciwko Wielkiej Brytanii (skarga nr 8691/79) i Copland przeciwko Wielkiej Brytanii (skarga nr 62617/00). W pierwszym z tych wyroków ETPC wskazał, że „pozyskiwanie danych zawartych w tzw. bilingach nie może wprawdzie być utożsamiane z podsłuchem rozmów telefonicznych, jednakże ujawnienie policji tego rodzaju danych bez zgody abonenta powinno być traktowane jako równoważne ingerencji w prawo zagwarantowane w art. 8 ust. 1 Konwencji (prawo do prywatności)”.

Stanowisko to potwierdziły w swoich wyrokach zarówno Trybunał Konstytucyjny, jak i Trybunał Sprawiedliwości Unii Europejskiej (TSUE). W związku z tym, jak wskazał TSUE „ochrona życia prywatnego w każdym wypadku wymaga, aby odstępstwa od ochrony danych osobowych i jej ograniczenia ograniczały się do tego, co jest absolutnie konieczne”.



## Protokół z głosowania

Decyzją Przewodniczącego Rady głosowanie zostało przeprowadzone w trybie obiegowym. Projekt uchwały nr 10 został przesłany członkom Rady w dniu 5 stycznia br. z terminem głosowania do dnia 13 stycznia br. W głosowaniu wzięło udział 19 członków Rady z czego oddano:

- 19 głosów „za” przyjęciem uchwały,
- 0 głosów „przeciw” oraz
- 0 głos „wstrzymuję się”.

Głosowanie zostało zamknięte w dniu 7 stycznia br. po oddaniu głosów przez wszystkich członków Rady.

Jarosław Lipszyc zgłosił uwagę merytoryczną do projektu uchwały.

**Uchwała nr 10 Rady do Spraw Cyfryzacji została przyjęta jednogłośnie w dniu 7 stycznia 2016 r. w głosowaniu jawnym.**

Szczegóły dotyczące głosowania przedstawia poniższa tabela.

Lp.	Imię	Nazwisko	Głos
1.	Michał	Chrzanowski	za
2.	Jan Maciej	Czajkowski	za
3.	Adam	Góral	za
4.	Patrycja	Gołos	za
5.	Piotr	Kabaj	za
6.	Lidia	Kołučka-Żuk	za
7.	Jarosław	Lipszyc	za
8.	Mariusz	Madejczyk	za
9.	Igor	Ostrowski	za
10.	Grzegorz	Sibiga	za
11.	Dominik	Skoczek	za
12.	Krzysztof	Szubert	za

13.	Katarzyna	Szymielewicz	za
14.	Alek	Tarkowski	za
15.	Elżbieta	Traple	za
16.	Jarosław	Tworóg	za
17.	Agata	Wacławik-Wejman	za
18.	Piotr	Wagłowski	za
19.	Iwona	Wendel	za

Warszawa, dnia 7 stycznia 2016 r.

  
**Przewodniczący Rady**