 Warszawa, 6 lipca 2022 r.

MINISTER DO SPRAW UNII EUROPEJSKIEJ

***Konrad Szymański***

Sygn. DPUE.920.873.2022.DL(2)

dot.: DRC.WL.06110.5.2022 z 15.06.2022 r.

**Pan Mateusz Morawiecki**

**Prezes Rady Ministrów**

**Minister Cyfryzacji**

**Opinia**

**o zgodności z prawem Unii Europejskiej *projektu ustawy o zwalczaniu nadużyć w komunikacji elektronicznej,* wyrażona przez ministra właściwego do spraw członkostwa Rzeczypospolitej Polskiej w Unii Europejskiej**

*Szanowny Panie Premierze,*

w związku z przedłożonym projektemustawypozwalam sobie wyrazić poniższą opinię.

1. Projektowana ustawa nakłada określone obowiązki na przedsiębiorców telekomunikacyjnych i dostawców poczty elektronicznej (art. 3 ust. 2 6, art. 8, art., 12, art. 13 i art. 21 projektu). Mogą one w mojej opinii zostać uznane za zasady dotyczące usług w rozumieniu art. 1 ust. 1 lit. e) *dyrektywy (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiającej procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego*, których projekt podlega obowiązkowi notyfikacji zgodnie z procedurą określoną w tej dyrektywie. Na mocy art. 1 ust. 3 dyrektywy 2015/1535 nie ma ona wprawdzie zastosowania do zasad odnoszących się do zagadnień objętych przepisami Unii w dziedzinie usług telekomunikacyjnych, jak jednak wskazano w uzasadnieniu projektu, materia regulowana projektowaną ustawą nie jest objęta przepisami *dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej*. Przywołane wyłączenie nie będzie miało zatem zastosowania w omawianym przypadku.

Decyzję o konieczności notyfikacji podejmuje projektodawca, w przypadku wątpliwości możliwe jest zasięgnięcie w tej kwestii opinii ministra właściwego do spraw gospodarki, który pełni funkcję koordynatora krajowego systemu notyfikacji norm i aktów prawnych.

Na marginesie powyższej uwagi pragnę dodatkowo zauważyć, że porozumienie pomiędzy Prezesem Urzędu Komunikacji Elektronicznej, a operatorami, o którym mowa w art. 10 ust. 1 projektu, może z kolei zostać uznane za przepis techniczny de facto zdefiniowany w art. 1 ust. 1 lit. f) ppkt (ii) dyrektywy 2015/1535. Jego projekt powinien zatem również zostać notyfikowany Komisji Europejskiej.

1. Zgodnie z projektowanym art. 14 ust. 2 ustawy przedsiębiorcy telekomunikacyjni mogą przetwarzać i wzajemnie udostępniać również komunikat elektroniczny w celu identyfikacji, zapobiegania i zwalczania smishingu. Ponadto, zgodnie z ust. 3 tego przepisu, przedsiębiorca telekomunikacyjny może przetwarzać:

1) treści krótkich wiadomości tekstowych (SMS), oraz

2) dane o usługach telekomunikacyjnych, które nie zostały przez tego przedsiębiorcę wykonane w związku z realizacją obowiązku, o którym mowa w art. 4 ust. 6 lub uprawnienia, o którym mowa w art. 7

– w celu realizacji obowiązku, o którym mowa w art. 3 ust. 2, art. 4 ust. 6 i art. 8 oraz realizacji uprawnienia, o którym mowa w art. 7, a także na cele związane z dochodzeniem roszczeń.

Wydaje się, że przywołane przepisy umożliwiają ingerencję w treść komunikatów elektronicznych oraz krótkich wiadomości tekstowych. Tymczasem na mocy art. 5 ust. 1 *dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)* państwa członkowskie mają zapewnić, poprzez ustawodawstwo krajowe, poufność komunikacji i związanych z nią danych o ruchu. W szczególności zakazane powinno być słuchanie, nagrywanie, przechowywanie lub inne rodzaje przejęcia lub nadzoru komunikatu i związanych z nim danych o ruchu przez osoby inne niż użytkownicy, bez zgody zainteresowanych użytkowników, z wyjątkiem upoważnienia zgodnego z art. 15 ust. 1.

Z kolei zgodnie z art. 15 ust. 1 dyrektywy 2002/58/WE państwa członkowskie mogą uchwalić środki ustawodawcze w celu ograniczenia zakresu praw i obowiązków przewidzianych w art. 5, 6, art. 8 ust. 1–4, i art. 9 tej dyrektywy, gdy takie ograniczenia stanowią środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego, obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej.

Możliwe jest zatem ustanowienie środków w tym zakresie, po pierwsze na podstawie zgody zainteresowanego użytkownika, a po drugie, w celu zapobiegania niedozwolonemu używaniu systemów łączności elektronicznej - pod warunkiem jednak, że środki te będą niezbędne, właściwe i proporcjonalne do tego celu.

W tym zakresie wyjaśnienia przez projektodawcę wymaga sposób przetwarzania informacji, o których jest mowa w projektowanym art. 14 ust. 2 i ust. 3 ustawy i tego, czy treści komunikatów elektronicznych oraz treści krótkich wiadomości tekstowych będą pozyskiwane od samych zainteresowanych użytkowników (np. tak jak to sugeruje obecne brzmienie art. 4 ust. 1 projektu, zgodnie z którym CSIRT NASK na podstawie otrzymanych od odbiorców krótkich wiadomości tekstowych (SMS) monitoruje występowanie smishingu), czy też przetwarzanie to będzie odbywało się w inny sposób, np. automatyczny, i będzie polegało na filtrowaniu treści komunikatów pod kątem występowania w nich niedozwolonych treści.

Uzasadnienie projektu ustawy nie zawiera w tym zakresie wyjaśnień, a kwestia ta jest istotna do właściwej oceny zgodności projektowanych rozwiązań z przepisami dyrektywy 2002/58/WE, jak również - jak się zdaje - z *rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)*. Należy bowiem pamiętać, że jakakolwiek ingerencja w treść komunikatów łączności elektronicznej powinna być dozwolona jedynie w bardzo jasno określonych warunkach i w konkretnych celach oraz powinna podlegać odpowiednim zabezpieczeniom przed nadużyciami.

1. Na podstawie art. 14 ust. 4 projektu ustawy do przetwarzania danych osobowych przez przedsiębiorców telekomunikacyjnych nie stosuje się przepisu art. 14 i 15 rozporządzenia 2016/679 w zakresie, w jakim jest to niezbędne dla identyfikacji, zapobiegania oraz zwalczania przestępstw na szkodę przedsiębiorcy telekomunikacyjnego.

Zwracam zatem uwagę na to, że na podstawie art. 23 ust. 1 rozporządzenia 2016/679 prawo Unii lub prawo państwa członkowskiego, któremu podlegają administrator danych lub podmiot przetwarzający, może aktem prawnym ograniczyć zakres obowiązków i praw przewidzianych w art. 12–22 i w art. 34, a także w art. 5 – o ile jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12–22 – jeżeli ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym określonym w tym ustępie celom. Można zatem wprowadzić ograniczenie w powyższym zakresie, które ma służyć np. celowi zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych lub wykonywania kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom (lit. d)), czy innym ważnym celom leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu Unii lub państwa członkowskiego, w tym kwestiom pieniężnym, budżetowym i podatkowym, zdrowiu publicznemu i zabezpieczeniu społecznemu (lit. e)). Jednak przy wprowadzaniu takich regulacji zasadne jest przedstawienie uzasadnienia wykazującego, że projektowane środki są niezbędne i proporcjonalne do takich celów, zgodnie z treścią wspomnianego art. 23 ust. 1 rozporządzenia 2016/679. Uzasadnienie projektu nie odnosi się do tej kwestii, potrzebne jest zatem jego uzupełnienie pod tym kątem.

Ponadto na podstawie art. 23 ust. 2 rozporządzenia 2016/679 akt prawny, który ma wprowadzać takie ograniczenia, musi zawierać szczegółowe przepisy przynajmniej – w stosownym przypadku – o:

1. celach przetwarzania lub kategorii przetwarzania;
2. kategoriach danych osobowych;
3. zakresie wprowadzonych ograniczeń;
4. zabezpieczeniach zapobiegających nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu;
5. określeniu administratora lub kategorii administratorów;
6. okresach przechowywania oraz mających zastosowanie zabezpieczeniach z uwzględnieniem charakteru, zakresu i celów przetwarzania lub kategorii przetwarzania;
7. ryzykach naruszenia praw lub wolności osoby, której dane dotyczą; oraz
8. prawie osób, których dane dotyczą, do uzyskania informacji o ograniczeniach, o ile nie narusza to celu ograniczenia.

Niezbędne jest więc wykazanie przez projektodawcę, że wymogi te zostaną spełnione oraz wskazanie, w jaki sposób. Uzasadnienie projektu ustawy nie zawiera wyjaśnień w tym zakresie.

**Projekt ustawy nie jest sprzeczny z prawem Unii Europejskiej, z zastrzeżeniem uwag zawartych w niniejszej opinii.**

*Z poważaniem*

Konrad Szymański

Minister do Spraw Unii Europejskiej

*/podpisano kwalifikowanym podpisem elektronicznym/*