

Czy prawo telekomunikacji elektronicznej osłabi cyberbezpieczeństwo?

29 marca 2023

W środę zbierze się sejmowa komisja cyfryzacji, która wznowi prace nad projektem prawa komunikacji elektronicznej. Posłowie i posłanki zadecydują, czy będziemy jeszcze bardziej inwigilowani (na czym skorzystają służby) i czy pozwolić Urzędowi Komunikacji Elektronicznej podpiąć się do sieci telekomunikacyjnych (na czym ucierpi bezpieczeństwo sieci). „A cóż to za dylemat?” – spytacie.

Projekt PKE wzbudza silne emocje nie tylko branży telekomunikacyjnej, która nie wie, czy szykować się na nowe obowiązki. Wprawdzie rząd wycofał rozszerzenie obowiązku retencji danych na nowe podmioty, ale dorzucił nowy, kontrowersyjny art. 311a. Zgodnie z nim firmy telekomunikacyjne będą zobowiązane instalować w swojej sieci urządzenia lub aplikacje przygotowane przez UKE. Mają one służyć „monitorowaniu ciągłości i jakości świadczenia usług dostępu do Internetu”. Firmy mają też obowiązek zapewnienia Prezesowi UKE dostępu do danych zebranych przez te urządzenia/aplikacje.

Takie sformułowanie jest nie dość precyzyjne. Nie wiadomo, jakie dane w związku z tym trafią do UKE. Czy będą to dane dotyczące indywidualnych użytkowników i użytkowniczek? To byłaby duża ingerencja w prawa jednostki.

Przedstawiciele branży telekomunikacyjnej (m.in. Polska Izba Informatyki i Telekomunikacji) zwracają też uwagę, że poprawka zagraża bezpieczeństwu sieci. Z bezpieczeństwem polskiej infrastruktury sieciowej jako takiej nie jest wprawdzie najlepiej (pamiętacie akcje spoofingowe na telefony

polityków?), ale nie ma powodu jeszcze bardziej go osłabiać. UKE wprowadzi do sieci coś, na co operatorzy nie będą mieli żadnego wpływu. W jaki sposób mają oni zagwarantować bezpieczeństwo systemu i zapobiegać np. wyciekom?

Komisja sejmowa zdecyduje o losie wszystkich poprawek: zarówno wycofujących rozszerzenie obowiązku retencji danych, jak i wprowadzających ciała obce do sieci telekomunikacyjnej.

Autorstwo: Anna Obem, Wojciech Klicki

Źródło: Panoptikon.org