KANCELARIA SENATU

BIURO LEGISLACYJNE

Warszawa, dnia 9 lipca 2018 r.

Opinia do ustawy o krajowym systemie cyberbezpieczeństwa

(druk nr 893)

I. Cel i przedmiot ustawy

Opiniowana ustawa ma na celu wdrożenie do polskiego porządku prawnego dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii. Dyrektywa ta formułuje obowiązki służące zapewnieniu cyberbezpieczeństwa systemów informacyjnych w sektorach usług mających kluczowe znaczenie dla utrzymania krytycznej działalności społeczno-gospodarczej, a więc w energetyce, transporcie, bankowości, instytucjach finansowych, sektorze ochrony zdrowia, zaopatrzenia w wodę i infrastrukturze cyfrowej.

Efektem regulacji, jak podkreślono w uzasadnieniu projektu ustawy (druk sejmowy nr 2505), ma być podniesienie odporności usług kluczowych świadczonych z wykorzystaniem technologii informatycznych na ataki pochodzące z cyberprzestrzeni. Tym samym ustawa ma przyczynić się do zapewnienia ciągłości działania tych usług, tak aby zarówno obywatele, jak i przedsiębiorstwa miały do nich stały i niezakłócony dostęp.

Opiniowana ustawa ma na celu określenie organizacji oraz sposobu funkcjonowania krajowego systemu cyberbezpieczeństwa, sposobu sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy oraz zakresu i trybu stanowienia Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej.

Ustawa w szczególności:

1) definiuje podstawowe pojęcia niezbędne dla krajowego systemu cyberbezpieczeństwa;
2) ustanawia krajowy system cyberbezpieczeństwa oraz określa podmioty do niego należące;

ul. Wiejska 6, 00-902 Warszawa, tel. . 22 694-93-38, fax 22 694-91-06, e-mail: Iwona.Kozera@senat.gov.pl

3) określa zasady wskazywania operatorów usług kluczowych, obowiązki dla operatorów usług kluczowych dotyczące wdrożenia systemu zarządzania bezpieczeństwem, obejmującego m.in. zarządzanie ryzykiem, procedury i mechanizmy zgłaszania i postępowania z incydentami czy organizację struktur na poziomie operatora;
4) wskazuje obowiązki nakładane na dostawców usług cyfrowych oraz na podmioty publiczne;
5) określa zadania CSIRT (Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego), odpowiedzialnych za przeciwdziałanie zagrożeniom cyberbezpieczeństwa o charakterze ponadsektorowym i transgranicznym, a także koordynację obsługi poważnych, istotnych i krytycznych incydentów;
6) przewiduje włączenie aspektów cyberbezpieczeństwa do sfery zarządzania państwem;
7) przewiduje utworzenie Zespołu do spraw Incydentów Krytycznych jako organu pomocniczego, powoływanego w sprawach obsługi i koordynacji incydentów krytycznych na poziomie krajowych CSIRT i Rządowego Centrum Bezpieczeństwa;
8) określa zasady dotyczące sposobu przekazywania do publicznej wiadomości komunikatów nt. cyberbezpieczeństwa oraz określa, zgodnie z wymaganiami rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 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), zasady przetwarzania danych osobowych w ramach funkcjonowania krajowego systemu cyberbezpieczeństwa, w tym zwłaszcza w zakresie przetwarzania danych dotyczących incydentów;
9) wskazuje organy właściwe ds. cyberbezpieczeństwa odpowiedzialne za sprawowanie nadzoru wobec operatorów usług kluczowych; organy te mają być elementem krajowego systemu cyberbezpieczeństwa odpowiedzialnym również za opracowywanie we współpracy z CSIRT wytycznych bezpieczeństwa teleinformatycznego w wymiarze sektorowym;
10) nakłada nowe obowiązki na ministra właściwego do spraw informatyzacji związane z prowadzeniem systemu teleinformatycznego wykorzystywanego do wymiany informacji między podmiotami tworzącymi krajowy system cyberbezpieczeństwa, do dynamicznego szacowania ryzyka na poziomie krajowym oraz do ostrzegania o zagrożeniach cyberbezpieczeństwa;

11) ustanawia Pojedynczy Punkt Kontaktowy, prowadzony przez ministra właściwego ds. informatyzacji, realizujący funkcje „łącznika" pomiędzy organami właściwymi ds. cyberbezpieczeństwa, organami władzy publicznej i CSIRT; Pojedynczy Punkt Kontaktowy ma zapewnić odbieranie i przekazywanie zgłoszeń incydentów poważnych i incydentów istotnych z innych państw członkowskich, reprezentację RP w Grupie Współpracy, współpracę z Komisją Europejską, współpracę między organami właściwymi ds. cyberbezpieczeństwa w RP i organami właściwymi państw członkowskich Unii Europejskiej, współpracę między organami władzy publicznej w RP z odpowiednimi organami w państwach członkowskich Unii Europejskiej;
12) określa zadania Ministra Obrony Narodowej związane z zakresem ustawy, zwłaszcza z zapewnieniem zdolności Siłom Zbrojnym RP do prowadzenia działań militarnych w przypadkach szczególnych zagrożeń, oceną wpływu incydentów na system obrony państwa oraz kierowaniem działaniami związanymi z obsługą incydentów w czasie stanu wojennego;
13) reguluje kwestie nadzoru i kontroli realizacji zadań określonych w ustawie;
14) określa zadania Pełnomocnika Rządu do spraw Cyberbezpieczeństwa (nowego podmiotu zajmującego się koordynacją działań dotyczących zapewnienia cyberbezpieczeństwa w RP) oraz Kolegium do spraw Cyberbezpieczeństwa (organu opiniodawczo-doradczego w sprawach cyberbezpieczeństwa), w celu zapewnienia koordynacji realizacji zadań na poziomie rządowym;
15) określa zasady realizacji i tworzenia Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej;

Opiniowana ustawa nowelizuje: ustawę z dnia 7 września 1991 r. o systemie oświaty, ustawę z dnia 4 września 1997 r. o działach administracji rządowej, ustawę z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, ustawę z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych, ustawę z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne oraz ustawę z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. Zmiany wprowadzane w tych ustawach obejmują konsekwencje wynikające z wprowadzenia nowej regulacji.

Ustawa wejdzie w życie po upływie 14 dni od dnia jej ogłoszenia.

II. Przebieg prac legislacyjnych

Projekt ustawy (druk sejmowy nr 2505) pochodził z przedłożenia rządowego i był przedmiotem prac sejmowych: Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii oraz Komisji Obrony Narodowej. Na etapie prac w komisjach wprowadzono do projektu poprawki o charakterze doprecyzowującym przepisy, uzupełniającym ustawę oraz techniczno-legislacyjne. W szczególności dodano przepisy zmieniające ustawę o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, ustawę – Prawo zamówień publicznych, a także uzupełniono przepisy przejściowe i dostosowujące (druk sejmowy nr 2659). Zmiany te nie wpłynęły jednak w sposób istotny na meritum rozwiązań zaproponowanych w projekcie.

Na etapie II czytania zgłoszono 12 poprawek, z których poparcie Izby uzyskały poprawki zmierzające do wskazania maksymalnego limitu wydatków z budżetu państwa dla części budżetowej 57 – Agencja Bezpieczeństwa Wewnętrznego, będącego skutkiem finansowym wejścia ustawy w życie, a także zwiększenia maksymalnego limitu wydatków z budżetu państwa dla części budżetowej 70 – Komisja Nadzoru Finansowego, będącego skutkiem finansowym ustawy.

Sejm uchwalił ustawę na 66. posiedzeniu w dniu 5 lipca 2018 r.

III. Uwagi szczegółowe

1) art. 8 pkt 1 – zgodnie z tym przepisem operator usługi kluczowej jest obowiązany do wdrożenia systemu zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej, zapewniającego prowadzenie **systematycznego** szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem. W związku z tym przepisem może powstać wątpliwość jak należy rozumieć pojęcie „systematycznego” szacowania ryzyka. Innymi słowy z jaką częstotliwością powinno odbywać się szacowanie ryzyka, aby można było uznać je, na gruncie ustawy, za systematyczne. Jest to o tyle istotne, że w myśl art. 73 ust. 1 operator usługi kluczowej, który nie przeprowadza systematycznego szacowania ryzyka, podlegać będzie karze pieniężnej w wysokości do 150 000 zł.

2) art. 12 ust. 1 pkt 5 i 6 – mając na względzie, że cały przepis art. 12 odnosi się do **zgłoszenia incydentu poważnego,** uwzględniając jednocześnie, że ustawodawca

wprowadził do ustawy definicję: „incydentu”, „incydentu krytycznego”, „incydentu poważnego”, „incydentu istotnego” i „incydentu w podmiocie publicznym”, należy zwrócić uwagę na niekonsekwencję w pkt 5 i pkt 6, które to przepisy stanowią o „incydencie”. Jeśli chodzi o pkt 5, wydaje się, że w istocie należałoby dokonać w nim korekty terminologicznej. Natomiast w odniesieniu do pkt 6 powstaje pytanie, czy jest to niekonsekwencja terminologiczna, czy ustawodawca chce poszerzyć obowiązki informacyjne operatorów usług kluczowych i zobowiązać ich do przekazywania informacji na temat każdego incydentu, który mógł mieć wpływ na świadczenie usługi kluczowej? Jeśli taka była wola ustawodawcy to pomiędzy art. 12 ust. 1 pkt 6, a art. 13 ust. 1 może zachodzić sprzeczność, ponieważ z art. 12 ust. 1 pkt 6 wynikać będzie obowiązek zgłaszania również innych incydentów aniżeli incydent poważny, natomiast z treści art. 13 ust. 1 wynika, że zgłaszanie informacji o innych incydentach jest dobrowolne.

Propozycja poprawki:

w art. 12 w ust. 1 w pkt 5 po wyrazie „incydent” dodaje się wyraz „poważny”;

3) art. 15 ust. 2 pkt 2 lit. c – biorąc pod uwagę zasady formułowania odesłań do innych przepisów, wynikające z § 156 Zasad techniki prawodawczej, uwzględniając rekomendacje dla legislatorów dotyczące wybranych zagadnień legislacyjnych (zaakceptowane przez kierownictwo Rządowego Centrum Legislacji, Biura Legislacyjnego Kancelarii Sejmu oraz Biura Legislacyjnego Kancelarii Senatu po szkoleniu „Ujednolicanie praktyki legislacyjnej rządowych i parlamentarnych służb legislacyjnych”), należy zwrócić uwagę, że w przepisach prawa należy unikać posługiwania się wyrażeniem „przepisy odrębne”, ponieważ jest to niewłaściwa metoda konstruowania odesłań. Nie informuje bowiem precyzyjnie adresata aktu, które normy ma w danej sytuacji zastosować.

Wydaje się, że w analizowanym przepisie nie ma potrzeby formułowania odesłania do konkretnych przepisów ustawowych, zaś sformułowanie „zgodnie z odrębnymi przepisami” powinno być z ustawy wyeliminowane jako niemające wartości normatywnej.

Podobną uwagę należy odnieść do art. 44 ust. 1 i art. 47 ust. 1

Propozycja poprawek:

w art. 15 w ust. 2 w pkt 2 w lit. c skreśla się wyrazy „, zgodnie z odrębnymi przepisami,”;

w art. 44 ust. 1 we wprowadzeniu do wyliczenia skreśla się wyrazy „, zgodnie z odrębnymi przepisami,”;

w art. 47 w ust. 1 skreśla się wyrazy „na zasadach określonych w przepisach odrębnych,”;

4) art. 26 ust. 11 – zasadą jest, że wskazanie ministra w przepisach ustawowych powinno być zgodne z nazwą działu administracji rządowej, którym kieruje, zgodnie z ustawą z dnia 4 września 1997 r. o działach administracji rządowej. Wyjątkiem w tym zakresie jest Minister Obrony Narodowej i Minister Sprawiedliwości, których wskazuje się ich nazwami własnymi. W związku z powyższym przepis art. 26 ust. 11 nie powinien stanowić o „Ministrze Cyfryzacji”, ale o „ministrze właściwym do spraw informatyzacji”. Takim (prawidłowym) określeniem posługuje się opiniowana ustawa w pozostałych przepisach.

   Propozycja poprawki:

w art. 26 w ust. 11 wyrazy „Ministra Cyfryzacji” zastępuje się wyrazami „ministra właściwego do spraw informatyzacji”;

5) art. 35 i art. 36 – przepisy dotyczą obsługi incydentów krytycznych a zatem powinny konsekwentnie posługiwać się określeniem „incydent krytyczny”, a nie „incydent”. Ustawodawca zdefiniował w ustawie 5 różnych incydentów, a skoro tak niewłaściwe jest posługiwanie się nimi zamiennie. Przepisy wymagają zatem korekty.

   Propozycja poprawek:

w art. 35 w ust. 2:

a) w pkt 1 we wprowadzeniu do wyliczenia oraz w lit. b po wyrazie „incydentu” dodaje się wyraz „krytycznego”,

b) w pkt 1 w lit. a i c po wyrazie „incydent” dodaje się wyraz „krytyczny”;

w art. 36 w ust. 7 w pkt 1, 2 oraz w pkt 5 po występującym po raz drugi wyrazie „incydentu” dodaje się wyraz „krytycznego”;

6) art. 49 ust. 1 pkt 1 – zgodnie z tym przepisem Pojedynczy Punkt Kontaktowy jest obowiązany przekazać Grupie Współpracy informacje, o których mowa w art. 45 ust. 1 pkt 3. Przepis art. 45 ust. 1 pkt 3 stanowi jednak nie o informacjach ale o „rocznych sprawozdaniach”. W związku z tym art. 49 ust. 1 pkt 1 wymaga doprecyzowania.

Propozycja poprawki:

w art. 49 w ust. 1 w pkt 1 wyraz „informacje” zastępuje się wyrazami „roczne sprawozdania”;

7) Zgodnie z art. 94 ustawa wejdzie w życie po upływie 14 dni od dnia jej ogłoszenia. Ze względu na zakres regulacji, w szczególności mając na uwadze, że ustawa nakłada obowiązki również na podmioty spoza sfery publicznej, można mieć wątpliwości, czy uchwalony przez Sejm okres vacatio legis jest wystarczający.

Wprawdzie w myśl art. 4 ust. 1 ustawy z dnia 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych minimalna, standardowa vacatio legis wynosi 14 dni, niemniej okres ten – jeżeli jest to uzasadnione przedmiotowo lub podmiotowo – powinien być dłuższy. Z art. 2 Konstytucji wynika bowiem nakaz zagwarantowania adresatom odpowiedniego okresu dostosowawczego. Odpowiednio długa vacatio legis jest warunkiem uznania ustawy za zgodną z konstytucyjną zasadą demokratycznego państwa prawnego.

Elementem państwa prawnego jest bowiem konieczność przeznaczenia **po uchwaleniu aktu normatywnego, a przed jego wejściem w życie, odpowiedniego czasu na zapoznanie się przez adresatów z jego treścią**. Zapewnienie stosownego okresu na dostosowanie się do treści przepisów służy pewności prawa i zaufaniu do państwa i tworzonego przez nie prawa. Stanowi też **jeden z warunków dopuszczalności ingerencji w prawa nabyte** (wyrok TK K 18/99). Zadaniem ustawodawcy jest zapewnienie adresatom czasu na przystosowanie się do zmienionej sytuacji i na bezpieczne podjęcie decyzji co do dalszego postępowania, szczególnie gdy nowe przepisy dotyczą działalności gospodarczej (orzeczenie TK K 2/94).

Twórca aktu normatywnego powinien wybrać taki moment wejścia w życie przepisów, by nie naruszyć jednej z podstawowych wartości państwa prawa, jaką jest

zaufanie obywateli do prawa, a więc by **nie zaskakiwać** adresatów norm wyrażonych w danym akcie nieoczekiwanym rozstrzygnięciem i stworzyć im **możliwość zapoznania** się z treścią stanowionych norm oraz – na podstawie tej wiedzy – **dostosowania swoich zachowań** do ich treści. Zgodnie z orzecznictwem TK *vacatio legis* musi mieć **długość odpowiednią do treści i charakteru aktu** (np. orzeczenie TK P 1/95). „Odpowiedniość" *vacatio legis* rozpatrywać trzeba w związku z koniecznością odpowiedniej reakcji na określone nowe przepisy. Wymóg *vacatio legis* należy odnosić do możliwości zapoznania się z nowym prawem i możliwością adekwatnego działania. Co więcej, odpowiednią *vacatio legis* należy odnosić nie do ochrony adresata normy prawnej przed pogorszeniem jego sytuacji, lecz do jego możliwości zapoznania się z nowym prawem i możliwości adaptacyjnych, a te bywają zróżnicowane.

Okres dostosowawczy powinien być dostosowany do możliwości poznawczych po stronie adresatów oraz do zakresu ingerencji w porządek prawny.

Iwona Kozera-Rytel
Główny legislator