IURIDICO

Wojciech Wołoszyk

Prawnik-lingwista w Trybunale Sprawiedliwości UE i Międzynarodowym Trybunale Karnym w Hadze, biegły sądowy z zakresu lingwistyki prawniczej, autor publikacji i szkoleniowiec z zakresu tłumaczeń prawniczych. Współzałożyciel i prezes IURIDICO Legal & Financial Translations sp. z o.o. świadczącej usługi tłumaczeń dla organów UE oraz polskiego wymiaru sprawiedliwości i administracji rządowej. Członek zarządu Związku Pracodawców Branży Tłumaczeniowej POLOT odpowiedzialny za kontakty z administracją rządową i rynek zamówień publicznych. Członek ekspert Polskiego Towarzystwa Tłumaczy Przysięgłych i Specjalistycznych.

Tłumaczenia maszynowe a cyberbezpieczeństwo w kontekście podstawy odrzucenia oferty z art. 89 ust. 1 pkt 7d ustawy Pzp

Co ma wspólnego Australijski Instytut Polityki Strategicznej (ang. Australian Strategic Policy Institute, ASPI) i Centralny Departament Propagandy ChRL z przesłankami odrzucenia oferty uregulowanymi w polskim prawie zamówień publicznych? Okazuje się, że całkiem sporo. Podobnie jak rosyjski państwowy fundusz venture capital oraz firmy tworzące tzw. amerykańską wielką piątkę technologiczną (GAFAM – Google, Amazon, Facebook, Apple i Microsoft).

Niestety wiedza na ten temat w polskim sektorze publicznym w zasadzie nie istnieje. A szkoda. Pociąga to bowiem za sobą poważne, a co gorsza nieuświadomione, ryzyko dla bezpieczeństwa informacji niejawnych istotnych dla polskiego interesu państwowego.

Celem niniejszego artykułu jest naświetlenie uwarunkowań związanych z korzystaniem z narzędzi do tłumaczeń maszynowych w procesie obsługi tłumaczeniowej polskich instytucji rządowych najwyższego szczebla oraz konieczność ich uwzględniania na etapie postępowania o udzielenie zamówienia publicznego w kontekście przesłanki odrzucenia oferty przewidzianej w art. 89 ust. 1 pkt 7d ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz.U.2019.1843 t.j. z dnia 27.09.2019 r.).

Raport Australijskiego Instytutu Polityki Strategicznej (ASPI) z 2019 r.[1] wskazuje na wykorzystywanie w Chinach przedsiębiorstw państwowych, które świadczą usługi tłumaczenia maszynowego, do gromadzenia danych dotyczących użytkowników spoza Chin. Autorka raportu, Samantha Hoffman, twierdzi, że najcenniejszymi narzędziami w chińskiej kampanii zbierania danych są technologie, z którymi użytkownicy wchodzą w interakcję w pełni dobrowolnie i dla własnej korzyści, czego najlepszym przykładem są usługi tłumaczenia maszynowego. Odbywa się to za pośrednictwem firmy GTCOM[2], którą Hoffman określa jako „wielojęzyczne big data", oferującej oprogramowanie i sprzęt do tłumaczeń maszynowych, przy wykorzystaniu których zbierane są później obszerne dane. Szacuje ona, że GTCOM, która współpracuje zarówno z klientami korporacyjnymi, jak i rządowymi, obsługuje równowartość do pięciu bilionów słów zwykłego tekstu dziennie, w 65 językach i w ponad 200 krajach. GTCOM jest spółką zależną chińskiego przedsiębiorstwa państwowego, nad którym bezpośredni nadzór sprawuje Centralny Departament Propagandy, w związku z czym zakłada się, że gromadzenie danych jest procesem aktywnym i ciągłym służącym w dużej mierze realizacji celów pozakomeryjnych. W raporcie wprost wskazuje się, że system do tłumaczeń maszynowych oferowany przez GTCOM służy m.in zbieraniu danych dla chińskiego wywiadu wojskowego.

Ewentualne zastosowanie takiego oprogramowania przy obsłudze tłumaczeniowej polskiego Ministerstwa Spraw Zagranicznych, Kancelarii Prezesa Rady Ministrów bądź innych organów centralnej administracji rządowej w sposób oczywisty powinno być traktowane jako potencjalne zagrożenie dla bezpieczeństwa informacji niejawnych istotnych z punktu widzenia interesu państwa polskiego. Tymczasem kwestia ta jest całkowicie ignorowana i nie podlega jakiejkolwiek kontroli.

Powyższy przykład jest jaskrawy i przemawiający do wyobraźni. Jednak również stosowanie innych powszechnie dostępnych narzędzi do tłumaczeń maszynowych w centralnej administracji rządowej powinno podlegać daleko idącej reglamentacji i kontroli. Pod tym kątem powinny być również badane oferty w postępowaniach o udzielenie zamówienia publicznego, których przedmiot obejmuje usługi tłumaczeń pisemnych.

Podkreślić należy, że ewentualne całkowite wykluczenie możliwości stosowania narzędzi do tłumaczeń maszynowych jest anachronizmem i nie wytrzymuje konfrontacji z branżową rzeczywistością, jak również trendami technologicznymi wspieranymi przez Unię Europejską. Komisja Europejska prowadzi w tej chwili, we współpracy z sektorem prywatnym, intensywne prace badawczo-rozwojowe, które mają prowadzić

[1] Raport nr 21/2019: Dr Samantha Hoffman, The Chinese Communist Party's data-driven power expansion, https://www.aspi.org.au/report/engineering-global-consent-chinese-communist-partys-data-driven-power-expansion.

[2] Global Tone Communication Technology Co. Ltd.

do upowszechnienia stosowania nowoczesnych technologii językowych na poziomie administracji krajowych. Dążenie do kompletnej eliminacji tłumaczeń maszynowych z procesu świadczenia usług językowych dla administracji publicznej jest całkowitą fikcją. Można by to porównać do ewentualnego zakazu stosowania systemów informacji prawnej przy świadczeniu obsługi prawnej na rzecz jednostek administracji publicznej.

Kluczowe jest natomiast zrozumienie różnic pomiędzy poszczególnymi narzędziami tłumaczeń maszynowych, wykluczenie stosowania określonych ich rodzajów – ze szczególnym uwzględnieniem rozwiązań nieodpłatnych oraz całkowite wyeliminowanie narzędzi „otwartych" w przypadku organów objętych krajowym systemem cyberbezpieczeństwa.

Podstawą do badania ofert pod kątem wykorzystywanych narzędzi do tłumaczeń maszynowych jest art. 89 ust. 1 pkt 7d) ustawy Pzp. Treść tego przepisu została zmodyfikowana w dniu 28 sierpnia 2018 r. z momentem wejścia w życie art. 80 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 r. poz. 1560). Zgodnie z aktualnym brzmieniem art. 89 ust. 1 pkt 7d ustawy Pzp zamawiający odrzuca ofertę, jeżeli jej przyjęcie naruszałoby bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa, w tym bezpieczeństwo podmiotów objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o której mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2018 r. poz. 1401), a tego bezpieczeństwa lub interesu nie można zagwarantować w inny sposób.

Po zmianie art. 89 ust. 1 pkt 7d Pzp oferta złożona w postępowaniu o udzielenie zamówienia publicznego podlegać będzie odrzuceniu m.in. w przypadku, gdy realizacja rozwiązań w niej przyjętych powodowałaby naruszenie bezpieczeństwa podmiotów wskazanych w jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, sporządzonym przez Dyrektora Rządowego Centrum Bezpieczeństwa.

Analizując zasadność odrzucenia oferty wykonawcy w oparciu o znowelizowaną w 2018 r. podstawę prawną – zamawiający będzie zobowiązany wykazać, że: (1) realizacja rozwiązań przyjętych w ofercie powodowałaby naruszenie bezpieczeństwa obiektów infrastruktury krytycznej objętej wykazem, (2) naruszenie to ma związek z naruszeniem bezpieczeństwa publicznego lub istotnego interesu bezpieczeństwa państwa, (3) bezpieczeństwa publicznego lub istotnego interesu bezpieczeństwa państwa nie można zagwarantować w inny sposób, niż przez odrzucenie oferty zawierającej rozwiązania prowadzące do naruszenia bezpieczeństwa podmiotów.

Charakterystyczne dla tej podstawy odrzucenia jest brak zawarcia w powołanym przepisie stosownych definicji bezpieczeństwa publicznego oraz istotnego interesu bezpieczeństwa państwa.

Należy również zwrócić uwagę na konieczność wykazania bezpośredniego skutku wybrania danej oferty w postaci naruszenia bezpieczeństwa publicznego lub istotnego interesu bezpieczeństwa państwa oraz braku możliwości uniknięcia powyższego naruszenia w inny sposób niż poprzez odrzucenie tej oferty. Niewystarczającym jest więc wyłącznie przywołanie hasła bezpieczeństwa publicznego lub pominięcie innych możliwości uniknięcia naruszenia niż odrzucenie oferty.

Aby nieco przybliżyć potencjalne zagrożenia bezpieczeństwa publicznego i interesu bezpieczeństwa państwa wynikające z korzystania z niewłaściwych narzędzi do tłumaczeń maszynowych należy dokonać analizy warunków świadczenia tych usług. Wymaga równocześnie podkreślenia, że umiejętnie i fachowo realizowany proces tłumaczeniowy uwzględniający tłumaczenie maszynowe w wielu przypadkach jest rozwiązaniem prawidłowym oraz zapewniającym odpowiednią jakość usługi i poufność danych.

Potencjalne zagrożenia dotyczą głównie bezpieczeństwa danych osobowych i informacji poufnych w związku ze stosowaniem chmurowych systemów do tłumaczeń maszynowych – zarówno płatnych, jak i bezpłatnych. Ryzyka te nie występują w przypadku stosowania rozwiązań opartych na własnych silnikach MT rozwijanych przez dostawców usług tłumaczeniowych.

Do najpopularniejszych i w zasadzie powszechnie dostępnych systemów chmurowych do tłumaczeń maszynowych należą obecnie: DeepL (wersja darmowa i PRO), SmartCat, Tłumacz Google (w wersji darmowej i płatnej) oraz Microsoft Translator. W dalszej części niniejszego opracowania autor przedstawił wyciąg z warunków świadczenia poszczególnych usług, które wskazują na ryzyka dla danych poufnych i wrażliwych, na które wprost godzi się każdy użytkownik takiej usługi.

Mogłoby się wydawać, że darmowe systemy tłumaczenia maszynowego, które nie mogą być wykorzystywane w celu świadczenia usług komercyjnych, nie są stosowane w profesjonalnym świadczeniu usług tłumaczeniowych. Niestety takie założenie okazałoby się nieprawdziwe. Autor niniejszego opracowania, jako biegły sądowy w zakresie juryslingwistyki oraz redaktor tłumaczeń prawniczych, wielokrotnie miał do czynienia z opłakanymi rezultatami nieodpowiedzialnego korzystania z takich systemów. Takie sytuacje zdarzają się również wśród pracowników administracji publicznej, którzy dla zaoszczędzenia czasu podpierają się narzędziami chmurowymi.

Analiza warunków umownych i regulaminów niektórych systemów tłumaczenia maszynowego:

DeepL Pro:

Polityka prywatności[3]: 5. „Prosimy pamiętać, że niewskazane jest korzystanie z naszych usług tłumaczeniowych w przypadku tekstów zawierających dane osobowe jakiegokolwiek rodzaju.[4]"

Warunki świadczenia usługi DeepL Pro[5]:

„6.4 Wszelkie prawa do Treści Klienta pozostają własnością Klienta. Klient udziela jednak DeepL niewyłącznego prawa do korzystania z Treści wyłącznie w celu świadczenia usług DeepL na rzecz Klienta. W szczególności

[3] https://www.deepl.com/privacy.html dostęp 25.03.2020 r.

[4] Co ciekawe w wersji angielskiej polityki prywatności DeepL pojawia się sformułowanie „Please note that you may not use our translation service for any texts containing personal data of any kind.", które wprowadza jednoznaczny zakaz korzystania z narzędzia przy tłumaczeniu dokumentów zawierających jakiekolwiek dane osobowe.

[5] https://www.deepl.com/pro-license.html#pro dostęp 25.03.2020 r.

Klient udziela DeepL prawa do tymczasowego przechowywania, modyfikowania, przetwarzania, tłumaczenia i przekazywania Treści oraz do udzielania podlicencji na powyższe prawa swoim podwykonawcom w zakresie wymaganym do świadczenia usług określonych w niniejszej Umowie.

7.3 Klient ma prawo korzystać z API i tłumacza internetowego wyłącznie w celu uzgodnionym pomiędzy stronami. W szczególności, Klient nie może zezwolić osobom trzecim na korzystanie z API i tłumacza internetowego, tłumaczeń utworzonych przy użyciu API i tłumacza internetowego, Dokumentacji lub innych danych, informacji lub usług dostarczanych przez DeepL, chyba że zostanie to wyraźnie zatwierdzone przez DeepL w formie pisemnej:

a. w związku z eksploatacją lub do celów eksploatacji infrastruktury krytycznej, takiej jak elektrownie, sprzęt wojskowy lub obronny, urządzenia medyczne lub inny sprzęt, którego awaria lub uszkodzenie powodowałoby nieprzewidywalne szkody gospodarcze lub fizyczne, w tym między innymi infrastruktury krytycznej w rozumieniu dyrektywy europejskiej 2008/114/WE;

(...)

g. do przekazywania DeepL danych, które nie mogą być przekazywane lub przetwarzane przez DeepL ze względu na przepisy o ochronie danych, zobowiązania umowne lub ustawowe, dotyczące poufności, ograniczenia eksportowe lub inne przepisy ustawowe lub prawa osób trzecich."

Powyższe postanowienia i warunki świadczenia usług wykluczają możliwość zastosowania tego narzędzia do tłumaczenia dokumentów zawierających dane poufne, dane osobowe oraz dokumentów dotyczących infrastruktury krytycznej, do której literalnie odwołuje się art. 89 ust. 1 pkt 7d) ustawy Pzp.

SmartCat:

Smartcat Terms of Use[6]

„VI. USER CONTENT

B. Any User that uploads its content on the Platform, grants Smartcat, its affiliates, subsidiaries and suppliers, a non-exclusive, royalty-free, transferable right to use, display, reproduce, distribute, and publish such content in connection with the features available on the Platform. Customer hereby also grants Smartcat the right to refer to Customer as a Customer in promotional materials by Customer name and using Customer logo in its unaltered form.

VII. DATA PROTECTION

D. You hereby provide written authorization to Smartcat to transfer your personal data collected by Smartcat from you pursuant to providing the Services or Supplementary Services to third party service and analytics providers for the purpose of providing, analysing and modifying the Services, Supplementary Services and the Platform, including cross-border transfers outside European Economic Area.

SmartCat Customer Agreement[7]

4. CONFIDENTIALITY AND NON-DISCLOSURE

4.1 **Restrictions**. Smartcat acknowledges that, in order to perform the Services or to provide Supplementary Services, it shall be necessary for Customer to disclose to Smartcat certain Confidential Information (defined below) of Customer. Smartcat agrees that it shall not disclose, transfer, use, copy, or allow access to any such Confidential Information to any third parties, except as authorized by Customer. Customer hereby authorizes Smartcat to provide Confidential Information to Suppliers, translation service providers, marketing services providers and infrastructure and development service providers, including those located in jurisdictions without adequate protection of personal data, on the terms established by Smartcat provided that Smartcat shall implement technical and organizational security measures in respect of processing of such data."

Powyższe warunki wykluczają w praktyce możliwość stosowania narzędzi SmartCat do tłumaczenia dokumentów zawierających dane poufne, dane osobowe oraz dokumentów dotyczących infrastruktury krytycznej, do której literalnie odwołuje się art. 89 ust. 1 pkt 7d) ustawy Pzp. Z uwagi na udzielaną nieodpłatną licencję na korzystanie z tłumaczonych treści przez właściciela platformy wyłączona jest również możliwość tłumaczenia tekstów objętych prawami autorskimi osób trzecich.

Tłumacz Google[8]:

„Przesyłając, wgrywając, dostarczając, zapisując, przechowując, wysyłając lub odbierając materiały do lub za pośrednictwem Usług, użytkownik udziela firmie Google (i jej współpracownikom) ważnej na całym świecie licencji na wykorzystywanie, udostępnianie, przechowywanie, reprodukowanie, modyfikowanie, przesyłanie, publikowanie, publiczne prezentowanie i wyświetlanie oraz rozpowszechnianie tych materiałów, a także na tworzenie na ich podstawie opracowań (dzieł pochodnych, na przykład przez wykonanie tłumaczenia, adaptacji lub innych zmian w celu zapewnienia lepszego działania z Usługami)."

Warunki świadczenia usług Google wykluczają możliwość zastosowania tego popularnego narzędzia do tłumaczeń maszynowych do tłumaczenia dokumentów zawierających dane osobowe, dane wrażliwe, informacje poufne bądź treści objęte prawami autorskimi osób trzecich.

Tłumacz Microsoft[9]:

„Jeśli Użytkownik udostępnia Treści Użytkownika innym osobom, wyraźnie zgadza się na to, aby każda osoba, której je udostępnił, mogła je na całym świecie bezpłatnie stosować, zapisywać, nagrywać, reprodukować, transmitować, przesyłać, udostępniać, wyświetlać lub w inny sposób rozpowszechniać (a w przypadku usługi HealthVault — usuwać). Jeśli Użytkownik nie chce, aby ktokolwiek miał taką możliwość, nie powinien używać Usług do udostępniania Treści Użytkownika."

(...)

[6] https://www.smartcat.ai/terms/ Warunki korzystania z usługi SmartCat z 01.08.2019 r., dostęp 27.03.2020 r.

[7] https://www.smartcat.ai/customer-agreement/ Umowa z Klientem SmartCat z 01.08.2019 r., dostęp 27.03.2020 r.

[8] https://policies.google.com/terms Warunki korzystania z usług Google z 22.01.2019 r., dostęp 25.03.2020 r.

[9] https://www.microsoft.com/pl-pl/servicesagreement/ Umowa dotycząca usług Microsoft obowiązująca od 30.08.2019 r., dostęp 27.03.2020 r.

„W zakresie koniecznym do świadczenia Usług Użytkownikowi i innym osobom (mogącym obejmować zmianę rozmiaru, kształtu lub formatu Treści Użytkownika w celu ich lepszego przechowywania lub wyświetlenia Użytkownikowi), zabezpieczenia Użytkownika i Usług oraz ulepszania produktów i usług Microsoft, Użytkownik udziela Microsoft obowiązującej na całym świecie i wolnej od opłat licencji w zakresie własności intelektualnej na używanie Treści Użytkownika, w tym na sporządzanie kopii, zachowywanie, przekazywanie, ponowne formatowanie, rozpowszechnianie za pośrednictwem narzędzi komunikacji oraz wyświetlanie Treści Użytkownika w Usługach. Jeśli Użytkownik opublikuje Treści Użytkownika w takich obszarach Usługi, które umożliwiają publiczny lub nieograniczony dostęp do Treści Użytkownika za pomocą Internetu, Treści Użytkownika mogą zostać wykorzystane w prezentacjach lub materiałach promujących Usługę."

Postanowienia umowy dotyczącej usług Microsoft wykluczają możliwość zastosowania tego narzędzia do tłumaczenia dokumentów zawierających dane osobowe, dane wrażliwe, informacje poufne bądź treści objęte prawami autorskimi osób trzecich.

Powyższe postanowienia i warunki można podsumować w ten sposób, że ich dostawcy albo wprost wyłączają możliwość stosowania swoich produktów do wykonywania tłumaczeń dokumentów obejmujących informacje poufne, dane osobowe lub treści objęte prawem autorskim osób trzecich (DeepL Pro), względnie zastrzegają sobie prawo przekazywania takich treści i danych bliżej nieokreślonemu kręgowi podmiotów trzecich poza granicami Unii Europejskiej (SmartCat), albo w końcu wprowadzają po swojej stronie bardzo szerokie uprawnienia do ich dalszego wykorzystywania i udostępniania (Google, Microsoft). Warto mieć również na uwadze kwestię pochodzenia poszczególnych narzędzi i struktury własnościowej podmiotów za nimi stojących. Warto wskazać, że platforma SmartCat została opracowana przez firmę rosyjską przy współfinansowaniu ze strony rosyjskiego państwowego funduszu venture capital[10].

[10] https://www.nimdzi.com/tms/smartcat/, dostęp 27.03.2020 r.

Już same warunki świadczenia usług wskazują, że niektóre spośród chmurowych narzędzi do tłumaczenia maszynowego posiadają właściwości, które mogą prowadzić do zagrożenia bezpieczeństwa sieci i systemów teleinformatycznych i powodować incydenty z tym związane. Z perspektywy organu administracji publicznej, który zleca usługi tłumaczeniowe identyfikacja zagrożenia na etapie badania ofert, może okazać się trudna lub wręcz niemożliwa.

Kwestie, które na poziomie urzędu gminy mogą nie mieć jakiegokolwiek praktycznego znaczenia, na poziomie Ministerstwa Spraw Zagranicznych, Kancelarii Premiera Rady Ministrów, czy też Kancelarii Sejmu i Kancelarii Prezydenta zaczynają mieć znaczenie dla bezpieczeństwa narodowego.

Eliminacji takich zagrożeń w przypadku powierzania wrażliwych informacji podmiotom zewnętrznym służyć ma między innymi uprawnienie zamawiającego do odrzucenia oferty w oparciu o art. 89 ust. 1 pkt 7d ustawy Pzp. Niestety problem opisany w niniejszym artykule pozostaje całkowicie nieuświadomiony po stronie centralnej administracji rządowej. Obsługa tłumaczeniowa realizowana jest w wielu przypadkach przy wykorzystaniu narzędzi, które do tego celu wykorzystywane być nie powinny.

Sprawę mogłoby znacząco uprościć przeprowadzenie badania wzmiankowanych narzędzi w trybie art. 33 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa w celu identyfikacji podatności, której wykorzystanie może zagrozić integralności, poufności, rozliczalności, autentyczności lub dostępności przetwarzanych danych, które może mieć wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa. Badanie takie powinno zostać przeprowadzone przez Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego.

Już same warunki świadczenia usług wskazują, że niektóre spośród chmurowych narzędzi do tłumaczenia maszynowego posiadają właściwości, które mogą prowadzić do zagrożenia bezpieczeństwa sieci i systemów teleinformatycznych i powodować incydenty z tym związane. Z perspektywy organu administracji publicznej, który zleca usługi tłumaczeniowe identyfikacja zagrożenia na etapie badania ofert, może okazać się trudna lub wręcz niemożliwa. Powołane w ustawie o krajowym systemie cyberbezpieczeństwa organy powinny zbadać dostępne na rynku systemy tłumaczeń maszynowych oparte na chmurze obliczeniowej i wydać stosowną rekomendację, uwzględniającą wytyczne, jakim powinny odpowiadać narzędzia do tłumaczenia maszynowego ewentualnie wykorzystywane do tłumaczenia dokumentów przekazywanych przez podmioty objęte krajowym systemem cyberbezpieczeństwa.

W efekcie wydania takiej rekomendacji stałoby się możliwe skuteczne stosowanie art. 89 ust. 1 pkt 7d ustawy Pzp w postępowaniach o udzielenie zamówienia publicznego na usługi tłumaczeń pisemnych dla centralnej administracji rządowej oraz innych podmiotów objętych krajowym systemem cyberbezpieczeństwa[11]. ■

[11] Na marginesie autor wskazuje, że pojęcie „cyberbezpieczeństwa" wprowadzone do tytułu ustawy o krajowym systemie cyberbezpieczeństwa należy uznać za nieprawidłowe. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, która implementowana jest do polskiego porządku prawnego za pośrednictwem ustawy o krajowym systemie cyberbezpieczeństwa, posługuje się zdefiniowanym sformułowaniem „bezpieczeństwo sieci i systemów informatycznych".