CYBERPOLICY

Review

Biuletyn NASK

Strategia. Policy. Rekomendacje.

NASK

Biuletyn NASK

Strategia. Policy. Rekomendacje.

Nr 3/ styczeń 2019

Redakcja: Magdalena Wrzosek

Słowo wstępu

Rok 2018 zakończył się porozumieniem w sprawie Cybersecurity Act. Tym samym rozstrzygnięta została bardzo ważna kwestia – certyfikacja produktów i usług ICT na Jednolitym Rynku Cyfrowym. Jej wprowadzenie to duże wyzwanie nie tylko dla struktur UE, ale także dla państw członkowskich.

Dodatkowo, KE zaproponowała nową propozycję legislacyjną: Rozporządzenie w sprawie Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych oraz sieci krajowych ośrodków koordynacji.

Trwa także dyskusja nad etycznymi aspektami rozwoju sztucznej inteligencji.

Najnowszy numer CyberPolicy Review adresuje wszystkie te tematy. Zapraszam do lektury.

Krzysztof Silicki, p.o. Dyrektor Państwowego Instytutu Badawczego NASK

Spis treści

Rafał Babraj

Ramy europejskiej certyfikacji: Rozporządzenie w sprawie certyfikacji cyberbezpieczeństwa

Rafał Babraj – *specjalista ds. komunikacji i nowoczesnych technologii w zespole Analiz Strategicznych i Wpływu Nowoczesnych Technologii w NASK PIB. Specjalizuje się w analizach dotyczących dezinformacji i fałszywych informacji, przede wszystkim w kontekście polityki UE i NATO. Jego zainteresowania badawcze koncentrują się nad wpływem rozwoju nowoczesnych technologii na bezpieczeństwo informacji. Twórca projektu bezpiecznewybory.pl.*

Doświadczenie zdobywał, pracując jako dziennikarz i redaktor stron internetowych, a także w biurach prasowych w administracji publicznej. Redaktor naczelny strony internetowej Mazowieckiego Urzędu Wojewódzkiego. Lider zespołu wprowadzającego standardy prostego języka w Ministerstwie Zdrowia, zaangażowany w prace nad rządowym portalem GOV.PL oraz odpowiedzialny za uruchomienie na nim strony resortu zdrowia. Absolwent Instytutu Edukacji Medialnej i Dziennikarstwa na Uniwersytecie Kardynała Stefana Wyszyńskiego w Warszawie.

Rozporządzenie jest integralną częścią *Cybersecurity Act*, w którego skład wchodzi także nowy mandat dla Europejskiej Agencji Bezpieczeństwa Sieci i Informacji (ENISA). Propozycja Cybersecurity Act została przedstawiona we wrześniu 2017 roku, jako kolejny, po Dyrektywnie NIS, etap budowy cyberbezpieczeństwa Jednolitego Rynku Cyfrowego. Jest to niezwykle istotne zadanie stojące przed Unią Europejską, jako że według szacunków połączenie 28 rynków krajowych, mogłoby przynieść unijnej gospodarce nawet 415 mld euro rocznie[1].

Rozporządzenie w sprawie certyfikacji cyberbezpieczeństwa to pierwsze prawo dotyczące rynku wewnętrznego, które odpowiada na potrzebę podniesienia poziomu bezpieczeństwa produktów, usług i procesów ICT. Tak więc **stworzenie europejskich ram certyfikacji cyberbezpieczeństwa to przełomowy krok**, który w efekcie umożliwi zniesienie barier, utrzymujących się na rynku cyfrowym. Aby to osiągnąć, konieczne jest wypracowanie harmonijnego podejścia do certyfikacji cyberbezpieczeństwa. Dlatego rozporządzenie określa mechanizm ustanawiania europejskich schematów certyfikacji cyberbezpieczeństwa oraz potwierdzania, że dane produkty bądź usługi spełniają określone wymogi bezpieczeństwa.

Celem regulacji jest doprowadzenie do sytuacji, w której konsument będzie mógł wybierać takie urządzenia i rozwiązania, które są przetestowane i spełniają odpowiednie normy bezpieczeństwa. Z kolei firmy będą mogły oszczędzić czas i pieniądze, ponieważ nie będą musiały ubiegać się o certyfikat w każdym kraju, w którym chciałyby oferować swoje usługi bądź produkty. Co więcej, firmy które zainwestują w cyberbezpieczeństwo, będą mogły wykorzystać ten fakt jako swoją przewagę nad konkurencją.

Wejście w życie tych przepisów może jednak oznaczać również pewne wyzwania dla państw, które nie podejmowały dotąd żadnych kroków w kierunku stworzenia krajowego systemu certyfikacji cyberbezpieczeństwa. W lepszej sytuacji znajdą się te państwa członkowskie, które nie będą musiały budować od podstaw odpowiednich kompetencji oraz infrastruktury potrzebnych np. do testowania certyfikowanego sprzętu.

Inicjowanie procesu certyfikacji UE

Proces certyfikacji mogą zainicjować zarówno Komisja Europejska jak i Europejska Grupa Certyfikacji Cyberbezpieczeństwa (ECCG, European Cybersecurity Certification Group). Różnica polega na tym, że **ENISA musi przygotować propozycję europejskiego schematu certyfikacji na wniosek KE**. Natomiast jeśli o przygotowanie propozycji schematu zawnioskuje EGCC, wówczas ENISA może taki wniosek odrzucić.

Ikona zaprojektowana przez Freepik.com

[1] *Priorytet: Jednolity rynek cyfrowy, Internet bez barier (dostęp na dzień 6.02.2019 https://ec.europa.eu/commission/priorities/digital-single-market_pl)*

Agencja musi jednak podać uzasadnienie, a każda decyzja odmowna jest podejmowana przez zarząd.

Co do zasady, wniosek powinien dotyczyć schematu, który odnosi się do produktów, usług i procesów ICT **ujętych w unijnym programie prac**. W uzasadnionych przypadkach możliwe jest jednak wnioskowanie o przygotowanie schematu nieuwzględnionego w wykazie. Wówczas program zostanie odpowiednio zaktualizowany.

Europejska Grupa Certyfikacji Cyberbezpieczeństwa

Europejska Grupa Certyfikacji Cyberbezpieczeństwa to jeden z najważniejszych organów, który powołuje do życia *Cybersecurity Act*. Grupa składa się z przedstawicieli krajowych organów certyfikacji cyberbezpieczeństwa lub innych właściwych organów krajowych. Każdy członek grupy może reprezentować nie więcej niż jedno państwo członkowskie.

Grupie przewodniczy Komisja Europejska, która zapewnia jej sekretariat, z pomocą ENISA. W pracach oraz posiedzeniach grupy mogą uczestniczyć również inne zainteresowane strony.

Zadania EGCC:

- doradzanie i pomoc KE, w celu zapewwwnienia **spójnego wdrożenia i stosowania przepisów** dotyczących m.in. unijnego programu prac, polityki certyfikacji cyberbezpieczeństwa czy europejskich schematów certyfikacji cyberbezpieczeństwa;
- doradzanie i współpraca z ENISA przy przygotowaniu propozycji schematu certyfikacji, w tym **opiniowanie propozycji schematu**;
- **występowanie do ENISA o przygotowanie propozycji** europejskiego schematu certyfikacji cyberbezpieczeństwa;
- kierowanie do KE opinii dotyczących **utrzymania i przeglądu istniejących europejskich schematów** certyfikacji cyberbezpieczeństwa;
- **badanie istotnych zmian w certyfikacji** cyberbezpieczeństwa oraz wymiana informacji i dobrych praktyk w tej dziedzinie;
- **ułatwianie współpracy między krajowymi organami certyfikacji** cyberbezpieczeństwa, a zwłaszcza wymiany informacji dotyczących certyfikacji;
  - **wsparcie we wdrażaniu mechanizmów wzajemnej oceny** zgodnie z zasadami ustanowionymi w europejskim schemacie certyfikacji cyberbezpieczeństwa;
  - ułatwianie **dostosowania europejskich schematów certyfikacji** cyberbezpieczeństwa do uznanych międzynarodowych standardów.

Ustanowienie schematu certyfikacji cyberbezpieczeństwa

1.Przygotowanie propozycji schematu

Za przygotowanie propozycji schematu certyfikacji (tzw. schemat kandydat) odpowiada ENISA. Podczas prac Agencja ma obowiązek konsultacji „schematu kandydata" ze wszystkimi zainteresowanymi interesariuszami oraz ustanowienia grupy roboczej, składającej się z ekspertów z państw członkowskich, która opracuje schemat. Wypracowana propozycja przekazywana jest do KE.

Dodatkowo pomoc i porady ekspertów zapewnia EGCC. Grupa wydaje również opinię odnośnie do przygotowanej propozycji schematu. Opinia ta nie jest wiążąca, a jej brak nie blokuje możliwości przekazania propozycji schematu do Komisji Europejskiej. ENISA powinna jednak w jak największym stopniu uwzględnić opinię EGCC. Daje to sektorowi publicznemu możliwość wpływu na przygotowywanie europejskich schematów certyfikacji.

2.Przyjęcie propozycji schematu

Komisja Europejska, w oparciu o otrzymaną propozycję, **może przyjąć akty wykonawcze**, które ustanowią europejskie schematy certyfikacji cyberbezpieczeństwa dla procesów, produktów i usług ICT.

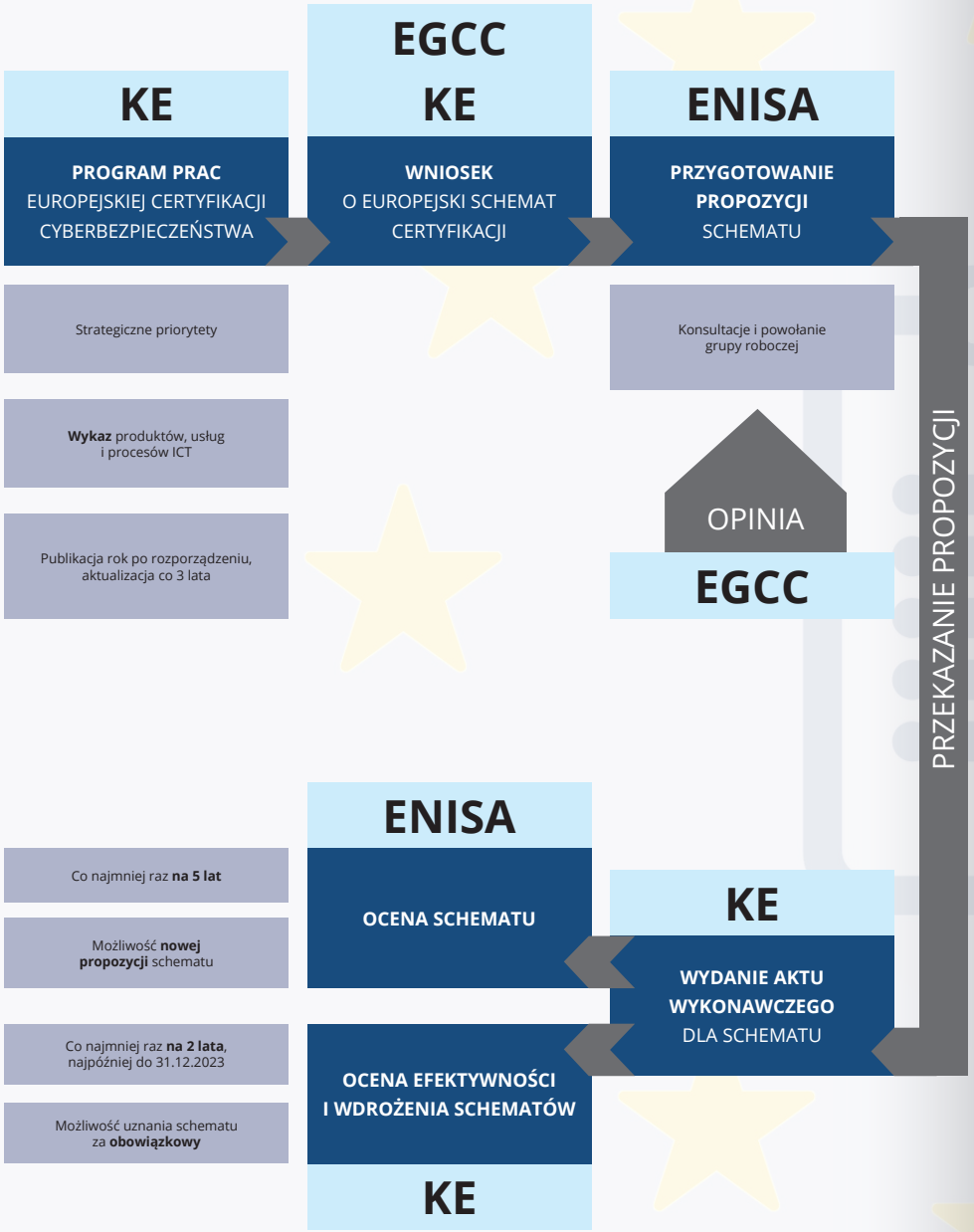
3.Przegląd schematów

Co najmniej raz na 5 lat ENISA **ocenia przyjęte europejskie schematy certyfikacji cyberbezpieczeństwa** pod względem ich użyteczności i aktualności. Komisja Europejska lub EGCC może zwrócić się do Agencji o opracowanie zmienionej propozycji schematu.

4.Informacje o europejskich schematach certyfikacji cyberbezpieczeństwa

Zadaniem ENISA jest utworzenie **specjalnej strony internetowej na temat certyfikacji cyberbezpieczeństwa.** Znajdą się tam m.in. informacje o aktualnych, wygasłych lub wycofanych schematach, certyfikatach czy oświadczeniach zgodności. Powinno się tam znaleźć również repozytorium linków do informacji dostarczanych przez producentów i dostawców z branży ICT.

Przygotowanie europejskiejgo schematu certyfikacji cyberbezpieczeństwa



Certyfikat oraz oświadczenie zgodności

Niezbędnym elementem każdego schematu jest również **określenie treści i formatu wydawanego certyfikatu lub oświadczenia zgodności.** Powinny one zawierać:

- Czas przez jaki powinno być udostępniane oświadczenie zgodności oraz dokumentacja techniczna.
- Okres ważności certyfikatu.
- Politykę ujawniania informacji o przyznanych, zmienionych i cofniętych certyfikatach.
- Warunki wzajemnego uznawania schematu certyfikacji z innymi państwami.
- Zasady wzajemnej oceny dla organów wydających europejskie certyfikaty cyberbezpieczeństwa dla wysokiego poziomu bezpieczeństwa.
- Procedury dostarczania i aktualizacji dodatkowych informacji cyberbezpieczeństwa oraz ich format.

Wymagania schematu nie mogą być sprzeczne z obowiązującymi wymogami prawnymi, zwłaszcza wynikającymi z ujednoliconego prawodawstwa UE.

Poziomy bezpieczeństwa europejskich schematów certyfikacji cyberbezpieczeństwa

Europejski schemat certyfikacji cyberbezpieczeństwa może określać trzy poziomy bezpieczeństwa: podstawowy, istotny i wysoki. Poziom wymaganego uwiarygodnienia dla danego urządzenia czy usługi ICT, powinien być **proporcjonalny do poziomu ryzyka**, na który składa się m.in. prawdopodobieństwo wystąpienia incydentu oraz jego potencjalny wpływ.

Wydany na określonym poziomie certyfikat zapewnia, że produkty, usługi i procesy ICT spełniają odpowiednie wymogi bezpieczeństwa i zostały ocenione zgodnie z obowiązującymi na danym poziomie wytycznymi.

Poziom bezpieczeństwa	Ryzyko	Wymagana ocena
Podstawowy	• znane podstawowe cyberzagrożenia	• dokumentacja techniczna
Istotny	• znane cyberzagrożenia • cyberatak prowadzony przez podmioty o ograniczonych umiejętnościach i zasobach	• czy nie zastosowano powszechnie znanych podatności • czy produkty bądź usługi prawidłowo wdrażają niezbędne funkcje bezpieczeństwa
Wysoki	• cyberatak prowadzany przez aktorów o znaczących umiejętnościach i zasobach	• czy nie zastosowano powszechnie znanych podatności • czy produkty bądź usługi prawidłowo wdrażają niezbędne funkcje bezpieczeństwa • odporność na ataki za pomocą testów penetracyjnych

Samoocena zgodności

Europejski schemat certyfikacji cyberbezpieczeństwa może zezwolić na przeprowadzenie **samooceny zgodności**. Przeprowadza ją producent lub dostawca produktów i usług ICT na swoją **wyłączną odpowiedzialność**. Taka ocena może dotyczyć tylko produktów i usług na **podstawowym poziomie bezpieczeństwa.**

Dostawca lub producent stwierdza, że spełnione zostały wymogi określone w europejskim schemacie certyfikacji i przyjmuje odpowiedzialność za ich zgodność. Oświadczenie zgodności oraz dokumentację techniczną należy przechowywać przez czas określony w danym europejskim schemacie certyfikacji. Kopię oświadczenia przedkłada się do krajowego organu certyfikacji cyberbezpieczeństwa i ENISA.

Wydawanie oświadczenia zgodności jest **dobrowolne**, chyba że inaczej stanowi unijne bądź krajowe prawo. Oświadczenie uznawane jest we wszystkich państwach członkowskich.

Certyfikacja cyberbezpieczeństwa

Procesy, produkty i usługi ICT, które zostały certyfikowane w ramach europejskiego schematu certyfikacji cyberbezpieczeństwa, uznaje się za zgodne z jego wymaganiami. Certyfikaty wydawane są na okres określony w danym schemacie certyfikacji i mogą być przedłużane, pod warunkiem że odpowiednie wymagania nadal są spełniane. Europejski certyfikat cyberbezpieczeństwa jest uznawany we wszystkich państwach członkowskich. **Certyfikacja jest dobrowolna**, chyba że prawo unijne lub państwowe stanowi inaczej.

Komisja Europejska będzie regularnie oceniać efektywność i wdrożenie przyjętych schematów certyfikacji. **Komisja sprawdza również czy konkretny schemat powinien zostać uznany jako obowiązkowy**, aby zapewnić odpowiedni poziom cyberbezpieczeństwa oraz usprawnić funkcjonowanie rynku wewnętrznego.

Obowiązkowa certyfikacja

Przeprowadzając ocenę, KE identyfikuje produkty, procesy i usługi ICT objęte istniejącym schematem certyfikacji, które **powinny podlegać obowiązkowej certyfikacji**. W pierwszej kolejności oceniane pod tym kątem będą sektory szczególnie wrażliwe, wymienione w załączniku II do Dyrektywy NIS: energetyka, transport, bankowość, infrastruktura rynków finansowych, służba zdrowia, zaopatrzenie w wodę pitną oraz infrastruktura cyfrowa. Ocenia się je najpóźniej dwa lata po przyjęciu pierwszego schematu.

Certyfikacja na poziomie krajowym – obowiązki państw członkowskich

O ile przygotowanie schematów certyfikacji cyberbezpieczeństwa odbywa się na poziomie europejskim, o tyle sam **proces certyfikacji przebiega na poziomie krajowym**. *Cybersecurity Act* nakłada na państwa członkowskie konkretne obowiązki, które mają pomóc w budowie sprawnego krajowego systemu certyfikacji cyberbezpieczeństwa.

Najważniejszym obowiązkiem nałożonym na państwa członkowskie jest **wyznaczenie co najmniej jednego krajowego organu certyfikacji cyberbezpieczeństwa**. Mają na to 24 miesiące po opublikowaniu rozporządzenia w Dzienniku Urzędowym Unii Europejskiej. Państwo członkowskie może powołać taki organ na swoim terytorium lub porozumieć się z innym państwem i wyznaczyć organ na jego terenie. Następnie należy poinformować Komisję Europejską o wyznaczonym organie, a jeśli jest więcej niż jeden – również o powierzonych im zadaniach. To również na państwach członkowskich spoczywa obowiązek **zapewnienia krajowym organom certyfikacji cyberbezpieczeństwa zasobów** do wykonywania powierzonych zadań.

Krajowe organy certyfikacji pełnią dwoistą rolę:

- wydają certyfikaty,
- prowadzą działania nadzorcze.

Obie te funkcje muszą być rozdzielone i niezależne od siebie. Krajowe organy muszą być również **niezależne od podmiotów, które nadzorują** – w kwestiach organizacji, decyzji finansowych, struktury prawnej czy przy podejmowaniu decyzji.

Krajowe organy certyfikacji współpracują ze sobą oraz z KE, a w szczególności wymieniają informacje, doświadczenia i dobre praktyki. Żeby skutecznie wprowadzać w życie przepisy rozporządzenia, powinny również uczestniczyć w pracach Europejskiej Grupy Certyfikacji Cyberbezpieczeństwa.

Zadania krajowych organów certyfikacji cyberbezpieczeństwa

- **egzekwują zasady zawarte w schematach**, aby monitorować zgodność produktów, procesów i usług ICT z wymogami certyfikatów wydanych na ich terytoriach;
  - monitorują i **egzekwują zobowiązania producentów lub dostawców**, którzy mają siedzibę na ich terenie, i **którzy przeprowadzają samoocenę zgodności**;
- **wspierają krajowe jednostki akredytujące** w monitorowaniu i nadzorowaniu działalności organów oceny zgodności;
  - monitorują **i nadzorują organy publiczne** wydające certyfikaty;

- **autoryzują organy oceny zgodności** oraz ograniczają, zawieszają lub cofają obowiązujące zezwolenia w przypadkach, gdy organy nie spełniają wymogów.

- **rozpatrują skargi** złożone przez osoby fizyczne lub prawne w związku z wydanymi certyfikatami lub samooceną zgodności;

- przedstawiają roczne zbiorcze sprawozdanie z podjętych działań;

- **współpracują z innymi krajowymi organami certyfikacji cyberbezpieczeństwa** lub organami publicznymi, dzielą się informacjami o niezgodnościach procesów, produktów i usług ICT z wymogami rozporządzenia lub europejskich schematów certyfikacji;

- **monitorują istotne zmiany** w dziedzinie certyfikacji cyberbezpieczeństwa.

Krajowe organy certyfikacji cyberbezpieczeństwa będą się wzajemnie oceniać, czyli podlegać tzw. **przeglądowi partnerskiemu**. Będzie on prowadzony na podstawie rzetelnych kryteriów oraz procedur oceny dotyczących struktury, zasobów ludzkich, wymagań procesowych, poufności i obsługi skarg.

Wzajemna ocena sprawdzać będzie:

- Czy działania krajowego organu certyfikacji cyberbezpieczeństwa związane z wydawaniem certyfikatów są rozdzielone i niezależne od działań nadzorczych.

- Procedury dotyczące nadzoru i monitorowania:
  - zgodności produktów, usług i procesów ICT z certyfikatami,
  - zobowiązań producentów i dostawców produktów, procesów lub usług ICT,
  - działalności organów oceny zgodności.

- Czy personel organów wydających certyfikaty dla wysokiego poziomu bezpieczeństwa posiada odpowiednią wiedzę specjalistyczną.

Wzajemna ocena odbywać się będzie c**o najmniej raz na pięć lat**. Prowadzą ją przynajmniej dwa krajowe organy certyfikacji cyberbezpieczeństwa z innych państw członkowskich oraz Komisja Europejska. W ocenie uczestniczyć może również ENISA.

Wyniki wzajemnej oceny bada Europejska Grupa Certyfikacji Cyberbezpieczeństwa, po czym przygotowuje streszczenie, które może być udostępnione publicznie. Jeśli zachodzi taka potrzeba, wydaje również wytyczne lub rekomendacje.

Bardzo istotnym ogniwem krajowego systemu certyfikacji cyberbezpieczeństwa są **Organy oceny zgodności**. **Mogą one wystawiać certyfikaty dla podstawowego i istotnego poziomu bezpieczeństwa**, a po przekazaniu takiego zadania przez krajowy organ certyfikacji cyberbezpieczeństwa – nawet dla poziomu wysokiego.

Organy oceny zgodności **są akredytowane przez krajową jednostkę akredytującą** tylko wtedy, gdy spełniają określone wymogi[2]. Akredytacja jest wydawana **maksymalnie na pięć lat** i może być przedłużana na tych samych warunkach, o ile organ oceny zgodności dalej spełnia wymogi.

Krajowe schematy certyfikacji i certyfikaty cyberbezpieczeństwa

Cybersecurity Act wpłynie na już funkcjonujące w niektórych państwach systemy certyfikacji. Nie należy się jednak obawiać, że wydane wcześniej krajowe certyfikaty nagle stracą ważność. Nawet jeśli zostały objęte nowymi europejskimi schematami certyfikacji, **zachowają ważność do daty wygaśnięcia określonej w przyznanym już certyfikacie.**

Jeśli zaś chodzi o krajowe schematy certyfikacji cyberbezpieczeństwa, które zostaną objęte europejskimi schematami certyfikacji, to **przestaną one wywoływać skutki** od daty ustalonej w akcie wykonawczym. Jeśli jednak **nie zostały objęte** europejskim schematem certyfikacji, nadal **mogą funkcjonować.**

Państwa członkowskie nie wprowadzają nowych krajowych schematów certyfikacji cyberbezpieczeństwa dla produktów, procesów i usług ICT, które zostały już objęte europejskim schematem certyfikacji.

Żeby uniknąć rozdrobnienia rynku wewnętrznego, państwa członkowskie informują Komisję i EGCC o planach opracowania nowych krajowych schematów certyfikacji.

[2] *Wymogi określa załącznik do Rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93 (Tekst mający znaczenie dla EOG)*

Sebastian Szymański

Czy należy obawiać się sztucznej inteligencji? Etyczne aspekty rozwoju nowoczesnych technologii

Sebastian Szymański *– doktor filozofii, pracuje na Wydziale „Artes Liberales" UW, zajmuje się problemami etycznymi związanymi z nowymi technologiami, ostatnio opublikował książkę Uzasadnienia teorii sprawiedliwości: dziedzictwo Johna Rawlsa, przewodniczący grupy ds. aspektów prawnych i etycznych, opracowującej wkład do Strategii Sztucznej Inteligencji dla Polski przy Ministerstwie Cyfryzacji.*

Rozważania nad potencjalnymi zagrożeniami związanymi ze sztuczną inteligencją pojawiły się niedługo po rozpoczęciu poważnych badań nad jej stworzeniem. Już w połowie lat 60. XX wieku Irving John Good, brytyjski matematyk, który podczas II wojny światowej pracował jako główny statystyk w Bletchley Park z Alanem Turingiem, zwrócił uwagę na następujący problem: „Zdefiniujmy maszynę ultrainteligentną jako maszynę, która dalece przewyższa na polu wszelkich aktywności intelektualnych dowolnego, choćby najinteligentniejszego człowieka. Ponieważ projektowanie maszyn jest jedną z tych aktywności intelektualnych, maszyna ultrainteligentna potrafi projektować jeszcze lepsze maszyny; dojdzie zatem bez wątpienia do „eksplozji inteligencji", w wyniku której inteligencja człowieka pozostanie daleko w tyle. A zatem pierwsza maszyna ultrainteligentna będzie ostatnim wynalazkiem, którego człowiek kiedykolwiek dokona — zakładając, że maszyna ta okaże się wystarczająco potulna, by powiedzieć nam, jak ją utrzymać pod kontrolą"[3].

Współcześnie podobne obawy wyrażają niektóre tuzy przemysłu informatycznego z Billem Gatesem i Elonem Muskiem na czele. Echa tych strachów pobrzmiewają również w kulturze masowej i publicystyce. Często słyszymy i czytamy o autonomicznych robotach, które zabiorą nam pracę, o algorytmach, które już wiedzą o nas więcej niż my sami, o inteligentnych systemach, które za chwilę będą w stanie przejąć kontrolę nad instytucjami wojskowymi i politycznymi, a nawet zetrzeć ludzkość z powierzchni ziemi. Tego rodzaju apokaliptyczne przewidywania mają niewielki związek z rzeczywistością i podsycane są przez publicznych intelektualistów, którzy często mylą popularne wyobrażenia rodem z science fiction z aktualnym stanem rozwoju technicznego.

Jednak te obawy, mimo że znajdują co najwyżej niewielkie oparcie w rzeczywistości, nie są zupełnie bezpodstawne. Nowe technologie stały się już nieodłączną częścią naszego życia, a co ważniejsze – przestały być widoczne dla swoich użytkowników. Podobnie jest w przypadku sztucznej inteligencji. Mało kto uświadamia sobie, że korzystanie z wyszukiwarki internetowej, optymalizowanie trasy przejazdu czy filtrowanie spamu w skrzynce mailowej oznacza korzystanie ze sztucznej inteligencji.

Warto zaznaczyć, że pojęciem tym często określa się urządzenie albo oprogramowanie zdolne do emulowania ogółu działań ludzkiego umysłu – jest to tak zwana uogólniona sztuczna inteligencja (*artificial general inteligence*, AGI). Tymczasem obecnie nie dysponujemy uogólnioną sztuczną inteligencją, a możliwość jej stworzenia jest kwestią budzącą poważne kontrowersje. Innymi słowy, lęki dotyczące sztucznej inteligencji nakierowane są na tę jej odmianę, której obawiać się nie ma powodu – przynajmniej na razie. Z drugiej strony, wyspecjalizowane sztuczne inteligencje, które wykorzystujemy już teraz, mogą rodzić poważne problemy etyczne.

Upowszechnianie technologii sztucznej inteligencji, którego jesteśmy obecnie świadkami, nie jest procesem obojętnym z etycznego punktu widzenia. W pewnym sensie jest to dalekosiężny eksperyment społeczny, którego skutki wcale nie są łatwe do przewidzenia. Oczywiście wprowadzenie każdej nowej technologii,

[2] *I. J. Good, Speculations concerning the first ultraintelligent machine, w: F. Alt, M. Ruminoff (red.), Advances in Computers, t. 6,, New York 1965, Academic Press, s 33.*

od ognia i koła po komputery i sztuczną inteligencję, jest eksperymentem, który ma dwie cechy bardzo istotne z etycznego punktu widzenia: można przeprowadzić go tylko raz i nie ma on ścisłych analogii w podobnych eksperymentach, których jako ludzkość, dokonywaliśmy wcześniej.

O społecznych skutkach komputeryzacji nie dowiedzielibyśmy się wiele, studiując konsekwencje upowszechnienia druku. Podobnie trudno przewidywać następstwa upowszechnienia sztucznej inteligencji na podstawie zmian, jakie wywołała komputeryzacja. Z uwagi na brak pewnej wiedzy dotyczącej następstw zmian społecznych wywoływanych przez sztuczną inteligencję, podstawową zasadą etyczną w tej sferze jest zasada ostrożności, która wyznacza ogólne ramy dopuszczalnych działań. Zasada ta głosi, że istnieje obowiązek ochrony ogółu przed szkodą albo krzywdą, kiedy wiadomo, że z badaniami naukowymi albo innowacjami technicznymi związane jest wiarygodne ryzyko. Rezygnacja z tej ochrony dopuszczalna jest jedynie w sytuacji, w której pojawią się wiarygodne świadectwa, najlepiej oparte na badaniach naukowych, że dane badania lub innowacje nie przyniosą szkody albo krzywdy.

Sztuczna inteligencja a pozycja jednostki w demokracji

Jedną z fundamentalnych wartości demokratycznych jest wzmacnianie pozycji jednostek. Mechanizmy kontrolne, prawa człowieka, różnego rodzaju gwarancje instytucjonalne – wszystko to są rozwiązania, które mają sprawiać, że jednostki nie będą bezsilne wobec procesów politycznych i gospodarczych, wykraczających poza ich możliwości oddziaływania. Rozwój i upowszechnienie sztucznej inteligencji może w znaczący sposób wpłynąć na sytuację jednostek w demokracji. Wśród potencjalnych wyzwań, które rodzą istotne problemy etyczne, można wskazać trzy główne obszary.

Przede wszystkim upowszechnienie różnych form sztucznej inteligencji może doprowadzić do osłabienia naszej pozycji jako użytkowników, czy szerzej klientów. Często spotkać można się ze stwierdzeniem, że sztuczna inteligencja to swojego rodzaju czarna skrzynka, której działania nie można zrozumieć i kontrolować, a interakcje z tym black box ograniczają się do dostarczania i użytkowania danych. Jednak ta teza jest dwuznaczna:

- sztuczna inteligencja może być traktowana jako **black box** dlatego, że użytkownicy nie rozumieją i nie potrafią jej kontrolować, a zatem problem kryje się w wiedzy i kompetencjach użytkowników;
- lub też sztuczna inteligencja może być niezrozumiała i niemożliwa do kontrolowania.

Co ciekawe, w powszechnym odbiorze przyjmuje się właśnie tą drugą możliwość, choć wydaje się, że tylko bardzo wąska klasa algorytmów wykorzystujących losowość może być nieprzewidywalna nawet dla specjalistów. Tymczasem to właśnie brak edukacji w zakresie funkcjonowania sztucznej inteligencji jest głównym źródłem największego ryzyka dla użytkowników.

Jedną z konsekwencji tego zjawiska jest gwałtowny wzrost nierówności sił w grze rynkowej – indywidualny użytkownik, który dla podmiotów wykorzystujących sztuczną inteligencję odgrywa podwójną rolę: źródła danych i konsumenta przetworzonych danych, nie jest w stanie stawić czoła globalnym firmom, które górują nad nim nawet bez technologii AI. Co istotniejsze, jest to wyścig z odwróconym **handicapem** – gracze, którzy już na starcie są silni, stają się w nim coraz silniejsi. Wystarczy pomyśleć, że Google, które już praktycznie dysponuje monopolem na wyszukiwanie w globalnej sieci, należy do firm przodujących w budowaniu komputera kwantowego. Połączenie tych dwóch technologii oznaczać będzie zyskanie siły politycznej i ekonomicznej trudnej obecnie do oszacowania.

Odpowiedzialność za wytwory sztucznej inteligencji

Kolejnym źródłem niespotykanych dotąd problemów etycznych jest rozwój algorytmów uczących się i samouczących, które wykorzystywane są między innymi w pojazdach autonomicznych. W tym przypadku użytkowanie ich oznacza w praktyce ich uczenie. Z tym samym zjawiskiem mamy zresztą do czynienia w przypadku tak zwanych inteligentnych asystentów czy filtrów antyspamowych, jednak te technologie nie mają prostego i bezpośredniego wpływu na zdrowie i życie ludzi.

Z etycznego punktu widzenia oznacza to zmianę rozkładu odpowiedzialności, który dotychczas uznawano za oczywisty: producent odpowiada za funkcjonalności produktu, a użytkownik za to, jak je wykorzysta. W przypadku technologii opartych na algorytmach (samo) uczących się, użytkownicy mają wpływ na ich funkcjonalności i zapewne będą ponosić część odpowiedzialności za ich działanie. Świadczą o tym między innymi projekty regulacji prawnych w zakresie inteligentnej robotyki i AI, nad którymi pracuje obecnie Parlament Europejski i Komisja Europejska – zakłada się, że integralną częścią regulacji prawnych będą kodeksy etyczne, również dla użytkowników.

Wpływ sztucznej inteligencji na rynek pracy

Upowszechnienie sztucznej inteligencji może również przyczynić się do osłabienia naszej pozycji jako pracowników. Istnieją

już dziesiątki raportów przewidujących poważne zmiany w strukturze zatrudnienia związane z algorytmizacją pewnych dziedzin gospodarki. Przewidywania dotyczące liczby pracowników, których dotkną te zmiany, są bardzo rozbieżne i nie zawsze wiarygodne. Jednak nie ma wątpliwości, że będzie to proces o rozległych i głębokich konsekwencjach, również etycznych.

Najbardziej oczywistym ryzykiem jest pogłębienie już istniejących i powstanie nowych nierówności. Praca z wykorzystaniem sztucznej inteligencji, czy może lepiej – współpraca ze sztuczną inteligencją – wymaga szczególnych kompetencji i umiejętności. Przy czym nie chodzi tu o kwalifikacje programistyczne wykorzystywane w tworzeniu i rozwijaniu sztucznej inteligencji, lecz o te potrzebne „zwykłym" użytkownikom. Istnieje poważne ryzyko, że doprowadzi to do pogłębienia i rozszerzenia wykluczenia cyfrowego, którego jednym z głównych źródeł jest właśnie brak kompetencji i umiejętności.

Wpływ sztucznej inteligencji na procesy demokratyczne

Wykorzystywanie sztucznej inteligencji pozwala również wywierać ogromny wpływ na procesy polityczne, czego skutkiem może być osłabienie naszej pozycji jako obywateli. Najlepszym tego przykładem jest głośny skandal związany z firmą Cambridge Analytica, która rzekomo wykorzystywała dane użytkowników Facebooka bez ich wiedzy i zgody do mikrotargetowania reklam podczas wyborów prezydenckich w Stanach Zjednoczonych. Niezależnie od tego, jaki był realny wpływ tych zabiegów, fakt, że wykorzystano w nich niezbyt wyrafinowane narzędzia, pokazuje jak wielki może być wpływ nowych „inteligentnych" technologii na politykę.

Przykładem mogą być tak zwane **fake newsy**, których fabrykowanie, dzięki technologiom manipulowania strumieniowaniem wideo w czasie rzeczywistym, stało się wręcz banalne. Nie bez znaczenie jest również to, że **Big Five**, czyli najwięksi i najważniejsi gracze na polu sztucznej inteligencji – Google, Facebook, Amazon, Apple i Microsoft – to wielonarodowe korporacje, mające siedziby w Stanach Zjednoczonych. Oznacza to, że narzędzia tworzone i wykorzystywane przez te podmioty wywierają wpływ na obywateli krajów, które z kolei mają niewielki wpływ polityczny na sposób funkcjonowania tych korporacji.

Nierówny rozkład zamożności, władzy i rozkładu ryzyka

Najbardziej zauważalną konsekwencją upowszechnienia sztucznej inteligencji jest zatem osłabienie naszej pozycji w różnych sferach. Z etycznego punktu widzenia istotne jest jednak pytanie: dlaczego to zjawisko jest złe? Osłabienie to polega na powstaniu bardzo dużych nierówności zamożności i władzy, które zbiegają się z nierównościami w rozkładzie ryzyka. Doskonale widać to na przykładzie rozkładu ryzyka związanego z danymi. Dla jednostki ogół jej danych stanowi integralny element tożsamości, a ich niekontrolowane ujawnienie prowadzić może do poważnego ryzyka. Na przykład ujawnienie danych dotyczących zdrowia może diametralnie zmienić pozycję jednostki wobec ubezpieczyciela lub pracodawcy.

Natomiast dla firmy przetwarzającej duże ilości danych, pełny zestaw informacji o jednostce jest mało znaczący z punktu widzenia całego zbioru danych. Ten zbieg nierówności prowadzi do podwójnej niesprawiedliwości – osoby raz poszkodowane tracą w dwójnasób, a wygrywający zyskują podwójnie.

Wracając do pytania postawionego w tytule – nie musimy obawiać się sztucznej inteligencji. To bardzo użyteczne i potężne narzędzie, którego wykorzystanie przyniosło już, i przynosi nadal, niezliczone korzyści na wielu polach, od ochrony zdrowia po badania naukowe. Jednak siła tego narzędzia przekłada się na nierówności między tymi, którzy z nich korzystają, w zależności od tego, którą pozycję zajmują w łańcuchu tworzenia i wykorzystania sztucznej inteligencji. To właśnie rodzi problemy etyczne i powinno być obiektem naszej bacznej uwagi.

Komentarz NASK:

W 2018 roku Komisja Europejska dużo uwagi poświęciła zagadnieniom związanym ze Sztuczną Inteligencją (AI) i etycznymi aspektami jej rozwoju.

25 kwietnia 2018 KE przedstawiony został Komunikat w sprawie AI (Sztuczna Inteligencja dla Europy). Dokument zakłada działania w dziedzinie technologii, etyki, prawa i kwestii ekonomicznych. AI została zidentyfikowana jako istotne wyzwanie strategiczne. KE podkreśla różnice w funduszach przeznaczanych na AI w Europie i na świecie – europejskie inwestycje w dziedzinie AI sięgają jedynie 2.4 – 3.2 bilionów Euro, podczas kiedy w Azji i Ameryce Północnej było to odpowiednio 6.5 – 9.7 oraz 12.1 – 18.6 bilionów Euro. Wyzwanie AI zostało zaadresowane w trzech aspektach:

- Zwiększenie zdolności technologicznej i przemysłowej UE oraz wykorzystania sztucznej inteligencji w różnych dziedzinach gospodarki
- Przygotowanie się do zmian społeczno – gospodarczych związanych z rozwojem Sztucznej Inteligencji
- Przygotowanie właściwych ram prawnych i etycznych dla rozwoju Sztucznej Inteligencji

W czerwcu KE powołała grupę 52 ekspertów ds. AI. W skład grupy weszli przedstawiciele ośrodków akademickich, biznesu i społeczeństwa obywatelskiego. Zadaniem grupy było opracowanie rekomendacji w zakresie rozwoju polityki sztucznej inteligencji. 18 grudnia Grupa zaproponowała Wytyczne w Zakresie Rozwoju i Wykorzystania Sztucznej Inteligencji (Ethics Guidelines for the Development and Use of Artificial Intelligence) . W dokumencie zaproponowano strukturę dla godnej zaufania AI. Dokument był przedmiotem konsultacji społecznych, a jego ostateczna wersja ma zostać opublikowana w marcu 2019 roku.

7 grudnia KE opublikowała Skoordynowany Plan dla Sztucznej Inteligencji. Dokument poodejmuje siedem głównych zagadnień:

- Wspólne cele i wysiłek na rzecz AI
- Partnerstwa publiczno – prywatne, finansowanie start – upów i innowacyjnych małych i średnich przedsiębiorstw
- Wzmacnianie wiarygodności AI i związanych z nią rozwiązań technologicznych
- Dostosowywanie programów i systemów szkolnych do wyzwań związanych z rozwojem sztucznej inteligencji
- Budowanie europejskiej przestrzeni danych niezbędnej dla sztucznej inteligencji w Europie
- Opracowanie wytycznych etycznych i zapewnienie ram prawnych sprzyjających innowacjom
- Aspekty związane z bezpieczeństwem AI

W 2018 roku po raz pierwszy rząd podjął prace nad tematem sztucznej inteligencji (AI). Jeszcze przed publikacją Komunikatu KE Sztuczna Inteligencja dla Europy, z inicjatyw Polski Grupa Wyszehradzka (V4) przyjęła wspólne stanowisko w sprawie sztucznej inteligencji i jej potencjału dla rozwoju gospodarki UE. Państwa V4 wezwały KE do dalszego zaangażowania w proces rozwoju AI, podkreślając potencjał rozwoju dla europejskich przedsiębiorców, w oparciu o wykorzystanie sztucznej inteligencji. Jednocześnie wskazano konieczność pogłębionej analizy prawnych i ekonomiczno – społecznych dla rozwoju AI.

Kolejnym krokiem było utworzenie przy Ministerstwie Cyfryzacji czterech grup roboczych w zakresie sztucznej inteligencji: gospodarka oparta na danych, finansowanie badań i rozwoju, edukacja, etyka i prawo. Prze kilka miesięcy eksperci pracowali nad rekomendacjami, które przedstawiono ostatecznie na początku listopada jako Założenia do strategii AI w Polsce.

Dokument podsumowuje prace grup roboczych i przedstawia plan działań w zakresie AI na lata 2018 – 2019.

Na rok 2019 zapowiedziano prace nad krajową strategią w zakresie sztucznej inteligencji.

Justyna Balcewicz

Udostępnianie i ponowne wykorzystywanie danych

Justyna Balcewicz *– Analityk ds. „czynnika ludzkiego w cyberbezpieczeństwie" i nowoczesnych technologiach w zespole Analiz Strategicznych i Wpływu Nowoczesnych Technologii w NASK PIB. Specjalizuje się w analizach z zakresu wpływu nowoczesnych technologii na rozwój społeczeństwa i związanych z tym wyzwaniami. Czynnie zaangażowana w prace grupy roboczej ds. edukacji, działającej w Ministerstwie Cyfryzacji, która opracowała wytyczne do strategii Sztucznej Inteligencji dla Polski.*

Doświadczenie zdobywała pracując w firmach sektora energetycznego oraz w sektorze finansowym, gdzie zajmowała się monitoringiem transakcji podejrzanych o pranie brudnych pieniędzy. Wcześniej pracowała jako koordynator projektów unijnych finansowanych ze Szwajcarsko-Polskiego Programu Współpracy i Norweskiego Mechanizmu Finansowego.

Absolwentka Socjologii Instytutu Stosowanych Nauk Społecznych Uniwersytetu Warszawskiego oraz studiów w Wyższej Szkole Finansów i Zarządzania. Ekspert w zakresie relacji międzyludzkich i ich wpływu na funkcjonowanie społeczeństwa oraz rozwoju kompetencji cyfrowych w świecie nowoczesnych technologii. W wolnych chwilach pisarka powieści dla dzieci i młodzieży.

Wraz z rozwojem nowoczesnych technologii, a także rosnącym zainteresowaniem tematyką Sztucznej Inteligencji, pojawia się kwestia udostępniania danych nieosobowych do ponownego wykorzystania. Mowa nie tylko o danych z instytucji publicznych, które są wytwarzane przy okazji wykonywania obowiązków przez administrację, ale również danych dotyczących badań naukowych, a także danych z sektora prywatnego. Tematem już od początku dwudziestego pierwszego wieku zajmuje się Unia Europejska. W ostatnim czasie kwestia udostępniania danych coraz częściej wraca w komunikatach Komisji Europejskiej, a tym samym stała się również obszarem zainteresowań polskiego rządu.

Dyrektywa PSI w sprawie ponownego wykorzystywania informacji sektora publicznego

W listopadzie 2003 roku Unia Europejska opublikowała Dyrektywę 2003/98/WE (dyrektywa PSI) w sprawie ponownego wykorzystywania informacji sektora publicznego. Już wtedy zwrócono uwagę na ogromny potencjał informacji zbieranych przez sektor publiczny w wielu obszarach (społecznym, ekonomicznym, geograficznym, turystycznym, gospodarczym, patentowym, pogodowym czy edukacyjnym). Ponowne wykorzystanie tych danych miało przyczynić się do rozwoju usług w skali całej Unii Europejskiej, pobudzić wzrost gospodarczy poprzez wsparcie firm europejskich, a także zwiększyć liczbę miejsc pracy. Autorzy dyrektywy podkreślali, że rozwój społeczeństwa informacyjnego w UE, a także sprawne funkcjonowanie rynku wewnętrznego, wymaga zminimalizowania różnic pomiędzy poszczególnymi państwami członkowskimi. Do tego celu konieczna była jednak standaryzacja wykorzystywania zasobów informacji sektora publicznego. Dlatego dyrektywa PSI zdefiniowała zestaw podstawowych reguł i praktycznych środków, umożliwiających wykorzystanie informacji z sektora publicznego. Zgodnie z dokumentem państwa członkowskie zadeklarowały gotowość do udostępniania informacji, z wyłączeniem dokumentów:

- których wydawanie jest działalnością poza zakresem zadań publicznych;
- z prawami własności intelektualnej osób trzecich;
- wyłączonych z dostępu (dotyczących bezpieczeństwa narodowego, tajemnicy statystycznej czy handlowej, z ograniczonym dostępem, zawierających dane osobowe, będących w posiadaniu publicznych nadawców, instytucji edukacyjnych i kulturalnych).

Procedura wniosku o ponowne wykorzystywanie informacji powinna zawierać wymagania dotyczące ewentualnej licencji, zasady postępowania w przypadku decyzji odmownej, środki odwoławcze,

a także regulacje pobierania opłat. Kwestia wynagrodzenia zależy od kosztów poniesionych w związku z reprodukowaniem i udostępnianiem informacji. Opłaty powinny być ustalone na podstawie obiektywnych, przejrzystych i sprawdzalnych kryteriów, wspólnych dla wszystkich państw członkowskich. W dyrektywie wskazano również konieczność wprowadzenia rozwiązań praktycznych, które ułatwiają wyszukiwanie dokumentów.

Przegląd dyrektywy został wykonany zgodnie z planem w kwietniu 2018 roku. W czasie konsultacji społecznych zebrano wnioski z dotychczasowej implementacji dyrektywy. Podsumowanie zostało opublikowane w dokumencie **Proposal for a revision of the Public Sector Information (PSI) Directive**. Autorzy zidentyfikowali cztery bariery, które wciąż spowalniają możliwość wykorzystywania danych z sektora publicznego:

1 Duża ilość danych finansowanych ze środków publicznych wciąż nie jest objęta dyrektywą PSI, choć są to dane z ogromnym potencjałem (generowane przez sektor mediów i transportu).

2 Brak dostępu do dynamicznych danych z aplikacji podróżnych i transportowych w czasie rzeczywistym. Dane te mają ogromny potencjał, szczególnie gdy są aktualne, a instytucje publiczne nie oferują możliwości wykorzystania ich.

3 Zbyt wysokie opłaty za wykorzystywanie danych, znacznie przewyższające koszty reprodukcji i rozpowszechniania. Koszty stanowią barierę szczególnie dla małych i średnich przedsiębiorstw.

4 Blokowanie dostępu do danych przez firmy, które współpracują z sektorem publicznym na wyłączność.

Ustawa o ponownym wykorzystywaniu informacji sektora publicznego

W Polsce prawo do ponownego wykorzystywania informacji sektora publicznego regulowane jest ustawą z dnia 25 lutego 2016 roku. Zgodnie z ustawą, każdemu przysługuje prawo do danych udostępnionych w systemach teleinformatycznych i na stronie Biuletynu Informacji Publicznej. Pozostałe informacje mogą zostać udostępnione na wniosek o ponowne wykorzystanie. Prawo to może podlegać ograniczeniu, między innymi ze względu na prywatność osoby fizycznej, tajemnicę przedsiębiorstwa czy ograniczenia wynikające z innych ustaw. Podmiot, który udostępnia i przekazuje informacje, nie może ograniczać korzystania z nich przez innych użytkowników, chyba że takie ograniczenie jest wymagane dla prawidłowego wykonywania zadań publicznych.

Dane przekazane do ponownego wykorzystania powinny zawierać informację o:

- warunkach wykorzystywania danych, które mogą być rozumiane jako:
  - obowiązek poinformowania o źródle,
  - obowiązek poinformowania o informacji ponownie wykorzystywanej,
  - zakres odpowiedzialności podmiotu za udostępniane informacje.
- wysokości opłat i czynnikach wpływających na ich ustalanie,
- środkach prawnych przy braku zgody na wykorzystywanie danych,
- ewentualnej umowie na udzielenie wyłącznego prawa do korzystania z danych wraz z powodami zawarcia takiej umowy.

Warto podkreślić, że muzea państwowe i samorządowe, biblioteki publiczne i naukowe, a także archiwa mają przywilej określenia własnych warunków. Jednak żadne z nich nie może w sposób nieuzasadniony ograniczać ponownego wykorzystywania informacji z sektora publicznego.

Co do zasady informacje sektora publicznego udostępnia się bezpłatnie. Nałożenie opłaty jest uzasadnione, gdy przygotowanie lub przekazanie informacji wymaga dodatkowych kosztów. Opłata nie powinna jednak przekroczyć poniesionych wydatków. Jedynie muzea państwowe i samorządowe są uprawnione do ustalenia wyższej opłaty, na którą składają się koszty gromadzenia, produkowania, reprodukowania, rozpowszechniania danych i ochrony ich praw.

Informacje, które nie zostały udostępnione w BIP lub w centralnym repozytorium, mogą zostać udostępnione na wniosek. Ustawa określa szczegółowe wytyczne dotyczące przygotowania wniosku, wymaganych danych oraz procedury rozpatrzenia wniosku. Z przepisów ustawy zostały wyłączone między innymi jednostki publicznej radiofonii i telewizji, państwowe instytucje kultury, uczelnie i jednostki naukowe, a także biblioteki naukowe, których organizatorami nie jest sektor publiczny.

Komunikaty Komisji Europejskiej

W kwietniu 2018 roku Komisja Europejska opublikowała komunikat **Towards a common European data space** – w kierunku wspólnej przestrzeni wymiany danych w Europie. Po raz kolejny podkreślono, że rozwój innowacyjnych rozwiązań opartych na danych jest główną siłą napędową wzrostu gospodarczego i rynku pracy w Europie. Zgodnie z przewidywaniami Komisji, do 2020 roku gospodarka oparta na danych podwoi się, dlatego też należy stworzyć odpowiednie warunki rozwoju, aby zachować konkurencyjność UE na arenie międzynarodowej.

Pierwszym krokiem do stworzenia wspólnej przestrzeni wymiany danych

w Europie są regulacje dotyczące ochrony danych osobowych (RODO), które stanowią ramy prawne, budujące wzajemne zaufanie w obszarze wymiany danych. Teraz konieczne jest wdrożenie kolejnych regulacji, które umożliwią wykorzystywanie ogromnego potencjału danych gromadzonych zarówno przez sektor publiczny jak i prywatny.

Dostęp do danych publicznych i finansowanych ze środków publicznych

Komisja Europejska zachęca do korzystania z danych publicznych, które stanowią cenny surowiec do rozwoju innowacyjnych usług cyfrowych. Dane z instytucji europejskich są gromadzone w ramach Europejskiego Otwartego Portalu Danych *(European Data Portal)*, który umożliwia ich łatwe wyszukiwanie, bez ograniczeń związanych z krajem i językiem.

Dostęp do danych naukowych finansowanych ze środków publicznych

W ramach realizacji koncepcji otwartej nauki, KE zachęca, aby instytucje naukowe udostępniały informacje o całym przebiegu procesu badawczego – od projektu, poprzez metodologię, poszczególne etapy pracy, aż do wyników. W celu stworzenia platformy do swobodnej wymiany danych w środowisku naukowym, Komisja Europejska uruchomiła otwartą chmurę dla nauki *(European Open Science Cloud)*.

25 kwietnia 2018 roku Komisja opublikowała komunikat bezpośrednio dotyczący zaleceń w sprawie dostępu do informacji naukowych i ich ochrony. W szczególny sposób zwrócono uwagę na kwestię dzielenia się wiedzą, przechowywanie i ponowne wykorzystywanie informacji naukowych, a także współpracę z instytucjami naukowymi i akademickimi. Zmiana związana z otwartym dostępem do nauki wymaga czasu i zaangażowania wielu środowisk: instytucji naukowych, osób działających w obszarze nauki, interesariuszy, dostawców i fundatorów. Nowe rekomendacje Komisji Europejskiej mają być wsparciem dla państw członkowskich i ustrukturyzować kwestię otwartego dostępu do nauki we wszystkich krajach.

Wymiana danych w ramach sektora prywatnego

Kolejnym filarem wspólnej przestrzeni wymiany danych w Europie jest dostęp do danych sektora prywatnego. Dzielenie się danymi między przedsiębiorstwami jest niezbędne do osiągnięcia obopólnej korzyści i przyspieszenia rozwoju innowacji. Ważne, aby budować odpowiednią świadomość wśród przedstawicieli biznesu i pokazywać, że wykorzystanie danych (również zagranicznych) w odmiennych sytuacjach i do projektów z różnych branż, nie wpływa na zmniejszenie konkurencyjności firm. Komisja opracowała kluczowe zasady, które powinny być wzięte pod uwagę przy udostępnianiu danych. Wspiera również finansowo przedsiębiorstwa budujące platformy wymiany danych i centra innowacji w ramach programu Horizon 2020.

Wymiana danych między sektorem prywatnym a publicznym

Dostęp do baz danych przedsiębiorstw jest coraz częściej wykorzystywany przez instytucje publiczne i może się przyczyniać do ulepszania usług publicznych, a także służyć szeroko pojętemu interesowi społecznemu. Wykorzystanie danych dla korzyści wszystkich obywateli może dotyczyć np. przeciwdziałania epidemii, planowania urbanistycznego, ulepszania bezpieczeństwa drogowego, ochrony środowiska czy ochrony konsumentów. Komisja zaznaczyła, że temat wymiany danych między sektorem prywatnym a publicznym zostanie szeroko przeanalizowany.

Stanowisko Rządu w związku z Komunikatem Komisji do Parlamentu Europejskiego, Rady Europejskiej, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów inteligencja dla Europy

Kwestia udostępniania danych została również zaznaczona w komunikacie Komisji dotyczącym rozwoju sztucznej inteligencji. Celem tego dokumentu jest wskazanie stanowiska Unii Europejskiej wraz z uwzględnieniem szans i identyfikacją zagrożeń wynikających z rozwoju tej technologii. Rząd RP opracował stanowisko, w którym zgodził się z Komisją co do konieczności udostępniania danych do ponownego wykorzystania. Pozytywnie wypowiedziano się też na temat inicjatyw związanych z zapewnieniem dostępu do danych jednostkom badawczym oraz działom badań i rozwoju. Rząd poparł działania UE zmierzające do upowszechnienia gospodarki opartej na danych, rozumianych jako dobro nie podlegające konkurencji i zużyciu. W dokumencie wspomniano o konieczności zbudowania zaufanych ekosystemów zwanych wirtualnymi składnicami danych *(virtual data warehouses)*, które mają być mechanizmami gromadzenia, wymiany i zarządzania danymi na potrzeby edukacji, badań i wdrożeń. Wirtualne składnice danych umożliwią rozwój sztucznej inteligencji w kluczowych dziedzinach polskiej gospodarki, takich jak medycyna, finanse, przemysł energetyczny, chemiczny, rolny czy ochrona środowiska i transport. Składnice mogłyby stanowić ogólnoeuropejskie inicjatywy w zakresie otwartych standardów, uznawania certyfikatów i zasad interoperacyjności. Umożliwiałyby firmom dobrowolne udostępnianie i dzielenie się danymi w zaufanym środowisku. W tym celu konieczne byłoby zapewnienie pełnego bezpieczeństwa wirtualnych składnic danych wraz z anonimizacją i poszanowaniem praw związanych z ochroną danych osobowych. Niezbędne

byłoby wdrożenie działań zachęcających przedsiębiorstwa prywatne do szerokiej wymiany danych, a także zapewnienie dostępu do jak największej ilości danych publicznych. Ostatnią kwestię wspiera projekt realizowany od czerwca 2017 roku przez Ministerstwo Cyfryzacji pn. „Otwarte dane: dostęp, standard, edukacja". W ramach projektu opracowywane są systemowe rozwiązania na rzecz zwiększenia dostępności i jakości danych publicznych, a także możliwości ich ponownego wykorzystania. Jeden z komponentów projektu zakłada otwarcie 6 rejestrów publicznych dotyczących m.in. danych statystycznych, danych ze służby zdrowia, budżetów jednostek samorządu terytorialnego, a także danych o pojazdach. Dodatkowo zostaną opracowane standardy otwierania danych.

Już w stanowisku Państw Grupy Wyszechradzkiej[3], zainicjowanym przez Polskę, podkreślono, że w działaniach na rzecz rozwoju sztucznej inteligencji niezbędny jest dostęp do informacji i danych pochodzących zarówno z sektora publicznego, jak i prywatnego. Udostępnianie danych jest aktualnie uważane za podstawę rozwoju w kierunku efektywnego wykorzystania technologii dla wspólnego dobrobytu. Dlatego też Rada Ministrów deklaruje stworzenie krajowej strategii w obszarze sztucznej inteligencji, która zostanie wypracowana przez Ministerstwo Cyfryzacji we współpracy z pozostałymi resortami, w szczególności z Ministerstwem Przedsiębiorczości i Technologii oraz Ministerstwem Nauki i Szkolnictwa Wyższego.

Zaprojektowane przez starline, fullvector / Freepik.com

[3] *https://www.gov.pl/web/cyfryzacja/stanowisko-grupy-wyszehradzkiej-dotyczace-sztucznej-inteligencji*

Magdalena Wrzosek

Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa – nowa propozycja w zakresie dysponowania funduszami europejskimi i nie tylko

Magdalena Wrzosek *– Kierownik Zespołu Analiz Strategicznych i Wpływu Nowoczesnych Technologii w NASK PIB, gdzie odpowiada za kwestie strategiczne, regulacyjne i organizacyjne związane z cyberbezpieczeństwem oraz rozwojem nowoczesnych technologii. Oficer Łącznikowy Europejskiej Agencji Bezpieczeństwa Sieci i Informacji (ENISA), koordynator Europejskiego Miesiąca Cyberbezpieczeństwa w Polsce. Twórca projektu CyberPolicy (https://cyberpolicy.nask.pl).*

W latach 2014-2016 pracowała w Ministerstwie Cyfryzacji, gdzie odpowiadała m.in. za negocjacje Dyrektywy NIS, planowanie i koordynację europejskich ćwiczeń cybernetycznych Cyber Europe (edycje 2014 i 2016), współpracę międzynarodową oraz implementację zapisów Polityki Ochrony Cyberprzestrzeni RP.

Politolog, kulturoznawca, absolwentka Uniwersytetu Warszawskiego oraz Uniwersytetu w Konstancji w Niemczech. Studia podyplomowe z zarządzania projektami, zarządzania bezpieczeństwem informacji, prawa międzynarodowego i służby zagranicznej. Ukończyła także Europejskie Centrum Studiów nad Bezpieczeństwem im. Greaorgea'a Marshall'a w Garmisch-Partenkirchen (Program on Cyber Security Studies (PCSS) oraz Seminar on Regional Security (SRS)). W 2016 roku brała udział w programie „International Visitor Leadership Program" poświęconym cyberbezpieczeństwu, organizowanym przez Departament Stanu USA. Doktorantka Akademii Sztuki Wojennej w Warszawie, gdzie wykłada zarządzanie kryzysowe i bezpieczeństwo publiczne.

12 września 2018 roku Komisja Europejska przedstawiła propozycję rozporządzenia ustanawiającego Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych wraz z siecią krajowych ośrodków koordynacji. Jest to propozycja współpracy, której celem jest stymulowanie europejskiego ekosystemu technologicznego i przemysłowego w dziedzinie cyberbezpieczeństwa. KE chce w ten sposób stymulować współpracę między branżami w dziedzinie cyberbezpieczeństwa oraz pomiędzy różnymi środowiskami naukowymi.

Zgodnie z propozycją KE powstanie Europejskie Centrum Cyberbepzieczeństwa – nowa instytucja, której zadaniem będzie przede wszystkim:

- ułatwianie i pomoc w koordynacji pracy sieci krajowych ośrodków koordynacji;
- zwiększanie możliwości i wiedzy, a także ulepszanie infrastruktury w zakresie cyberbezpieczeństwa, z korzyścią dla gałęzi przemysłu, sektora publicznego i środowisk naukowych;
- wnoszenie wkładu w powszechne wdrażanie w całej gospodarce nowoczesnych produktów i rozwiązań w dziedzinie cyberbezpieczeństwa;
- poprawa zrozumienia kwestii cyberbezpieczeństwa i wnoszenie wkładu w ograniczanie niedoborów kwalifikacji w zakresie cyberbezpieczeństwa w UE;
- przyczynianie się do wzmacniania badań naukowych i rozwoju w dziedzinie cyberbezpieczeństwa w UE;
- zacieśnienie współpracy między kręgami cywilnymi i obronnymi w odniesieniu do technologii i aplikacji podwójnego zastosowania w dziedzinie cyberbezpieczeństwa;
- zwiększanie synergii między wymiarem cywilnym i wymiarem obronnym cyberbezpieczeństwa w odniesieniu do Europejskiego Funduszu Obronnego.

Komisja argumentuje, że zasadniczą rolą centrum ma być dystrybuowanie funduszy europejskich w dziedzinie cyberbezpieczeństwa z poziomu europejskiego na poziom państw członkowsich. Dodatkowo centrum ma gromadzić wiedzę i komptencje w zakresie cyberbepzieczeństwa.

Zgodnie z propozycją KE, centrum składa się z:

- Rady Zarządzającej, w której skład wchodzi po jednym przedstawicielu kazdego państwa członkowskiego oraz pięciu przedstawicieli Komisji Europejskiej;
- Dyrektora Wykonawczego, zatrudnianego przez centrum, a wybieranego i mianowanego przez Radę Zarządzającą z listy wskazanej przez Komisję Europejską;
- Rady Konsultacyjnej ds. Przemysłowych i Naukowych, która liczy maksymalnie 16 członków i jest mianowana przez Radę Zarządzającą spośród przedstawicieli podmiotów, którzy są częścią środowiska, posiadającego kompetencje w dziedzinie cyberbezpieczeństwa.

Poza Europjeskim Centrum Cyberbezpieczeństwa powstanie sieć krajowych ośrodków koordynacji. Ośrodki te nominowane będą przez kraje członkowskie, a następnie akredytowane przez Komisję Europejską. Instytucje te mają wspierać działania centrum. Poza tym zadania ośrodków są następujące:

- ułatwianie przemysłowi i innym podmiotom na szczeblu państwa członkowskiego udziału w projektach transgranicznych;
- udział wspólnie z Centrum Kompetencji w określaniu i eliminowaniu stojących przed przemysłem wyzwań w dziedzinie cyberbezpieczeństwa, które dotyczą konkretnych sektorów;
- pełnienie roli punktu kontaktowego na szczeblu krajowym na potrzeby środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa i Centrum Kompetencji;
- dążenie do tworzenia synergii z odpowiednimi działaniami na szczeblu krajowym i regionalnym;
- wdrażanie poszczególnych działań, na które Centrum Kompetencji przyznało dotacje;
- promowanie i rozpowszechnianie przez sieć, środowisko posiadające kompetencje w dziedzinie cyberbezpieczeństwa i Centrum Kompetencji odpowiednich wyników prac na szczeblu krajowym i regionalnym;
- ocena wniosków o włączenie do środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa składanych przez podmioty, które mają siedzibę w tym samym państwie członkowskim co ośrodek koordynacji.

Poza Krajowym Ośrodkiem Koordynacji w państwach członkowsich mają powstać środowiska posiadające kompetencje w dziedzinie cyberbepzieczeństwa, które mają współpracować z Europejskim Centrum oraz przyczyniać się do ropowszechniania fachowej wiedzy z zakresu cyberbezpieczeństwa. Jego członkowie mają pochodzić z różnych środowisk, tak aby reprezentować różne punkty widzenia. To dlatego w skład środowiska mają wchodzić organizacje przemysłowe, akademickie, organizacje naukowe non-profit oraz stowarzyszenia i podmioty publiczne. Warunkiem akredytacji na członka środowiska jest wykazanie się fachową wiedzą z zakresu cyberbezpieczeństwa w co najmniej jednej z dziedzin:

- badania naukowe;
- rozwój przemysłu;
- szkolenie i kształcenie.

Akredytacji dokonuje Europejskie Centrum Komptencji, jednak jest ona poprzedzona wyznaczeniem danych organizacji na członków środowiska na mocy prawa krajowego, po tym jak krajowy ośrodek zweryfikuje podmioty kandydujące na członków środowiska. Poza tym na członków środowiska mogą zostać powołane także organy, agencje i urzędy Unii Europejskiej.

Zadania członków środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa obejmują:

- wsparcie Centrum Kompetencji w wypełnianiu misji i osiąganiu celów określonych w art. 3 i 4 rozporządzenia oraz ścisłą współpracę w tym celu z Centrum Kompetencji i właściwymi krajowymi ośrodkami koordynacji;
- uczestniczenie w działaniach promowanych przez Centrum Kompetencji i krajowe ośrodki koordynacji;
- w stosownych przypadkach uczestniczenie w grupach roboczych ustanowionych przez Radę Zarządzającą Centrum Kompetencji w celu realizacji poszczególnych działań określonych w planie prac Centrum Kompetencji;
- w stosownych przypadkach wspieranie Centrum Kompetencji i krajowe ośrodki koordynacji w promowaniu poszczególnych projektów;
- promowanie i rozpowszechnianie stosownych wyników działań i projektów prowadzonych w ramach społeczności

Propozycja rozporządzenia w sprawie Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych budzi wiele kontrowersji. Przede wszystkim nie do końca uzasadniona wydaje się dominująca rola Komisji Europejskiej w Radzie Zarządzającej, a także uzależnienie prawa głosu w radzie dla państw członkowskich od funduszy wpłacanych na centrum. Dodatkowo część zadań centrum wyraźnie pokrywa się z nowym mandatem Europejskiej Agencji Bezpieczeństwa Sieci i Informacji (ENISA).

Flash z Komisji Europejskiej

Michał Czerniawski, Justyna Romanowska

Stałe Przedstawicielstwo przy Unii Europejskiej w Brukseli

Od stycznia 2019 roku Rumunia objęła półroczną Prezydencję w Radzie UE.

Priorytety prezydencji rumuńskiej będą następujące: innowacje, cyberbezpieczeństwo, e-umiejętności oraz kobiety w sektorze technologii informacyjno-komunikacyjnych (ICT).

Rumunia będzie kontynuować prace nad następującymi projektami aktów legislacyjnych:

- rozporządzenie ws. Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa oraz sieci krajowych ośrodków koordynacji,
- rozporządzenie o e-prywatności,
- przegląd dyrektywy ws. ponownego wykorzystania informacji sektora publicznego (PSI),
- rozporządzenie ws. domeny .eu (jedynie formalne przyjęcie przez Radę UE, gdyż uzgodnienie tego dossier w trilogu z Parlamentem Europejskim nastąpiło za prezydencji austriackiej),
- program "Cyfrowa Europa" (DEP),
- Instrument "Łącząc Europę" (tzw. CEF 2).

Z uwagi na wybory do Parlamentu Europejskiego wspomniane projekty muszą zostać uzgodnione między Radą UE a Parlamentem Europejskim oraz przyjęte do wiosny 2019 r.

Jeżeli chodzi o plany pracy Komisji Europejskiej na 2019 rok, to określa je komunikat z końca 2018 r. pn. „Agenda na rzecz bardziej zjednoczonej, silniejszej i bardziej demokratycznej Europy" (COM(2018)800). Dokument ten nie zawiera tematów cyfrowych. Prezydencja rumuńska planuje także wiele wydarzeń na poziomie ministerialnym oraz eksperckim.

Poziom ministerialny:

- **1 marca 2019, Bukareszt**
  – nieformalne spotkanie ministrów ds. telekomunikacji połączone z konferencją ministerialną dotyczącą Partnerstwa Wschodniego nt. harmonizacji rynków cyfrowych
- **7 czerwca 2019, Luksemburg**
  – posiedzenie Rady UE ds. TTE
- **12 czerwca 2019, Bukareszt**
  – spotkanie ministerialne ws. e-umiejętności

Pozostałe wydarzenia:

- **18–19 lutego 2019**
  – konferencja wysokiego szczebla na temat e-administracji
- **21-22 marca 2019, Cluj**
  – Start-up Europe Summit

- **14-15 maja 2019, Timisoara**
  – E-commerce Interactive Dialogue oraz Danube Strategy Event
- **28-29 maja 2019, Bukareszt**
  – Bucharest CyberDrill
- **13-14 czerwca 2019, Bukareszt**
  – Zgromadzenie Cyfrowe

CYBERPOLICY

NASK

cyberpolicy.nask.pl