PISM POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

POLICY PAPER

NR 22 (208), GRUDZIEŃ 2021 © PISM

Redakcja: Sławomir Dębski, Patrycja Sasnal, Wojciech Lorenz

Cyfrowy protekcjonizm: lokalizowanie danych

Oskar Szydłowski

W ostatnich latach, wykorzystując pretekst ochrony bezpieczeństwa narodowego oraz prywatności obywateli, państwa wprowadziły szereg środków protekcjonistycznych w odniesieniu do danych cyfrowych. Najważniejszym z nich jest prawo lokalizowania danych, nakazujące przechowywanie i przetwarzanie danych w określonym państwie. W praktyce często służy ono rządom autorytarnym do uzyskiwania większego nadzoru nad obywatelami dzięki nieograniczonemu dostępowi do danych oraz kontroli nad nimi. Ponadto ma negatywny wpływ na światową gospodarkę, zwłaszcza na handel międzynarodowy. Wyzwaniem pozostaje stworzenie regulacji na poziomie globalnym w miejsce niekompatybilnych systemów lokalnych.

Prawo lokalizacji danych wprowadza ograniczenia geograficzne w odniesieniu do przetwarzania i przechowywania danych. Jest ono cyfrową formą innego środka protekcjonistycznego – wymogów lokalnej zawartości, które precyzują, jaka część produktu musi zostać wyprodukowana bądź nabyta w danym państwie. Istnieją dwa rodzaje lokalizacji danych: miękka (stale aktualizowana kopia danych musi znajdować się w danym państwie) oraz twarda – zakazująca przetwarzania danych poza krajem i w ten sposób uniemożliwiająca ich transfer za granicę. Dotyczą one przede wszystkim danych osobowych i handlowych wytworzonych w danym państwie – są zatem skierowane do firm przetwarzających takie dane, np. dużych platform internetowych. Ogromna większość tego typu rozwiązań odnosi się jedynie do „danych w spoczynku" (nieaktywnych, przechowywanych), w przeciwieństwie do „danych w ruchu" (w trakcie transferu np. z jednego serwera na inny), co do których ograniczenia wymagałyby zmian w infrastrukturze technicznej internetu.

Prawo lokalizowania danych na świecie

Rozwiązania ograniczające dostęp do danych i zwiększające ich ochronę, takie jak lokalizowanie danych, zyskały popularność w drugiej dekadzie XXI w., w szczególności po arabskiej wiośnie (2010–2012) oraz ujawnieniu przez Edwarda Snowdena skali inwigilacji społeczeństw przez amerykańskie służby (w 2013 r.).

Rozwiązania ograniczające dostęp do danych i zwiększające ich ochronę, takie jak lokalizowanie danych, zyskały popularność w drugiej dekadzie XXI w., w szczególności po arabskiej wiośnie (2010–2012) oraz ujawnieniu przez Edwarda Snowdena skali inwigilacji społeczeństw przez amerykańskie służby (w 2013 r.). W ostatnich latach ponad 70 krajów zaktualizowało istniejące bądź wprowadziło nowe przepisy z tego obszaru.

Można wyróżnić trzy podejścia do lokalizowania danych: otwarte, restrykcyjne i hybrydowe. Najczęściej są one zbieżne ze stosunkiem danego państwa do kwestii globalizacji, barier handlowych i współpracy międzynarodowej. Podejście otwarte (liberalne) charakteryzuje się minimalnymi ograniczeniami w przetwarzaniu i przechowywaniu danych oraz w pełni wolnymi przepływami zagranicznymi. Takie stanowisko reprezentują USA, Wielka Brytania, Japonia i Nowa Zelandia. Nie oznacza to, że prywatność danych nie jest tam chroniona, bądź że wszystkie dane mogą przekraczać granicę. Ograniczenia stosowane przez te kraje są minimalne i dotyczą np. danych medycznych czy militarnych.

Stanowisko restrykcyjne oznacza stosowanie twardego prawa lokalizacji danych, często wzmocnionego regulacjami, które rozszerzają prawo do danych w ruchu. Takie podejście realizują Chiny, Rosja, Indonezja czy Nigeria. Rosja i Chiny wprowadziły lokalizowanie danych odpowiednio w 2015 r. (Ustawa Federalna nr 242 zaostrzona w 2019 r.) i 2017 r. (Prawo cyberbezpieczeństwa). Oba państwa planują ponadto rozszerzenie restrykcji wobec dostawców usług internetowych w celu centralizacji i zwiększenia kontroli nad lokalnym internetem. Część działań została już podjęta w wyniku uchwalenia prawa dotyczącego tzw. suwerennego internetu w Rosji oraz regulacji o zarządzaniu bezpieczeństwem danych w Chinach. Zasady te stanowią istotną ingerencję w sferę techniczną globalnego funkcjonowania internetu. W wyniku ich wprowadzenia część firm wycofała swoje usługi z rynków obu państw. Działalność tych, które według regulatorów nie przestrzegały nowych przepisów, została zakazana, (np. LinkedIn w Rosji).

RODO nie odnosi się wprost do lokalizowania danych, jednak w praktyce ogranicza ich eksport, gdyż jako zagraniczny transfer traktowany jest również dostęp do nich spoza UE.

Podejścia hybrydowe zakładają jedynie podstawowe ograniczenia geograficzne w odniesieniu do danych, najczęściej w formie lokalizacji miękkiej. Stosują je także państwa, które złagodziły swoje wcześniejsze – restrykcyjne – przepisy lokalizowania, m.in. Indie i Wietnam. Specyficznym przypadkiem jest Unia Europejska, która kładzie bardzo duży nacisk na ochronę prywatności danych. Wykorzystuje w tym celu Ogólne rozporządzenie o ochronie danych (RODO), które reguluje przetwarzanie danych w UE, dopuszczając ich transfer za granicę jedynie do państw i organizacji, które realizują politykę ochrony danych zgodną z unijnymi przepisami. RODO nie odnosi się wprost do lokalizowania danych, jednak w praktyce ogranicza ich eksport, gdyż jako zagraniczny transfer traktowany jest również dostęp do nich spoza UE.

Prywatność i bezpieczeństwo narodowe

Dwa główne argumenty, które są wykorzystywane przez rządy w celu wprowadzenia prawa lokalizowania danych, odnoszą się do ochrony prywatności danych oraz bezpieczeństwa narodowego. Oba postulują ograniczenie dostępu do danych, zwłaszcza podmiotom zagranicznym. Lokalizowanie danych faktycznie ogranicza ten dostęp, jednak tylko w przypadku lokalizacji twardej z uniemożliwieniem międzynarodowych transferów. W przeciwnym przypadku stale aktualizowana kopia danych może być przechowywana poza granicami państwa. Lokalizowanie danych ułatwia natomiast dostęp do nich aparatowi państwa, w którym są zlokalizowane (w tym służbom specjalnym i organom ścigania), co umożliwia rozwój cyfrowego autorytaryzmu wykorzystującego powszechny nadzór i cenzurę. Stanowi to istotne zagrożenie dla demokracji oraz praw człowieka, takich jak prawo do wolności słowa czy dostępu do informacji o działaniach władz.

Geograficzna lokalizacja danych nie ma bezpośredniego wpływu na ich bezpieczeństwo. Może być także niekorzystna dla bezpieczeństwa narodowego, ponieważ po przyjęciu tego rozwiązania liczba centrów przechowujących dane zwiększa się, czyniąc je bardziej podatnymi na ataki. Co więcej, nie wszystkie państwa posiadają odpowiednią infrastrukturę czy zasoby ludzkie, by zapewnić odpowiedni standard bezpieczeństwa krajowych centrów danych. Im więcej jest różnych praw lokalizowania danych w skali międzynarodowej, tym trudniejsze jest także ich współdzielenie, np. przez służby wywiadowcze różnych państw czy przez instytucje międzynarodowe. Prowadzi to też do ograniczenia współpracy międzynarodowej oraz funkcjonowania państw w odrębnych cyfrowych sieciach, gdzie przepływ informacji ze świata zewnętrznego jest ograniczony, co zwiększa izolację państw i sprawia, że działania dyplomatyczne stają się trudniejsze.

Konsekwencje ekonomiczne

Dane stają się głównym motorem światowego wzrostu gospodarczego, a zależność ta będzie rosnąć wraz z procesami cyfryzacji i automatyzacji. Przyśpieszenie widoczne jest już teraz – w konsekwencji pandemii COVID-19 ruch internetowy wzrósł o kilkadziesiąt procent rok do roku, a wiele usług, w tym publicznych, zostało przeniesionych do sfery cyfrowej. Wartość dodaną przepływu danych między granicami szacowano w 2014 r. na 2,8 bln dol. W przypadku UE szacunki wskazują, że w 2030 r. wartość dodana będąca efektem zagranicznych transferów danych, nie uwzględniając transferów wewnątrz Unii, wyniesie 3 bln euro.

Lokalizowanie danych znacząco ogranicza możliwość ich przepływu między granicami, drastycznie zwiększając – zarówno w przypadku lokalizacji miękkiej, jak i twardej – koszt prowadzenia działalności gospodarczej, zwłaszcza międzynarodowej. Koszt utrzymywania i aktualizowania kopii danych może stanowić barierę wejścia na poszczególne rynki. Dotyczy to najbardziej małych

i średnich przedsiębiorstw bądź firm planujących umiędzynarodowienie działalności. W konsekwencji konkurencyjność i innowacyjność gospodarki są hamowane, a faworyzowane są ponadnarodowe korporacje, które prawdopodobnie przerzucą na konsumentów wyższe koszty hostingu i innych usług. Lokalizowanie danych jako środek protekcjonistyczny, choć ogranicza konkurencję z zewnątrz, jednocześnie zamyka obywatelom dostęp do usług zagranicznych, które mogą być tańsze lub których odpowiedników nie ma na rynku krajowym. Badania wykonane przez firmę doradczą Frontier Economics na zlecenie Komisji Europejskiej (KE) szacują straty w wysokości 2 bln euro i do 2 mln miejsc pracy na koniec dekady cyfrowej (do 2030 r.), jeśli międzynarodowy przepływ danych nie zostanie zliberalizowany. Ponad połowa poniesionych strat ma wynikać z lokalizacji danych przez samą UE.

W kierunku globalnych rozwiązań

Najgłośniejszym wezwaniem do prac nad globalnym rozwiązaniem kwestii lokalizacji danych był „Digital Economy Report" Konferencji Narodów Zjednoczonych ds. Handlu i Rozwoju (UNCTAD), który opublikowano 29 września br. Wskazywał on, że obecnie największą wartość z danych pozyskuje niewielka grupa państw i dużych firm technologicznych. Jest to jednak wartość o wiele niższa niż możliwa do uzyskania, co jest niekorzystne zwłaszcza dla państw rozwijających się i dla lokalnych przedsiębiorstw. Raport wskazuje na potencjalne korzyści globalnej regulacji nie tylko w wymiarze redukcji nierówności między państwami i zwiększenia wartości dodanej pozyskiwanej z danych, lecz także wzrostu zaufania do gospodarki cyfrowej. UNCTAD aktualnie nie prowadzi prac nad rozwiązaniem, które mogłoby być przyjęte globalnie, istnieją jednak polityczne i techniczne fora światowej współpracy w sprawie międzynarodowych przepływów danych – np. w ramach WTO toczą się negocjacje dotyczące e-handlu. Zawarcie porozumienia pozostaje jednak dalekie, gdyż państwa rozwijające się, głównie Chiny, wskazują na potrzebę zbadania wyzwań i konsekwencji związanych z lokalizowaniem danych przed rozpoczęciem faktycznych rozmów.

Zawarcie porozumienia pozostaje jednak dalekie, gdyż państwa rozwijające się, głównie Chiny, wskazują na potrzebę zbadania wyzwań i konsekwencji związanych z lokalizowaniem danych przed rozpoczęciem faktycznych rozmów.

Można jednocześnie zaobserwować liczne próby tworzenia regionalnych i ponadregionalnych rozwiązań. Dane są jednym z głównych obszarów działań Rady ds. Handlu i Technologii współtworzonej przez UE i USA. USA już wcześniej, w ramach zastępującej NAFTA umowy Stany Zjednoczone – Meksyk – Kanada czy Partnerstwa Transpacyficznego (TPP), skutecznie przeforsowały własne liberalne podejście do przepływów danych, zakazując ich lokalizowania przez członków tych porozumień. Podobne zapisy znalazły się także w bilateralnych umowach handlowych podpisanych przez wiele państw regionu Azji i Pacyfiku.

Trzecią drogą osiągnięcia globalnej standaryzacji przepisów są systemy certyfikujące uzgadniane na poziomie międzypaństwowym. Działają one podobnie do decyzji wydawanych przez KE w sprawie transferu danych do państw trzecich w ramach RODO. Stanowią także kompromis między nieograniczonym przepływem danych a licznymi – niekompatybilnymi – krajowymi przepisami o lokalizacji danych. Najpopularniejszym tego typu systemem jest CBPR stworzony przez APEC (Wspólnotę Gospodarczą Azji i Pacyfiku). W jego ramach organizacje bądź kraje, które pozytywnie przejdą proces weryfikacji zabezpieczeń prywatności danych, mogą swobodnie przetwarzać dane pochodzące z obszarów partycypujących członków. Obecnie jest to dziewięć państw: Australia, Filipiny, Japonia, Kanada, Korea Południowa, Meksyk, Singapur, Tajwan i USA.

Wnioski i rekomendacje

W najbliższych latach należy oczekiwać wzrostu liczby przepisów lokalizujących dane w skali globalnej, a także rozszerzenia ich zakresu – na przykład na dane w ruchu. Proces ten będzie miał miejsce przede wszystkim w krajach autorytarnych, na czele z Rosją i Chinami, które będą blokować globalne próby regulacji przepływów danych na poziomie WTO i ONZ. Jednocześnie rozwijane będą systemy certyfikacyjne (takie jak CBPR), będzie się także zwiększać liczba porozumień regionalnych znoszących istniejące ograniczenia. Zwiększa to ryzyko fragmentaryzacji (bałkanizacji) internetu, który w dużej mierze korzysta ze swojej otwartej i zdecentralizowanej architektury. Fragmentaryzacja nie doprowadzi do powstania konkurujących ze sobą sieci, lecz do wprowadzenia technicznych ograniczeń części ruchu internetowego. Państwa, które zdecydują się na takie rozwiązania, zyskają kontrolę nad sferą cyfrową, ale odczują negatywne konsekwencje ekonomiczne.

Z perspektywy Unii Europejskiej priorytetem powinno być osiągnięcie porozumienia z USA – głównym partnerem w obszarze technologii – oraz budowanie jak największej kompatybilności RODO z innymi systemami, zwłaszcza amerykańskim. W tym celu szczególnie istotne jest promowanie unijnego modelu – stawiającego w centrum prywatność danych użytkowników – wśród krajów rozwijających się, a także udzielanie im finansowej i technicznej pomocy w tym zakresie. Dalsze funkcjonowanie otwartego internetu zależeć będzie od tego, jak szeroką koalicję państw uda się zbudować UE oraz USA. Będzie to mieć pośredni wpływ na stan demokracji i ochrony praw człowieka na świecie. Jednocześnie UE powinna, w ramach trwających już projektów, zintensyfikować prace nad zwiększeniem unijnych możliwości przechowywania oraz przetwarzania danych. W ten sposób, zmniejszając bariery stojące przed przedsiębiorstwami, możliwe będzie obniżenie kosztów tego typu usług.

Dalsze funkcjonowanie otwartego internetu zależeć będzie od tego, jak szeroką koalicję państw uda się zbudować UE oraz USA.