PISM POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

POLICY PAPER

NR 4 (217), LIPIEC 2024 © PISM

Redakcja: Sławomir Dębski, Wojciech Lorenz

Zagrożenia związane z przetwarzaniem zagranicznych danych przez Chiny

Marcin Przychodniak

Popularność chińskich urządzeń elektronicznych, pojazdów elektrycznych, aplikacji zakupowych czy mediów społecznościowych daje ChRL dostęp do dużych ilości danych. Kontrola chińskich władz nad przetwarzaniem tych informacji oznacza możliwość ich wykorzystania przeciwko USA i UE. W interesie Unii i jej państw członkowskich jest zwiększanie w społeczeństwach świadomości zagrożenia i wzmacnianie regulacji działania chińskich podmiotów w ramach jednolitego rynku.

Skala zagrożenia

Chiny odpowiadają za ponad 23% międzynarodowych przepływów danych, a według szacunków International Data Corporation do 2025 r. będą kontrolować ich prawie 28%, wyprzedzając obecnego lidera, USA. Jednym z narzędzi ich pozyskiwania jest działalność chińskich firm na świecie – funkcjonowanie chińskich urządzeń elektronicznych (m.in. w ramach tzw. internetu rzeczy), telefonów komórkowych, pojazdów elektrycznych, monitoringu wizyjnego, aplikacji zakupowych i do wideokonferencji czy mediów społecznościowych. W większości tych sektorów chińskie firmy już posiadają największy udział w rynku, m.in. dzięki niższym cenom, możliwym za sprawą państwowych subsydiów. Dostawcy sprzętu do monitoringu wizyjnego – Dahua i Hikvision – mają monopolistyczną pozycję w większości państw Europy Środkowej (m.in. Rumunii, Mołdawii i Bułgarii). Chińskie firmy dostarczają też technologie monitoringu oparte na sztucznej inteligencji (m.in. dotyczące profilowania) do 67 państw na świecie (m.in. Niemiec, Francji, Włoch, Rumunii, Mongolii, Rosji i USA). W 13 państwach członkowskich UE zaangażowanie chińskich producentów w infrastrukturę 4G przekracza 50%. Dodatkowo dane pozyskiwane są przez ChRL bezpośrednio z sieci. Australian Strategic Policy Institute zidentyfikował m.in. zależną od Departamentu Propagandy Komitetu Centralnego (KC) Komunistycznej Partii Chin (KPCh) firmę Global Tone Communications Company, która rocznie przetwarza ponad 2 petabajty danych – ekwiwalent 20 mld zdjęć w mediach społecznościowych – głównie dotyczących AI i technologii rozpoznawania twarzy, i poddaje je analizie pod kątem zagrożeń dla bezpieczeństwa ChRL, a także wykorzystania przeciwko UE i USA.

Działania Chin służą im do poznawania poglądów społeczeństw zachodnich i oddziaływania na ich postawy, m.in. przez kształtowanie debaty dotyczącej ChRL.

Działania te służą Chinom do poznawania poglądów społeczeństw zachodnich i oddziaływania na ich postawy, m.in. przez kształtowanie debaty dotyczącej ChRL. Przetwarzanie zagranicznych danych stwarza także możliwość dzielenia się informacjami i narzędziami ich analizy z Rosją, która może to wykorzystać w działaniach wobec UE i NATO. Możliwe jest użycie przez Chiny pozyskanych danych w operacjach hybrydowych (np. wpływania na proces wyborczy, w tym na wybory w USA w br.), do dezinformacji, manipulacji czy nawet destabilizacji sytuacji społeczno-politycznej (jak np. podczas pandemii koronawirusa). Zagrożenia dotyczą również infrastruktury krytycznej, w tym np. powiązania danych osobowych z konkretnymi obiektami, np. pracowników lokalnej jednostki wojskowej. Systemy i oprogramowanie obsługujące chińskie samochody, w tym elektryczne, pozwalają producentom gromadzić dane lokalizacyjne użytkowników i informacje o okolicy. Duże ilości danych pozyskują również aplikacje zakupowe (np. SHEIN czy TEMU) i media społecznościowe. Możliwość poznania preferencji konsumentów i sugerowania wyboru ma zastosowanie w odniesieniu do produktów, ale może również służyć promocji przekazu społecznego czy politycznego o znacznym zasięgu (TikTok tylko w USA ma ponad 170 mln użytkowników, a w UE ponad 140 mln). Na zagrożenia z tym związane wskazywały m.in. raporty wywiadu estońskiego i norweskiego opublikowane w br. W 2022 r. TikTok przyznał (w ramach prowadzonego w firmie śledztwa dotyczącego wycieku informacji), że przekazał chińskiemu właścicielowi, firmie ByteDance, dane amerykańskich dziennikarzy, i zwolnił z pracy osoby za to odpowiedzialne.

Zacieśnianie kontroli ChRL

W 2017 r., podczas sesji poświęconej znaczeniu dużych zbiorów danych (*big data)* Biuro Polityczne KPCh uznało zwiększanie nadzoru organów państwowych i partyjnych nad przetwarzaniem informacji za istotny element modernizacji chińskiej gospodarki. Przewodniczący ChRL Xi Jinping zdefiniował wówczas dane jako jeden z czynników produkcji, który tak jak kapitał, technologia czy ziemia muszą podlegać

Xi Jinping zdefiniował dane jako jeden z czynników produkcji, który tak jak kapitał, technologia czy ziemia muszą podlegać wzmożonej kontroli instytucji partyjnych.

wzmożonej kontroli instytucji partyjnych. Dlatego w ostatnich latach chińskie władze zintensyfikowały działania w zakresie kontroli przekazywania informacji z sektora prywatnego do partii oraz instytucji państwowych. Już w 2018 r. w ponad 90% z 500 największych chińskich firm prywatnych istniały komórki KPCh. W zależności od znaczenia prywatnych firm dla bezpieczeństwa instytucje państwowe przejmują w nich 1% udziałów (tzw. złoty udział). W 2021 r. spotkało to ByteDance – właściciela TikToka.

Obowiązki chińskich firm w sferze przetwarzania danych określa przede wszystkim ustawa o cyberbezpieczeństwie z 2017 r. (nowelizowana w 2018 r. i 2022 r.). Jej przepisy w odniesieniu do *big data* rozwinęła ustawa o bezpieczeństwie danych z 2021 r. Definiuje ona kategorie i rangi zbieranych informacji, które mają wpływ na bezpieczeństwo kraju, oraz wprowadza kary finansowe za odmowę ich przekazania organom państwowym. Szczególny charakter ma ustawa w sprawie ochrony informacji prywatnych z 2021 r. Pod pozorem dbałości o prawa użytkowników wprowadziła dodatkowe mechanizmy nadzoru nad firmami technologicznymi przez Urząd ds. Cyberprzestrzeni (CAC). Na czele tej instytucji od 2018 r. stoi Zhuang Rongwen, jednocześnie wiceszef departamentu propagandy KC. Partyjny nadzór nad CAC zapewnia Centralna Komisja ds. Cyberbezpieczeństwa i Informatyzacji w ramach KC, której pracami od sierpnia 2023 r. kieruje prawdopodobnie Cai Qi, zaufany współpracownik Xi i członek Stałego Komitetu KPCh. Nadzór władz nad chińskimi firmami wzmacniają też regulacje eksportowe w zakresie „technologii przetwarzania informacji" z 2020 r., które zabraniają sprzedaży zagranicznym firmom produktów bez aprobaty władz. Dotyczy to m.in. systemów analizy tekstu, rozpoznania głosu i algorytmów sugestii treści. Są to często najważniejsze rozwiązania techniczne danej firmy, jak w wypadku wyjątkowego algorytmu rekomendacji TikToka odpowiadającego za międzynarodowy sukces aplikacji.

Chiny starają się też zwiększać wpływ na globalne regulacje dotyczące ochrony danych. W 2020 r. zaproponowały Globalną Inicjatywę Bezpieczeństwa Danych, którą wsparła m.in. Rosja, co znalazło wyraz w oświadczeniach po rozmowach Xi–Putin w 2022 i 2023 r. W tekście komunikatu po ich spotkaniu z 2024 r. nie wymieniono już jej nazwy, ale wskazano (tak jak w poprzednich latach) na współpracę obu państw w zakresie internetu rzeczy, bezpieczeństwa sieci i danych, m.in. w ramach oenzetowskiej grupy roboczej ds. bezpieczeństwa informacyjnego (2021–2025). Chińska inicjatywa i współpraca z Rosją były odpowiedzią na program ogłoszony w 2020 r. przez administrację Donalda Trumpa „Clean Network". Miał on aktywizować współpracę USA i państw demokratycznych wobec chińskich zagrożeń w obszarze 5G i sektora cyfrowego, obejmując m.in. rezygnację z udziału Huawei i ZTE w tworzeniu infrastruktury krytycznej.

Działania UE i USA

W UE sfera bezpieczeństwa jest domeną państw członkowskich. Są one odpowiedzialne za nadzór nad unijnymi przepisami o ochronie danych osobowych (RODO). Za ich złamanie w postaci nielegalnego przetwarzania danych osób nieletnich kary na chińskie firmy nałożyły już np. Irlandia i Holandia. Część państw członkowskich (Francja, Szwecja) podjęła też działania ograniczające udział chińskich firm w tworzeniu infrastruktury 5G, zgodnie z unijnymi zaleceniami ze stycznia 2020 r., których część krajów (np. Polska) nadal nie implementowała do swoich porządków prawnych. Wprowadzane są także ograniczenia dotyczące korzystania z chińskich kamer w monitoringu – w czerwcu br. zakaz w tej sprawie wprowadził m.in. Amsterdam. Rozwiązaniem przyjmowanym przez państwa członkowskie wobec przetwarzania danych przez Chiny są więc decyzje niedotyczące stricte kwestii bezpieczeństwa, ale pozycji firm na rynku, ograniczania skali ich działania i możliwości rozwoju, a w przypadku aplikacji internetowych i mediów społecznościowych także moderacji treści. W Polsce SHEIN i TEMU są obiektem postępowania UOKiK

Rozwiązaniem przyjmowanym przez państwa członkowskie wobec przetwarzania danych przez Chiny są więc decyzje niedotyczące stricte kwestii bezpieczeństwa, ale pozycji firm na rynku.

odnośnie do nieuczciwej konkurencji, czyli np. niezgodnego z wymogami prawa europejskiego informowania konsumentów. W maju br. Ministerstwo Finansów zapowiedziało też kontrole skarbowe tych podmiotów, choć na razie nie ma konkretnych informacji. W lipcu Ministerstwo Rozwoju i Technologii zapowiedziało współpracę z KE, aby przyśpieszyć działania mające zmusić platformy do funkcjonowania zgodnego z europejskim prawem. Komisja Europejska zapowiada bowiem zniesienie w bm. progu 150 euro zwalniającego z ceł produkty sprowadzane spoza UE, głównie za pośrednictwem chińskich platform. Podejście Komisji Europejskiej (KE) także koncentruje się nie tylko na kwestiach związanych z bezpieczeństwem, ale też na regulacjach funkcjonowania chińskich firm czy sprawach społecznych. Takim instrumentem stało się rozporządzenie w sprawie zagranicznych subsydiów zastosowane ostatnio przez KE wobec chińskiej firmy Nuctech, dostawcy systemów monitoringu w terminalach lotniczych i na przejściach granicznych. Jest ona oskarżana o wykorzystanie przewagi cenowej wynikającej z subsydiów do wygrywania przetargów, w tym finansowanych przez UE. W 2020 r. opracowanie przygotowane na zlecenie rządu kanadyjskiego informowało, że skanery RTG tej firmy mogą bez wiedzy użytkowników zbierać i przekazywać informacje, w tym do Chin.

KE wykorzystuje także Akt o usługach cyfrowych (DSA), który na firmy prowadzące serwisy o aktywnej liczbie użytkowników powyżej 45 mln nakłada obowiązek m.in. skutecznej moderacji treści (niezastosowanie się może skutkować karą do 6% globalnych obrotów firmy). W kwietniu br. KE rozpoczęła tę procedurę wobec SHEIN, w maju wobec PDD Group, właściciela marki TEMU (ma ponad 75 mln użytkowników w UE), a rok wcześniej w odniesieniu do TikToka. W br. KE wszczęła też śledztwo w sprawie łamania przez TikToka przepisów DSA w związku uruchomionym w kilku krajach Unii programem promocyjnym, który nagradzając użytkowników za częste korzystanie z aplikacji, miał uzależniać od niej dzieci, a jednocześnie zwiększać ilość gromadzonych danych. Po rozpoczęciu postępowania TikTok zawiesił kampanię. Na mocy Aktu o rynku cyfrowym z 2022 r. (DMA) KE we wrześniu 2023 r. wskazała ByteDance (razem z m.in. Amazonem, Alphabetem czy Metą) jako tzw. *gatekeepers*, co obliguje je do przejrzystości mechanizmów ochrony danych i niewykorzystywania dominującej pozycji rynkowej. TikTok i Meta odwołały się od tej decyzji. W czerwcu br. sąd w Luksemburgu odrzucił skargę TikToka, któremu przysługuje jeszcze prawo apelacji do Trybunału Sprawiedliwości UE. Od 2023 r. istnieje też w UE zakaz instalowania tej aplikacji na sprzęcie służbowym pracowników PE, KE i Rady Europejskiej oraz rekomendacja jej usunięcia z urządzeń prywatnych.

W USA próby przeciwdziałania zagrożeniom związanym z przetwarzaniem danych przez chińskie firmy podejmowane są zarówno na szczeblu federalnym, jak i stanowym. Na mocy National Defense Authorization Act amerykańskie instytucje obronne i związane z infrastrukturą krytyczną mają m.in. zakaz korzystania z urządzeń monitoringu wizyjnego dostarczanych przez Huawei, Hytera, Hikvision, Dahua i ZTE. Część z tych firm jest też objęta amerykańskimi sankcjami ze względu na udział w represjach wobec Ujgurów w Sinciangu. Administracja Trumpa w grudniu 2020 r. zakazała urzędnikom federalnym używania TikToka, choć z kilkoma wyjątkami (obejmującymi np. sytuacje dotyczące bezpieczeństwa narodowego, ścigania przestępczości czy badań na rzecz bezpieczeństwa). Zakazy używania aplikacji przez urzędników stanowych i firmy współpracujące z administracją funkcjonują w ponad 30 stanach USA. W 2020 r. administracja Trumpa próbowała na mocy rozporządzenia wykonawczego nakazać chińskiemu właścicielowi sprzedaż TikToka, co jednak najpierw podważył sąd, a potem (w 2021 r.) odwołał prezydent Joe Biden. W kwietniu br. Kongres ostatecznie przyjął, a prezydent podpisał ustawę o ochronie danych Amerykanów przed państwami wrogimi (ChRL, KRLD, Rosja, Iran), zgodnie z którą TikTok ma dziewięć miesięcy, aby sprzedać większościowe udziały podmiotowi spoza tych krajów – w przeciwnym wypadku nie będzie mógł działać w USA. Firma zaskarżyła tę decyzję w sądzie, powołując się m.in. na wolność słowa, co najpewniej wydłuży cały proces. Oficjalnie TikTok wyklucza taką transakcję, argumentując m.in., że nie pozwala na to zakaz sprzedaży algorytmów narzucony przez władze ChRL.

Obostrzenia w innych państwach i organizacjach

Oprócz UE i USA inicjatywy wymierzone w chińskie firmy przetwarzające dane podejmują też inne podmioty. W 2022 r. Wielka Brytania i Australia zakazały wykorzystywania w budynkach administracji państwowej sprzętu do monitoringu produkowanego przez Hikvision czy Dahua. Obostrzenia dotyczą także TikToka, a motywacja części państw ma źródło w braku możliwości nadzoru lokalnych władz nad działaniem aplikacji. W sierpniu 2023 r. zakaz używania TikToka wprowadził Senegal, domagając się od aplikacji blokowania treści wspierających liderów opozycji, które zdaniem rządu prowadziły do destabilizacji sytuacji społeczno-politycznej. Indie zakazały używania tej aplikacji dwukrotnie, najpierw na kilka dni w 2019 r., a w 2020 r. już całkowicie. Wiąże się to z nakazem usunięcia możliwości jej pobrania na urządzenia, podobnie jak łącznie 58 innych chińskich aplikacji (m.in. SHEIN czy WeChat), ponieważ zostały one uznane za zagrożenie dla suwerenności państwa. Obostrzenia obowiązują w Iranie (jako element systemu cenzury), Jordanii (po śmierci policjanta w wyniku zamieszek w 2022 r. wspieranych z wykorzystaniem platformy; zakaz wprowadzono czasowo, ale obowiązuje do dzisiaj), Kirgistanie (od sierpnia 2023 r. jako zagrożenie dla rozwoju nieletnich), Nepalu (od listopada 2023 r. pod zarzutami destabilizacji społecznej), Tajwanie (od grudnia 2022 r., ale tylko na urządzeniach należących do członków administracji), Uzbekistanie (od lipca 2022 r., ze względu na łamanie przepisów o ochronie danych użytkowników) i Kosowie (od czerwca br., na urządzeniach służbowych administracji państwowej).

Od marca 2023 r. wprowadzono też zakaz instalowania TikToka na urządzeniach służbowych w ramach NATO. Poszły za tym podobne obostrzenia w państwach członkowskich Sojuszu – Belgii, Danii, Estonii, Francji (dodatkowo w maju 2023 r. zakazano jej całkowicie na Nowej Kaledonii, traktując to jako element przeciwdziałania zamieszkom), Łotwie, Holandii, Norwegii, Wielkiej Brytanii, Kanadzie, a także u partnerów NATO – Australii i Nowej Zelandii czy w państwach neutralnych – Austrii, Irlandii i Malcie.

Wnioski i rekomendacje

Wraz z rosnącą ilością danych zagranicznych przetwarzanych przez chińskie podmioty, kontrolą tego procesu przez władze ChRL, a jednocześnie realizacją ich ambicji mocarstwowych, zwiększa się zagrożenie wrogiego wykorzystania pozyskanych informacji przeciwko UE i USA. Konsolidacja rządów przez KPCh, brak niezależnego sądownictwa i transparentności działań wykluczają możliwość zapobiegania nadużyciom przez właścicieli danych – inne państwa, firmy i osoby prywatne. Ten aspekt odróżnia też podmioty z Chin od korporacji amerykańskich, które nierzadko w równie agresywny sposób pozyskują dane i stosują podobne algorytmy, ale czynią to głównie z powodów biznesowych. W państwach demokratycznych, w tym w UE, istnieją mechanizmy zabezpieczające przed wykorzystaniem danych do działań niezgodnych z interesem państw członkowskich. Kwestie ochrony i dostępu do danych są już przedmiotem współpracy UE i USA w ramach Rady ds. Handlu i Technologii. Wraz z powołaniem nowej KE Rada powinna kontynuować prace, a sprawy bezpieczeństwa danych mogłyby stać się jednym z głównych obszarów jej działania. W tym kontekście potrzebne są jednocześnie – głównie na poziomie państw członkowskich – silniejsze środki ograniczające przetwarzanie danych przez podmioty z Chin.

Konsolidacja rządów przez KPCh, brak niezależnego sądownictwa i transparentności działań wykluczają możliwość zapobiegania nadużyciom przez właścicieli danych.

Jednym z nowych narzędzi mogłyby stać się ustawowe regulacje (a przynajmniej zalecenia władz) w sprawie wprowadzania restrykcji w poruszaniu się chińskich pojazdów elektrycznych w okolicy obiektów administracji i infrastruktury krytycznej, a także dostępu innych urządzeń przetwarzających dane (np. w ramach internetu rzeczy) w strefach wrażliwych z punktu widzenia bezpieczeństwa państwa. Warto rozważyć rozszerzenie na kolejne dziedziny (np. monitoring wizyjny) procedur określania „dostawców wysokiego ryzyka", które są wprowadzane przez państwa członkowskie przy

budowie sieci 5G. Uzasadnieniem takich działań może stać się unijny akt w sprawie danych z grudnia 2023 r., który w art. 23 zobowiązuje dostawców usług (w tym firmy z ChRL) do nieprzekazywania danych rządom państw trzecich. Dlatego kluczowe jest dokończenie przez część państw UE procesu dostosowania legislacji do standardów unijnych z 2020 r., w tym finalizacja przez Polskę nowelizacji kodeksu cyberbezpieczeństwa. Rozwiązaniem ograniczającym możliwość manipulacji treściami i promocji dezinformacji może być – zgodnie z postulatami organizacji pozarządowych – rozwój w UE platform dających użytkownikowi możliwość wyboru systemów rekomendujących treści (nie uwzględniono tego w DSA). Ograniczyłoby to działanie algorytmów nastawionych na sugerowanie odbiorcy konkretnych treści (zamiast wymuszania ich wyboru przez użytkownika) i utrudniło ewentualne dotarcie z prochińskim przekazem. Wiąże się to również z koniecznością wzmocnienia edukacji społeczeństwa na temat sposobu działania korporacji cyfrowych, w tym z ChRL.

Na poziomie państw członkowskich UE i NATO podstawowym elementem jest wprowadzenie zakazu używania TikToka i innych chińskich aplikacji, np. Zoom, na urządzeniach należących do instytucji publicznych. W Polsce w tej kwestii obowiązuje jedynie rekomendacja Ministerstwa Cyfryzacji. Jest to szczególnie istotne w odniesieniu do podmiotów działających w obszarze infrastruktury obronnej i krytycznej.