Ograniczenia wiekowe to odpowiedź na uzależniającą architekturę platform cyfrowych – mówi prof. Mariusz Krzysztofek

Posted on 2026-06-30

Weryfikacja wieku i szerzej – regulacja dostępu do mediów społecznościowych na podstawie wieku, bo przecież po to ta weryfikacja ma być prowadzona – oraz przeciwdziałanie deepfake'om, to dwa najważniejsze wyzwania – mówi prof. Mariusz Krzysztofek, członek Społecznego Zespołu Ekspertów przy Prezesie UODO.

W Polsce trwają obecnie prace nad wdrażaniem unijnych przepisów o sztucznej inteligencji. Ich przeciwnicy często podnoszą argument, że tylko Unia reguluje AI, co krępuje biznes, a inni gracze, jak Chiny czy USA tego nie robią. Czy faktycznie tak jest, że w tych krajach nie ma w ogóle przepisów o sztucznej inteligencji?

Ograniczenia wiekowe to odpowiedź na uzależniającą architekturę platform cyfrowych – mówi prof. Mariusz Krzysztofek

To popularny mit, że wyłącznie Unia reguluje AI, a inni gracze – nie, i tu rzeczywiście najczęściej wskazuje się Stany Zjednoczone i Chiny. Jest prawdą, że Stany Zjednoczone nie przyjęły dotychczas ustawy federalnej regulującej kompleksowo sztuczną inteligencję, w sposób analogiczny do AI Act. Ten obszar podlega jednak licznym, choć rozproszonym regulacjom, o różnej randze, oraz typowemu dla tego państwa podejściu sektorowemu, oraz wielu ustawom na poziomie stanów. W Chinach też nie uchwalono kompletnej ustawy w tej dziedzinie, ale przyjęto wiele dojrzałych regulacji na różnych poziomach legislacji, z których szczególnie ważne są te wydawane przez Chińską Administrację Cyberprzestrzeni (CAC). W Chinach ogłoszono też plany prac legislacyjnych Rady Państwa – czyli rządu – i Stałego Komitetu Ogólnochińskiego Zgromadzenia Przedstawicieli Ludowych – czyli Parlamentu.

Dobrym, aktualnym przykładem pokazującym, że teza, jakoby tylko Unia regulowała AI, jest mitem, są chińskie przepisy CAC dotyczące oznaczania treści syntetycznych generowanych przez sztuczną inteligencję. Gdy w Europie nadal czekamy na ostateczne wytyczne Komisji Europejskiej dotyczące stosowania art. 50 AI Act, a część obowiązków jest przedmiotem prac w ramach AI Omnibus, w Chinach te obowiązki weszły w życie już we wrześniu 2025 r.

A wychodząc poza te kraje – AI Act pozostanie zawsze pierwszym, ale od stycznia 2026 r. nie już jedynym na świecie kompleksowym aktem prawnym regulującym sztuczną inteligencję, bo w Korei Południowej weszła w życie ustawa o rozwoju sztucznej inteligencji, która jest drugim na świecie po AI Act i pierwszym w Azji kompleksowym aktem tej rangi regulującym sztuczną inteligencję. Podkreślę – ustawowej rangi, bo jak wspomniałem w Chinach jest wiele szczegółowych regulacji rangi niższej, ale niezwykle ważnych w tym systemie prawnym.

Jaka jest różnica w podejściu chińskim, amerykańskim i europejskim do uregulowania tej dziedziny?

Jak wspomniałem wcześniej, ani w Chinach ani w Stanach Zjednoczonych nie uchwalono kompleksowej ustawy regulującej AI na szczeblu odpowiednio centralnym ani federalnym,

ale przyjęto liczne, rozproszone regulacje o różnej randze w tej dziedzinie. W Stanach sztuczna inteligencja na poziomie federalnym jest regulowana po pierwsze w formie prezydenckich Rozporządzeń Wykonawczych (Executive Orders). Jednak nie można ich porównywać z AI Actem, nie określają bowiem systemowo obowiązków dostawców i podmiotów stosujących ani innych uczestników rynku, lecz politykę i strategię władz federalnych wobec AI. Na tym szczeblu AI jest regulowana również w ramach podejścia sektorowego, np. w sektorze finansowym oraz w niewiążących wytycznych.

Są też liczne regulacje w dziedzinie sztucznej inteligencji na poziomie stanowym. Proces legislacyjny, którego przedmiotem były ogólne ustawy o sztucznej inteligencji, został zakończony w sześciu stanach: Kalifornii, Utah, Kolorado, Teksasie, Illinois i Nowym Jorku (w odróżnieniu od licznych ustaw sektorowych regulujących zastosowania AI, których przyjęto już kilkadziesiąt – w około połowie stanów).

A jak to wygląda w Państwie Środka?

W Chinach AI jest regulowana przez rozporządzenia administracyjne Rady Państwa, przepisy lokalne (np. w miastach na prawach prowincji), przepisy resortowe (wydawane przez ministerstwa i agencje rządowe), ale szczególne znaczenie mają w tej dziedzinie regulacje wydawane przez Chińską Administrację Cyberprzestrzeni (CAC). U podstawy tej piramidy znajdują się standardy i normy, zarówno obligatoryjne, jak i rekomendowane, ale nawet te drugie są ważnymi instrumentami zapewniania zgodności, bo ich dobrowolna implementacja pozwala wykazać zgodność z prawem.

Interesującym elementem chińskiego procesu legislacyjnego w obszarze nowych technologii jest stosowanie pilotaży, a następnie etapowego wdrażania przepisów. Do najważniejszych w dziedzinie AI regulacji CAC, czyli głównego chińskiego organu nadzorującego internet i bezpieczeństwo danych, należą rozporządzenia administracyjne dotyczące: algorytmów rekomendacji, algorytmów głębokiej syntezy (deepfake’ów) i generatywnej AI. Jednym z rozwiązań jest prowadzony przez CAC rejestr generatywnych narzędzi AI.

No właśnie, jak sobie te państwa radzą z generatywną AI i jej skutkami, tj. deepfake'ami?

To ważna dziedzina, dostrzegana przez ustawodawców w obu krajach. W Stanach wspólnym mianownikiem ustawy federalnej („Take It Down Act") i ustaw stanowych jest to, że są skierowane głównie na przeciwdziałanie niechcianym deepfake'om o charakterze seksualnym, w niektórych stanach szczególnie zawierającym wizerunki dzieci, a często również przeciwko deepfake'om zmierzającym do manipulacji procesem wyborczym.

Wspominałem już o niektórych chińskich regulacjach w tej dziedzinie, ale dodam jeszcze przykłady przepisów zakazujących oferowania różnym użytkownikom różnych cen w oparciu o zebrane cechy osobowe lub historię zachowań oraz wymagających od dostawców usług internetowych uwzględniania potrzeb starszych użytkowników, szczególnie w kontekście zapobiegania oszustwom.

Czyli Chińczycy mają zakaz profilowaniu użytkowników? Kłóci się to z kolejnym popularnym mitem dotyczącym powszechnego w Państwie Środka „social scoringu". Jak to naprawdę wygląda w Chinach – zarówno w sferze prawa, jak i praktyki?

Nie ująłbym tego jako absolutny zakaz profilowania, nie jest ono całkowicie zabronione również w Unii, ale profilowanie w celach komercyjnych zostało w Chinach poddane rygorom, które w pewnych aspektach idą daleko; to m.in. zakaz dyskryminacji cenowej przez algorytmiczne różnicowanie cen, a przeciwdziałanie oszustwom na szkodę starszych użytkowników wpisuje się w kulturowy szacunek dla tych osób w chińskim społeczeństwie.

A co do social scoringu – dominującym tonem komentarzy jest całkowita krytyka chińskiego systemu zaufania społecznego (Social Credit System), wręcz porównania do systemu orwellowskiego. Ale sądząc po tym, do jakich opisów tego systemu się ona odnosi zakładam, że dotyczy lokalnych programów pilotażowych sprzed korekt z 2021 r. Rzeczywiście, były bardzo inwazyjne, ale nie ma większego sensu wracanie do nich dzisiaj, bo rząd chiński zapowiedział w 2014 r. wdrożenie systemu zaufania społecznego do 2020 r., jednak

wdrożenie tak funkcjonującego systemu nie nastąpiło. Przykładem jest pilotaż prowadzony w mieście Rongcheng, w którym punkty w programie przyznawano za liczne społecznie pozytywne zachowania, jak segregowanie śmieci, działalność charytatywną, honorowe krwiodawstwo, a użytkownik tracił je za wykroczenia, przestępstwa, zaległości podatkowe i inne zaległości płatnicze, ale także np. za spędzanie nieproporcjonalnie wiele czasu na grach on-line. Te radykalne i sprzeczne z zasadami ochrony danych osobowych programy, po okresie pilotażu i krytyce, która na nie spadła, nie były w tej formie kontynuowane.

Do głównych celów systemu w obecnym kształcie, należą te gospodarcze (więc system obejmuje również, a nawet w istotnym stopniu przedsiębiorców), z których podstawowym jest wywieranie presji na niesolidnych dłużnikach. Powołana przez Kongres USA Komisja do analizy relacji gospodarczych z Chinami oceniła ten system w obecnym kształcie jako odpowiednik sytuacji, w której amerykańskie instytucje podatkowe, śledcze, edukacyjne, sądy, komisariaty policji i kluczowe przedsiębiorstwa użyteczności publicznej udostępniałyby swoją dokumentację na jednej platformie.

System czarnej i białej listy (w Chinach nazywanej czerwoną) istnieje i obejmuje nie tylko podmioty gospodarcze, ale też osoby fizyczne. Jednak w ich przypadku istotą czarnej listy są rejestry niesolidnych dłużników. System opiera się na założeniu, że osoby niewywiązujące się z obowiązku spłaty zadłużenia (laolai) nie powinny kupować dóbr luksusowych, m.in. biletów lotniczych i na koleje dużych prędkości lub pierwszej klasy, noclegów w hotelach wysokiej kategorii, korzystać z pól golfowych, kupować nieruchomości, kupować pojazdów, które nie służą prowadzeniu działalności gospodarczej, opłacać czesnego w drogich szkołach prywatnych.

Ograniczenia wiekowe to odpowiedź na uzależniającą architekturę platform cyfrowych – mówi prof. Mariusz Krzysztofek

Wpis na listę nie jest profilowaniem, ponieważ nieuiszczenie płatności jest faktem, a nie wynika ze statystycznie prawdopodobnego wnioskowania. Skoro w przypadku osób fizycznych głównym celem jest wywieranie presji na niesolidnych dłużników, to z perspektywy europejskiej i amerykańskiej ma funkcje zbliżone do znanych z wielu krajów rejestrów kredytowych i rejestrów długów. Około 1% firm i tylko 0,3% osób fizycznych rocznie dotykają sankcje wynikające z funkcjonowania Social Credit System (to dane z 2023 r.). Nie oznacza to, że system nadzoru, np. powszechne kamery, nie istnieje, jednak to zupełnie inny temat.

Czy chińskie firmy realnie przestrzegają zasad RODO i czy organy UE i państw członkowskich mogą to na nich wymusić? Bo w przypadku np. chińskich platform sprzedażowych egzekucja przepisów pozostawia wiele do życzenia.

W rzeczywistości egzekucja RODO wobec chińskich podmiotów to walka dwóch prędkości: giganci tacy jak TikTok czy Alibaba deklarują zgodność i tworzą europejskie centra danych, by uniknąć dotkliwych sankcji operacyjnych, podczas gdy wiele mniejszych platform pozostaje poza zasięgiem unijnego nadzoru ze względu na brak fizycznej obecności w UE, chociaż adresują towary lub usługi do Europejczyków. Przy czym decyzja irlandzkiego Data Protection Commission z 30 kwietnia 2025 r. i kara w wysokości 530 mln euro nałożona na TikToka za transfery danych do Chin w formie zdalnego dostępu pracowników ByteDance oraz niewykazanie równoważnego poziomu ochrony pokazują, że po pierwsze, nawet tacy giganci niekoniecznie zapewniają zgodność z RODO. A po drugie, odpowiada to na Pana pytanie o sprawczość Unii – przynajmniej na poziomie prowadzenia postępowań i nakładania sankcji.

W opublikowanym 11 czerwca orzeczeniu Irish High Court podtrzymał znaczną część

działań egzekucyjnych organu ochrony danych przeciwko TikTokowi i potwierdził, że ten naruszył przepisy RODO o transferach i o transparentności, chociaż kwestia zawieszenia transferów może jeszcze wymagać rozpatrzenia, więc piłka nadal jest w grze. Przypadki takie, jak postępowania wobec TikToka pokazują asymetrię europejskiej suwerenności cyfrowej. Z jednej strony Unia dysponuje potężnymi regulacjami i sankcjami finansowymi, z drugiej jednak cierpi na deficyt niezależności technologicznej. Brak własnej infrastruktury chmurowej, modeli AI czy ekosystemów e-commerce, które kontrolują dziś Amerykanie i Chińczycy, sprawia, że unijna sankcja ostateczna w postaci groźby odcięcia od europejskiego rynku staje się trudna do realnego wyegzekwowania.

Może trochę na marginesie, ale warto pamiętać, że presja regulacyjna ze strony Europy w obszarze nowych technologii coraz częściej uruchamia szerszą grę geopolityczną, w której chińska administracja aktywnie wspiera swoich narodowych czempionów. Tu przykładem jest ograniczanie udziału Huawei w budowie sieci 5G z powodu obaw o cyberbezpieczeństwo i ryzyko tzw. backdoorów. Jednocześnie sankcje amerykańskie – w tym ograniczenie dostępu do usług Google – nie wyeliminowały tego producenta z rynku. W niektórych segmentach Huawei wręcz umocnił pozycję i osiągnął bardzo wysokie wyniki sprzedaży.

Wskazał Pan na słabość UE w egzekwowaniu przepisów wobec BigTechów. Czy zgodzi się Pan z tezą, że koszmarem wielkich korporacji byłoby „europejskie prawo egzekwowane po amerykańsku?”

Amerykańska metoda egzekwowania jest faktycznie inna, choć trudna do porównania z europejską z jednego zasadniczego powodu. My mamy prawo obejmujące całą UE, w którym są jasno wskazane sankcje. Amerykanie nie mają ustawy na poziomie federalnym, choć dwa razy próbowali je przyjąć w ostatnich latach. Mają zamiast tego mozaikę przepisów stanowych. W wielu przypadkach te przepisy nie mają jednak takiego poziomu kompleksowości, jak RODO – chociaż na przykład w Kalifornii jest on zbliżony. I tam działa

regulator, który może się upomnieć o jego przestrzeganie.

Po drugie, zupełnie inny jest mechanizm karania.

W Europie sufit kary wyznacza pułap 20 milionów EUR albo 4% globalnego obrotu firmy, w zależności od tego, która z tych kwot jest wyższa. W USA karę nalicza się „od liczby naruszeń", czyli upraszczając: od każdego pojedynczego użytkownika, którego prawa naruszono, więc gdyby ten sam mechanizm zastosować bezwzględnie wobec administratora mającego miliony klientów, kwoty stałyby się zabójcze. Stawki są różne, w zależności od ustawy, ale np. w przypadku kalifornijskiego Prokuratora Generalnego i organu ochrony danych CPPA wynoszą do 2500 USD za każde nieumyślne i do 7500 USD za każde umyślne naruszenie lub dotyczące danych osób poniżej 16. roku życia. To mógłby być ten amerykański koszmar, który na szczęście na razie się nie ziścił. Kiedy w Kalifornii ukarano europejski podmiot – sieć Sephora – za działania, które na marginesie są tam kwalifikowane jako „sprzedaż danych" (z europejskiej perspektywy rozumiemy ją inaczej), to kara wyniosła 1,2 miliona USD.

Czy analogicznie UE ma szanse wymusić przestrzeganie innych przepisów z pakietu nowo technologicznego, jak np. AI Akt, ale też weryfikacja wieku użytkowników socialmediów, zwalczania dezinformacji czy deepfake'ów?

Myślę, że rzeczywiście weryfikacja wieku i szerzej – regulacja dostępu do mediów społecznościowych na podstawie wieku, bo przecież po to ta weryfikacja ma być prowadzona – oraz przeciwdziałanie deepfake'om, to dwa najważniejsze wyzwania w tym kontekście. Pierwsze – bo ograniczenia wiekowe to odpowiedź na uzależniającą architekturę platform cyfrowych. Ale Chiny w regulowaniu ochrony dzieci w internecie i przed deepfake'ami są dziś dalej niż Europa. Mają obowiązkową weryfikację wieku, bardzo restrykcyjne zasady dotyczące czasu korzystania z aplikacji, oraz regulacje dotyczących oznaczania deepfake'ów. Chińczyków nie trzeba na te zagrożenia uczulać.

Ograniczenia wiekowe to odpowiedź na uzależniającą architekturę platform cyfrowych – mówi prof. Mariusz Krzysztofek

W Europie, w Polsce też, dyskutujemy m.in. nad rozwiązaniami inspirowanymi głośną ustawą australijską o banie na określone (nie wszystkie) social media poniżej – w zależności od kraju – 15, 16 roku życia oraz nad sposobami weryfikacji wieku. W niektórych krajach te prace i proces legislacyjny są już zaawansowane. A w związku z Omnibus AI nad walką z nudify (czyli kreowaniem „rozbieranych" wizerunków innej osoby). Natomiast ilustracją chińskiego podejścia jest egzekwowanie (na podstawie przepisów Chińskiej Administracja Cyberprzestrzeni – CAC) dziennego limitu czasu gry, w tym możliwość automatycznego przerywania gry po jego przekroczeniu, aby zapobiegać uzależnieniu od gier i internetu, wraz z systemem rejestracji i weryfikacji tożsamości. Natomiast ocena chińskich przepisów to inny temat.

Ale czy Unia może wymusić przestrzeganie tych przepisów?

DSA już formułuje obowiązki dostawców bardzo dużych platform internetowych, dotyczące np. zapewnienia alternatywnej opcji rekomendacji treści, która nie opiera się na profilowaniu. Akt ten zakazuje też stosowania reklam opartych na profilowaniu wobec małoletnich, wymaga wysokiego poziomu prywatności i bezpieczeństwa dla tej grupy, wymusza też moderację, przejrzystość algorytmów oraz raportowanie ryzyk systemowych. I przewiduje sankcje za niedopełnienie tych obowiązków.

Wiemy też, że dokonano do tej pory konkretnych i – trzeba powiedzieć – niepokojących ustaleń. Orzeczenie wstępne Komisji Europejskiej i orzeczenie sądu w Stanach Zjednoczonych potwierdzają, że problem uzależniającego projektowania usług online ma charakter systemowy. Komisja Europejska stwierdziła, że funkcje projektowania o charakterze uzależniającym stosowane przez TikToka, w szczególności nieskończone przewijanie (infinite scroll) oraz automatyczne odtwarzanie treści, mogą prowadzić użytkowników do kompulsywnego korzystania z platformy, co narusza DSA.

A w pierwszym w USA procesie dotyczącym szkód wyrządzonych młodym użytkownikom przez media społecznościowe ława przysięgłych w Los Angeles uznała, że Meta i YouTube są

odpowiedzialne za celowe konstruowanie funkcji o charakterze uzależniającym, które doprowadziły do poważnych szkód w zdrowiu psychicznym dziecka. Wspominam o tym, bo argumentowano, że to współczesny odpowiednik „inżynierii uzależnienia", porównywanej do strategii stosowanych kiedyś przez przemysł tytoniowy.

Czyli powinniśmy traktować usługi cyfrowe jak szkodliwe używki?

I to jest ważna konkluzja – jest w tym kontekście formułowany argument, że Big Techy po prostu oferują produkt, z którego wystarczy nie korzystać. Otóż nie – oferują produkt wyposażony w funkcjonalność, której celem jest uzależnienie od niego, a znaczącym segmentem klientów są dzieci. Analogia do procesów przegranych kiedyś przez koncerny tytoniowe jest słuszna, przy czym nikt, włącznie z producentami, nie kwestionuje zakazu sprzedaży papierosów dzieciom, a próby uregulowania dostępu wieku do social mediów są oceniane jako zamach na wolność.

A więc Unia może zrobić tutaj całkiem dużo, a kary finansowe to jeden ze sposobów, Może też wymagać wyjaśnień, audytów, i w skrajnych przypadkach zawieszać usługi. Ale globalne platformy zawsze będą prowadziły grę na dwóch boiskach – regulacyjnym i politycznym – i tu napięcie rośnie. Przykład: w USA ByteDance został zobowiązany do sprzedaży TikToka podmiotowi niezwiązanemu z Chinami, pod groźbą zakazu działania aplikacji w USA.

Niektórzy zwracają jednak uwagę, że treści, które TikTok oferuje młodzieży na Zachodzie, są znacznie bardziej szkodliwe niż te kierowane do młodych Chińczyków. Wskazuje się nawet, iż jest to pewnego rodzaju zemsta za wojny opiumowe – zalewanie Europy i USA „cyfrową trucizną", co powoduje uzależnienia, osłabienie koncentracji, kryzys zdrowia psychicznego itd. Chodzi więc bardziej o zmuszenie chińskich platform, by dbały też o bezpieczeństwo użytkowników w Europie.

Porównanie do „cyfrowego opium" i celowego podtruwania Zachodu przez Chiny jest głośne. Dotyczy różnic polegających na tym, że Chiny młodym Chińczykom zapewniają TikToka w

wydaniu edukacyjnym, pożytecznym, a reszcie świata podsyłają wersję „opiumową", uzależniającą, pełną bezwartościowej treści. To, że zachodni TikTok nie jest platformą, którą należy rekomendować dzieciom i zostawiać je z nią na wiele godzin dziennie – bardzo przepraszam za sarkazm – to nie wymaga przekonywania, i mówiliśmy już tutaj o architekturze uzależniania i o badaniach potwierdzających destrukcyjny wpływ nadużywania tego rodzaju mediów na zdrowie psychiczne.

Ale nie mam żadnych dowodów, aby twierdzić, że Chiny, a więc chińskie władze celowo różnicują treści, aby te docierające do młodych użytkowników na Zachodzie były uzależniające i toksyczne w przeciwieństwie do tych chińskich. A boję teorii spiskowych.

Natomiast faktem jest, że to co dziecko lub nastolatek widzi na ekranie swojego telefonu w Chinach i na Zachodzie rzeczywiście się różni. Jest również faktem, że chińskie prawo chroni dzieci poniżej 14. roku życia przed uzależnieniami w sieci i przed toksycznymi treściami. Ale nikt nie zabrania ustawodawcom europejskim zrozumieć, że jest czas dyskusji i czas decyzji i wreszcie podjąć decyzję o dalszej ochronie dzieci w Europie. Można kręcić głową (w pełni to rozumiem!) nad chińskim modelem. Ale gdy jesteśmy zasypywani badaniami potwierdzającymi, że media takie jak TikTok (nie tylko on) mają destrukcyjny wpływ na dzieci to czas na dalej idące działania niż dyskusje, które nie mają końca.

Chiński regulator CAC wymaga od platform wdrożenia dla dzieci poniżej 14. roku życia „trybu młodzieżowego", czyli limitu czasu i korzystania, przestrzegania trybu nocnego i promowania materiałów patriotycznych, naukowych i historycznych. Na marginesie – chiński TikTok to Douyin, działa wyłącznie na rynku chińskim, ma tego samego właściciela, ale to nie ten sam podmiot co TikTok „zachodni", który w Chinach nie działa.

TikTok na Zachodzie, ale przecież nie tylko TikTok, bo dotyczy to po prostu platform, działa według kryterium „engagement" (zaangażowania, zainteresowania) i pozwala sobie na architekturę uzależnienia, o której wspominałem. Mamy DSA, ale… Powtórzę – nie mam podstaw aby twierdzić, że treści na platformach różnią się, bo tymi treściami steruje

zakulisowo chiński rząd. Otwarcie mówi, że chroni swoją młodzież, i zamiast pytać jak zmusić Chińczyków do tego, aby nie serwowali nam szkodliwych treści (nie wiemy nawet czy je serwują) należy działać tu, w Europie. Prawo europejskie jest kształtowane w Europie, a nie w Chinach.

Czyli, żeby to zmienić, musielibyśmy zacząć regulować treści, jakie mogą być udostępniane w tego rodzaju aplikacjach?

Regulacja treści nie może oznaczać cenzury prewencyjnej, w naszej kulturze prawnej i politycznej jest rzeczą niewyobrażalną. Ale pewne formy regulacji treści są stosowane. Unijny akt o usługach cyfrowych (DSA) wymaga moderowania contentu na platformach, przewiduje procedurę zgłaszania i usuwania treści nielegalnych, czyli niezgodnych z prawem Unii lub państwa członkowskiego. A więc np. pornografii dziecięcej lub wezwań do przemocy. Chociaż trzeba zwrócić uwagę na ryzyko efektu mrożącego – prewencyjnego usuwania treści, które nie są nielegalne, ale presja czasu oraz ocena ryzyka sankcji prowadzi do wniosku, że ich usunięcie jest decyzją pragmatyczną. Przykłady to usuwanie satyry jako mowy nienawiści czy materiałów z zakresu edukacji zdrowotnej kobiet jako pornografii. Ale trzeba podkreślić, że DSA przewiduje ten problem i nakazuje działać proporcjonalnie i z uwzględnieniem wolności wypowiedzi i mediów.

Myślę jednak, że zgodzimy się, że ocena wartości treści legalnych należy wyłącznie do ich odbiorców, a jeżeli odbiorcami są dzieci – również do ich rodziców. Wspominałem już o weryfikacji wieku i regulacji dostępu do mediów społecznościowych na podstawie wieku, ze względu na uzależniającą architekturę platform cyfrowych. Podsumowując, przez regulację treści rozumiałbym egzekwowanie DSA oraz więcej stanowczości w pracach legislacyjnych nad ograniczeniem wieku dostępu do mediów społecznościowych, a więc zasady bezpieczeństwa produktów BigTechów.

Czyli skuteczne zablokowanie tego dostępu dla małoletnich nie będzie łatwe?

Ograniczenia wiekowe to odpowiedź na uzależniającą architekturę platform cyfrowych – mówi prof. Mariusz Krzysztofek

W kontekście zakazu dostępu poniżej określonego wieku dotykamy jeszcze jednego ważnego wątku – trudno go teraz rozwijać, ale warto zasygnalizować. Rozróżnienie na platformy objęte zakazem i wyłączone spod zakazu pomija fakt, że na tej samej platformie, nawet jeżeli badania wskazują na jej potencjalnie szkodliwy wpływ na młodych użytkowników – publikowane są również treści pozytywne, których poszukuje świadomy, nieuzależniony nastolatek, takie jak kanały z poradami treningowymi, przepisami kulinarnymi czy historyczne. Kluczowe wyzwanie regulacyjne polega więc na tym, w jaki sposób ustawodawca może wymusić na platformach zdolność rozróżniania treści szkodliwych od wartościowych oraz ograniczenia praktyk projektowania uzależniającego młodych użytkowników.

Zakaz dostępu do określonej platformy poniżej ustalonego progu wieku, analogiczny do zakazu sprzedaży alkoholu nieletnim, skutecznie odcina młodych użytkowników od treści szkodliwych, lecz jednocześnie pozbawia ich dostępu do treści wartościowych, których twórcy nie mają zamiaru uzależniać odbiorców. Alternatywą wobec pełnego zakazu korzystania z mediów społecznościowych może być poprawa sposobu funkcjonowania platform zgodnie z DSA. Jednak zważywszy, że rezygnacja z architektury uzależniania użytkowników jest wbrew modelowi biznesowemu platform, ograniczenie dostępu poniżej określonego wieku może okazać się, wobec braku alternatywy i współpracy ze strony platform, pragmatycznym rozwiązaniem.

Podobnie sytuacja wygląda z platformami zakupowymi. Te dostępne w Europie to inne platformy, niż te, z których korzystają Chińczycy (a ceny na nich są jeszcze niższe). Czy to tylko i wyłącznie kwestia strategii cenowych i logistycznych, czy jest w tym jednak jakieś drugie dno?

Rzeczywiście w Europie korzystamy z innych chińskich platform zakupowych niż klienci w samych Chinach. Popularne w Europie Temu czy AliExpress są skierowane głównie do klientów zagranicznych, a w Chinach dominują platformy takie jak Taobao, Pinduoduo czy

JD.com. Warto też zauważyć, że Amazon nie prowadzi działalności e-commerce w Chinach.

Prawdopodobnie ekonomista odpowiedziałby na to pytanie bardziej precyzyjnie, ale chyba nie pomylę się, jeżeli powiem, że źródeł niezwykle niskich cen na chińskich platformach należy szukać przede wszystkim w ogromnej skali produkcji i konkurencji na tamtym rynku oraz niskich marżach i agresywnej polityce cenowej służącej zdobywaniu udziałów w rynku europejskim.

Przez wiele lat dodatkowym czynnikiem były również luki w europejskim systemie celnym dotyczące przesyłek o niewielkiej wartości, które dopiero w ostatnich latach zaczęły być stopniowo ograniczane.

Jak to jest z chińskimi obywatelami? Czy chińskie społeczeństwo jest takie grzeczne i karne? Czy wszyscy przestrzegają zakazów związanych z ograniczonym dostępem do całego internetu?

Na początku wyjaśnijmy na czym polega zakaz – system Great Firewall monitoruje i blokuje dostęp Chińczyków do globalnego internetu. A więc mają oni dostęp przede wszystkim do swojego chińskiego ekosystemu, natomiast usługi takie jak wyszukiwarka Google, poczta Gmail, YouTube, Facebook, WhatsApp, są zablokowane. Wielu chińskich użytkowników może tego braku nie odczuć jako dotkliwy, bo te aplikacje mają swoje lokalne odpowiedniki, a więc zamiast dominacji Google mają dominację wyszukiwarki Baidu, odpowiednikiem Facebooka jest WeChat. Zresztą ta „lokalność" chińskich aplikacji nie jest aż tak lokalna – np. WeChat ma ponad 1 mld użytkowników, trudno bez niego funkcjonować w Chinach, bo ma rozbudowaną funkcjonalność – komunikacji, rezerwacji usług, płatności, i jest jednym z dwóch głównych systemów płatności obok Alipay.

A czy Chińczycy omijają Great Firewall?

Sam mechanizm z VPN wydaje się oczywiście prosty, jednak to kraj bardzo zaawansowany technologicznie, więc – o ile wiem potwierdzają to statystyki – skala jest dużo mniejsza, niż

mogłoby się wydawać. Widziałem dane, że kilka procent użytkowników może korzystać z VPN. Chociaż dłuższy lub częstszy pobyt w dużych miastach i w środowiskach akademickich może pozwolić odnieść wrażenie, że ta statystyka jest większa.

Komisja Europejska zakazała swoim użytkownikom korzystania z TikToka, a chińskich dostawców potraktowano w NIS2 bardziej restrykcyjnie niż amerykańskich. Tymczasem w odniesieniu do USA mamy pewność, że dane przekazywane były służbom, a w przypadku Chin nie ma takiego potwierdzenia. Czy to jednak nie paradoks?

Rzeczywiście, sprawy Snowdena i Schremsa sprawiły, że widzieliśmy jak działają amerykańskie programy, takie jak PRISM na podstawie głośnej sekcji 702 ustawy FISA. Ale z drugiej strony unieważnianie kolejnych tarcz prywatności przez TSUE doprowadziło do korekty tych zasad po stronie amerykańskiej, nadania im proporcjonalności, wprowadzono też mechanizm zaskarżenia, bo powstał niezależny sąd ds. przeglądu ochrony danych.

Natomiast w Chinach obowiązek przekazywania danych jest wprost zapisany w prawie. Artykuł 7 chińskiej ustawy o wywiadzie narodowym z 2017 roku nakłada na wszystkie organizacje i obywateli bezwzględny obowiązek wspierania i współpracy z państwowymi organami wywiadowczymi.

Natomiast odnosząc się do NIS2 – to nie tylko TikTok, Huawei w budowie sieci 5G z powodu obaw o cyberbezpieczeństwo, ale też innym tego rodzaju zakazem jest niedopuszczanie chińskich samochodów na tereny baz wojskowych. Ale wszystkie te obostrzenia wynikają w tym przypadku nie z ochrony danych osobowych, a z kwestii bezpieczeństwa narodowego i cyberbezpieczeństwa. A pamiętajmy, że przepisy dotyczące bezpieczeństwa narodowego uzasadniają ograniczenie zakresu RODO, zresztą również AI Aktu nie stosuje się do systemów AI wykorzystywanych do celów bezpieczeństwa narodowego. Dzisiejszy samochód jest wyposażony m.in. w zestaw kamer, GPS, zbiera mnóstwo danych o otoczeniu i jest zarządzany z poziomu aplikacji producenta, więc świadomość tych zagrożeń, idących znacznie dalej niż ochrona danych osobowych, to nie kwestia uprzedzeń tylko dojrzałej

oceny ryzyka.

Czy najnowsze porozumienie o transferze danych do USA pozwala w końcu sądzić, że przekazywanie danych do tego państwa jest bezpieczne? Czy w związku z tym nie jest już potrzebna tak duża ostrożność przy przechowywaniu danych w chmurze?

W przeszłości podważenie Safe Harbor i Privacy Shield, miało swoje uzasadnienie (i samo ujawnienie przez Edwarda Snowdena programu PRISM w 2013 roku było wstrząsem) – szczególnie Safe Harbor. I powiedziałbym, że zarzut podnoszony wtedy i potem – masowej inwigilacji danych europejskich użytkowników przez National Security Agency przesłonił inny zarzut, moim zdaniem, nie mniej ważny. Biała Księga opublikowana później m.in. przez Departament Handlu pokazywała, że dla większości komercyjnych firm ryzyko inwigilacji przez amerykańskie służby jest marginalne. Wskazano, że w praktyce przeciętne przedsiębiorstwo przetwarzające zwykłe dane handlowe, kadrowe, logistyczne czy konsumenckie (np. transakcje w sklepach) w ogóle nie znajduje się w sferze zainteresowań agencji wywiadowczych (takich jak NSA).

Natomiast problemem powinno być, że ten mechanizm certyfikacji był wtedy fikcją, że deklaracje importerów amerykańskich o przynależności do Safe Harbor były składane, mimo że nie spełniały warunków tego programu. Na przykład lista wpisów znacznie przekraczała liczbę rzeczywistych uczestników programu, bo wielu nie odnowiło certyfikacji albo już nie istniało. A dziś mamy w tej sprawie spokój, kurz opadł. W wyroku z 3 września 2025 r. w sprawie Latombe Sąd UE utrzymał ważność decyzji o adekwatności EU–US Data Privacy Framework (DPF), bo potwierdził, że wprowadzone przez stronę amerykańską reformy zapewniają równoważny poziom ochrony, dają wystarczające gwarancje niezależności dla powołanego Data Protection Review Court i ograniczają działania wywiadowcze niezbędnego zakresu.

Przez lata uwaga opinii publicznej i regulatorów koncentrowała się głównie na transferach danych do Stanów Zjednoczonych, podczas gdy dużo mniej mówiło się o transferach do

innych państw trzecich, takich jak Chiny czy Rosja. Czy ta asymetria była uzasadniona i czy dziś patrzymy na te transfery inaczej?

To prawda, nawet jeżeli skutki Schremsa I i II są uniwersalne i obowiązek przeprowadzania Transfer Impact Assessment dotyczy także Chin i innych państw trzecich, to cała energia skupiła się na transferach do Stanów Zjednoczonych. Transfery do innych państw trzecich nie były w centrum uwagi. Chińskim elementem tej układanki – długo brakującym, bo debata była zdominowana przez wątek amerykański – była decyzja irlandzkiego organu ochrony danych z 2025 r. dotycząca TikToka i kara w wysokości 530 mln euro za transfer danych do Chin w formie zdalnego dostępu pracowników ByteDance oraz niewykazanie odpowiedniego poziomu ochrony. Zastrzeżenia kilku europejskich organów pojawiły się także wobec DeepSeek.

Ale mówiąc o tej asymetrii – uważam, że jeszcze bardziej uderzające jest to, że przez lata energia w sprawie transferów koncentrowała się na Stanach Zjednoczonych, natomiast praktycznie nie poświęcano uwagi Rosji. Ten brak jest zdumiewający, szczególnie w kontekście wojny w Ukrainie. Wprawdzie EROD w oświadczeniu wydanym po agresji Rosji na Ukrainę przypomniała eksporterom danych o konieczności oceny skuteczności zabezpieczeń, zwłaszcza w kontekście dostępu władz publicznych do danych, ale też znalazła się tam wzmianka o „bliskich więziach historycznych” niektórych państw europejskich z Rosją. Co w naszej części Europy, ze względu na historię, brzmi niedobrze. Trzeba było czekać do 2026 r. na decyzję holenderskiego organu ochrony danych, który nałożył na operatora europejskiej wersji aplikacji karę 100 mln euro za przekazywanie do Rosji danych osobowych z Norwegii i Finlandii.

Ograniczenia wiekowe to odpowiedź na uzależniającą architekturę platform cyfrowych – mówi prof. Mariusz Krzysztofek