Architektura cyfrowego zaufania: od ochrony danych po odporność demokracji w świecie Tools and Weapons

AUTOR

Fundacja Dobre Państwo

STRESZCZENIE / ABSTRACT

Artykuł analizuje przejście od centralizacji danych do modelu „Visit The Data", gdzie obliczenia są przenoszone bezpośrednio do źródeł informacji zamiast ich gromadzenia w jednym miejscu. Autor podkreśla różnicę między prawem do zasobu a prawem do operacji, co pozwala na analitykę bez utraty kontroli nad danymi przez pierwotnych dysponentów. Kluczowym elementem tej architektury jest zasada minimalizacji ekspozycji, realizowana poprzez technologie PET-s, takie jak prywatność różnicowa. W przeciwieństwie do prostej anonimizacji rozwiązania te chronią przed re-identyfikacją osób na podstawie quasi-identyfikatorów, wprowadzając kontrolowaną losowość do wyników statystycznych. To podejście buduje fundamenty cyfrowego zaufania i suwerenności informacyjnej w świecie zdominowanym przez algorytmy AI.

The article analyzes the transition from data centralization to the 'Visit The Data' model, where computations are moved directly to the information sources instead of gathering them in one place. The author emphasizes the difference between the right to a resource and the right to an operation, which allows for analytics without the original controllers losing control over the data. A key element of this architecture is the principle of exposure minimization, implemented through PETs technologies such as differential privacy. Unlike simple anonymization, these solutions protect against the re-identification of individuals based on quasi-identifiers by introducing controlled randomness into statistical results. This approach builds the foundations of digital trust and informational sovereignty in a world dominated by AI algorithms.

Artykuł analizuje krytyczny moment przejścia w architekturze informacji: od modelu centralizacji danych ku rozproszonemu zarządzaniu władzą poznawczą. Autor stawia

tezę, że w obliczu technologicznej ambiwalencji – gdzie narzędzia chroniące prywatność (takie jak kryptografia homomorficzna czy uczenie federacyjne) mogą współistnieć z algorytmami radykalizującymi społeczeństwa – niezbędne jest przejście od pasywnego pośrednictwa platform do pełnej odpowiedzialności za projektowanie środowisk informacyjnych. Tekst dowodzi, że technologia sama w sobie nie gwarantuje etyki ani suwerenności; może ona jedynie ograniczać możliwości nadużyć, podczas gdy prawdziwe bezpieczeństwo demokratycznych instytucji zależy od stworzenia „architektury odpornej niezgody". W tym ujęciu ochrona danych i walka z polaryzacją afektywną nie są problemami czysto technicznymi, lecz politycznymi i antropologicznymi. Kluczowym wyzwaniem staje się zatem nie tylko zabezpieczenie bitów przed dostępem, ale przede wszystkim ochrona wspólnego pola odniesienia faktualnego przed algorytmicznym rozszczepieniem, które przekształca wolność komunikacji w infrastrukturę plemiennej izolacji.

SŁOWA KLUCZOWE

architektura cyfrowego zaufania | visit the data | prywatność różnicowa | szyfrowanie homomorficzne | bezpieczne obliczenie wielostronne SMPC | uczenie federacyjne | minimalizacja ekspozycji | budżet prywatności | dozowanie władzy poznawczej | odporność demokracji | privacy-enhancing technologies PETs | automatyzacja sądu AI | suwerenność informacyjna | model query-only

Przeniesienie obliczeń do danych zamiast ich centralizacji

Algorytm, który odwiedza dane. Analityka bez przejmowania informacji. Skoro własność, kontrola i powiernictwo danych nie są tym samym, kolejny krok staje się niemal nieunikniony: trzeba zakwestionować przekonanie, że analiza informacji zawsze wymaga uprzedniego zgromadzenia ich w jednym miejscu. Przez większą część historii informatyki centralizacja była naturalnym warunkiem obliczeń. Dane sprowadzano do wspólnej bazy, ponieważ właśnie tam znajdował się komputer zdolny je przetworzyć. Najpierw budowano magazyn informacji, a dopiero później wpuszczano do niego analityka. Chmura doprowadziła tę logikę do skali przemysłowej. Jednak ta

sama dojrzałość technologiczna, która umożliwiła gigantyczną koncentrację danych, zaczyna obecnie podważać konieczność ich gromadzenia. Powstaje nowa maksyma architektury informacyjnej: nie zawsze trzeba przenosić dane do obliczeń; czasami można przenieść obliczenia do danych.

Źródłowy materiał ujmuje tę intuicję w niezwykle plastycznej formule Visit the Data. Dane pozostają tam, gdzie powstały lub gdzie sprawuje nad nimi kontrolę pierwotna instytucja – w szpitalu, laboratorium, przedsiębiorstwie czy jednostce administracji – natomiast algorytm "odwiedza" poszczególne zasoby, wykonuje dozwoloną operację i zwraca wynik. W modelu federacyjnym nie musi więc istnieć jeden gigantyczny magazyn zawierający kopie wszystkich rekordów. Można stworzyć wspólnotę analityczną bez budowania wspólnego archiwum. W źródłach idea ta zostaje powiązana z Cascadia Data Discovery Initiative oraz szerszym dążeniem do przełamywania silosów informacyjnych bez odbierania pierwotnym dysponentom kontroli nad zbiorami. Zmiana ta jest głębsza, niż sugeruje techniczny język architektury systemów.

Przez stulecia dostęp do wiedzy i dostęp do nośnika wiedzy były niemal nierozłączne. Kto chciał przeczytać dokument, musiał go otrzymać albo wejść do miejsca, w którym się znajdował. Kto chciał przeanalizować kartotekę, musiał ją otworzyć. Technologia cyfrowa stwarza możliwość bardziej subtelną: można zaprojektować relację, w której badacz lub system otrzymuje odpowiedź na pytanie, nie zyskując swobodnego dostępu do całego archiwum. Z punktu widzenia teorii informacji jest to przejście od prawa do zasobu ku prawu do operacji. To rozróżnienie może okazać się jednym z najważniejszych bezpieczników społeczeństwa danych. Posiadanie pełnej kopii zbioru daje możliwość zadawania nieograniczonej liczby nowych pytań, łączenia rekordów z innymi źródłami i ponownego wykorzystywania informacji w przyszłości. Prawo do wykonania konkretnego zapytania jest znacznie węższe. Jeśli analityk chce wiedzieć, ilu pacjentów spełnia określone kryterium kliniczne, system może – w pewnych warunkach – zwrócić wynik statystyczny bez ujawniania listy wszystkich osób. Jeżeli badacz chce porównać skuteczność terapii w kilku szpitalach, nie zawsze musi tworzyć centralną bazę zawierającą historie chorób wszystkich uczestników. Informacja może zostać użyta bez pełnego przesunięcia władzy nad informacją.

Smith przedstawia kilka technologicznych dróg prowadzących do takiej architektury. Wskazuje na prywatność różnicową, rozwiązania określane jako Private AI, modele query-only oraz ideę "zamkniętego kontenera", w którym dozwolone jest wykonywanie określonych operacji bez przekazywania surowych rekordów analitykowi. Trzeba jednak doprecyzować ich znaczenie, gdyż są to technologie odmienne, rozwiązujące różne fragmenty problemu. Wspólna jest im nie konkretna metoda matematyczna, lecz zasada minimalizacji ekspozycji: podmiot powinien otrzymać tylko tyle informacji, ile jest konieczne do osiągnięcia uprawnionego celu.

Prywatność różnicowa jest dobrym przykładem tej zmiany myślenia. Jej istotą nie jest zwykłe "anonimizowanie" danych ani mechaniczne usuwanie imion i nazwisk. System ma być zaprojektowany tak, aby wynik analizy statystycznej nie zmieniał się w sposób umożliwiający łatwe ustalenie, czy dane konkretnej osoby znalazły się w analizowanym zbiorze. Do odpowiedzi lub procesu obliczeniowego wprowadza się kontrolowany mechanizm losowości, tworząc kompromis pomiędzy precyzją statystyki a ochroną wkładu jednostki. To podejście głęboko odmienne od naiwnego przekonania, że wystarczy usunąć kolumnę "nazwisko", aby dane przestały mówić o człowieku. Rozróżnienie to jest niezbędne, ponieważ współczesne zbiory zawierają ogromną liczbę quasi-identyfikatorów. Człowiek może zostać rozpoznany nie przez nazwisko, lecz przez niezwykłą kombinację wieku, lokalizacji, zawodu, zdarzeń medycznych albo wzorców zachowania. Historia badań nad prywatnością wielokrotnie pokazywała, że zestaw pozornie anonimowych cech może po połączeniu z zewnętrznym źródłem pozwolić ponownie ustalić tożsamość.

Dlatego prawdziwa ochrona nie może polegać wyłącznie na zdjęciu etykiety z pojemnika. Trzeba kontrolować również to, ile można wywnioskować z zawartości.

Kryptografia jako techniczne ograniczenie nadużyć władzy

Współczesne podejście regulacyjne wyraźnie odróżnia pseudonimizację od anonimizacji. Pseudonimizacja utrudnia bezpośrednie powiązanie informacji z osobą, lecz relacja ta może zostać odtworzona przy użyciu dodatkowych danych; dlatego informacje pseudonimizowane wciąż pozostają danymi osobowymi. Dopiero skuteczna anonimizacja, w której identyfikacja nie jest rozsądnie możliwa, zmienia status prawny danych. Europejska Rada Ochrony Danych w 2026 roku nadal rozwija tę problematykę, co dowodzi, że techniczna granica między „danymi o osobach” a „danymi naprawdę anonimowymi” jest znacznie trudniejsza do wyznaczenia, niż sugeruje potoczny język. Inną metodą jest bezpieczne obliczenie wielostronne (SMPC). Jego idea brzmi niemal paradoksalnie: kilka podmiotów może wspólnie obliczyć funkcję na swoich prywatnych danych, nie ujawniając sobie nawzajem pełnych danych wejściowych. Szpitale mogą zatem posiadać odrębne zbiory pacjentów, przedsiębiorstwa różne fragmenty informacji, a instytucje publiczne oddzielne rejestry – przy czym wspólna analiza nie musi oznaczać fizycznego połączenia wszystkich tabel w jednej lokalizacji. Kryptografia staje się tu technologią współpracy pomiędzy podmiotami, które nie muszą sobie ufać w stopniu wymaganym do wzajemnego ujawnienia całych baz. NIST opisuje secure multiparty computation właśnie jako możliwość obliczenia funkcji na rozproszonych

prywatnych wejściach bez ujawniania tych wejść uczestnikom ponad to, co wynika z dozwolonego rezultatu.

Jest to niezwykle interesujące z perspektywy teorii instytucji. Przez większą część historii współpraca wymagała albo zaufania, albo przekazania zasobu trzeciemu arbitrowi. Kryptografia wprowadza trzeci wariant: część zaufania można zastąpić weryfikowalną architekturą procesu. Nie muszę ufać partnerowi, że nie skopiuje mojego zbioru, jeśli protokół w ogóle mu go nie przekazuje. Nie oznacza to końca zaufania – trzeba przecież ufać implementacji, urządzeniom, procedurom zarządzania kluczami i osobom nadzorującym system – zmienia się jednak jego lokalizacja. Moralną obietnicę można częściowo zastąpić technicznym ograniczeniem możliwości nadużycia.

kryptografia realizuje starą intuicję konstytucjonalizmu: najlepszą gwarancją przeciwko nadużyciu nie zawsze jest obietnica, że władza nie skorzysta z możliwości, lecz takie zaprojektowanie systemu, aby pewnych możliwości w ogóle nie posiadała. Konstytucja ogranicza kompetencje instytucji, a kryptografia może ograniczać kompetencje informacyjne systemu. Obie technologie – prawna i matematyczna – próbują odpowiedzieć na ten sam problem antropologiczny: nie budować bezpieczeństwa wyłącznie na przekonaniu, że posiadacz władzy zawsze będzie dobry.

Kryptografia chroni dane, lecz nie gwarantuje etyki

Jeszcze dalej idzie szyfrowanie homomorficzne. Umożliwia ono, w uproszczeniu, wykonywanie operacji na danych zaszyfrowanych w taki sposób, aby wynik po odszyfrowaniu był tożsamy z rezultatem operacji wykonanej na danych jawnych. Brzmi to jak odwrócenie starej logiki sejfu. Dotychczas trzeba było go otworzyć, by pracować z zawartością; tutaj można wykonać pewne działania, nie poznając treści bezpośrednio.

NIST traktuje fully homomorphic encryption jako jedno z podstawowych narzędzi kryptografii wzmacniającej prywatność, zaznaczając jednocześnie wysoki koszt obliczeniowy i fakt, że jego praktyczność zależy od konkretnego zastosowania. Nie oznacza to jednak, że szyfrowanie homomorficzne rozwiązuje wszystkie problemy związane z prywatnością. Zabezpiecza ono określony etap obliczeń, lecz nie odpowiada na pytania o legalność celu, jakość danych, uprzedzenia modelu czy późniejsze wykorzystanie wyniku. Można wykonać moralnie niedopuszczalną analizę w technicznie perfekcyjnie chronionym środowisku. Podobnie jak wcześniej bezpieczeństwo nie gwarantowało sprawiedliwości, tak kryptografia nie gwarantuje etyki. Można prywatnie obliczyć coś, czego w ogóle nie powinno się obliczać.

Ta uwaga jest kluczowa, gdyż fascynacja technologiami ochrony prywatności może łatwo przerodzić się w nowy technokratyczny optymizm. Pojawia się pokusa twierdzenia, że skoro system stosuje federated learning, differential privacy albo homomorphic encryption, problem praw człowieka został rozwiązany. W rzeczywistości technologie te ograniczają jedynie określone rodzaje ryzyka. Nie rozstrzygają one, czy istnieje prawidłowa podstawa prawna przetwarzania, czy dane są adekwatne, czy cel jest proporcjonalny, czy model dyskryminuje, ani czy rezultat zostanie wykorzystany zgodnie z pierwotnym uzasadnieniem.

Prowadzi to do istotnego rozróżnienia pomiędzy prywatnością wejścia, procesu i wyniku. Można zabezpieczyć dane przed ujawnieniem podczas ich przekazywania, a mimo to model końcowy może niechcący zdradzić informacje o danych treningowych. Można bezpiecznie trenować model federacyjny, lecz przechwycenie aktualizacji parametrów w określonych konfiguracjach pozwala wnioskować o informacjach lokalnych. Można ukryć poszczególne rekordy, a następnie opublikować zbyt szczegółową statystykę, która umożliwi rekonstrukcję części zbioru. Prywatność jest więc właściwością całego procesu, a nie pojedynczej techniki.

Z tego względu federated learning należy przedstawiać ostrożniej niż jako system, w którym „dane nigdy nie opuszczają urządzenia, więc są bezpieczne”. W typowym modelu lokalne dane rzeczywiście pozostają u uczestników, a do koordynatora trafiają aktualizacje modelu zamiast surowych rekordów.

Ochrona prywatności jako dozowanie władzy poznawczej

Same aktualizacje mogą jednak zawierać informacje wymagające dodatkowej ochrony, co wymusza zastosowanie bezpiecznej agregacji, prywatności różnicowej i kryptografii. NIST podkreśla, że prywatność w uczeniu federacyjnym wymaga zabezpieczenia nie tylko lokalnych danych i aktualizacji, ale również gotowego modelu przed ujawnieniem informacji o zbiorach treningowych. Ta techniczna subtelność niesie istotną konsekwencję filozoficzną: nie wystarczy stwierdzić, że informacja "została u właściciela". Należy zapytać, co dokładnie opuściło jego środowisko.

Być może nie wysłano rekordu, lecz gradient modelu. Być może nie nazwiska, a reprezentację statystyczną. Możliwe, że nie przekazano danych medycznych, ale wynik pozwalający wywnioskować zbyt wiele. Władza informacyjna nie musi podróżować w formie kopii oryginalnej tabeli. Stąd model query-only, opisany w książce, cechuje się szczególną elegancją. Analityk nie otrzymuje surowego zbioru, lecz dostęp do określonego interfejsu pytań. Można go porównać do

uczonego stojącego przed zamkniętym archiwum i komunikującego się z bibliotekarzem przez niewielkie okno. Zamiast wchodzić do magazynu, przekazuje pytanie; bibliotekarz sprawdza, czy jest ono dopuszczalne, wykonuje operację i zwraca odpowiedź. Istota problemu przesuwa się wówczas z ochrony drzwi na zarządzanie pytaniami.

Prowadzi to jednak do nowego niebezpieczeństwa. Seria pozornie nieszkodliwych pytań może wspólnie ujawnić informację, której pojedyncza odpowiedź nie zdradzała. Jeśli ktoś może dowolnie formułować setki zapytań do małej populacji, może próbować różnicować wyniki i rekonstruować cechy poszczególnych osób. Ochrona wymaga więc nie tylko ograniczenia treści odpowiedzi, ale również budżetu prywatności, monitorowania liczby i charakteru zapytań oraz oceny ryzyka wynikającego z ich kombinacji. W przeciwnym razie "okienko w archiwum" może stać się sposobem stopniowego wynoszenia archiwum kawałek po kawałku.

W tym miejscu matematyka spotyka się z teorią prawa w niezwykle interesujący sposób. Prawo również zna problem obchodzenia normy poprzez serię działań, z których każde z osobna wydaje się dopuszczalne. Nadużycie prawa, obchodzenie celu regulacji i kumulacja ingerencji przypominają informatyczny problem wielu zapytań. System odpowiedzialności nie może zatem oceniać wyłącznie pojedynczego ruchu – musi dostrzegać sekwencję.

Z tej perspektywy najlepiej rozumieć privacy-enhancing technologies nie jako narzędzia "ukrywające dane", lecz jako technologie dozowania władzy poznawczej. Ustalają one, kto może dowiedzieć się czego, w jakiej formie i z jaką dokładnością. Tradycyjny model bezpieczeństwa koncentrował się na autoryzacji: osoba ma dostęp albo go nie ma. Nowoczesna prywatność pozwala budować stopnie dostępu: można znać agregat bez rekordu, wspólną statystykę bez cudzych wejść, wynik modelu bez pełnej bazy czy korelację bez identyfikacji jednostki.

Pojawia się nowa wersja starej zasady need to know. W wojsku i administracji tajemnic dostęp do informacji ograniczano według potrzeby funkcjonalnej. Technologie ochrony prywatności pozwalają przenieść tę logikę bezpośrednio w sferę obliczeń. Podmiot nie tylko formalnie zobowiązuje się, że nie przeczyta niepotrzebnych danych – system może zostać skonstruowany tak, aby ich nie otrzymał.

Jest to szczególnie obiecujące w medycynie. Źródłowe odwołanie do Fred Hutchinson Cancer Research Center ilustruje społeczną wartość analizy rozproszonych informacji medycznych. Onkologia, epidemiologia, genomika czy badania chorób rzadkich cierpią często nie na brak danych, lecz na ich fragmentację. Każdy szpital posiada niewielki fragment obrazu, a najbardziej wartościowe zależności ujawniają się dopiero po analizie większej populacji. Jednocześnie dane medyczne należą do informacji, wobec których społeczeństwo oczekuje szczególnej poufności. Stary

model sugerował dramatyczny wybór: albo prywatność, albo nauka. Jeżeli dane pozostają zamknięte w lokalnych silosach, badanie jest słabsze; jeśli wszystkie zostaną przesłane do centralnego repozytorium, rośnie ryzyko.

Model federacyjny jako infrastruktura kooperacji i zaufania

Model federacyjny dąży do zmiany samej struktury wyboru. Nie eliminuje on konfliktu, lecz może zmniejszyć jego ostrość, sprawiając, że nauka i prywatność przestają być przeciwległymi biegunami jednej osi. To przykład szerszej zasady projektowej: najskuteczniejsza technologia regulacyjna nie tyle rozstrzyga o prymacie jednej wartości nad drugą, co przeprojektowuje system tak, aby sam konflikt był mniej dotkliwy. Pas bezpieczeństwa nie rozwiązuje dylematu między mobilnością a ryzykiem poprzez zakaz korzystania z samochodów, a oczyszczalnia ścieków nie wybiera w sposób zero-jedynkowy między produkcją a czystością wody.

Podobnie technologie ochrony prywatności poszukują trzeciej drogi pomiędzy całkowitym zamknięciem informacji a ich nieograniczonym ujawnieniem. W ekonomii instytucjonalnej rozwiązania te można rozumieć jako obniżanie kosztu transakcyjnego zaufania. Dwie organizacje mogą pragnąć wspólnej analizy danych, obawiając się jednocześnie utraty tajemnicy handlowej, naruszenia prawa lub przejęcia zasobów przez partnera. Jeśli architektura kryptograficzna pozwala uzyskać wspólny wynik bez odsłonięcia pełnych baz, współpraca staje się możliwa tam, gdzie wcześniej blokował ją brak zaufania. W tym ujęciu prywatność przestaje być wyłącznie kosztem – może stać się infrastrukturą kooperacji.

Jest to istotna korekta powszechnego przekonania, że regulacje dotyczące prywatności zawsze hamują innowacyjność. Źle zaprojektowane prawo rzeczywiście może podnosić koszty i zamykać dane w silosach, jednak silna ochrona prywatności potrafi zbudować zaufanie niezbędne do udostępnienia informacji w kontrolowanym modelu. Pacjent chętniej weźmie udział w badaniu, wiedząc, że jego pełna dokumentacja nie opuści szpitala; przedsiębiorstwo zgodzi się na analizy sektorowe, jeśli konkurent nie otrzyma surowych danych handlowych.

Państwa również mogą współpracować, o ile technologia pozwala zachować suwerenność nad narodowymi zbiorami. Model federacyjny posiada zatem wymiar geopolityczny: jeśli dane pozostają w określonej jurysdykcji, a algorytm przemieszcza się między miejscami ich przechowywania, pewne formy współpracy międzynarodowej mogą odbywać się bez klasycznego transferu całego zasobu. Idea ta łączy się z koncepcją „społeczności państw szanujących prawa” i

możliwością kooperacji bez całkowitej utraty suwerenności informacyjnej. Jest to wizja atrakcyjna, choć nie wolno jej absolutyzować – samo lokalne przechowywanie rekordów nie oznacza automatycznie braku prawnie relewantnego przetwarzania transgranicznego ani zniknięcia problemów jurysdykcyjnych. To ważne ostrzeżenie.

Technologia ochrony danych nie zastępuje odpowiedzialności prawnej i etycznej

Architektura techniczna i kwalifikacja prawna to dwie różne kwestie. Fakt, że surowe dane fizycznie nie opuszczają serwera, nie rozstrzyga automatycznie oceny prawnej. Dostęp zdalny, wymiana aktualizacji modelu, kontrola systemu z innej jurysdykcji, możliwość identyfikacji osób czy charakter wspólnie ustalonych celów mogą nadal generować obowiązki prawne. W prawie ochrony danych lokalizacja bitów jest tylko jednym z elementów relacji. Powraca tu zasada towarzysząca całemu artykułowi: technologia może zmniejszyć ryzyko, lecz nie może sama nadać sobie legalności. Privacy by design jest metodą realizacji normy, a nie jej substytutem.

Kryptografia odpowiada na pytanie „jak ograniczyć dostęp?", ale milczy w kwestii tego, „kto powinien być uprawniony?". Federacja wyjaśnia, „jak analizować bez centralizacji?", lecz nie rozstrzyga, „czy analiza jest sprawiedliwa?". Differential privacy wskazuje, „jak ograniczyć ujawnienie wkładu jednostki?", ale nie rozstrzyga, czy cel statystyczny jest moralnie dopuszczalny. W tym miejscu technologia ochrony prywatności spotyka się z filozofią Hansa Jonasa.

Odpowiedzialność nie polega na wykazaniu, że dysponujemy narzędziem zabezpieczającym, lecz na przewidywaniu skutków całej struktury działania. Inżynier może poprawnie zaimplementować protokół kryptograficzny, podczas gdy organizacja wykorzysta jego rezultat do podjęcia społecznie szkodliwej decyzji. Analiza normatywna musi zatem obejmować cały łańcuch: dane, sposób dostępu, algorytm, cel, wynik i późniejsze użycie. Można to ująć jeszcze ostrzej: prywatność danych nie gwarantuje prywatności konsekwencji. Model może zostać wytrenowany w sposób chroniący indywidualne rekordy, a następnie wykorzystany do masowego profilowania określonej grupy. Nie musi ujawniać nazwiska konkretnego człowieka, aby wpływać na jego szanse kredytowe, ubezpieczeniowe, zawodowe czy polityczne. Ochrona prywatności indywidualnej i ochrona przed dyskryminacją grupową są więc odrębnymi problemami.

Ta różnica stanie się szczególnie istotna w części poświęconej sztucznej inteligencji. Na tym etapie wystarczy zauważyć, że PETs rozwiązują problem ekspozycji informacji, a niekoniecznie problem sprawiedliwości wnioskowania. Można nie znać historii konkretnej osoby i nadal tworzyć model,

który statystycznie gorzej traktuje grupę, do której ona należy. Technologia może chronić jednostkę jako rekord, lecz skrzywdzić ją jako członka kategorii. Z tego wynika potrzeba wielowarstwowej architektury odpowiedzialności. Pierwsza warstwa dotyczy legalności pozyskania i celu; druga – minimalizacji i jakości danych; trzecia – bezpieczeństwa infrastruktury; czwarta – prywatności samego obliczenia; piąta – informacji ujawnianej przez wynik; szósta zaś – skutków decyzji podjętej na jego podstawie.

Dopiero analiza wszystkich warstw pozwala rzetelnie ocenić, czy technologia służy człowiekowi. W tej perspektywie Visit the Data przestaje być nazwą rozwiązania technicznego, a staje się maksymą politycznej filozofii informacji: nie przenoś władzy nad całym zasobem, jeżeli do realizacji celu wystarczy przeniesienie pytania; nie ujawniaj rekordu, jeżeli wystarczy wynik; nie centralizuj pamięci, jeżeli współpraca może odbyć się bez jej centralizacji. Jest to cyfrowy odpowiednik zasady subsydiarności: pozostaw informację możliwie blisko miejsca, w którym powstała, a na wyższy poziom wynoś tylko to, czego wspólne działanie rzeczywiście wymaga.

Nie zawsze będzie to jednak możliwe ani racjonalne. Centralizacja może poprawiać jakość danych, ułatwiać audyt, obniżać koszt obliczeń lub umożliwiać badania, których system federacyjny nie wykona efektywnie. Rozproszenie zwiększa natomiast złożoność, utrudnia standaryzację i tworzy własne powierzchnie ataku. Nie istnieje jedna architektura dobra dla wszystkich zastosowań. Dojrzałość polega właśnie na odejściu od dogmatu, że „więcej danych w jednym miejscu” jest zawsze synonimem większego postępu. Warto w tym miejscu przywołać metaforę archiwum.

Konflikt jurysdykcji w architekturze chmury

Klasyczny badacz podróżował do miejsca, w którym znajdowały się źródła. Era digitalizacji przyzwyczaiła nas do sytuacji odwrotnej: to źródła mają przyjechać do badacza. Analityka federacyjna dokonuje zaskakującego powrotu do starego modelu – tyle że zamiast człowieka podróżuje kod. Algorytm staje się uczonym przemieszczającym się od archiwum do archiwum, otrzymując tylko taki dostęp, jaki przyzna mu lokalny kustosz.

Ten obraz prowadzi bezpośrednio do problemu, którego nawet najbardziej wyrafinowana kryptografia nie rozwiąże samodzielnie: prawo którego państwa pełni rolę tego kustosza? Jeśli jeden zbiór znajduje się w Polsce, drugi w Niemczech, trzeci w Stanach Zjednoczonych, a usługodawca ma siedzibę w jeszcze innym kraju, techniczna możliwość wspólnego obliczenia zderza się z wielością systemów prawnych. Dane mogą nie podróżować, lecz kompetencje państw nadal się przecinają. Po rozwiązaniu kwestii „jak analizować bez zabierania danych” pozostaje pytanie trudniejsze: kto ma prawo zażądać dostępu do informacji tam, gdzie one pozostają?

W tym miejscu mapa techniczna staje się mapą geopolityczną. Światowa chmura spotyka granice państw, nakazy sądowe i konflikty jurysdykcji. Warto zatem opuścić laboratorium kryptografa i wejść na salę sądową. Punktem wyjścia będzie pozornie proste zdarzenie: amerykański prokurator chce otrzymać wiadomości przechowywane na serwerze w Irlandii. Za tym żądaniem kryje się jednak fundamentalne pytanie XXI wieku: czy dane mają narodowość, a jeśli nie – kto może nad nimi sprawować suwerenną władzę? Prawo ponad granicami, dane poza terytorium. Suwerenność w epoce chmury.

Nowoczesne państwo nauczyło się myśleć terytorium. Granica wyznaczała przestrzeń obowiązywania prawa; urząd wiedział, gdzie zaczyna się i kończy jego jurysdykcja, policjant przekraczający granicę innego kraju tracił większość swoich kompetencji, a dokument w zagranicznym archiwum wymagał współpracy z miejscowymi władzami. Chmura obliczeniowa wprowadziła do tego porządku element niemal anarchiczny: informacja może należeć do człowieka mieszkającego w jednym państwie, zostać wytworzona w drugim, przetwarzana przez przedsiębiorstwo z siedzibą w trzecim, przechowywana na serwerze w czwartym i posiadać kopię zapasową w piątym. W rezultacie pytanie, które przez stulecia należało do geografii, stało się pytaniem o architekturę informatyczną.

Dane nie znoszą granic państwowych. Ujawniają natomiast, że klasyczne granice stworzono dla rzeczy poruszających się znacznie wolniej niż informacja. Samochód można zatrzymać na przejściu granicznym, kontener w porcie, samolot na lotnisku. Pakiet danych może przekroczyć kilka jurysdykcji w czasie krótszym, niż człowiek potrzebuje na przeczytanie jednego zdania. Światło nie zatrzymuje się przed tablicą z nazwą państwa. Prawo musi zatem próbować odtworzyć kontrolę normatywną nad środowiskiem, w którym fizyczna łatwość przepływu informacji jest nieporównywalna z instytucjonalną szybkością uzgadniania kompetencji.

Konflikt geografii sieci z suwerennością państwową

Stąd bierze się konflikt pomiędzy dwiema geografiami. Pierwsza to geografia państwa: granic, suwerenności, sądów i terytorialnych kompetencji. Druga zaś to geografia sieci: opóźnień transmisji, lokalizacji centrów danych, redundancji, dostępności mocy obliczeniowej i optymalizacji technicznej. Dostawca chmury może umieścić dane w konkretnym regionie dlatego, że zmniejsza to latencję, zapewnia odporność, obniża koszt energii lub pozwala spełnić oczekiwania klienta. Dla prokuratora ta sama decyzja może jednak oznaczać, że dowód znalazł się poza granicami państwa.

Spór Microsoftu z władzami Stanów Zjednoczonych o dane przechowywane w Irlandii stał się czymś więcej niż procesem dotyczącym kilku wiadomości elektronicznych. Był eksperymentem

konstytucyjnym przeprowadzonym na globalnej chmurze. W 2013 roku amerykańskie organy ścigania uzyskały, na podstawie Stored Communications Act, nakaz dotyczący treści wiadomości jednego z klientów Microsoftu.

Część informacji znajdowała się jednak na serwerze w Dublinie. Microsoft odmówił wydania danych przechowywanych w Irlandii, argumentując, że amerykańskie prawo nie powinno być interpretowane jako automatycznie nadające nakazowi skutek eksterytorialny. Smith przedstawia tę sprawę jako moment, w którym przedsiębiorstwo znalazło się "między młotem a kowadłem": z jednej strony obowiązek podporządkowania się prawu państwa macierzystego, z drugiej ryzyko naruszenia suwerenności i zaufania klientów w państwie, w którym dane faktycznie się znajdowały. W istocie problem był jednak głębszy. Gdyby sama siedziba globalnego dostawcy wystarczała do nieograniczonego sięgania po informacje przechowywane na całym świecie, państwo siedziby przedsiębiorstwa zyskałoby niezwykle szeroką władzę nad cudzymi cyfrowymi archiwami. Można wyobrazić sobie odwrócenie tej sytuacji, co natychmiast obnaża polityczny ciężar problemu.

Gdyby przedsiębiorstwo europejskie posiadało globalną infrastrukturę, a sąd europejski uznał, że może nakazać mu przekazanie danych przechowywanych w Stanach Zjednoczonych niezależnie od prawa amerykańskiego, Waszyngton również mówiłby o ingerencji w suwerenność. Jeżeli podobne roszczenie zgłosiłoby państwo autorytarne wobec globalnego operatora posiadającego filię na jego terytorium, problem stałby się jeszcze bardziej niepokojący. Prawdziwe pytanie nie brzmi zatem: czy amerykańskim organom należało ułatwić prowadzenie konkretnego śledztwa? Brzmi ono: jaką zasadę chcielibyśmy uznać za słuszną wtedy, gdy zastosuje ją każde państwo świata? Jest to klasyczny test uniwersalizacyjny przypominający Kantowskie pytanie o regułę, którą można uczynić powszechną. Prawo eksterytorialne wydaje się wygodne, gdy korzysta z niego "nasze" państwo przeciwko sprawcy ciężkiego przestępstwa. Staje się mniej atrakcyjne, gdy dokładnie tę samą konstrukcję próbuje zastosować obca władza wobec dziennikarza, opozycjonisty albo przedsiębiorcy znajdującego się pod ochroną naszego systemu prawnego. Suwerenność cyfrowa ujawnia stary problem polityki międzynarodowej: państwa chętnie uznają uniwersalność własnych uprawnień i partykularyzm cudzych.

Anachronizm prawa wobec rozproszonej infrastruktury danych

Sprawa Microsoftu obnażyła anachronizm prawa tworzonego dla wcześniejszej epoki technologicznej. Electronic Communications Privacy Act oraz zawarty w nim Stored Communications Act powstały w 1986 roku, gdy Internet był środowiskiem radykalnie innym, a

globalna chmura w dzisiejszym rozumieniu po prostu nie istniała. Prawodawca regulował wówczas rzeczywistość elektronicznych usług komunikacyjnych, nie przewidując świata, w którym przedsiębiorstwo może automatycznie rozmieszczać fragmenty danych klienta pomiędzy kontynentami. Nie jest to jednak cecha wyłącznie prawa technologicznego; prawo niemal zawsze dziedziczy po przeszłości pojęcia stworzone dla wcześniejszej infrastruktury. Samochód najpierw pojawił się na drogach przeznaczonych dla koni, samolot w systemie prawnym nieznającym nowoczesnej przestrzeni powietrznej, a Internet w prawie komunikacji rozwijanym w epoce telefonu i poczty. Problem pojawia się wtedy, gdy stara kategoria nie tylko niedokładnie opisuje nowy przedmiot, ale prowadzi do realnej redystrybucji władzy. W sporze irlandzkim kluczowe stało się pytanie: gdzie właściwie znajduje się akt przeszukania?

Zwolennik szerokiego dostępu mógł argumentować, że nakaz kierowany jest do przedsiębiorstwa podlegającego jurysdykcji USA, a firma może technicznie sprowadzić dane do Stanów Zjednoczonych za pomocą własnej infrastruktury. Przeciwnicy wskazywali natomiast, że przedmiot zainteresowania – prywatna komunikacja – znajduje się w zagranicznym centrum danych i jej przymusowe pozyskanie stanowi ingerencję wykraczającą poza terytorium państwa. Cyfrowość komplikuje samo pojęcie miejsca działania. Gdzie „odbywa się" dostęp do danych, jeśli pracownik w Nowym Jorku wpisuje polecenie, serwer wykonuje je w Dublinie, pakiety przechodzą przez kilka krajów, a rezultat pojawia się na ekranie w USA? Prawo oparte na fizycznym miejscu czynności musi zatem nauczyć się analizować operacje, których materialność jest rozproszona.

W tym kontekście istotne staje się pojęcie digital neutrality: ochrona informacji nie powinna znikać tylko dlatego, że plik został przeniesiony z biurka właściciela na zagraniczny serwer. Jest to zasada szczególnie silna jako postulat normatywny. Gdyby bowiem przeniesienie danych do chmury automatycznie osłabiało prawa jednostki, cała gospodarka chmurowa tworzyłaby paradoks polegający na wymianie wygody technologicznej na degradację ochrony prawnej. Neutralność cyfrowa nie może jednak oznaczać, że lokalizacja danych nie ma żadnego znaczenia – byłby to drugi skrajny błąd.

Dane pozostają w konkretnej infrastrukturze i podlegają określonym regulacjom; mogą korzystać z lokalnych gwarancji konstytucyjnych, a miejsce ich przetwarzania może generować ryzyko dostępu władz. Lokalizacja nie powinna automatycznie odbierać człowiekowi praw, lecz może wpływać na to, które systemy prawne te prawa chronią lub ograniczają.

Tym samym pojawia się problem konfliktu praw. Dostawca chmury może zostać zobowiązany przez jedno państwo do ujawnienia informacji, podczas gdy prawo innego państwa ogranicza ich przekazanie. Nie istnieje tu proste rozwiązanie techniczne. Szyfrowanie nie rozstrzygnie, któremu prawu należy dać pierwszeństwo; lokalizacja centrum danych nie usunie roszczenia państwa wobec

przedsiębiorstwa, a regulamin klienta nie może uchylić obowiązku wynikającego z nakazu sądowego. Konflikt ten musi zostać rozwiązany instytucjonalnie. Tradycyjnym mechanizmem była międzynarodowa pomoc prawna, w tym system MLAT. Państwo potrzebujące dowodu zwracało się do drugiego państwa, aby to ono – przy użyciu własnych organów i zgodnie z własnym prawem – pomogło w pozyskaniu informacji. Konstrukcja ta szanuje suwerenność, gdyż policjant jednego państwa nie występuje w roli policjanta drugiego.

CLOUD Act i narodziny dyplomacji elektronicznego dowodu

Problemem stała się jednak szybkość. Procedury stworzone dla świata dokumentów papierowych i klasycznej współpracy sądowej przestały nadążać za śledztwami, w których elektroniczny dowód może zostać skasowany, przesunięty lub zaszyfrowany w mgnieniu oka.

Konflikt pomiędzy suwerennością a szybkością stał się jednym z głównych motorów amerykańskiego CLOUD Act. Kongres uchwalił ustawę w marcu 2018 roku, gdy sprawa Microsoftu znajdowała się już przed Sądem Najwyższym.

Nowe prawo zasadniczo przesądziło, że dostawca podlegający Stored Communications Act ma obowiązek zachować, zabezpieczyć lub ujawnić dane znajdujące się w jego posiadaniu, pieczy lub kontroli – niezależnie od tego, czy są one fizycznie przechowywane w Stanach Zjednoczonych, czy poza nimi. Po wydaniu nakazu opartego na znowelizowanych przepisach spór przed Sądem Najwyższym utracił przedmiot. Była to prawna odpowiedź sprzeczna ze stanowiskiem, które Microsoft prezentował w pierwotnej sprawie.

Kongres nie przyjął zasady, według której lokalizacja zagranicznego serwera całkowicie blokuje amerykański nakaz. Wprowadzono zasadę "possession, custody, or control": kluczowe staje się to, czy dostawca podlegający jurysdykcji USA kontroluje dane, a nie wyłącznie to, gdzie fizycznie znajduje się dysk. Na pierwszy rzut oka wydaje się to zwycięstwem państwa nad terytorialnością danych, jednak CLOUD Act jest konstrukcją bardziej złożoną. Ustawa przewiduje mechanizmy rozstrzygania konfliktów z prawem innych państw oraz umożliwia zawieranie umów wykonawczych z krajami spełniającymi określone wymagania dotyczące praworządności, prywatności i wolności obywatelskich. Ich ideą jest pozwolenie organom jednego państwa na kierowanie kwalifikowanych nakazów bezpośrednio do dostawców w drugim kraju, bez konieczności każdorazowego przechodzenia przez pełny, tradycyjny mechanizm pomocy prawnej.

To nie jest zniesienie dyplomacji, lecz jej przeniesienie do infrastruktury. Państwa z góry uzgadniają reguły, według których organy mogą później działać szybciej. Tradycyjny MLAT przypominał każdorazową podróż dyplomatyczną dokumentu. CLOUD Act próbuje zbudować most, po którym określone rodzaje wniosków mogą poruszać się według wcześniej uzgodnionych zasad. Pierwszym działającym przykładem tego mechanizmu stała się umowa pomiędzy Stanami Zjednoczonymi a Wielką Brytanią, obowiązująca od października 2022 roku.

Jej znaczenie nie ogranicza się jedynie do skrócenia procedury. Świadczy ona o narodzinach nowej kategorii traktatowej: dyplomacji elektronicznego dowodu. Państwa nie negocjują już wyłącznie ekstradycji człowieka, pomocy w przesłuchaniu świadka czy wydania dokumentu. Negocjują zasady bezpośredniej komunikacji pomiędzy własnym wymiarem sprawiedliwości a prywatną infrastrukturą informacyjną znajdującą się pod jurysdykcją partnera.

To przesuwa również pozycję przedsiębiorstwa technologicznego. Dawny bank przechowywał dokumentację klienta i mógł otrzymywać żądania lokalnego sądu. Globalna chmura otrzymuje żądania wynikające z wielu systemów prawnych; musi klasyfikować ich podstawę, zakres, skutek terytorialny oraz możliwy konflikt z innym prawem. Korporacyjny dział prawny zaczyna wykonywać funkcje, które przypominają miniaturowe ministerstwo spraw zagranicznych połączone z kancelarią konstytucyjną. Z tego procesu wypływa idea techplomacy – dyplomacji technologicznej. Termin ten nie powinien jednak sugerować, że przedsiębiorstwa stają się państwami w sensie formalnym. Nie dysponują one suwerennością, monopolem legalnego przymusu ani demokratycznym mandatem. Zaczynają natomiast pełnić funkcję pośredników pomiędzy suwerennościami, ponieważ kontrolują infrastrukturę, której nie panuje w całości żadne pojedyncze państwo. Ta pozycja jest politycznie niewygodna.

Proceduralizacja konfliktu zamiast korporacyjnej suwerenności

Z jednej strony firma technologiczna może bronić klienta przed żądaniem, które uzna za nadmierne, i zaskarżyć je do sądu. Z drugiej jednak nie może rościć sobie prawa do samodzielnego decydowania o tym, które demokratycznie uchwalone prawo jest słuszne. Gdyby prywatna korporacja miała ostatecznie rozstrzygać, które nakazy państwa zostaną wykonane, sama stałaby się pozakonstytucyjnym ośrodkiem władzy.

Optymalny model nie zakłada ani bezkrytycznego podporządkowania firmy każdemu żądaniu organów państwowych, ani korporacyjnej suwerenności. Rozwiązaniem jest proceduralizacja

konfliktu. Dostawca powinien mieć możliwość zakwestionowania nakazu, sąd winien kontrolować podstawę ingerencji, a państwo – instrumenty obrony własnego porządku prawnego. Jednocześnie użytkownik musi dysponować środkami ochrony w sytuacjach, gdy ich zastosowanie nie zniweczy uzasadnionego celu śledztwa.

Cyfrowa suwerenność nie może bowiem oznaczać suwerenności absolutnej. Gdyby każde państwo wymagało, aby wszystkie dane jego obywateli pozostawały wyłącznie na jego terytorium, globalna sieć uległaby postępującej fragmentacji. Lokalizacja danych może zwiększać kontrolę regulacyjną i ograniczać ryzyka eksterytorialnego dostępu, lecz jednocześnie podnosi koszty, osłabia redundancję i ułatwia lokalnym władzom przejęcie kontroli nad informacją. Stąd paradoks data localization: demokratyczne państwo może żądać lokalizacji danych, by chronić obywateli przed obcym nadzorem, podczas gdy reżim autorytarny może żądać tego samego, aby dane znajdowały się w zasięgu jego służb. Ten sam instrument prawny może zatem chronić suwerenność lub wzmacniać represję; narzędzie od broni różni tu przede wszystkim kontekst instytucjonalny.

W książce problem ten zestawiono z historycznym doświadczeniem Niemiec i Stasi oraz pytaniem, czy dostawca globalnej chmury powinien rozmieszczać infrastrukturę w państwach o wysokim ryzyku naruszeń praw człowieka. Jest to logiczna konsekwencja tezy o fizyczności chmury. Decyzja o lokalizacji centrum danych nie jest bowiem wyłącznie kwestią logistyczną, lecz wyborem jurysdykcji. Można tu mówić o geopolityce serwerowni. Państwa konkurują o centra danych ze względu na inwestycje, miejsca pracy i znaczenie strategiczne. Jednocześnie przedsiębiorstwa oceniają jakość prawa, stabilność energetyczną, ryzyko polityczne oraz możliwość ochrony danych klientów. Serwerownia, podobnie jak port morski w epoce handlu oceanicznego, staje się punktem, w którym geografia gospodarcza łączy się z suwerennością.

Prawne API jako narzędzie zarządzania suwerennością współzależną

W Europie rozwój prawa dotyczącego dowodów elektronicznych podążył równoległą drogą. Szczególnie znamienne jest to, że 18 sierpnia 2026 roku — zaledwie kilka dni przed momentem, w którym prowadzona jest niniejsza analiza — zaczęto stosować unijne rozporządzenie e-Evidence. Wprowadza ono europejskie nakazy wydania i zabezpieczenia dowodów elektronicznych, dzięki którym organ sądowy jednego państwa członkowskiego może, w określonych warunkach, zwrócić się bezpośrednio do wyznaczonej jednostki lub przedstawiciela prawnego dostawcy w innym państwie członkowskim.

Znaczenie tej zmiany nie jest przypadkowe. Unia Europejska mierzy się z problemem podobnym do tego, przed którym stanęły Stany Zjednoczone: tradycyjna pomoc prawna okazuje się zbyt powolna w obliczu dynamiki danych cyfrowych. Nowy system zachowuje jednak strukturę gwarancji, obejmującą między innymi sądowy charakter procedury, środki ochrony, mechanizmy notyfikacji w określonych przypadkach oraz procedurę rozstrzygania konfliktów prawnych.

Dostawca ma co do zasady dziesięć dni na przekazanie danych, a w przypadkach nagłych termin ten może zostać skrócony do ośmiu godzin. Ów ośmiogodzinny limit jest symbolem prawdziwego problemu współczesnego prawa: państwo próbuje przyspieszyć normę do tempa informacji. Dawna dyplomacja mogła operować w cyklach tygodni i miesięcy; cyfrowe śledztwo czasem liczy godziny. Prawo wchodzi w świat czasu niemal maszynowego. Nie powinno to jednak prowadzić do wniosku, że szybkość jest wartością nadrzędną. Najszybszym systemem byłby taki, w którym każdy organ mógłby natychmiast otworzyć dowolną bazę danych — byłby to jednak system nie do pogodzenia z wolnością. Dojrzałość e-Evidence i podobnych konstrukcji będzie zatem oceniana nie tylko przez pryzmat liczby spraw obsłużonych szybciej, lecz przede wszystkim przez skuteczność mechanizmów zapobiegających nadużyciom.

W tym kontekście pojawia się pojęcie comity — trudne do przełożenia na jeden polski termin, lecz kluczowe dla funkcjonowania globalnej chmury. Oznacza ono instytucjonalną powściągliwość wynikającą z uznania, że inne państwo również posiada uprawniony porządek prawny. Nie chodzi tu o bezwarunkowe podporządkowanie się cudzym normom, lecz o to, aby własnej jurysdykcji nie wykonywać tak, jak gdyby inne systemy prawne nie istniały. Cyfrowa neutralność wymaga zatem czegoś więcej niż tylko neutralności technicznej; wymaga pluralizmu prawnego.

Globalna infrastruktura musi nauczyć się funkcjonować w świecie, w którym różne demokracje mogą odmiennie wyważać prywatność, bezpieczeństwo, wolność słowa i kompetencje organów ścigania, a mimo to pozostawać partnerami respektującymi wspólny rdzeń praw człowieka. Nie każdą różnicę można jednak uznać za równoprawny pluralizm. Jeśli państwo domaga się danych w celu prześladowania przeciwnika politycznego, dziennikarza czy grupy religijnej, problem przestaje być zwykłym konfliktem proceduralnym. Powraca pytanie o granicę współpracy z systemem, który wykorzystuje prawo jako instrument represji. Z tego powodu umowy CLOUD Act wymagają określonych standardów praworządności, ochrony prywatności i wolności obywatelskich.

Dostęp do szybszej współpracy informacyjnej staje się zatem przywilejem związanym z jakością instytucji. Można w tym dostrzec narodziny nowej wspólnoty normatywnej: państwa nie tworzą już tylko sojuszy wojskowych i handlowych, lecz również sojusze zaufania informacyjnego. Aby pozwolić obcej policji na szybszy dostęp do danych przechowywanych przez własnych dostawców,

państwo musi uznać, że partner dysponuje dostatecznie wiarygodnym systemem prawa. Elektroniczny dowód staje się sprawdzianem głębokości politycznego zaufania.

Jednocześnie globalna infrastruktura techniczna powoduje, że klasyczna suwerenność przestaje być samowystarczalna. Żadne państwo europejskie nie jest w stanie samodzielnie kontrolować wszystkich usług komunikacyjnych używanych przez swoich obywateli. Nawet wielkie mocarstwa zależą od podmiotów posiadających infrastrukturę w wielu jurysdykcjach. Państwo zachowuje władzę prawną, lecz potrzebuje współpracy sieciowej. To prowadzi do paradoksu suwerenności współzależnej. Im bardziej społeczeństwo staje się cyfrowe, tym bardziej państwo potrzebuje innych krajów i prywatnych przedsiębiorstw, aby skutecznie wykonywać własne suwerenne funkcje. Dochodzenie w sprawie popełnionej we własnym kraju może wymagać danych z zagranicy; bezpieczeństwo infrastruktury może zależeć od zagranicznego producenta; system chmurowy administracji może korzystać z globalnego dostawcy. Suwerenność nie znika, lecz zmienia charakter: z posiadania pełnej kontroli przechodzi w zdolność negocjowania i egzekwowania reguł w sieci współzależności.

Z perspektywy filozofii politycznej jest to zmiana doniosła. Jean Bodin definiował suwerenność przez najwyższą i trwałą władzę we wspólnocie. Cyfrowość pokazuje jednak, że najwyższa władza prawna może współistnieć z głęboką zależnością funkcjonalną. Parlament może uchwalić ustawę, ale wykonanie jej wobec globalnej platformy wymaga technicznej zdolności, jurysdykcyjnego punktu zaczepienia i często współpracy innych podmiotów. Formalna suwerenność bez operacyjnej zdolności może stać się jedynie deklaracją.

Przyszłość prawa danych będzie w coraz większym stopniu prawem interfejsów pomiędzy suwerennościami. Nie wystarczy określić praw jednostki i obowiązków firmy; trzeba ustalać, jak nakazy jednego państwa przechodzą przez system drugiego, jak rozstrzyga się konflikt norm, kto ma prawo odmówić, jak informuje się użytkownika, jakie są terminy i gdzie można zaskarżyć decyzję. Kod potrzebuje protokołów komunikacji; globalne prawo danych potrzebuje ich odpowiedników instytucjonalnych. CLOUD Act i europejskie e-Evidence są próbami zbudowania prawnych API pomiędzy państwem a globalną infrastrukturą.

Metafora ta jest celowo techniczna. API określa, jakie żądania można wysłać do systemu, w jakiej formie i jakiej odpowiedzi można oczekiwać. Prawo transgranicznego dostępu do danych robi coś podobnego: standaryzuje żądanie, określa uprawnionego nadawcę, adresata, warunki wykonania i wyjątki. Różnica jest jednak zasadnicza: w prawnym API po drugiej stronie znajdują się prawa człowieka.

Dlatego nie można go optymalizować wyłącznie pod kątem przepustowości. Jeśli szybkość stanie się jedynym kryterium, narzędzie współpracy może przeobrazić się w instrument transgranicznego nadzoru. Jeżeli natomiast każda procedura pozostanie tak powolna jak w epoce papierowej, prawo okaże się nieskuteczne wobec współczesnej przestępczości. Dojrzała odpowiedź leży pośrodku: szybkość bez samowoli, dostęp bez jurysdykcyjnego imperializmu, współpraca bez likwidacji praw jednostki. Nie jest to pojedyncze rozwiązanie techniczne, lecz architektura instytucjonalna wymagająca ciągłego równoważenia. Sprawa irlandzkiego serwera Microsoftu pozostaje w tym kontekście symbolicznym punktem zwrotnym.

Pokazała ona, że dane mogą znajdować się równocześnie w trzech przestrzeniach: fizycznej, organizacyjnej i prawnej. Fizycznie spoczywają na serwerze w określonym kraju; organizacyjnie pozostają pod kontrolą globalnego przedsiębiorstwa; prawnie zaś podlegają roszczeniom wielu systemów. Żadna z tych sfer nie może być ignorowana bez wprowadzenia nowego rodzaju arbitralności. Z tej historii wynika maksyma cyfrowego ładu: prawo powinno podążać za odpowiedzialnością, lecz nie może bez ograniczeń podążać za techniczną możliwością dostępu. To, że przedsiębiorstwo może nacisnąć przycisk i pobrać dane z innego kontynentu, nie przesądza o tym, że każde państwo ma prawo kazać mu ten przycisk nacisnąć. Jednocześnie fakt, że dysk znajduje się po drugiej stronie oceanu, nie powinien automatycznie tworzyć bezpiecznej przystani dla dowodu poważnego przestępstwa.

Świat cyfrowy potrzebuje nie likwidacji granic, lecz mądrzejszych granic. Takich, które będą przepuszczalne dla legalnej współpracy, ale odporne na arbitralną ingerencję; zdolnych chronić suwerenność, lecz nie zamieniających Internetu w zbiór odizolowanych intranetów państwowych. W przeciwnym razie cyfrowa żelazna kurtyna może powstać nie tylko między mocarstwami, ale pomiędzy każdym systemem prawnym broniącym własnego fragmentu sieci. Zanim jednak dojdziemy do globalnej fragmentacji, należy zająć się bardziej gwałtownym rodzajem przekraczania granic. Nakaz sądowy próbuje przejść przez granicę za pomocą prawa; cyberatak robi to bez pytania. Nie potrzebuje traktatu, umowy wykonawczej ani komitywy między państwami.

Kod może okrążyć świat w ciągu minut, wykorzystać jedną lukę i sparaliżować szpital, przedsiębiorstwo albo fragment administracji. Po sporze o to, kto może legalnie uzyskać dostęp do danych, pojawia się pytanie bardziej elementarne: kto potrafi dostać się do nich bezprawnie – i co dzieje się wtedy z państwem, które całą swoją pamięć i sprawczość oparło na systemach cyfrowych? To prowadzi nas do definicji cyberbezpieczeństwa jako obrony cywilnej XXI wieku.

Przez większą część XX wieku bezpieczeństwo państwa kojarzyło się z armią, granicą, wywiadem, policją, zapasami strategicznymi i odpornością infrastruktury fizycznej. Elektrownia musiała produkować energię, wodociąg dostarczać wodę, szpital leczyć, bank rozliczać płatności, kolej przewozić ludzi i towary, a administracja zachowywać zdolność wydawania decyzji. Cyfryzacja nie unieważniła tych funkcji, lecz wprowadziła nową, wspólną warstwę zależności: każda z nich zaczęła wymagać sprawnego systemu informacyjnego. W rezultacie cyberbezpieczeństwo przestało być specjalistyczną domeną informatyków i stało się współczesną odmianą obrony cywilnej. Zmiana ta jest trudna do dostrzeżenia, ponieważ technologie informatyczne działają najlepiej wtedy, gdy pozostają niewidoczne. Pacjent widzi lekarza, nie serwer uwierzytelniający dostęp do dokumentacji. Podróżny widzi pociąg, a nie system sterowania ruchem.

Klient banku widzi saldo, nie dziesiątki warstw oprogramowania rozliczających transakcję. Urzędnik widzi ekran rejestru, nie zależności sieciowe łączące urząd z centrami danych, dostawcami tożsamości, aktualizacji i usług komunikacyjnych. Im skuteczniej działa infrastruktura cyfrowa, tym łatwiej uznać ją za naturalne tło rzeczywistości. Dopiero awaria odsłania, że współczesne państwo posiada cyfrowy układ nerwowy. WannaCry z maja 2017 roku stał się czymś więcej niż epizodem historii ransomware. Atak objął setki tysięcy komputerów w wielu państwach i szczególnie dotknął brytyjską National Health Service. Część szpitali i przychodni utraciła dostęp do systemów, odwoływano wizyty i zabiegi, a niektóre oddziały ratunkowe musiały przekierowywać pacjentów. Brytyjskie dokumenty publiczne mówiły później o niemal dwudziestu tysiącach odwołanych wizyt i operacji oraz o kilkudziesięciu trustach NHS, których działanie zostało zakłócone. To nie była już „awaria IT" w potocznym znaczeniu – kod uderzył w samą zdolność systemu ochrony zdrowia do wykonywania jego podstawowej funkcji.

Cyberatak może przypominać sabotaż infrastruktury fizycznej bez niszczenia budynków. Szpital nadal stoi, lekarze posiadają wiedzę, aparatura jest sprawna, ale jeżeli przepływ informacji zostaje przerwany, organizacja traci zdolność działania. Cyfrowość tworzy zatem nowy rodzaj kruchości: instytucja może pozostawać materialnie nienaruszona, a funkcjonalnie sparaliżowana.

Wnioski te są kluczowe dla teorii bezpieczeństwa. Infrastruktura krytyczna nie jest już tylko zbiorem obiektów, lecz zbiorem zależności. Elektrownia zależy od systemów sterowania, szpital od dokumentacji, administracja od rejestrów, logistyka od sieci komunikacyjnych, bankowość od systemów rozliczeniowych, a wszystkie te sektory od oprogramowania, aktualizacji, tożsamości cyfrowej i dostawców usług. Najważniejszym zasobem nie zawsze jest urządzenie; czasem jest nim ciągłość relacji pomiędzy urządzeniami. Smith ujmuje tę zmianę w postaci jednej z centralnych mantr: „nie ma bezpieczeństwa narodowego bez cyberbezpieczeństwa". Zdanie to może brzmieć jak slogan konferencyjny, lecz opisuje rzeczywistą zmianę paradygmatu.

Konflikt między ofensywnym wywiadem a bezpieczeństwem zbiorowym

Państwo, którego administracja, energetyka, ochrona zdrowia, łączność i finanse zostały głęboko zinformatyzowane, może posiadać doskonale strzeżone granice fizyczne, a jednocześnie pozostawać podatne na atak przeprowadzony z drugiego końca świata. WannaCry dostarczyło przy tym niepokojącej lekcji na temat odpowiedzialności państwa za luki w oprogramowaniu, które służby mogą wykryć wcześniej niż producenci i użytkownicy. Atak wykorzystywał błąd w systemach Windows, a mechanizm ten był powiązany z narzędziami ujawnionymi po wycieku arsenału przypisywanego amerykańskiej NSA. W metaforyce „Tools and Weapons" exploit przypomina pocisk opracowany w państwowym arsenale, który po utracie kontroli może zostać przejęty przez osoby trzecie. Materiał określa to obrazowo jako sytuację "skradzionego pocisku Tomahawk na pendrive". Metafora ta jest celowo dramatyczna, lecz trafia w istotę problemu.

Państwowe służby wywiadowcze mają uzasadniony interes w poznawaniu podatności oprogramowania, gdyż pozwalają one prowadzić działania wywiadowcze, kontrwywiadowcze i wojskowe. Jednak nieujawniona luka nie jest zwykłą bronią przechowywaną w zamkniętym magazynie – istnieje ona w systemach używanych przez miliony cywilów i przedsiębiorstw. Dopóki producent nie pozna błędu lub nie przygotuje poprawki, luka pozostaje otwartym wejściem do sieci szpitali, szkół, banków i administracji. Powstaje klasyczny konflikt między korzyścią ofensywną a bezpieczeństwem zbiorowym. Wywiad dąży do zachowania podatności ze względu na jej użyteczność operacyjną, podczas gdy społeczeństwo potrzebuje jej ujawnienia, gdyż każda godzina zwłoki zwiększa ryzyko, że ten sam mechanizm odkryje inny napastnik. Państwo staje się zatem jednocześnie strażnikiem bezpieczeństwa obywateli i użytkownikiem narzędzia, którego skuteczność zależy od utrzymywania systemów tychże obywateli w stanie podatności.

Hans Jonas wskazałby zapewne, że jest to podręcznikowy przypadek odpowiedzialności za skutki odległe i pośrednie. Decyzja o zachowaniu exploita nie dotyczy wyłącznie konkretnej operacji służb; może ona generować ryzyko dla nieokreślonej liczby podmiotów. Im bardziej powszechne jest podatne oprogramowanie, tym większa odpowiedzialność za decyzję o zatajeniu luki. Moralność zmienia skalę wraz ze skalą systemu. Nie wynika z tego jednak prosty postulat natychmiastowej publikacji każdej luki – istnieją rzeczywiste potrzeby bezpieczeństwa państwa i sytuacje, w których przedwczesne ujawnienie mogłoby stworzyć dodatkowe zagrożenia. Wynika natomiast konieczność wprowadzenia procedur. Decyzja o zatrzymaniu podatności nie może być jedynie techniczną decyzją jednostki operacyjnej oceniającej wartość wywiadowczą; powinna uwzględniać

rozpowszechnienie produktu, prawdopodobieństwo odkrycia luki przez innych, konsekwencje dla infrastruktury krytycznej oraz skalę potencjalnych szkód.

Jest to cyfrowy odpowiednik dawnej zasady kontroli arsenałów. Broń szczególnie niebezpieczna nie powinna pozostawać wyłącznie w dyspozycji tego, kto potrafi ją skonstruować. Niezbędne są reguły przechowywania, użycia, ujawniania oraz odpowiedzialności za utratę kontroli nad narzędziem. Problem polega na tym, że w cyberprzestrzeni „utrata broni" nie oznacza fizycznego zniknięcia jednego egzemplarza – kod można skopiować, nie odbierając go pierwotnemu posiadaczowi.

Cyberbezpieczeństwo jako ochrona zdolności do prawidłowego wiedzenia

Proliferacja zagrożeń następuje wyjątkowo szybko. Kilka tygodni po WannaCry świat otrzymał jeszcze brutalniejszą lekcję. NotPetya, który pojawił się w czerwcu 2017 roku, początkowo przypominał ransomware, jednak jego działanie miało przede wszystkim charakter destrukcyjny. Brytyjski rząd przypisał ten atak rosyjskiemu wojsku, podkreślając, że głównym celem były ukraińskie sektory finansowe, energetyczne i rządowe, podczas gdy niekontrolowane rozprzestrzenianie się kodu uderzyło również w przedsiębiorstwa poza Ukrainą. NotPetya obnażył zjawisko, którego klasyczna teoria wojny nie znała w takiej postaci: granica pomiędzy celem a ofiarą uboczną może być niezwykle cienka. Kod przeznaczony do destabilizacji jednego państwa, poprzez globalne zależności gospodarcze, może dotknąć podmioty zupełnie niebędące stroną konfliktu. Smith wymienia Maersk, FedEx i Merck, opisując globalny paraliż systemów logistycznych jako efekt rykoszetu ataku skierowanego przeciwko Ukrainie.

Przypadek Maersk stał się niemal archetypem cyfrowej kruchości wielkiej korporacji. Firma dysponowała statkami, kontenerami, terminalami i globalnym personelem, a mimo to utrata funkcjonalności infrastruktury IT dramatycznie ograniczyła zdolność zarządzania tymi zasobami. W narracji pojawia się obraz "ciszy w biurze": komputery i telefony przestają działać, a system, który dotąd był niewidzialnym spoiwem przedsiębiorstwa, nagle znika. Ta cisza ma wymiar filozoficzny.

Pokazuje ona, że nowoczesna organizacja nie jest jedynie zbiorem pracowników i aktywów, lecz przede wszystkim systemem synchronizacji. Informatyka wskazuje ludziom, gdzie znajdują się zasoby, który kontener ma trafić na dany statek, jaka faktura została opłacona oraz jakie zadanie należy wykonać w następnej kolejności. Gdy znika warstwa koordynacyjna, fizyczny majątek pozostaje, lecz traci zdolność wspólnego działania.

Cyberbezpieczeństwo nie powinno być zatem rozumiane wyłącznie jako ochrona poufności. Klasyczna triada bezpieczeństwa informacji obejmuje poufność, integralność i dostępność. W debacie publicznej dominuje pierwsza z tych wartości, gdyż wyciek danych łatwo utożsamić z naruszeniem prywatności. WannaCry i NotPetya przypominają jednak, że dla infrastruktury krytycznej kluczowa jest dostępność. System szpitalny, do którego nikt niepowołany nie uzyskał dostępu, ale którego lekarz nie może uruchomić, pozostaje systemem niebezpiecznym.

Integralność jest kwestią jeszcze subtelniejszą. Jeśli dane zostaną zmienione zamiast skasowane, organizacja może funkcjonować w przekonaniu, że jej obraz rzeczywistości jest prawdziwy, podczas gdy jest on fałszywy. Błędny wynik laboratoryjny, zmieniony parametr przemysłowego systemu sterowania, zmanipulowana lista beneficjentów czy zmodyfikowane dane nawigacyjne mogą być groźniejsze niż całkowite wyłączenie systemu, ponieważ awaria staje się niewidoczna. Można rzec, że cyberatak uderza nie tylko w maszyny, lecz w epistemologię instytucji. Organizacja operuje w zaufaniu, że informacje wyświetlane przez system odpowiadają rzeczywistości. Cyberbezpieczeństwo jest zatem ochroną zdolności instytucji do prawidłowego wiedzenia. Jeśli państwo traci ufność we własne dane, traci nie tylko sprawność techniczną, ale i zdolność do racjonalnego działania.

Odporność staje się więc pojęciem ważniejszym niż sama ochrona. Nie istnieje system całkowicie odporny na włamanie; można jednak projektować organizację tak, aby pojedynczy incydent nie przerodził się w katastrofę. Redundancja, segmentacja, kopie zapasowe, zarządzanie tożsamością, kontrola uprzywilejowanych kont, aktualizacje, testy odtwarzania, plan ciągłości działania i ćwiczenia kryzysowe służą jednemu celowi: atak ma być zdarzeniem, a nie końcem organizacji.

To ten sam sposób myślenia, który stosuje się w przypadku centrów danych. Dojrzały system nie zakłada braku problemów; przyjmuje on, że wystąpi awaria, atak lub błąd i buduje możliwość dalszego funkcjonowania mimo uszkodzeń. Odporność jest więc filozofią instytucjonalnego pesymizmu konstruktywnego. Nie ufa ona bezbłędności pojedynczego komponentu, lecz architekturze zdolnej przetrwać jego porażkę.

Cyberbezpieczeństwo w tym ujęciu jest bliskie klasycznej obronie cywilnej. Ta nie zakłada, że nigdy nie dojdzie do pożaru, powodzi czy nalotu, lecz buduje schrony, procedury ewakuacji i alternatywne kanały komunikacji. Cyfrowa obrona cywilna wymaga podobnej logiki: zapasowych systemów, odseparowanych kopii, procedur działania ręcznego, jasnych kompetencji kryzysowych oraz możliwości szybkiego wsparcia zewnętrznego.

Cyberbezpieczeństwo jako obowiązek organizacyjny i dobro wspólne

Europejskie regulacje coraz wyraźniej przyjmują ten paradygmat. Dyrektywa NIS2 obejmuje osiemnaście sektorów krytycznych, nakładając na wiele średnich i dużych podmiotów obowiązki w zakresie zarządzania ryzykiem cybernetycznym oraz raportowania znaczących incydentów. Katalog ten nie ogranicza się już tylko do energetyki, transportu, bankowości, zdrowia, gospodarki wodnej czy infrastruktury cyfrowej; obejmuje teraz m.in. administrację publiczną, usługi pocztowe i kurierskie, gospodarkę odpadami, część przemysłu oraz wybrane platformy cyfrowe. To istotna ewolucja języka prawa.

Cyberbezpieczeństwo przestaje być dobrowolną „dobrą praktyką IT", a staje się elementem obowiązku organizacyjnego. Zarząd nie może traktować bezpieczeństwa systemów jako domeny wyłącznie administratora sieci, podobnie jak kierownictwo fabryki nie może traktować bezpieczeństwa pożarowego jako prywatnego hobby konserwatora. Ryzyko cyfrowe jest dziś ryzykiem działalności.

NIS2 kładzie nacisk na bezpieczeństwo łańcucha dostaw, obsługę incydentów, zarządzanie podatnościami, kryptografię oraz ciągłość działania. To odpowiedź na rzeczywistość, w której przedsiębiorstwo może być dobrze zabezpieczone wewnętrznie, a mimo to paść ofiarą ataku przeprowadzonego przez słabego dostawcę oprogramowania lub usług. W cyberprzestrzeni bezpieczeństwo najbardziej odpornego podmiotu często zależy od najsłabszego ogniwa jego ekosystemu. Powraca tu znany z innych dziedzin paradoks dobra wspólnego.

Przedsiębiorstwo inwestujące w zabezpieczenia nie chroni wyłącznie siebie, lecz ogranicza prawdopodobieństwo, że jego infrastruktura stanie się punktem wyjścia do ataku na innych. Zaniedbanie prywatnego systemu może generować koszt publiczny. Cyberbezpieczeństwo przypomina pod tym względem epidemiologię: infekcja jednego organizmu ma znaczenie nie tylko dla niego samego, ale i dla całej sieci kontaktów. Ta analogia pozwala lepiej zrozumieć rolę aktualizacji bezpieczeństwa. Patch jest cyfrowym odpowiednikiem szczepienia, gdyż redukuje podatność nie tylko pojedynczego użytkownika, ale i powierzchnię, po której może rozprzestrzeniać się zagrożenie. Choć analogia ta nie jest doskonała, trafnie oddaje charakter zewnętrzności.

Organizacja ignorująca krytyczne poprawki naraża nie tylko własny majątek, lecz może stać się częścią szerszej infrastruktury ataku. Z tej perspektywy kluczowy jest Cyber Resilience Act. Unijne rozporządzenie przesuwa ciężar odpowiedzialności z użytkownika na producenta produktów z elementami cyfrowymi. Bezpieczeństwo nie ma być dodatkiem nakładanym po sprzedaży, lecz

integralną częścią projektowania, rozwoju i utrzymania produktu. Komisja opisuje CRA jako horyzontalne ramy nakładające wymagania cyberbezpieczeństwa na hardware i software przez cały ich cykl życia. Jest to cywilizacyjnie ważna korekta starego modelu rynku. Przez lata obowiązywała cicha asymetria: producent mógł sprzedać urządzenie lub oprogramowanie z niedostatecznym poziomem zabezpieczeń, podczas gdy koszt późniejszego ataku ponosił użytkownik, ubezpieczyciel, infrastruktura publiczna bądź całe społeczeństwo.

Cyberbezpieczeństwo jako nowa forma obrony cywilnej

CRA próbuje przenieść część tej odpowiedzialności wcześniej – do fazy projektowania. W chwili powstawania niniejszego tekstu, 22 sierpnia 2026 roku, szczególnie znamienny jest moment wdrażania tych przepisów. Od 11 września 2026 roku, a więc za niespełna trzy tygodnie, producenci objęci CRA będą musieli raportować aktywnie wykorzystywane podatności oraz poważne incydenty bezpieczeństwa dotyczące produktów z elementami cyfrowymi. Wczesne ostrzeżenie powinno nastąpić co do zasady w ciągu 24 godzin, a pełniejsze zgłoszenie w ciągu 72 godzin. Główna część obowiązków CRA zacznie natomiast obowiązywać od 11 grudnia 2027 roku.

Symbolika tej zmiany jest silna. Podatność przestaje być wyłącznie wewnętrzną informacją producenta; staje się daną o potencjalnym znaczeniu publicznym, którą w określonych warunkach należy wprowadzić do instytucjonalnego obiegu reagowania. Prawo odpowiada w ten sposób na problemunaoczniony przez WannaCry: luka w powszechnym oprogramowaniu może być czymś więcej niż wadą produktu – może stać się elementem ryzyka systemowego. Jednocześnie Unia rozbudowuje zdolność reagowania na kryzysy o charakterze ponadnarodowym. Cyber Solidarity Act, obowiązujący od lutego 2025 roku, ustanowił m.in. europejski system cyberalertów oraz mechanizm reagowania kryzysowego, w tym EU Cybersecurity Reserve – rezerwę usług zaufanych dostawców, która może zostać uruchomiona na wniosek w przypadku poważnego lub wielkoskalowego incydentu.

Sama nazwa „rezerwa” jest znacząca. Państwa od dawna utrzymują rezerwy paliw, leków, sprzętu wojskowego i zdolności ratowniczych; teraz zaczynają gromadzić rezerwę kompetencji cybernetycznych. To dowód na to, że wiedza specjalistów reagujących na incydenty stała się zasobem strategicznym, porównywalnym z innymi zdolnościami kryzysowymi. Cyberbezpieczeństwo wymaga jednak czegoś więcej niż regulacji przedsiębiorstw. NotPetya pokazał, że państwo może traktować kod jako instrument geopolityczny. W takim scenariuszu klasyczny model prawa karnego okazuje się niewystarczający.

Sprawca może znajdować się poza jurysdykcją, być powiązany ze strukturami wojskowymi innego państwa i działać w warunkach, w których techniczna atrybucja jest trudna oraz politycznie obciążona. Atrybucja staje się więc odpowiednikiem ustalenia, kto oddał strzał. Nie wystarczy wiedzieć, że infrastruktura przestała działać; trzeba ustalić, kto przygotował operację, kto ją autoryzował i jaki był jej cel.

Brytyjski rząd wraz z partnerami publicznie przypisał WannaCry aktorom północnokoreańskim, a NotPetya rosyjskiemu wojsku. Takie akty publicznej atrybucji są już elementem dyplomacji bezpieczeństwa: służą nie tylko opisaniu przeszłości, ale próbie podniesienia politycznego kosztu przyszłych operacji. Problem polega na tym, że cyberprzestrzeń osłabia mechanizmy odstraszania znane z epoki nuklearnej. Rakietę balistyczną stosunkowo łatwo powiązać z państwem posiadającym określone systemy; atak cyfrowy może zostać przeprowadzony przez pośredników, z przejętej infrastruktury, przy użyciu narzędzi dostępnych wcześniej innym aktorom. Niepewność atrybucji bywa częścią samej strategii agresora. W takim środowisku szczególnego znaczenia nabierają normy zachowania państw. Postulowana przez Microsoft „Cyfrowa Konwencja Genewska" jest próbą ustanowienia zasady ochrony cywilów i infrastruktury krytycznej przed państwowymi cyberatakami w czasie pokoju. Nie jest to obowiązujący traktat odpowiadający formalnie konwencjom genewskim, lecz normatywna propozycja przeniesienia na cyberprzestrzeń jednej z najważniejszych intuicji prawa humanitarnego: nawet konflikt posiada granice. Postulat ten zasługuje na uwagę, gdyż współczesne społeczeństwo cywilne jest nierozerwalnie splecione z systemami informatycznymi.

Atak na serwer szpitala może oddziaływać na pacjenta równie realnie jak uszkodzenie budynku. Atak na system energetyczny może odciąć ogrzewanie i wodę bez fizycznego niszczenia elektrowni. Atak na logistykę może zatrzymać dostawy leków i żywności. Rozróżnienie między "cyfrowym" i "realnym" skutkiem staje się coraz bardziej sztuczne.

Odpowiedzialność systemowa zamiast indywidualnej cyberhigieny

Jednocześnie należy zachować ostrożność wobec języka wojennego. Nie każdy incydent cybernetyczny jest „cyberwojną", podobnie jak nie każde włamanie do magazynu stanowi operację wojskową. Nadużywanie retoryki wojennej może prowadzić do militaryzacji całej polityki cyfrowej, osłabiając tym samym znaczenie prawa karnego, regulacji oraz standardowego zarządzania ryzykiem. Większość incydentów organizacje powinny traktować jako problem bezpieczeństwa, przestępczości lub odporności, a nie jako casus belli.

Cyberbezpieczeństwo to obszar, w którym źródła zagrożeń są radykalnie zróżnicowane: błąd użytkownika, wadliwa konfiguracja, grupa przestępcza, aktywista, dostawca, insider, służba wywiadowcza czy wojsko mogą wykorzystywać niemal identyczne techniki. Ta sama podatność może służyć kradzieży pieniędzy, szpiegostwu przemysłowemu, represjom politycznym lub przygotowaniu pola walki. Narzędzie samo w sobie nie ujawnia intencji sprawcy, co ponownie prowadzi do centralnego motywu Tools and Weapons. Kod nie zmienia swojej natury fizycznej, gdy przechodzi z laboratorium bezpieczeństwa do arsenału; zmieniają się jedynie cel, uprawnienie i skala skutków.

Exploit może pomóc zespołowi red-team wykryć słabość własnej organizacji lub umożliwić napastnikowi jej zniszczenie. Malware może być obiektem badań albo narzędziem ataku, a skaner podatności może służyć zarówno do zabezpieczania sieci, jak i mapowania celów. Cyberprzestrzeń jest być może najbardziej dosłownym laboratorium ambiwalencji narzędzia.

Etyka odpowiedzialnego ujawniania podatności ma znaczenie znacznie większe, niż sugerowałby język profesjonalnej praktyki. Badacz odkrywający lukę zyskuje chwilową władzę nad przyszłością tysięcy lub milionów urządzeń. Producent otrzymujący zgłoszenie posiada władzę nad szybkością naprawy, natomiast państwo odnajdujące tę samą lukę staje przed wyborem między jej wykorzystaniem a ujawnieniem. Każdy z tych aktorów zajmuje inne miejsce w strukturze instytucjonalnej, lecz wszyscy uczestniczą w zarządzaniu wspólnym ryzykiem.

Można tu zastosować zasadę analogiczną do medycznego primum non nocere. Nie oznacza ona zakazu eksperymentowania ani badań nad ofensywnym bezpieczeństwem, lecz obowiązek świadomości, że wraz ze wzrostem mocy narzędzia rośnie koszt błędu. Smith rozwija tę intuicję aż do postulatu swoistej „przysięgi Hipokratesa” dla programistów. Nie należy jednak przerzucać całej odpowiedzialności na indywidualnego inżyniera, co jest częstym błędem kultury technologicznej.

Jeżeli organizacja nagradza szybkość wdrożenia, ignoruje bezpieczeństwo, ogranicza testy i traktuje aktualizacje jako zbędny koszt, moralny heroizm pojedynczego programisty nie naprawi systemu. Bezpieczeństwo musi stać się elementem ładu korporacyjnego, budżetu, procesu zakupowego i odpowiedzialności zarządu. Podobnie państwo nie może oczekiwać od obywatela, że samodzielnie zapewni bezpieczeństwo środowiska cyfrowego poprzez „mocne hasło”. Indywidualna higiena ma znaczenie, lecz współczesne systemy są zbyt złożone, by odpowiedzialność spoczywała przede wszystkim na użytkowniku końcowym. Jeśli lodówka, samochód, router, implant medyczny czy system przemysłowy zawiera podatne oprogramowanie, konsument często nie posiada technicznej możliwości jego naprawy. Odpowiedzialność musi zatem przesuwać się w stronę producentów, dostawców i instytucji zdolnych faktycznie zmieniać architekturę ryzyka.

Rozwój NIS2, CRA i Cyber Solidarity Act można odczytać jako stopniowe przejście od cyberhigieny indywidualnej do cyberodporności instytucjonalnej. Pierwsza generacja polityki bezpieczeństwa mówiła użytkownikowi: zainstaluj antywirusa i nie otwieraj podejrzanych załączników.

Cyberbezpieczeństwo jako nauka o ciągłości instytucji

Nowa generacja stawia organizacji konkretne wymagania: zarządzaj ryzykiem, kontroluj łańcuch dostaw, raportuj incydenty, aktualizuj produkty, planuj odtworzenie, ćwicz reakcję i przyjmij odpowiedzialność za cykl życia technologii. To proces dojrzewania analogiczny do historii bezpieczeństwa przemysłowego. W XIX wieku wypadek w fabryce mógł być traktowany jedynie jako nieszczęście robotnika. Z czasem jednak wypracowano normy konstrukcyjne, wprowadzono inspekcje i obowiązki pracodawców, procedury awaryjne oraz odpowiedzialność producentów. Społeczeństwo uznało, że ryzyko nie może spoczywać wyłącznie na osobie stojącej najbliżej maszyny.

Cyberbezpieczeństwo przechodzi dziś podobną drogę. Kluczową kategorią tej ewolucji jest odporność społeczna. Nie chodzi tu tylko o ochronę serwerów, lecz o zdolność całego społeczeństwa do zachowania podstawowych funkcji mimo ataku. Czy szpital potrafi działać w trybie awaryjnym? Czy administracja posiada alternatywne kanały komunikacji? Czy istnieją kopie danych odporne na zaszyfrowanie? Czy sektor prywatny może liczyć na wsparcie państwa, a państwa mogą wzajemnie udostępniać sobie kompetencje?

Czy opinia publiczna otrzyma wiarygodną informację zamiast chaosu? Odpowiedź na te pytania decyduje o tym, czy incydent pozostanie zwykłą awarią, czy przerodzi się w kryzys państwowy. Cyberbezpieczeństwo jest bowiem w ostatecznym rachunku nie nauką o komputerach, lecz nauką o ciągłości instytucji. Można sformułować kolejną maksymę niniejszego artykułu: nie ma odpornej cyfrowo organizacji, jeśli jej plan bezpieczeństwa kończy się na zapobieganiu atakowi. Dojrzała organizacja musi zakładać kompromitację części systemu i wiedzieć, jak funkcjonować dalej. Bezpieczeństwo mierzy się nie tylko liczbą udaremnionych włamań, ale czasem odtworzenia, zakresem szkody i zdolnością do zachowania podstawowych usług.

WannaCry i NotPetya nie były jedynie atakami. Były testami architektury cywilizacji cyfrowej. Pokazały, że kod może przekroczyć granice szybciej niż dyplomacja, zaatakować cywilów bez użycia pocisku i uderzyć w organizację poprzez zależność, której wcześniej nie uznawano za strategiczną. Obnażyły również fakt, że narzędzie stworzone przez jednego aktora może po utracie kontroli zostać wykorzystane przez innego, a jego skutki mogą dotknąć ludzi całkowicie nieuczestniczących w pierwotnym konflikcie.

Odpowiedź na te zagrożenia nie może ograniczać się do budowania wyższych murów. Potrzebna jest cała architektura odpowiedzialności: bezpieczne projektowanie, aktualizacje, zarządzanie podatnościami, rozsądne decyzje państw dotyczące exploitów, współpraca międzysektorowa, transparentność, atrybucja, normy międzynarodowe i zdolność odtworzenia po incydencie.

Od ochrony infrastruktury do odpowiedzialności za środowisko informacyjne

Cyberpokój nie jest stanem braku ataków, lecz zdolnością społeczeństwa do ograniczania ich skutków i nakładania kosztów na tych, którzy próbują przekształcić wspólną infrastrukturę w broń.

Pojawia się jednak kolejny problem. Cyberatak może zatrzymać serwer, ale nie musi. Infrastrukturę informacyjną można przejąć w sposób znacznie subtelniejszy: nie niszcząc jej, lecz wykorzystując do wpływania na to, co ludzie widzą, komu ufają i jakie treści uznają za prawdziwe. W takim scenariuszu komputer działa poprawnie, platforma jest dostępna, a użytkownik nawet nie wie, że znalazł się na polu walki.

Po bezpieczeństwie infrastruktury przychodzi zatem kwestia bezpieczeństwa środowiska informacyjnego. Pytanie przestaje brzmieć: kto włamał się do systemu?, a zaczyna: kto i według jakiej logiki decyduje o tym, co system pokazuje człowiekowi? Czy platforma jest listonoszem, wydawcą, czy może architektem przestrzeni informacyjnej?

Choć cyberbezpieczeństwo często opisuje się jako obronę zdolności instytucji do działania, istnieje drugi rodzaj bezpieczeństwa cyfrowego. Jest on znacznie trudniejszy do uchwycenia, ponieważ system nie musi w nim przestać działać. Przeciwnie: może funkcjonować zgodnie z projektem, dostarczać miliony komunikatów na sekundę i perfekcyjnie personalizować strumień treści, a jednocześnie przyczyniać się do degradacji wspólnej sfery informacyjnej.

Cyberatak niszczy lub przejmuje system; operacja wpływu po prostu z niego korzysta. Jeszcze bardziej skomplikowana sytuacja powstaje wtedy, gdy nie ma zewnętrznego napastnika, a źródłem problemu okazują się standardowe mechanizmy biznesowe platform: rankingi, rekomendacje, optymalizacja uwagi czy automatyczne wzmacnianie treści, na które użytkownicy reagują najintensywniej.

W tym kontekście stary spór o odpowiedzialność pośrednika okazuje się niewystarczający. Tradycyjna metafora przeciwstawiała listonosza wydawcy. Listonosz przenosi cudzą wiadomość i

zasadniczo nie odpowiada za jej sens. Wydawca natomiast wybiera, co ukaże się w gazecie, redaguje materiał, ustala hierarchię tematów i świadomie kształtuje przekaz.

Internet stworzył podmioty, które nie mieszczą się w żadnej z tych kategorii. Platforma może nie napisać żadnego z miliardów postów, a jednocześnie zdecydować, który z nich zobaczy milion osób, który zniknie w tle i jaki materiał pojawi się na ekranie po przesunięciu palcem. Ewolucja ta oznacza odejście od roli pasywnego pośrednika ku odpowiedzialności zarządcy; technologie projektowane jako kanały komunikacji zaczęły same organizować warunki widzialności przekazu. Wymaga to jednak istotnego doprecyzowania prawnego.

Analiza zestawia w jednym obrazie Electronic Communications Privacy Act, Stored Communications Act oraz sekcję 230 amerykańskiego Communications Decency Act. Choć funkcjonalnie wszystkie dotyczą relacji pośrednika z komunikacją użytkowników, dogmatycznie rozwiązują różne problemy. ECPA i Stored Communications Act skupiają się na prywatności komunikacji i dostępie do jej treści, natomiast sekcja 230 dotyczy odpowiedzialności usług internetowych za informacje dostarczane przez innych. Rozdzielenie tych porządków jest konieczne, aby metafora listonosza nie zastąpiła rzetelnej analizy prawnej.

Sekcja 230 do dziś zachowuje swoją główną zasadę: dostawca lub użytkownik interactive computer service nie powinien być traktowany jako wydawca lub mówca informacji dostarczonej przez innego information content provider. Jednocześnie amerykański ustawodawca od początku chciał nie tylko chronić rozwój usług internetowych, ale także usuwać bodźce zniechęcające je do moderowania treści. Według stanu prawa obowiązującego w sierpniu 2026 roku konstrukcja ta pozostaje elementem amerykańskiego porządku prawnego, a jej historyczna racjonalność jest zrozumiała.

Odpowiedzialność za architekturę dystrybucji zamiast treści

Gdyby dostawca forum internetowego ponosił automatyczną odpowiedzialność za każdy cudzy komunikat na takich samych zasadach, jak redakcja za własny artykuł, rozwój otwartych usług sieciowych byłby niezwykle trudny. Platforma obsługująca miliardy wypowiedzi nie jest w stanie przeprowadzać kontroli przedpublikacyjnej analogicznej do pracy redakcji gazety. Koszt takiej odpowiedzialności stworzyłby ponadto silny bodziec do nadmiernego usuwania treści. W obawie przed pozwem przedsiębiorstwo racjonalnie eliminowałoby nie tylko wpisy nielegalne, lecz także kontrowersyjne, ryzykowne czy politycznie niewygodne. Odpowiedzialność mająca chronić

społeczeństwo przed szkodliwą mową mogłaby w rezultacie drastycznie zawęzić przestrzeń legalnej wypowiedzi.

Problem polega na tym, że współczesna platforma coraz rzadziej przypomina zwykłą tablicę korkową, na której użytkownicy sami przypinają kartki. Podaż informacji jest tak ogromna, że samo wyświetlenie jakiejkolwiek treści wymaga selekcji. Ranking nie jest więc funkcją dodatkową, lecz warunkiem użyteczności systemu. Użytkownik nie otrzymuje całego Internetu ani wszystkich wpisów osób, z którymi pozostaje w relacji – otrzymuje wybrane uporządkowanie możliwości.

W tym punkcie pojęcie rekomendacji nabiera znaczenia politycznego. Algorytm nie musi tworzyć treści, aby wpływać na jej społeczny odbiór; wystarczy, że zmienia prawdopodobieństwo spotkania człowieka z daną informacją. Dziesięć identycznych komunikatów umieszczonych w różnych miejscach interfejsu nie posiada tej samej siły oddziaływania. Widzialność jest zasobem. Kolejność jest zasobem. Powtórzenie jest zasobem. Sugestia „następnego filmu" czy powiadomienie wysłane w odpowiednim momencie są również zasobami. W gospodarce uwagi dystrybucja staje się częścią znaczenia.

Przeciwstawienie sobie haseł „platforma nie stworzyła treści" i „platforma odpowiada za treść" jest zbyt ubogie. Pomiędzy autorstwem a biernym przesyłaniem istnieje trzecia sfera: odpowiedzialność za architekturę dystrybucji. Można nie odpowiadać za to, że człowiek wypowiedział określone zdanie, a jednocześnie ponosić odpowiedzialność za system, który zdecydował się rekomendować to zdanie milionom odbiorców według wcześniej zaprojektowanego kryterium.

Proponuję zastąpić binarny podział na „listonosza" i „wydawcę" pojęciem architekta środowiska informacyjnego. Architekt nie pisze dialogów ludzi przebywających w budynku, ale kształtuje przestrzeń, w której te rozmowy się odbywają. Decyduje, gdzie znajduje się wejście, dokąd prowadzą korytarze, które pomieszczenie mieści tysiąc osób, a które pięć, oraz jakie bariery oddzielają poszczególne strefy. Platforma czyni podobnie z naszą uwagą: projektuje ścieżki przemieszczania się pomiędzy treściami. Metafora ta nie oznacza jednak, że platforma powinna odpowiadać za każde zdanie wypowiedziane w „budynku" – architekt teatru nie odpowiada przecież za poglądy aktorów.

Odpowiada jednak za bezpieczeństwo konstrukcji, wyjścia ewakuacyjne i parametry przestrzeni, które sam zaprojektował. Podobnie odpowiedzialność platformy powinna być związana przede wszystkim z tymi właściwościami systemu, nad którymi posiada realną kontrolę. Tak rozumiana odpowiedzialność może być stopniowana według kilku zmiennych: wiedzy o ryzyku, zdolności kontroli, stopnia aktywnego wzmacniania treści, przewidywalności skutków oraz ekonomicznego udziału w procesie.

Odpowiedzialność za architekturę cyrkulacji zamiast treści

Hosting pojedynczego, nielegalnego wpisu, o którym operator nie wiedział, nie jest tym samym, co świadome utrzymywanie rozpoznanego mechanizmu systematycznie zwiększającego zasięg określonych treści mimo udokumentowanych szkód. Inaczej należy zatem oceniać neutralne narzędzie wyszukiwania, a inaczej system zoptymalizowany pod kątem maksymalizacji konkretnych reakcji, jeśli właśnie ta optymalizacja generuje przewidywalne ryzyko.

Warto jednak zachować ostrożność wobec uproszczonej tezy, że „algorytmy promują skrajności". Choć Smith silnie eksponuje algorytmiczną akceleracją nienawiści, monetyzację emocji i rozwój cyfrowych plemion – a literatura szeroko bada związek systemów rekomendacji z polaryzacją – przyczynowość nie jest tu jednokierunkowa. Algorytm operuje na materiale dostarczonym przez ludzi; odpowiada na zachowania użytkowników i pozostaje uwiązany do modelu biznesowego, struktury sieci społecznej oraz kultury politycznej. Platformy nie stworzyły ludzkiej skłonności do gniewu, plemienności czy poszukiwania sensacji, ale mogą te tendencje skalować. Rozróżnienie to pozwala uniknąć pułapki technologicznego determinizmu.

Polaryzacja istniała przed mediami społecznościowymi, propaganda przed Internetem, a tabloidyzacja przed algorytmami rekomendacji. Nowością jest przede wszystkim szybkość, personalizacja, możliwość eksperymentowania na ogromnych populacjach oraz automatyczne sprzężenie zwrotne. System uczy się reakcji użytkownika, dostarcza więcej podobnych treści, obserwuje kolejną odpowiedź i dokonuje korekty.

To już nie jest zwykłe publikowanie, lecz adaptacyjna dystrybucja informacji. Współczesny feed przypomina raczej dynamiczną redakcję tworzoną indywidualnie dla każdego odbiorcy niż tradycyjną stronę gazety. Różnica pozostaje jednak zasadnicza: człowiek-redaktor posiada intencję semantyczną i rozumie znaczenie wybranych artykułów, podczas gdy system rekomendacji optymalizuje matematyczny wskaźnik bez „rozumienia" politycznego sensu treści. Brak intencji maszyny nie znosi jednak intencji organizacji, która definiuje funkcję celu.

Funkcja celu jest politycznie najważniejszym elementem systemu rekomendacyjnego. Jeśli celem jest maksymalizacja czasu spędzonego w usłudze, liczby kliknięć, sesji, reakcji lub przychodu z reklam, algorytm będzie poszukiwał treści i sekwencji najlepiej realizujących ten rezultat.

Nie trzeba programować polecenia „promuj konflikt". Wystarczy, że konflikt w określonych warunkach skutecznie podnosi wybrany wskaźnik. Norma powstaje zatem jako efekt uboczny

optymalizacji. Tu powraca myśl Lessiga, że kod reguluje. Architektura cyfrowa nie potrzebuje regulaminu sformułowanego w języku zakazów, aby wpływać na zachowania. Przycisk, kolejność wyświetlania, opcja domyślna, wielkość pola tekstowego, licznik popularności, autoplay, infinite scroll, rekomendacja czy powiadomienie to elementy mikroarchitektury decyzji. Każdy z nich osobno może wydawać się banalny, lecz ich suma kształtuje rytm zachowań milionów ludzi.

Europejski Digital Services Act (DSA) odchodzi od prostego pytania o to, czy platforma jest wydawcą, koncentrując się na obowiązkach zarządzania systemem. Artykuł 27 wymaga od operatorów systemów rekomendacji opisania głównych parametrów decydujących o doborze treści oraz wskazania możliwości wpływania na nie przez użytkownika. W przypadku bardzo dużych platform dochodzą obowiązki dotyczące systemowych ocen ryzyka; DSA nakazuje analizować m.in. wpływ algorytmów i systemów rekomendacji, a środki łagodzące mogą obejmować zmianę projektu lub sposobu działania usługi.

Jest to zasadniczo inny model odpowiedzialności niż klasyczna odpowiedzialność wydawcy. Unia Europejska nie uznaje każdej platformy za gazetę, w której operator odpowiada jak redaktor naczelny za każdy wpis użytkownika. Przyjmuje raczej, że im większą władzę systemową posiada platforma, tym większy ma obowiązek rozumieć ryzyka wynikające z własnej architektury i podejmować proporcjonalne działania ograniczające szkody. To przejście od odpowiedzialności za pojedynczy komunikat do odpowiedzialności za warunki cyrkulacji komunikatów.

Takie podejście lepiej oddaje rzeczywistą funkcję wielkich platform, lecz generuje nowe problemy. Regulator nie może po prostu nakazać systemowi „nie polaryzuj społeczeństwa”, gdyż nie istnieje prosty parametr techniczny odpowiadający abstrakcyjnej wartości demokratycznej. Każda próba ograniczania szkód może bowiem wpływać na wolność wypowiedzi, pluralizm, konkurencję polityczną i zdolność mniejszości do przebicia się do opinii publicznej.

Od moderacji treści do odpowiedzialności za architekturę systemów

Współczesny stan egzekwowania DSA pokazuje, że regulacja przesuwa punkt ciężkości z samej treści na projekt systemów. W 2026 roku Komisja Europejska prowadziła postępowania dotyczące między innymi systemów rekomendacji i ryzyk projektowych, a w lipcu tego samego roku wspólny raport Komisji i Europejskiej Rady ds. Usług Cyfrowych ponownie wskazał na zagrożenia wynikające z cech projektowych oraz wpływu systemów rekomendacji na użytkowników.

Jest to istotna zmiana filozofii regulacyjnej. Prawo przestaje traktować interfejs i algorytm jako neutralne opakowanie usługi, a zaczyna widzieć w nich element usługi o znaczeniu społecznym. W lipcu 2026 roku Komisja przedstawiła wstępne ustalenia wobec projektowych cech Facebooka i Instagrama, odnosząc się m.in. do infinite scroll, autoplay, powiadomień oraz wysoce spersonalizowanych systemów rekomendacji. Choć nie jest to jeszcze ostateczny wyrok w kwestii odpowiedzialności, pokazuje on kierunek europejskiej polityki: ocenie podlega nie tylko pojedynczy post, lecz sposób, w jaki platforma organizuje zachowania użytkownika.

Amerykański model pozostaje odmienny. W sprawie Gonzalez v. Google Sąd Najwyższy miał możliwość zajęcia stanowiska wobec relacji między sekcją 230 a rekomendacjami YouTube, jednak w 2023 roku świadomie nie rozstrzygnął szeroko tego problemu. Uznano wówczas, że po wydaniu orzeczenia w powiązanej sprawie Twitter v. Taamneh roszczenia powodów i tak wydawały się niewystarczające. W sprawie Taamneh Sąd uznał – w konkretnym kontekście odpowiedzialności za aiding and abetting terroryzm – że algorytmy rekomendacyjne opisane w pozwie działały zasadniczo jako część ogólnej infrastruktury sortującej treści, a nie jako szczególne wsparcie ISIS.

Rozstrzygnięcia te są ważne, ale nie rozwiązują filozoficznego problemu odpowiedzialności platform. Pokazują raczej, dlaczego nie wolno utożsamiać samego faktu zastosowania algorytmu z aktywnym wspieraniem każdej treści, którą ten wyświetlił. System rankingowy jest niezbędny do funkcjonowania ogromnej bazy informacji; gdyby każda rekomendacja automatycznie generowała odpowiedzialność równą świadomej aprobacie materiału, praktycznie każdy mechanizm wyszukiwania i filtrowania stałby się prawnym ryzykiem. Pytanie powinno więc brzmieć inaczej: kiedy rekomendacja przestaje być neutralną organizacją nadmiaru informacji, a zaczyna być normatywnie istotnym aktem wzmacniania?

Nie da się odpowiedzieć na to za pomocą jednego kryterium. Znaczenie mają konstrukcja funkcji celu, wiedza o ryzyku, stopień personalizacji, charakter treści, skala zasięgu, możliwość wpływania użytkownika na rekomendacje, model monetyzacji oraz reakcja platformy po uzyskaniu wiarygodnej wiedzy o szkodach.

Ekonomia uwagi staje się tu częścią teorii odpowiedzialności. Platforma finansowana z reklam sprzedaje reklamodawcy dostęp do uwagi użytkownika, podczas gdy treści generowane przez samych użytkowników mogą być bezpłatnym surowcem podtrzymującym tę uwagę. W takim modelu przedsiębiorstwo nie jest obojętnym gospodarzem rozmowy – ekonomicznie korzysta z intensywności interakcji. Nie oznacza to, że każda reklama czyni platformę współautorem każdego komunikatu, ale sugeruje, że bodźce biznesowe muszą zostać uwzględnione w analizie tego, dlaczego system promuje jedne zachowania częściej niż inne.

Shoshana Zuboff opisywała gospodarkę cyfrową przez pojęcie kapitalizmu nadzoru i niezależnie od oceny szerokości tej teorii, jej istotna intuicja dotyczy asymetrii poznawczej. Platforma posiada znacznie więcej wiedzy o działaniu własnego systemu niż użytkownik. Wie, jakie przeprowadza eksperymenty, jakie metryki mierzy, które grupy reagują na konkretne bodźce i jak niewielkie zmiany interfejsu wpływają na zachowanie populacji. Użytkownik widzi jedynie gotowy feed i często nie potrafi odtworzyć, dlaczego wyświetlono mu właśnie tę informację.

Ta asymetria poznawcza uzasadnia wymagania transparentności, jednak ona również ma swoje granice. Opublikowanie setek stron dokumentacji technicznej nie musi dawać obywatelowi realnej wiedzy; można być formalnie przejrzystym i praktycznie nieczytelnym. Dlatego kluczowa staje się rozliczalność poprzez instytucje pośrednie: audytorów, regulatorów, naukowców, organizacje społeczne i uprawnionych badaczy zdolnych ocenić systemy na podstawie danych.

DSA rozwija właśnie taki model. Bardzo duże platformy mają nie tylko publikować informacje, ale wykonywać okresowe oceny ryzyka, podlegać audytom oraz – w określonych ramach – umożliwiać dostęp do danych niezbędnych do badania ryzyk systemowych. W lipcu 2026 roku Komisja zaakceptowała plan działań X dotyczący m.in. poprawy dostępu kwalifikowanych badaczy do danych oraz przejrzystości repozytorium reklam. Odpowiedzialność przesuwa się więc od zasady „zaufaj regulaminowi firmy" ku formule „umożliw zewnętrzne sprawdzenie skutków działania systemu". Jest to analogiczne do wcześniejszego przejścia od prywatności deklarowanej do privacy by design. W obu przypadkach społeczeństwo przestaje zadowalać się obietnicą.

Dostawca chmury ma wykazać bezpieczeństwo i rozliczalność, a platforma – że ocenia systemowe konsekwencje architektury rekomendacji. Dojrzała infrastruktura cyfrowa nie powinna być oceniana wyłącznie według tego, co deklaruje, lecz według tego, co potrafi udowodnić o własnym działaniu. Jednocześnie nie można oddać regulatorowi prawa do budowy jednego oficjalnego strumienia prawdy. Demokratyczne społeczeństwo potrzebuje niezgody, satyry, herezji intelektualnej, błędnych hipotez i ostrych sporów. Historia nauki i polityki pełna jest poglądów, które były kiedyś marginalne lub uznawane za niedorzeczne, a później okazały się kluczowe. System bezpieczeństwa informacyjnego, który usuwałby wszystko, co odstaje od konsensusu, sam stałby się narzędziem stagnacji i kontroli.

Należy zatem oddzielać treść nielegalną od treści szkodliwej, lecz legalnej. Pierwsza podlega konkretnym normom prawa; druga wymaga znacznie większej ostrożności.

Odpowiedzialność za architekturę widzialności zamiast cenzury treści

Fałszywe opinie, teorie spiskowe, agresywne wypowiedzi, pseudonaukowe narracje czy polityczne manipulacje mogą szkodzić społeczeństwu, lecz państwo demokratyczne nie powinno automatycznie zyskiwać prawa do ich zakazywania. Właśnie dlatego europejski model ryzyka systemowego częściej nakazuje platformom analizę projektu i ograniczanie amplifikacji, zamiast tworzyć generalny katalog dopuszczalnych poglądów, których obywatel nie mógłby zobaczyć.

Taki podział pozwala zachować konstytucyjny sens wolności słowa. Wolność wypowiedzi nie oznacza prawa do gwarantowanego zasięgu. Człowiek może mieć prawo opublikować daną treść, nie posiadając jednocześnie roszczenia, by prywatny algorytm rekomendował ją milionom użytkowników. Z drugiej strony platforma dysponująca ogromną władzą nad widzialnością nie powinna dowolnie i bez przejrzystych zasad niszczyć zasięgów wypowiedzi tylko dlatego, że są one politycznie niewygodne. Wyłania się zatem nowa warstwa proceduralnych praw cyfrowych: prawo do informacji o regułach moderacji, uzasadnienia decyzji, możliwości odwołania, spójności w egzekwowaniu regulaminu oraz wiedzy o głównych zasadach rekomendacji i realnego wpływu na własny strumień treści.

Nie są to dokładne odpowiedniki konstytucyjnych praw obywatela wobec państwa, gdyż platforma pozostaje prywatnym przedsiębiorstwem. Funkcjonalnie jednak pełnią one podobną rolę: ograniczają arbitralność w środowisku, które stało się kluczową przestrzenią życia publicznego. Habermasowska sfera publiczna zakładała przestrzeń, w której argumenty mogą krążyć, być krytykowane i kształtować opinię publiczną. W epoce platform należy postawić pytanie, którego Habermas w klasycznej teorii nie musiał stawiać z dzisiejszą intensywnością: kto projektuje mechanizm widzialności argumentów? Jeśli debata publiczna przenosi się do prywatnych środowisk sterowanych algorytmicznie, infrastruktura komunikacji zaczyna bezpośrednio wpływać na warunki demokracji. Nie oznacza to, że platforma staje się parlamentem czy sądem konstytucyjnym – takie porównania bywają nadmiarowe. Oznacza natomiast, że prywatna decyzja projektowa może nieść publiczne następstwa. Zmiana algorytmu rekomendacji wprowadzona w siedzibie firmy może zmienić strukturę widzialności politycznej w wielu państwach jednocześnie.

Mamy tu do czynienia z niezwykłą koncentracją funkcjonalnej władzy, choć pozbawioną klasycznej legitymacji publicznej. Najbardziej adekwatną odpowiedzią nie jest zatem przekształcanie platform w urzędy, lecz stworzenie konstytucji odpowiedzialności pośredników. Jej fundamentem powinno być rozdzielenie trzech rodzajów odpowiedzialności: za cudzą treść platforma nie powinna odpowiadać automatycznie jak jej autor; za własne decyzje moderacyjne powinna odpowiadać

według przejrzystych reguł proceduralnych; natomiast za projekt systemów rekomendacji, reklam i amplifikacji winna ponosić odpowiedzialność proporcjonalną do własnej kontroli, skali oraz przewidywalnego ryzyka.

Taki podział pozwala uniknąć dwóch skrajności. Pierwsza głosi: „to tylko platforma, niczego nie tworzy, więc za nic nie odpowiada". Druga twierdzi: „platforma wyświetla treść, zatem odpowiada jak autor każdego słowa". Obie są błędne. Współczesny pośrednik jest jednocześnie gospodarzem cudzej wypowiedzi, projektantem mechanizmów widzialności i przedsiębiorstwem zarabiającym na przepływie uwagi. Każda z tych ról generuje inny rodzaj zobowiązania. Można więc sformułować kolejną maksymę niniejszej analizy: nie odpowiadasz za każde słowo wypowiedziane w przestrzeni, którą stworzyłeś, ale odpowiadasz za reguły, według których jedne słowa otrzymują megafon, a inne zostają bez publiczności. To właśnie „megafon" staje się kluczowym przedmiotem polityki cyfrowej.

Dawny cenzor kontrolował, czy tekst wolno wydrukować. Współczesna władza nad informacją działa subtelniej: tekst pozostaje formalnie dostępny, lecz jest niemal niewidzialny lub przeciwnie – zostaje automatycznie wzmocniony do milionowego zasięgu. W społeczeństwie przeciążonym informacją istnienie treści i jej widzialność to dwie różne rzeczy.

Przyszłe prawo platform będzie prawdopodobnie coraz rzadziej pytać wyłącznie o prawo do publikacji, a coraz częściej o prawo do architektury dystrybucji, która nie byłaby arbitralna, ukryta i społecznie niekontrolowana. Nie chodzi tu o likwidację rekomendacji – bez selekcji współczesny Internet stałby się niemal bezużyteczny.

Algorytmiczna plemienność jako infrastruktura rozszczepienia

Kwestią kluczową jest to, aby system, który nieuchronnie dokonuje selekcji treści, potrafił wykazać zasady, według których wybiera, oraz sposób, w jaki reaguje na przewidywalne szkody wynikające z własnego projektu. W tym miejscu kończy się problem prawnego statusu pośrednika, a zaczyna kwestia psychologii i socjologii odbiorcy. Nawet najlepiej uregulowana platforma oddziałuje bowiem na człowieka wyposażonego w potrzebę przynależności, potwierdzania własnych przekonań oraz identyfikowania przeciwnika w celu podziału świata na „nas" i „ich". Technologia nie stworzyła plemienności, lecz dała jej natychmiastową sieć, nieograniczony zasięg i algorytm zdolny błyskawicznie odnaleźć kolejnego członka grupy.

Warto zatem zejść z poziomu prawa platform na poziom antropologii demokracji. Pytanie brzmi: co dzieje się ze wspólnotą polityczną, gdy każdy obywatel może otrzymać własną, spersonalizowaną

wersję świata? To problem wolności, która nas dzieli — demokracji w epoce algorytmicznej plemienności.

Doprecyzowanie prawne pokazuje, że amerykański ECPA/Stored Communications Act oraz sekcja 230 regulują odrębne problemy, dlatego metafora „wydawca-listonosz" powinna być traktowana jako heurystyka, a nie dokładny opis dogmatyczny. Sekcja 230 nadal opiera się na zasadzie, że usługodawca nie jest traktowany jako wydawca lub nadawca cudzej informacji. Europejski DSA przyjmuje odmienną logikę: obowiązki dotyczą przejrzystości systemów rekomendacji, ocen ryzyka oraz ograniczania wpływu algorytmów; bardzo duże platformy muszą oferować również opcję rekomendacji niewykorzystującą profilowania. Warto odnotować, że Sąd Najwyższy USA w sprawie Gonzalez v. Google nie rozstrzygnął szeroko kwestii ochrony rekomendacji algorytmicznych przez sekcję 230, natomiast w Twitter v. Taamneh uznał — w specyficznym kontekście roszczenia o pomocnictwo terroryzmowi — że ogólne algorytmy rekomendacyjne nie stanowiły same w sobie aktywnego wspierania ISIS.

Jeśli spojrzymy na platformę jako architekta środowiska informacyjnego, kolejny krok musi dotyczyć człowieka zamieszkującego tę architekturę. Technologia nie komunikuje się bowiem z abstrakcyjnym, idealnie racjonalnym obywatelem teorii politycznej, lecz spotyka człowieka społecznego: poszukującego przynależności, uznania i prostych narracji porządkujących złożoność świata. To właśnie dlatego media społecznościowe mogą jednocześnie zwiększać wolność komunikacji i osłabiać zdolność społeczeństwa do prowadzenia wspólnej rozmowy. Jest to paradoks wolności, która nas dzieli: technologia zaprojektowana jako infrastruktura połączenia może stać się infrastrukturą rozszczepienia.

Nie byłoby jednak naukowo uczciwe twierdzić, że Internet wynalazł plemienność. Człowiek dzielił świat na swoich i obcych na długo przed powstaniem pisma czy sieci społecznościowych. Socjologia konfliktu i psychologia społeczna wskazują, że identyfikacja grupowa jest jedną z elementarnych struktur organizujących relacje społeczne. Henri Tajfel w eksperymentach „minimal group" wykazał, że nawet arbitralne przypisanie do grupy uruchamia preferencje wobec „swoich". Technologia nie stworzyła zatem skłonności do plemienności; może jednak dramatycznie obniżyć koszt odnalezienia grupy, powiększyć jej zasięg i utrzymywać człowieka w ciągłym kontakcie z sygnałami potwierdzającymi przynależność.

Dawne plemię polityczne wymagało miejsca: klubu, gazety, kościoła czy kawiarni. Cyfrowe plemię potrzebuje wyłącznie połączenia z siecią. Człowiek o niezwykle rzadkim przekonaniu może w ciągu kilku minut znaleźć tysiące osób myślących podobnie. Jest to jedno z największych demokratyzujących osiągnięć Internetu, szczególnie dla grup rozproszonych, mniejszości czy obywateli żyjących pod presją większości.

Algorytmiczna personalizacja niszczy wspólne pole odniesienia

Ta sama właściwość pozwala jednak łączyć także ruchy ekstremistyczne, środowiska paranoicznych teorii i wspólnoty zbudowane wokół wzajemnie wzmacnianej nienawiści. Narzędzie to nie posiada bowiem własnego kryterium dobra wspólnoty. Smith określa takie struktury mianem cybertribes, wiążąc ich rozwój z bańkami informacyjnymi oraz algorytmami nastawionymi na treści angażujące.

Pojęcie to jest użyteczne, o ile nie zamieni się w łatwy slogan. Cyfrowa wspólnota nie staje się plemieniem tylko dlatego, że jej członkowie podzielają podobne poglądy – demokracja potrzebuje przecież partii, ruchów społecznych, środowisk intelektualnych i wspólnot światopoglądowych. Problem zaczyna się w momencie, gdy przynależność grupowa reorganizuje kryteria prawdy i moralności: informacja staje się wiarygodna tylko dlatego, że pochodzi od "naszych", przeciwnik jest oceniany nie przez pryzmat argumentów, lecz tożsamości, a kompromis zostaje uznany za zdradę.

W tym kontekście pomocne jest pojęcie polaryzacji afektywnej. Nie oznacza ono zwykłego wzrostu różnic w poglądach. Społeczeństwo może prezentować skrajnie odmienne stanowiska w sprawie podatków, migracji, religii czy polityki zagranicznej i nadal funkcjonować demokratycznie.

Polaryzacja afektywna opisuje raczej wzrost emocjonalnej niechęci wobec ludzi z przeciwnego obozu. Przeciwnik nie tylko myli się co do wysokości podatków; staje się kimś głupim, nieuczciwym, niebezpiecznym albo moralnie skażonym. Spór o politykę przechodzi w spór o człowieczeństwo przeciwnika. Ustrój demokratyczny nie wymaga przecież zgody, lecz uznania przeciwnika za legalnego współuczestnika wspólnoty – kogoś, kto może wygrać wybory bez poczucia u przegranych, że państwo zostało przejęte przez egzystencjalnego wroga. Demokracja potrafi żyć ze sporem o politykę, lecz znacznie gorzej znosi sytuację, w której połowa społeczeństwa interpretuje drugą połowę jako moralnie niedopuszczalną obecność.

Tu powraca Habermasowska idea sfery publicznej. Demokracja potrzebuje nie tylko możliwości wypowiadania się, ale przestrzeni, w której argumenty różnych środowisk mogą się spotkać. Nie chodzi o naiwne przekonanie, że racjonalna debata zawsze doprowadzi do konsensusu, lecz o coś skromniejszego i ważniejszego: społeczeństwo potrzebuje wspólnego pola odniesienia, w którym różne strony rozpoznają przynajmniej sam przedmiot sporu. Cyfrowa personalizacja komplikuje tę konstrukcję.

Dwóch obywateli może formalnie uczestniczyć w tej samej debacie wyborczej, a jednocześnie żyć w radykalnie odmiennych środowiskach informacyjnych. Jeden codziennie ogląda materiały dokumentujące rzekome zepsucie jednej strony, drugi otrzymuje strumień pokazujący wyłącznie patologie strony przeciwnej. Każdy dysponuje bogactwem przykładów potwierdzających własną diagnozę, przez co może doświadczać swojego stanowiska nie jako jednej z możliwych interpretacji rzeczywistości, lecz jako oczywistego rezultatu kontaktu z faktami. W tradycyjnych mediach społeczeństwo również nie posiadało jednego obrazu świata – gazety miały linie polityczne, radio i telewizja dokonywały selekcji, a ludzie wybierali źródła zgodne z ich przekonaniami. Nowość środowiska algorytmicznego polega jednak na indywidualizacji selekcji. Redakcja tworzyła jeden numer gazety dla wielu czytelników; system rekomendacyjny może tworzyć miliony odmiennych sekwencji informacji, aktualizowanych w czasie rzeczywistym pod każdego użytkownika. Powstaje tym samym szczególny epistemiczny problem demokracji: obywatele nie tylko inaczej oceniają te same wydarzenia, lecz mogą coraz częściej w ogóle nie doświadczać tych samych zdarzeń jako społecznie istotnych.

Algorytmy jako wzmacniacze istniejących podziałów społecznych

W jednym środowisku informacyjnym dominującym tematem tygodnia jest korupcja, w drugim migracja, w trzecim przemoc, a w czwartym zagrożenie wojenne. Agenda publiczna przestaje być wspólną kolejką tematów i staje się personalizowaną mapą lęków oraz zainteresowań. Nie należy jednak nadmiernie upraszczać roli algorytmów. Najważniejsze badania eksperymentalne dotyczące Facebooka i Instagrama podczas wyborów w USA w 2020 roku ukazały obraz bardziej złożony niż popularna opowieść o „algorytmie produkującym polaryzację". Ograniczenie ekspozycji na treści pochodzące od osób o podobnych poglądach rzeczywiście zmieniało to, co widzieli użytkownicy, lecz w krótkim okresie nie prowadziło do istotnego zmniejszenia polaryzacji postaw. Badania te wskazują, że choć środowisko platform ma znaczenie, przekonania polityczne są zakorzenione znacznie głębiej i nie można ich „naprawić" pojedynczą zmianą feedu.

To istotne ostrzeżenie przed technologicznym determinizmem. Algorytm może wzmacniać strukturę podziałów, ale nie jest ich jedynym źródłem. Polaryzację budują również nierówności, konflikty kulturowe, historia, organizacja partii, system wyborczy, media tradycyjne, liderzy polityczni oraz realne sprzeczności interesów. Technologia bywa akceleratorem, lecz nie wolno uczynić jej wygodnym kozłem ofiarnym dla konfliktów, które społeczeństwo posiadało już wcześniej. Trafniejsza jest tu metafora wzmacniacza niż generatora. Mikrofon nie tworzy głosu, lecz

sprawia, że usłyszy go cały stadion. System rekomendacyjny nie generuje ludzkiego gniewu, ale potrafi odnaleźć treść zdolną go pobudzić i rozprowadzić ją na wielką skalę. Sieć nie kreuje potrzeby przynależności, lecz pomaga znaleźć grupę, która nazwie frustrację jednostki, wskaże winnego i zapewni społeczne potwierdzenie.

W tym kontekście warto przywołać koncepcję Sherry Turkle i figurę „samotnych razem" (alone together). Paradoks ten jest trafny: urządzenia komunikacyjne potrafią jednocześnie zwiększać liczbę relacji, a zmniejszać intensywność współobecności. Człowiek siedzi przy stole z rodziną, lecz jego uwaga przebywa w kilku odległych wspólnotach; jest fizycznie obecny lokalnie, a społecznie zakotwiczony gdzie indziej. Nie oznacza to, że relacje cyfrowe są z definicji płytsze, lecz że technologia umożliwiła oderwanie wspólnoty psychologicznej od wspólnoty przestrzennej. Ma to fundamentalne konsekwencje polityczne.

Demokracja terytorialna opiera się na współistnieniu ludzi, którzy nie wybrali siebie nawzajem. Mieszkańcy jednego miasta czy państwa muszą wspólnie finansować drogi i szpitale, choć różnią się wartościami i stylem życia. Społeczność internetowa może natomiast powstać poprzez dobrowolną selekcję podobieństwa. Jeśli coraz większa część tożsamości kształtuje się w środowiskach homogenicznych, fizyczny sąsiad staje się psychologicznie bardziej obcy niż nieznajomy z drugiego końca świata. Alexis de Tocqueville widział w stowarzyszeniach szkołę demokracji, gdyż uczyły one współpracy poza strukturami państwa. Cyfrowe zrzeszanie się może pełnić podobną funkcję, pod warunkiem że wspólnota pozostawia otwarte przejścia do innych grup. Gdy jednak grupa nie tylko buduje wewnętrzną solidarność, ale systematycznie demonizuje otoczenie, stowarzyszenie staje się fabryką granic. Wtedy najważniejszym produktem komunikacji politycznej przestaje być argument, a staje się nim tożsamość przeciwnika. Treść zyskuje wartość tylko dlatego, że pokazuje, jacy „oni" są naprawdę. Pojedyncze, skandaliczne zachowanie członka drugiej grupy zaczyna być przedstawiane jako reprezentatywne dla wszystkich – wyjątek staje się esencją.

Media społecznościowe są szczególnie podatne na ten mechanizm: materiał wywołujący moralne oburzenie jest łatwy do zrozumienia i udostępnienia, a użytkownikowi daje natychmiastową możliwość publicznego zamanifestowania przynależności. Polaryzacja zmienia się w performans. Użytkownik nie tylko dowiaduje się o wydarzeniach na świecie; on pokazuje własnej grupie, że stoi po właściwej stronie. Udostępnienie czy oburzony komentarz pełnią funkcję informacyjną i tożsamościową. Platforma staje się więc teatrem moralnego pozycjonowania.

Mechanizm ten jest niezwykle atrakcyjny dla aktorów prowadzących operacje wpływu. Nie muszą oni przekonywać społeczeństwa do jednej doktryny; wystarczy zwiększać wzajemną podejrzliwość, radykalizować linie konfliktu i wmawiać grupom, że państwo nie jest już wspólnym

przedsięwzięciem. Sukces propagandy nie polega tu na tym, że wszyscy uwierzą w to samo, lecz na tym, że nikt nie będzie już wierzył nikomu spoza własnego obozu.

Ten aspekt podkreśla analiza działań rosyjskiej Internet Research Agency (IRA). Dwupartyjny raport senackiej komisji ds. wywiadu USA z 2019 roku potwierdził, że operacja IRA wykorzystywała media społecznościowe do siania niezgody i ingerowania w debatę wokół wyborów prezydenckich w 2016 roku. Najbardziej niepokojącą cechą takich operacji jest to, że propaganda może podszywać się pod autentyczną aktywność obywatelską. Konto nie musi występować jako głos obcego rządu; może udawać lokalnego aktywistę, medium regionalne czy zwykłego, oburzonego użytkownika. Wówczas komunikat nie przychodzi z zewnątrz wspólnoty – on udaje, że narodził się w jej wnętrzu.

Od dominacji narracji do systemowego cynizmu

Analizy Senatu dotyczące IRA opisywały szerokie wykorzystywanie różnorodnych platform, tożsamości i tematów społecznych w celu zaogniania napięć. Przesłuchania ekspertów wskazywały ponadto na możliwość manipulowania mechanizmami trendów, wyszukiwania i rekomendacji, co pozwalało materiałom pozornie oddolnym uzyskać znacznie większą widzialność.

Mamy tu do czynienia z nową postacią starej propagandy: to już nie plakat zawieszony przez jawnego nadawcę, lecz komunikat włączony w organiczny rytm rozmowy. O ile propaganda XX wieku często dążyła do zbudowania jednej, dominującej narracji, o tyle propaganda sieciowa może operować nadprodukcją treści sprzecznych. Zamiast przekonywać odbiorcę do jednej wersji wydarzeń, bombarduje się go ich wielością, aż utraci on wiarę w samą możliwość poznania prawdy. Cynizm staje się wtedy politycznym rezultatem operacji informacyjnej. Obywatel przestaje mówić „wierzę w tę wersję", a zaczyna twierdzić: „wszyscy kłamią".

Degradacja procedur faktualnych niszczy fundamenty demokracji

Jest to dla demokracji szczególnie destrukcyjne, ponieważ system przedstawicielski opiera się na instytucjonalizowanym sporze, lecz wymaga pewnego minimalnego poziomu zaufania epistemicznego. Możemy różnić się w kwestii polityki budżetowej, ale musimy mieć możliwość uzgodnienia, czy parlament uchwalił ustawę. Możemy odmiennie oceniać wybory, jednak muszą istnieć procedury zdolne wiarygodnie ustalić ich wynik. Możemy krytykować sąd, lecz musi istnieć rozpoznawalny dokument wskazujący, jakie orzeczenie wydał.

Demokracja nie potrzebuje pełnego konsensusu co do prawdy, lecz instytucji wspólnego ustalania faktów. Nauka, sądy, profesjonalne media, statystyka publiczna, komisje wyborcze i audyt pełnią odmienne role, ale łączy je funkcja epistemiczna: tworzą procedury pozwalające społeczeństwu rozstrzygać spory bez uciekania się do przemocy. Gdy zaufanie do tych mechanizmów zostaje całkowicie podporządkowane tożsamości politycznej, demokratyczny konflikt zaczyna tracić wspólną podłogę. Hannah Arendt, analizując naturę kłamstwa politycznego i totalitaryzmu, zwracała uwagę na znaczenie faktualności dla przestrzeni publicznej. Nie chodzi tu o naiwną wizję polityki wolnej od perswazji czy interpretacji – polityka zawsze dotyczy ocen. Jednak każda ocena wymaga świata, który w pewnym stopniu pozostaje wspólny.

Jeśli każda grupa posługuje się własnymi faktami, a kryterium prawdziwości staje się lojalność grupowa, spór polityczny traci swój przedmiot.

Najgroźniejszą postacią dezinformacji nie zawsze jest pojedyncze fałszywe zdanie, gdyż fałsz można sprostować. Znacznie groźniejsza jest degradacja zaufania do procedury korygowania fałszu. Jeżeli obywatel uznaje każde sprostowanie za dowód spisku, każdą ekspertyzę za kupioną, każdy sąd za polityczny, a każde medium spoza własnej bańki za propagandę, system traci zdolność samokorekty.

Analogia do cyberbezpieczeństwa okazuje się w tym miejscu niezwykle produktywna. O ile WannaCry niszczył dostępność systemów, o tyle dezinformacja może niszczyć integralność epistemiczną wspólnoty. Pierwszy rodzaj ataku sprawia, że instytucja nie może dostać się do własnych informacji; drugi sprawia, że społeczeństwo nie wie, którym informacjom można ufać. W obu przypadkach uszkodzeniu ulega zdolność działania. Estonia stanowi w tym kontekście symbol przejścia między tymi dwoma wymiarami bezpieczeństwa. Cyberataki z 2007 roku uderzały w strony internetowe i usługi publiczne silnie zinformatyzowanego państwa, unaoczniając zależność społeczeństwa od infrastruktury cyfrowej.

Należy jednak zwrócić uwagę na pewną skrótowość w kwestii atrybucji. Choć estońskie władze wskazywały na rosyjskie źródła i szerszy kontekst polityczny, NATO już w 2007 roku podkreślało trudność definitywnego ustalenia pochodzenia ataków. Bezspornym skutkiem politycznym było natomiast przyspieszenie rozwoju natowskiej polityki cyberobrony. Estonia jest interesująca także z innego powodu.

Budowa architektury odpornej niezgody i zaufania poznawczego

Im bardziej państwo wdraża technologie w usługach publicznych, tym silniej jego sukces zależy nie tylko od bezpieczeństwa technicznego, lecz przede wszystkim od zaufania obywatela do cyfrowej instytucji. E-państwo przestaje funkcjonować, gdy obywatel uznaje każdy rejestr za zmanipulowany, wynik wyborczy za sfałszowany, a komunikaty władzy za operacje propagandowe. Cyfryzacja demokracji zwiększa zatem znaczenie infrastruktury zaufania. Smith odnosi się do tego problemu poprzez programy takie jak AccountGuard oraz ElectionGuard, definiując obronę demokracji jako zadanie wymagające jednoczesnego zaangażowania prawników, inżynierów i kryptografów. Jest to trafna intuicja.

Bezpieczeństwo demokratyczne nie może być już wyłączną domeną komisji wyborczych czy kontrwywiadu. Kampanie polityczne stały się organizacjami cyfrowymi, systemy wyborcze opierają się na technologii, a infrastruktura komunikacyjna należy w dużej mierze do podmiotów prywatnych. Nie wolno przy tym mylić technicznej integralności wyborów z politycznym zaufaniem do nich. Można stworzyć kryptograficznie doskonały system i mimo to przegrać walkę społeczną, jeśli wyborcy nie rozumieją sposobu jego działania lub nie ufają instytucjom go nadzorującym. Bezpieczeństwo, którego obywatel nie potrafi rozpoznać jako takiego, może okazać się niewystarczające do wytworzenia legitymizacji. Stawia to przed demokracją podwójne zadanie: system musi być odporny, a jednocześnie poznawczo dostępny. Audyt, obserwacja wyborów, transparentne procedury, niezależność instytucji i możliwość weryfikacji nie są biurokratycznymi kosztami demokracji – są technologiami społecznego zaufania.

W podobny sposób należy myśleć o przeciwdziałaniu dezinformacji. Odpowiedzią nie może być wyłącznie masowe usuwanie treści; taki model nie tylko zagraża wolności słowa, ale może wzmacniać narrację o ukrytej elicie kontrolującej dopuszczalne poglądy. Potrzebna jest odporność poznawcza: edukacja medialna, zdolność rozpoznawania manipulacji, transparentność reklamy politycznej, uwierzytelnianie źródeł, dostęp badaczy do danych, odpowiedzialność platform za skoordynowane operacje oraz profesjonalne instytucje zdolne do szybkiego dostarczania sprawdzalnych informacji. Klasyczna obrona informacji polegała na zamknięciu bramy. Demokratyczna ochrona środowiska informacyjnego musi działać inaczej, gdyż nie może po prostu zamknąć debaty. Jej zadaniem jest utrzymanie otwartości bez popadania w bezbronność.

Jest to wyzwanie trudniejsze niż cyberbezpieczeństwo. Złośliwy kod identyfikuje się po jego technicznym zachowaniu; złośliwa idea może być jednocześnie legalną opinią. Zhakowany serwer jest zdarzeniem bezpieczeństwa, natomiast człowiek przekonany do radykalnego poglądu nadal

korzysta z wolności politycznej. Demokracja nie może więc zabezpieczać własnej przestrzeni informacyjnej tymi samymi środkami, którymi chroni sieć komputerową. Wolność słowa jest jednocześnie źródłem siły demokracji i jej powierzchnią ataku. Państwo autorytarne łatwiej kontroluje przestrzeń informacyjną, dysponując narzędziami cenzury, które demokracja słusznie odrzuca. Otwarte społeczeństwo jest podatniejsze na manipulację właśnie dlatego, że nie chce prewencyjnie zamykać kanałów komunikacji. Karl Popper pisał o paradoksie tolerancji: porządek tolerancyjny musi rozważyć, jak reagować na działania zmierzające do zniszczenia samej tolerancji.

Cyfrowa demokracja mierzy się z analogicznym paradoksem otwartości. Jej system komunikacyjny powinien pozostać dostępny dla krytyki, protestu i radykalnych idei, lecz właśnie tę otwartość mogą eksploatować aktorzy dążący do zniszczenia zaufania do systemu. Rozwiązaniem nie jest „ministerstwo prawdy", lecz architektura odpornej niezgody. Demokratyczna wspólnota powinna być zdolna do prowadzenia ostrych sporów bez utraty minimalnej zgody co do legalności przeciwnika i procedur pokojowego rozstrzygania konfliktów. Politycy mogą kwestionować rząd, media polityków, obywatele media, a nauka samą siebie – jednak każda z tych instytucji potrzebuje procedur pozwalających odróżnić korektę od czystego cynizmu.

Wolność słowa nie może być redukowana do wolności emisji. W epoce nadmiaru informacji równie ważne stają się kompetencje odbiorcy: krytyczna interpretacja, rozpoznawanie źródeł, rozumienie niepewności oraz umiejętność odróżnienia argumentu od tożsamościowego bodźca. Edukacja obywatelska XXI wieku powinna zatem obejmować nie tylko wiedzę o konstytucji i wyborach, lecz także epistemologię codzienności cyfrowej.

Obywatel musi mieć świadomość, że popularność nie dowodzi prawdziwości, viralność nie jest miarą znaczenia, pewność wypowiedzi nie stanowi dowodu kompetencji, a liczba powtórzeń nie zamienia twierdzenia w fakt. Musi rozumieć, że algorytm rekomendacji nie jest encyklopedią, lecz systemem dokonującym selekcji według określonych kryteriów.

Od wolności komunikacji do odpowiedzialnej architektury sądu

W świecie druku analfabetyzm oznaczał niemożność przeczytania tekstu. W świecie algorytmicznym można biegle czytać i pozostawać funkcjonalnie niepiśmiennym wobec sposobu, w jaki tekst został do nas dostarczony.

Demokratyczne znaczenie edukacji łączy się tu nierozerwalnie z architekturą platform. Nie można wymagać od obywatela absolutnej odporności na system projektowany przez tysiące specjalistów,

którzy analizują miliardy interakcji i eksperymentują ze sposobami utrzymywania uwagi. Odpowiedzialność musi być zatem podzielona: jednostka potrzebuje kompetencji, platforma obowiązków projektowych, państwo rozsądnej regulacji, nauka dostępu badawczego, media norm zawodowych, a politycy minimalnych zasad odpowiedzialności za własną komunikację.

Problem cyberplemienności przestaje być w ten sposób kwestią "złych ludzi w Internecie". Staje się problemem instytucjonalnego ekosystemu, w którym ludzkie predyspozycje, komercyjne modele biznesowe, strategie polityczne i algorytmiczna optymalizacja wzajemnie się wzmacniają.

Nie powinniśmy pytać, czy media społecznościowe są dobre albo złe dla demokracji. Tak zadane pytanie przypomina pytanie o to, czy druk był dobry albo zły dla Europy. Druk umożliwił rozwój nauki, reformację, edukację i nowoczesną administrację, ale jednocześnie otworzył drogę propagandzie, pamfletom nienawiści i masowym mobilizacjom. Technologia komunikacyjna zmienia strukturę możliwości, a społeczeństwo w późniejszym etapie walczy o instytucje zdolne tę strukturę cywilizować.

Błędem pierwszych dekad mediów społecznościowych mogła być wiara, że sama obfitość komunikacji automatycznie poprawi jakość sfery publicznej. Więcej głosów oznacza większą wolność wypowiedzi, lecz niekoniecznie więcej wiedzy. Więcej połączeń zwiększa zdolność organizacji, ale nie automatycznie buduje solidarność. Większy dostęp do informacji daje możliwość poznania świata, ale jednocześnie pozwala wybierać wyłącznie te fragmenty rzeczywistości, które potwierdzają wcześniejsze przekonania.

Można sformułować następującą maksymę: demokracja nie potrzebuje społeczeństwa, które myśli jednakowo; potrzebuje społeczeństwa, które mimo różnic potrafi rozpoznać wspólny świat. Jeżeli narzędzia komunikacji niszczą tę zdolność, wolność może paradoksalnie osłabiać własne instytucjonalne fundamenty. Nie jest to wyraz nostalgii za epoką kilku stacji telewizyjnych i redakcyjnych gatekeeperów – dawny system również wykluczał głosy, reprodukował hierarchie i koncentrował władzę nad informacją.

Internet naprawił wiele z tych wad. Zadaniem nie jest powrót do świata, w którym nieliczni decydowali o tym, co miliony mają usłyszeć. Wyzwaniem jest stworzenie świata, w którym miliony mogą mówić, ale mechanizmy organizujące ich uwagę nie stają się niewidzialną machiną wzajemnej radykalizacji.

Źródłowa formuła "wolność, która nas dzieli" nie powinna być odczytana jako oskarżenie wolności. Jest raczej ostrzeżeniem przed pomyleniem braku barier komunikacyjnych z istnieniem zdrowej sfery publicznej. Wolność wymaga czegoś więcej niż tylko otwartej bramy – potrzebuje kultury

odpowiedzialności, instytucji zaufania, prawa proceduralnego i człowieka zdolnego żyć obok kogoś, kto myśli inaczej.

Czas wejść w problem jeszcze głębszy. Dotychczas algorytmy wybierały przede wszystkim to, co człowiek zobaczy. Sztuczna inteligencja coraz częściej uczestniczy jednak w określaniu tego, co system uzna za prawdopodobne, ryzykowne, wiarygodne, właściwe albo dopuszczalne. Przechodzimy od automatyzacji dystrybucji do automatyzacji oceny. To jakościowo nowa granica. Podczas gdy system rekomendacji układa kolejność wiadomości, system AI może klasyfikować twarz, przewidywać zachowanie, wspierać diagnozę, oceniać ryzyko, generować argument, prowadzić rozmowę, rekomendować decyzję albo uczestniczyć w wyborze celu wojskowego.

Wraz z tym przesunięciem pytanie o wolność informacyjną przechodzi w pytanie o delegowanie sądu maszynie. Myśl więc powinna rozpocząć się tam, gdzie algorytm przestaje tylko porządkować świat, a zaczyna go oceniać: AI – od automatyzacji działania do automatyzacji sądu.

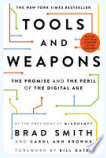
*

Wyraźną oś książki stanowią: "wolność, która nas dzieli", cyberplemiona, alone together, Estonia, rosyjskie operacje wpływu oraz koncepcja ochrony demokracji przez połączenie prawa i technologii. Jednocześnie skorygowałam dwie pokusy nadmiernego uproszczenia obecne w materiale: współczesne badania nie pozwalają sprowadzić polaryzacji politycznej do prostego skutku algorytmu feedu, a atrybucja ataków na Estonię z 2007 roku nie była wówczas przez NATO przedstawiana jako definitywnie rozstrzygnięta. Oficjalne ustalenia senackiej komisji ds. wywiadu USA potwierdzają natomiast szerokie wykorzystanie mediów społecznościowych przez Internet Research Agency do siania społecznej niezgody wokół wyborów w 2016 roku. Badania eksperymentalne Meta i niezależnych uczonych z 2023 roku pokazują zaś ważną rzecz dla całej argumentacji artykułu: algorytmy wpływają na ekspozycję informacyjną, ale krótkoterminowa zmiana struktury feedu nie wystarczyła do znaczącego obniżenia polaryzacji postaw, co przemawia za modelem wieloprzyczynowym, a nie technologicznym determinizmem. Fundacja Dobre Państwo prosi o zapoznanie się z kolejnym esejem.

> Wkraczamy w erę, w której maszyny przestają jedynie porządkować strumienie informacji, a zaczynają automatyzować sam proces oceny i sądu nad rzeczywistością. Pozostaje zatem pytanie: czy w świecie, gdzie algorytm decyduje o tym, co jest prawdopodobne lub właściwe, zdołamy zachować przestrzeń dla ludzkiego błędu, intuicji i autentycznego sporu? Być może największym ryzykiem nie jest to, że AI nas

> oszuka, lecz to, że dobrowolnie oddamy jej prawo do definiowania tego, co w ogóle uznajemy za prawdę.

Inspiracje

[1] 

"Tools and Weapons" Brad Smith

2019 | Penguin Press | ISBN: 978-1984879929

Bradford L. Smith (ur. 1959) to amerykański prawnik i dyrektor ds. technologii, który pełni funkcję wiceprzewodniczącego i prezesa firmy Microsoft. Dołączył do firmy w 1993 roku i odegrał kluczową rolę w radzeniu sobie z wyzwaniami prawnymi i regulacyjnymi Microsoftu, w tym w sporach antymonopolowych i międzynarodowych kwestiach prywatności. Smith jest powszechnie uznawany za orędownika etycznego rozwoju sztucznej inteligencji, cyberbezpieczeństwa i ochrony praw człowieka w erze cyfrowej. Często współpracuje z rządami i organizacjami międzynarodowymi, aby kształtować politykę technologiczną. Poza obowiązkami korporacyjnymi jest znanym mówcą publicznym i autorem, który koncentruje się na styku technologii, prawa i społeczeństwa. Smith jest absolwentem Uniwersytetu Princeton i Columbia Law School, a wcześniej pracował jako asystent sędziego federalnego i adwokat w prywatnej kancelarii.

Bradford L. Smith (born 1959) is an American lawyer and technology executive who serves as the Vice Chair and President of Microsoft. He joined the company in 1993 and has played a central role in navigating Microsoft's legal and regulatory challenges, including antitrust litigation and international privacy issues. Smith is widely recognized for his advocacy regarding the ethical development of artificial intelligence, cybersecurity, and the protection of human rights in the digital age. He frequently engages with global governments and international organizations to shape technology policy. Beyond his corporate responsibilities, he is a prominent public speaker and author who focuses on the intersection of technology, law, and society. Smith holds degrees from Princeton University and Columbia Law School, and he previously worked as a clerk for a federal judge and as an attorney in private practice.

Microsoft

Literatura uzupełniająca

Książki

Książki autorów przywoływanych i literatura pokrewna:



[1] "In the age of the smart machine: The future of work and power"

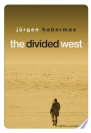
Shoshana Zuboff



[2] "The age of surveillance capitalism: The fight for a human future at the new frontier of power"

Shoshana Zuboff

Hachette UK | ISBN: 9781610395700



[3] "The Divided West"

Jürgen Habermas

John Wiley & Sons | ISBN: 9780745694580



[4] "The Past as Future"

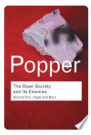
Jürgen Habermas

U of Nebraska Press | ISBN: 9780803272668



[5] "Protestbewegung und Hochschulreform"

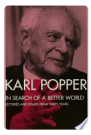
Jürgen Habermas



[6] "The Open Society and Its Enemies"

Karl Popper

2005 | Routledge | ISBN: 9781135552633



[7] "In Search of a Better World"

Karl Popper

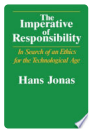
Psychology Press | ISBN: 9780415135481



[8] "Objective Knowledge"

Karl Popper

Taylor & Francis | ISBN: 9781040621004



[9] "The Imperative of Responsibility"

Hans Jonas

1984 | University of Chicago Press | ISBN: 9780226405971



[10] "The Gnostic Religion"

Hans Jonas

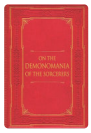
Beacon Press | ISBN: 9780807058008

[11] "De la Démonomanie des sorciers"

Jean Bodin

[12] "I sei libri della Republica, tradotti da Lorenzo Conti"

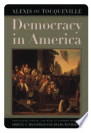
Jean Bodin



[13] "On the Demonomania of the Sorcerers"

Jean Bodin

Independently Published | ISBN: 9798306988702



[14] "Democracy in America"

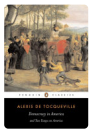
Alexis De Tocqueville

University of Chicago Press | ISBN: 9780226924564



[15] "On the Penitentiary System in the United States and its Application in France"

Alexis De Tocqueville



[16] "Democracy in America and Two Essays on America"

Alexis de Tocqueville

2003 | National Geographic Books | ISBN: 9780140447606



[17] "Responsibility and Judgment"

Hannah Arendt

2003 | Schocken

Artykuły naukowe

Prace autorów przywoływanych w tekście:

[1] "The Imperative of Responsibility: In Search of an Ethics in the Technological Age"

Millett Granger Morgan, Hans Jonas

1985 | Journal of Policy Analysis and Management | DOI: 10.2307/3324683

Źródło

[2] **"The Imperative of Responsibility: In Search of an Ethics for the Technological Age"**

Hans Jonas

1985 | DigitalGeorgetown (Georgetown University Library)

Źródło

[3] **"Philosophical Essays: From Ancient Creed to Technological Man."**

Daniel Sommer Robinson, Hans Jonas

1974 | Philosophy and Phenomenological Research | DOI: 10.2307/2106643

Źródło

[4] **"Technology and Responsibility: Reflections on the New Tasks of Ethics"**

Hans Jonas

2014 | Palgrave Macmillan UK eBooks | DOI: 10.1057/9781137349088_3

Źródło

[5] **"Critique of the Power of Judgment"**

Immanuel Kant

2000 | Cambridge University Press eBooks | DOI: 10.1017/cbo9780511804656

Źródło

[6] **"Anthropology from a Pragmatic Point of View"**

Immanuel Kant

1974 | DOI: 10.1007/978-94-010-2018-3

Źródło

[7] **"Proposing Pattern Growth Methods for Frequent Pattern Mining on Account of Its Comparison Made with the Candidate Generation and Test Approach for a Given Data Set"**

Vaibhav Kant Singh

2018 | Advances in Intelligent Systems and Computing | DOI: 10.1007/978-981-10-8848-3_20

Źródło

[8] **"Jean Bodin: On Sovereignty"**

Jean Bodin

1992 | Cambridge University Press eBooks | DOI: 10.1017/cbo9780511802812

Źródło

[9] **"On sovereignty : four chapters from The six books of the commonwealth"**

Jean Bodin, Julian H. Franklin

1992 | Cambridge University Press eBooks

Źródło

[10] **"Book I, chapter 8, On sovereignty"**

Jean Bodin

Jean Bodin: On Sovereignty | DOI: 10.1017/cbo9780511802812.008

Źródło

[11] **"Free culture: how big media uses technology and the law to lock down culture and control creativity"**

Lawrence Lessig

2004 | Choice Reviews Online | DOI: 10.5860/choice.42-1641

Źródło

[12] **"The future of ideas: the fate of the commons in a connected world"**

Lawrence Lessig

2002 | Choice Reviews Online | DOI: 10.5860/choice.40-0535

Źródło

[13] **"The Regulation of Social Meaning"**

Lawrence Lessig

1995 | The University of Chicago Law Review | DOI: 10.2307/1600054

Źródło

[14] **"Web Privacy with P3p"**

Lorrie Faith Cranor, Lawrence Lessig

2002 | Medical Entomology and Zoology

Źródło

[15] **"In The Age of the Smart Machine: The Future of Work and Power."**

Carmen J. Sirianni, Shoshana Zuboff

1989 | Contemporary Sociology A Journal of Reviews | DOI: 10.2307/2073307

Źródło

[16] **"Big other: Surveillance Capitalism and the Prospects of an Information Civilization"**

Shoshana Zuboff

2015 | Journal of Information Technology | DOI: 10.1057/jit.2015.5

Źródło

[17] **"The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power"**

Shoshana Zuboff

2019

Źródło

[18] **"Surveillance Capitalism and the Challenge of Collective Action"**

Shoshana Zuboff

2019 | New Labor Forum | DOI: 10.1177/1095796018819461

Źródło

[19] **"Political Communication in Media Society: Does Democracy Still Enjoy an Epistemic Dimension? The Impact of Normative Theory on Empirical Research"**

Jürgen Habermas

2006 | Communication Theory | DOI: 10.1111/j.1468-2885.2006.00280.x

Źródło

[20] **"Constitutional Democracy"**

Jürgen Habermas

2001 | Political Theory | DOI: 10.1177/0090591701029006002

Źródło

[21] **"Remarks on Dieter Grimm's 'Does Europe Need a Constitution?'"**

Jürgen Habermas

1995 | European Law Journal | DOI: 10.1111/j.1468-0386.1995.tb00034.x

Źródło

[22] **"Beyond the nation state?"**

Jürgen Habermas

1998 | Peace Review | DOI: 10.1080/10402659808426149

Źródło

[23] "The Social Identity Theory of Intergroup Behavior"

Henri Tajfel, John C. Turner

2004 | Political Psychology | DOI: 10.4324/9780203505984-16

Źródło

[24] "An Integrative Theory of Intergroup Conflict"

Henri Tajfel, John C. Turner

2000 | DOI: 10.1093/oso/9780199269464.003.0005

Źródło

[25] "Social Psychology of Intergroup Relations"

Henri Tajfel

1982 | Annual Review of Psychology | DOI: 10.1146/annurev.ps.33.020182.000245

Źródło

[26] "Social categorization and intergroup behaviour"

Henri Tajfel, M. G. Billig, R. P. Bundy, Claude Flament

1971 | European Journal of Social Psychology | DOI: 10.1002/ejsp.2420010202

Źródło

[27] "Democracy in America."

D. John Pierce, Alexis de Tocqueville, Phillips Bradley, Harold Joseph Laski

1945 | American Sociological Review | DOI: 10.2307/2086177

Źródło

[28] "On the Penitentiary System in the United States and Its Application in France."

Edwin M. Lemert, Gustave de Beaumont, Alexis de Tocqueville, Thorsten Sellin, Herman R. Lantz

1965 | American Sociological Review | DOI: 10.2307/2091170

Źródło

[29] "On the Penitentiary System in the United States and its Application to France"

Gustave de Beaumont, Alexis de Tocqueville

2018 | DOI: 10.1007/978-3-319-70799-0

Źródło

[30] "Federal Theory in Democracy in America"

Alexis de Tocqueville

2005 | Palgrave Macmillan US eBooks | DOI: 10.1007/978-1-137-05549-1_12

Źródło

Artykuły naukowe autora:

[31] "Définir les règles de notre avenir numérique : l'UE est-elle sur la bonne voie ?"

Brad Smith

2021 | RED | DOI: 10.3917/red.003.0139

Źródło

[32] "Direito e Regulação na Internet: desafios jurídicos e oportunidades para o crescimento econômico"

Brad Smith

2012 | Law, State and Telecommunications Review | DOI: 10.26512/lstr.v4i1.21579

Źródło

Treść tworzy Fundacja Dobre Państwo.
Redaguje i publikuje APA ONE, autorski system redakcyjny Fundacji oparty na AI.
APA ONE Publishing System
Fundacja Dobre Państwo © 2026
Article ID: 0b666d42-7570-4692-9aa1-f101e1ddd198