Narzędzia i bronie: architektura odpowiedzialności w cyfrowym archiwum pamięci

AUTOR

Fundacja Dobre Państwo

STRESZCZENIE / ABSTRACT

Tekst analizuje paradoks technologii jako narzędzia i broni, argumentując, że kod komputerowy nie jest neutralny, lecz stanowi środowisko regulujące ludzkie działania. Autor odwołuje się do koncepcji Brada Smitha oraz filozoficznego pojęcia telos, wskazując na niebezpieczny rozdźwięk między techniczną możliwością wykonania zadania a etyczną dopuszczalnością jego realizacji. W dobie AI i wielkich zbiorów danych, twórcy technologii przestają być jedynie producentami, a stają się architektami władzy publicznej. Artykuł postuluje zmianę gramatyki odpowiedzialności: przejście od pytania o to, co systemy potrafią zrobić, ku pytaniu o to, czego powinny dokonywać, aby uniknąć cyfrowego panoptykonu i nadużyć wynikających z asymetrii informacyjnej.

The text analyzes the paradox of technology as both a tool and a weapon, arguing that computer code is not neutral but constitutes an environment regulating human actions. The author refers to Brad Smith's concepts and the philosophical notion of telos, pointing to the dangerous gap between the technical possibility of performing a task and the ethical permissibility of its execution. In the era of AI and big data, technology creators cease to be mere producers and become architects of public power. The article calls for a change in the grammar of responsibility: moving from asking what systems are capable of doing to asking what they should do to avoid a digital panopticon and abuses resulting from information asymmetry.

Współczesna technologia, wbrew powszechnemu przekonaniu o jej neutralności, nie jest jedynie zestawem narzędzi, lecz potężnym wzmacniaczem intencji i struktur władzy. Artykuł stawia tezę, że w dobie cyfrowej asymetrii – gdzie moc obliczeniowa i zdolność do masowej inwigilacji wyprzedzają dojrzałość instytucji nadzorczych – musimy odejść

od naiwnego instrumentalizmu na rzecz modelu odpowiedzialnego powiernictwa (stewardship). Autor analizuje ewolucję archiwum: od glinianych tabliczek po globalną chmurę, która przestała być tylko magazynem danych, a stała się aktywną maszyną predykcyjną i środowiskiem regulującym ludzkie zachowania. Kluczowym wyzwaniem nie jest już samo gromadzenie informacji, lecz stworzenie architektury rozproszonej władzy, w której ochrona prywatności wynika z technicznego oddzielenia możliwości działania od moralnego uprawnienia do jego wykonania. Tekst postuluje przejście od traktowania danych jako 'ropy' (zasobu do wydobycia) ku metaforze 'powietrza' (środowiska), gdzie dostawca infrastruktury nie jest właścicielem, lecz depozytariuszem, a wolność obywatela zależy od istnienia sztywnych granic kontekstowych i realnej możliwości wyjścia z systemu.

SŁOWA KLUCZOWE

architektura odpowiedzialności | cyfrowe archiwum pamięci | moralność skali | powiernictwo danych | stewardship | asymetria instytucjonalna | kod jako architektura władzy | minimalizacja władzy informacyjnej | odpowiedzialność kaskadowa | suwerenność operacyjna | interoperacyjność chmurowa | cyfrowy panoptikon | determinizm technologiczny | governance danych | Data Act

Technologia nie jest neutralnym narzędziem

TOOLS. Kiedy narzędzie staje się bronią. Filozofia narzędzia. Historia cywilizacji jest w znacznej mierze historią narzędzi, lecz byłoby intelektualnym uproszczeniem uznać ją jedynie za kronikę coraz doskonalszych przedmiotów. Narzędzie nie jest bowiem tylko rzeczą sytuującą się pomiędzy dłonią człowieka a materią świata. Jest przedłużeniem zamiaru, multiplikatorem możliwości, magazynem wiedzy i zarazem mechanizmem przesuwającym granicę odpowiedzialności.

Młotek może zbudować dom lub rozbić czaszkę, nóż przygotować posiłek bądź stać się narzędziem przemocy, a kod komputerowy kierować rozrusznikiem serca albo sparaliżować szpital. Właśnie w tym sensie tytułowa antynomia Tools and Weapons Brada Smitha i Carol Ann Browne nie opisuje dwóch odrębnych klas technologii, lecz dwie możliwości wpisane w tę samą strukturę. Najprostsze

narzędzie zawiera już embrion tego paradoksu: jego konstrukcja sugeruje konkretne zastosowanie, lecz nie gwarantuje, że zostanie użyte zgodnie z przeznaczeniem.

Podobnie komputer nie posiada wpisanej w krzem moralności, sieć telekomunikacyjna nie rozróżnia prawdy od kłamstwa, a model sztucznej inteligencji nie otrzymuje wraz z mocą obliczeniową autonomicznego kompasu etycznego. Narzędzie zwiększa zdolność działania, nie powiększając automatycznie zdolności rozpoznawania dobra. Im większy staje się rozdźwięk pomiędzy tymi dwiema sferami, tym poważniejszy jest problem cywilizacyjny. Człowiek potrafi bowiem nauczyć maszynę wykonywać zadania znacznie szybciej, niż zdąży zbudować instytucje zdolne ustalić, które z tych zadań w ogóle powinny być realizowane.

Ta intuicja ma długą genealogię. Greckie technē oznaczało coś więcej niż współczesną technikę; obejmowało umiejętność wytwarzania opartą na wiedzy o celu, materiale i sposobie działania. U Arystotelesa sztuka wytwarzania nie była oderwana od pytania o telos, czyli cel. Jest to kluczowe dla współczesnego sporu technologicznego, ponieważ nowoczesność stopniowo oddzieliła pytanie „jak?" od pytania „po co?". Laboratorium, fabryka i później przedsiębiorstwo technologiczne doskonaliły przede wszystkim samą możliwość wykonania operacji.

Etyka, prawo i polityka miały pojawiać się później – często dopiero w momencie wystąpienia kosztów zewnętrznych. W kulturze cyfrowej owo opóźnienie stało się szczególnie niebezpieczne: pomiędzy prototypem a globalnym wdrożeniem może upłynąć nie pokolenie, lecz kilka miesięcy. Francis Bacon, utożsamiany z maksymą o związku wiedzy i potęgi, trafnie zapowiadał nowoczesny model cywilizacji technicznej. Wiedzieć znaczy coraz częściej móc. Poznanie genomu daje możliwość ingerencji w kod genetyczny, znajomość zachowań milionów konsumentów umożliwia przewidywanie ich decyzji, a gromadzenie gigantycznych zbiorów danych pozwala profilować jednostkę dokładniej, niż mogłoby to uczynić tradycyjne państwo policyjne z armią urzędników.

Jednak w epoce cyfrowej Baconowską maksymę należy uzupełnić: kto potrafi wiedzieć, ten potrafi oddziaływać; a kto potrafi oddziaływać na wielką skalę, ten wchodzi w przestrzeń odpowiedzialności publicznej. W tym punkcie przedsiębiorstwo technologiczne przestaje być wyłącznie producentem. Można zatem zaproponować pierwszą zasadę analityczną niniejszego wywodu: im większa jest zdolność technologii do organizowania zachowań zbiorowych, tym słabsza staje się obrona oparta na twierdzeniu, że jej twórca jedynie dostarczył neutralne narzędzie.

Producent młotka zazwyczaj nie wie, w którą ścianę zostanie wbity gwóźdź. Operator platformy społecznościowej może natomiast projektować mechanizm rekomendacji, obserwować jego skutki, modyfikować kryteria widoczności i zarabiać na konsekwencjach tych wyborów.

Technologia jako środowisko regulujące możliwości działania

Dostawca chmury zna architekturę bezpieczeństwa, lokalizację serwerów, sposób szyfrowania, reguły dostępu oraz prawdopodobne scenariusze ataku. Projektant systemu AI wybiera dane treningowe, funkcję celu i mechanizm walidacji. W obu tych przypadkach technologia nie jest jedynie gotowym przedmiotem, lecz środowiskiem regulującym możliwości działania innych ludzi. Dlatego słynna formuła, którą można wyprowadzić z argumentacji Smitha – nie pytajmy jedynie, co komputery potrafią zrobić, lecz czego powinny dokonywać – nie stanowi retorycznego ornamentu technologicznego humanizmu. Jest zmianą gramatyki odpowiedzialności.

Pierwsze pytanie należy do inżynierii i opisuje możliwość. Drugie dotyczy równocześnie etyki, prawa, ekonomii politycznej i filozofii państwa, gdyż odnosi się do dopuszczalności. Pomiędzy „można" a „wolno" rozciąga się przestrzeń, w której powstaje cywilizacja. Społeczeństwo rezygnujące z tego rozróżnienia przekazuje normatywną władzę temu, kto pierwszy potrafił skonstruować działający system.

Historia Microsoftu opowiadana przez Smitha jest interesująca nie tylko jako kronika przedsiębiorstwa; można ją czytać jak studium dojrzewania instytucjonalnego sektora technologicznego. Wczesna kultura Doliny Krzemowej opierała się w znacznej mierze na przekonaniu, że innowacja zasługuje na domniemanie niewinności. Programista miał tworzyć, przedsiębiorca skalować, rynek wybierać, a państwo nie przeszkadzać. Dopiero konflikty antymonopolowe oraz spory o prywatność, transgraniczny dostęp do danych, cyberbezpieczeństwo i sztuczną inteligencję pokazały, że firma technologiczna może osiągnąć skalę, przy której jej decyzje zaczynają pełnić funkcje quasi-publiczne. To, co początkowo było produktem, staje się infrastrukturą; to, co innowacją – instytucją; to, co kodem – zaczyna organizować rzeczywistość społeczną.

Nie oznacza to jednak, że deklaracje odpowiedzialności korporacyjnej należy przyjmować bezkrytycznie. Etyka przedsiębiorstwa technologicznego może być zarazem autentycznym systemem norm i elementem strategii konkurencyjnej. Prywatność może być prawem człowieka, a jednocześnie cechą produktu budującą przewagę rynkową. Cyberbezpieczeństwo może chronić społeczeństwo, a jednocześnie wzmacniać zaufanie klientów do konkretnego dostawcy chmury. Zasada odpowiedzialnej AI może ograniczać nadużycia i równocześnie tworzyć barierę wejścia dla podmiotów niezdolnych ponieść kosztów zgodności regulacyjnej. Nie ma w tym koniecznie sprzeczności.

Nauki społeczne uczą raczej, że trwałe instytucje powstają często właśnie wtedy, gdy interes i norma zostają splecione. Problem zaczyna się wówczas, gdy język etyki przesłania ekonomię władzy. Martin Heidegger, analizując istotę techniki, ostrzegał przed redukowaniem technologii do zbioru neutralnych instrumentów. Narzędzie nie tylko wykonuje nasze polecenia, lecz zmienia sposób, w jaki ujmujemy rzeczywistość. Samochód nie jest wyłącznie szybszym koniem; przeorganizowuje miasto, przestrzeń, handel, relacje sąsiedzkie i rytm życia. Smartfon nie jest po prostu przenośnym telefonem; zmienił pojęcie obecności, uwagi, prywatności, pamięci i dostępności człowieka dla innych. Wyszukiwarka nie jedynie „znajduje" wiedzę, ale współdecyduje, jaka wiedza stanie się dla odbiorcy widzialna. Model generatywny nie jest tylko szybszą maszyną do pisania; ingeruje w proces wytwarzania tekstu, argumentacji, obrazu i decyzji. Narzędzia wraz z upowszechnieniem zaczynają konstruować warunki, w których sami definiujemy normalność.

Z tego powodu prosty determinizm technologiczny jest równie niewystarczający jak naiwny instrumentalizm. Pierwszy głosiłby, że technologia sama prowadzi społeczeństwo w określonym kierunku; drugi – że wszystko zależy wyłącznie od człowieka, ponieważ narzędzie jest niewinne. Bardziej przekonujący jest model współkonstytuowania.

Człowiek projektuje technologię, lecz następnie technologia restrukturyzuje zbiór możliwych zachowań człowieka. Architektura autostrady wpływa na rozwój przedmieść; architektura aplikacji na sposób komunikowania; architektura algorytmu rekomendacyjnego na dystrybucję uwagi; architektura chmury na geograficzne i prawne położenie danych.

Kod jako architektura władzy i regulacji

Kod nie odbiera człowiekowi wolnej woli, lecz może sprawić, że jedne zachowania staną się tańsze, a inne droższe; jedne zostaną wyeksponowane, inne ukryte, jedne nagrodzone, a pozostałe uczynione praktycznie niewidzialnymi. Lawrence Lessig ujął tę zależność w prowokacyjnej intuicji: kod również reguluje. O ile w świecie analogowym zachowanie obywatela ograniczały przede wszystkim prawo, normy społeczne, rynek i fizyczne właściwości środowiska, o tyle w rzeczywistości cyfrowej do tego zestawu dołącza architektura oprogramowania.

Drzwi można otworzyć mimo zakazu, godząc się na konsekwencje prawne. System informatyczny może natomiast sprawić, że określona operacja będzie technicznie niedostępna. Regulacja przesuwa się zatem z poziomu normy nakazującej zachowanie na poziom architektury, która to zachowanie prekonfiguruje. Właśnie dlatego dyskusja o programowaniu jest w istocie dyskusją o ustroju: pytamy, kto ustala reguły, kto może je zmienić, kto kontroluje kontrolującego i kto ponosi odpowiedzialność za rezultat.

Technologia styka się tu z klasycznym problemem politycznym, opisanym na wieki przed powstaniem pierwszego komputera: problemem władzy. Władza nie sprowadza się bowiem wyłącznie do możliwości wydania polecenia. Oznacza ona również zdolność do wyznaczania pola wyboru, gromadzenia informacji, określania widzialności czy definiowania kategorii, według których człowiek jest oceniany, a nawet przewidywania jego zachowań. Michel Foucault wykazał, że nowoczesna władza nie musi stale uderzać pałką; może obserwować, klasyfikować, rejestrować i normalizować. Benthamowski panoptikon był budynkiem. Cyfrowy panoptikon nie potrzebuje centralnej wieży, ponieważ obserwacja może zostać rozproszona pomiędzy urządzenia, serwery, sensory, aplikacje i modele analityczne. Nie oznacza to jednak, że chmura, platforma czy sztuczna inteligencja nieuchronnie prowadzą do totalitaryzmu.

Taki wniosek byłby publicystycznym skrótem, a nie analizą. Wynika z tego natomiast coś bardziej wymagającego: infrastruktura zdolna do obserwowania, klasyfikowania i przewidywania zachowań posiada potencjał władzy niezależnie od deklarowanych intencji jej aktualnego administratora. Demokratyczne instytucje projektuje się właśnie po to, by nie uzależniać wolności od nadziei, że władza zawsze znajdzie się w dobrych rękach. Konstytucja nie jest komplementem dla dobrego monarchy; jest zabezpieczeniem na wypadek pojawienia się złego.

Moralność skali i asymetria między technologią a instytucjami

Analogicznie prywatność, szyfrowanie, kontrola dostępu, audytowalność algorytmów i zasada minimalizacji danych nie są wyrazem nieufności wobec technologii jako takiej. Stanowią one technologiczne odpowiedniki podziału władz. Z tej perspektywy szczególnego znaczenia nabiera maksyma obecna w filozofii Tools and Weapons: jeżeli twoja technologia zmienia świat, nie możesz umywać rąk od świata, który pomogłeś stworzyć. W tym zdaniu pobrzmiewa problem odpowiedzialności znacznie starszy niż informatyka. Hans Jonas, konstruując etykę odpowiedzialności dla cywilizacji technologicznej, zwracał uwagę, że tradycyjna moralność była przygotowana przede wszystkim do oceny działań bliskich w czasie i przestrzeni. Tymczasem nowoczesna technologia generuje skutki rozproszone, globalne, długotrwałe, trudne do odwrócenia i często niemożliwe do przypisania pojedynczemu sprawcy. Elektrownia, sieć społecznościowa, globalna chmura czy duży model AI zmieniają horyzont etyki, ponieważ skala skutku staje się większa niż bezpośrednie doświadczenie podmiotu działającego. W informatyce problem ten zostaje jeszcze zaostrzony przez skalowalność.

Błąd rzemieślnika może uszkodzić jeden przedmiot. Błąd w szeroko wykorzystywanym oprogramowaniu może dotknąć milionów urządzeń jednocześnie. Uprzedzenie jednego urzędnika krzywdzi osoby, z którymi przyjdzie mu wejść w interakcję; uprzedzenie zakodowane w systemie automatycznej kwalifikacji może zostać zastosowane tysiące razy dziennie. Kłamstwo wypowiedziane w gospodzie ma naturalnie ograniczony zasięg; fałszywa informacja promowana przez mechanizm wiralności może obiec planetę przed obiadem. Cyfrowość wprowadza zatem nową kategorię: moralność skali. Czyn znany historii uzyskuje właściwość dotąd rzadką – niemal zerowy koszt reprodukcji.

W tym kontekście metafora brzytwy w ręku dziecka uzyskuje swój ciężar. Problemem nie jest złośliwość dziecka ani złośliwość brzytwy, lecz asymetria pomiędzy siłą narzędzia a dojrzałością podmiotu, który nim rozporządza. Cywilizacja cyfrowa doświadcza podobnej asymetrii instytucjonalnej. Rozwinęła systemy zdolne wykonywać miliardy operacji, zanim stworzyła wystarczająco dojrzałe reguły ich wykorzystania. Technologia przyspiesza wykładniczo, podczas gdy prawo zmienia się deliberacyjnie, polityka wyborczo, kultura pokoleniowo, a moralność poprzez powolny proces społecznego uczenia.

"Szybcy" inżynierowie i "wolne" instytucje nie są zatem tylko dwoma zawodowymi temperamentami. Reprezentują dwie różne temporalności nowoczesności. Nie należy przy tym mylić szybkości prawa z jego jakością. Próba legislacyjnego ścigania każdej innowacji może prowadzić do regulacyjnej gorączki, w której norma dezaktualizuje się przed wejściem w życie. Alternatywą nie jest jednak laissez-faire. Potrzebne są zasady bardziej odporne na zmiany technologiczne niż szczegółowe katalogi urządzeń: ochrona godności, prywatności i autonomii, możliwość zakwestionowania decyzji, odpowiedzialność człowieka za użycie systemu, proporcjonalność ingerencji, przejrzystość tam, gdzie jej brak tworzy asymetrię władzy, bezpieczeństwo projektowane od początku oraz możliwość audytu. Prawo nie musi wiedzieć, jaki procesor zostanie skonstruowany za pięć lat, aby wiedzieć, że człowieka nie wolno pozbawiać podstawowych praw tylko dlatego, że decyzję podjęła maszyna. Rozróżnienie między tool i weapon nie przebiega więc przez katalog produktów, lecz przez sposób organizacji instytucji.

Ten sam mechanizm rozpoznawania obrazu może pomagać osobie niewidomej rozumieć otoczenie lub służyć aparatowi państwa do identyfikowania demonstrantów. Ten sam system analizy języka może wspierać lekarza w dokumentacji albo umożliwiać przemysłową produkcję dezinformacji. Ta sama chmura może przechowywać dokumentację medyczną ratującą życie i tworzyć techniczne warunki masowej inwigilacji. Ta sama luka bezpieczeństwa może służyć państwu jako narzędzie wywiadowcze, by po utracie kontroli zostać wykorzystana przez przestępców przeciwko szpitalom, przedsiębiorstwom i obywatelom.

Technologia jako wzmacniacz intencji i instytucji

Narzędzie i broń to często ten sam artefakt, zależnie od tego, z której strony systemu odpowiedzialności na niego spojrzymy. Stąd wyłania się druga zasada niniejszej analizy: nie istnieje odpowiedzialna technologia bez odpowiedzialnej architektury instytucjonalnej. Etyka programisty jest niezbędna, lecz sama w sobie niewystarczająca.

Wymagane są procedury organizacyjne, odpowiedzialność zarządów, prawo i nadzór sądowy, standardy techniczne oraz naukowa falsyfikacja twierdzeń. Konieczne są niezależne audyty, prawo pracowników do sprzeciwu, konkurencja rynkowa i demokratyczna kontrola państwa. Równie niebezpieczny jak niekontrolowany Big Tech byłby regulator przekonany, że państwowa pieczęć automatycznie nadaje technice moralną niewinność. Historia inwigilacji uczy, że państwo samo może stać się najbardziej zmotywowanym użytkownikiem cyfrowej broni. Dlatego prawdziwym przeciwieństwem technologicznego chaosu nie jest wszechmoc regulacyjna, lecz system rozproszonej odpowiedzialności. Monteskiuszowski instynkt podziału władz zachowuje zaskakującą aktualność w epoce serwerów.

Należy ograniczać sytuacje, w których jeden podmiot jednocześnie gromadzi dane, ustala cel ich wykorzystania, projektuje algorytm, dokonuje oceny, podejmuje decyzję i sam rozpatruje skargę na własne działanie. Im bardziej infrastruktura informacyjna koncentruje te funkcje, tym bardziej przypomina władzę ustrojową, nawet jeśli formalnie pozostaje własnością prywatną. W ten sposób dochodzimy do trzeciej i najważniejszej maksymy otwierającej dalszą analizę: technologia nie jest sumieniem cywilizacji; jest wzmacniaczem jej intencji i instytucji.

Demokratyczne państwo może dzięki niej zwiększać dostęp do wiedzy, bezpieczeństwo, ochronę zdrowia i sprawność usług publicznych. Państwo autorytarne z kolei może budować system kontroli o precyzji niedostępnej dawnym policjom politycznym. Odpowiedzialne przedsiębiorstwo może szyfrować dane i przeciwstawiać się nadmiernym żądaniom władz, podczas gdy inne będzie zarabiać na wydobywaniu uwagi, manipulacji lub społecznej podatności.

Chmura jako materialne archiwum ludzkiej pamięci

Sama moc obliczeniowa nie rozstrzyga żadnego z tych wyborów. Największym złudzeniem epoki cyfrowej byłoby zatem przekonanie, że postęp techniczny i moralny poruszają się po tej samej krzywej. Nie istnieje taki automatyzm. Mamy coraz doskonalsze narzędzia, lecz starożytne namiętności; globalne sieci, lecz lokalne uprzedzenia; natychmiastową komunikację, lecz nie natychmiastową mądrość. Możemy transmitować informację wokół Ziemi w ułamku sekundy, ale

wciąż spieramy się o prawdę, władzę, sprawiedliwość, wolność i bezpieczeństwo, posługując się pojęciami rozwijanymi przez tysiąclecia.

Paradoks nowoczesności polega więc nie na tym, że maszyny stają się podobne do ludzi. Być może bardziej niepokojące jest to, że ludzie pozostają ludźmi, otrzymując narzędzia o skali dawniej przypisywanej bogom. Właściwym początkiem rozważań o chmurze nie jest serwer, kabel ani procesor, lecz pytanie o pamięć. Każda cywilizacja istnieje dlatego, że potrafiła przechować więcej doświadczenia, niż mieściło się w pamięci pojedynczego człowieka. Gliniana tabliczka, papirus, kodeks, drukowana książka, archiwum państwowe, kartoteka i dysk twardy są ogniwami jednej historii: historii eksternalizacji ludzkiej pamięci. Współczesna chmura jest jej największym dotychczasowym przedsięwzięciem.

Gdy jednak człowiek przenosi pamięć do infrastruktury, powierza jej nie tylko fotografie i dokumenty. Przenosi fragment własnej tożsamości: historię zdrowia, relacji, majątku, pracy, przekonań i politycznej egzystencji. Kolejny etap analizy musi zatem rozpocząć się od pozornie banalnego pytania: czym naprawdę jest chmura? Nazwa sugeruje coś lekkiego, niematerialnego i unoszącego się ponad światem, podczas gdy rzeczywistość jest niemal odwrotna.

Za metaforą kryją się beton, stal, energia, kable, systemy chłodzenia, jurysdykcje, ochroniarze, kryptografia, umowy, kopie zapasowe i ogromne centra danych. Aby zrozumieć władzę cyfrową, trzeba więc najpierw zejść z chmury na ziemię i wejść do archiwum — od glinianej tabliczki po światową szafę kartoteczną.

Narzędzie jest przedłużeniem ludzkiego działania, archiwum zaś przedłużeniem ludzkiej pamięci. Rozróżnienie to ma większe znaczenie, niż mogłaby sugerować historia bibliotekoznawstwa. Człowiek jest gatunkiem biologicznie wyposażonym w pamięć ograniczoną, zawodną i śmiertelną, a mimo to zbudował cywilizację zdolną kumulować doświadczenia tysięcy pokoleń. Dokonał tego dzięki konsekwentnemu przenoszeniu pamięci poza ciało. Opowieść przekazywana przy ogniu, znak wyryty w kamieniu, gliniana tabliczka, papirus, kodeks, księga drukowana, księga rachunkowa, archiwum państwowe, kartoteka, fotografia, taśma magnetyczna, dysk twardy i chmura obliczeniowa należą do tej samej genealogii. Zmienia się materiał, szybkość dostępu i skala zasobu, ale podstawowa funkcja pozostaje niezmienna: uczynić doświadczenie nieobecnego człowieka dostępnym dla człowieka obecnego.

Pismo było zatem nie tylko wynalazkiem komunikacyjnym, lecz pierwszą wielką technologią rozdzielenia informacji od biologicznej pamięci jej autora. Dopóki wiedza funkcjonowała przede wszystkim oralnie, jej przetrwanie wymagało istnienia wspólnoty pamiętających. Zapis pozwolił informacji przeżyć śmierć świadka.

Archiwum jako instrument władzy i administracji

Jednocześnie stworzyło to nowy rodzaj władzy. Kto potrafił zapisywać, klasyfikować i przechowywać, ten mógł naliczać podatki, rozstrzygać o własności, rejestrować długi, prowadzić wojsko, ustanawiać prawo i odtwarzać poprzednie decyzje. Archiwum od samego początku było zatem jednocześnie magazynem wiedzy i instrumentem administracji. Ten związek pomiędzy pamięcią a władzą powraca w całej historii państwa.

Nieprzypadkowo nowoczesna biurokracja rozwijała się równolegle z coraz doskonalszymi technikami dokumentowania. Państwo bez ewidencji jest organizacją cierpiącą na amnezję. Nie wie, kto jest obywatelem, komu przysługuje własność, kto zapłacił podatek, gdzie przebiega granica, kto został skazany ani jakie zobowiązania przyjęto wczoraj. Max Weber widział w dokumentach i aktach jeden z fundamentów racjonalnej biurokracji. Urząd jest instytucją pamiętającą, a jego przewaga nad jednostką polega między innymi na tym, że posiada pamięć trwalszą niż kadencja urzędnika i dłuższą niż życie petenta.

Biblioteka i archiwum reprezentują jednak dwa odmienne typy pamięci. Biblioteka przechowuje wiedzę przeznaczoną do czytania; archiwum zaś ślady działań, które mogą zostać kiedyś przywołane jako dowód. Biblioteka Aleksandryjska stała się w kulturze Zachodu symbolem ambicji zgromadzenia wiedzy świata, nawet jeśli późniejsze legendy o jej zasobach i zagładzie wielokrotnie wykraczały poza to, co można pewnie odtworzyć historycznie. Jej znaczenie symboliczne pozostaje jednak potężne. Zgromadzenie wiedzy w jednym miejscu było projektem epistemicznym i politycznym zarazem: kto posiada bibliotekę świata, ten tworzy miejsce, do którego świat przychodzi po pamięć.

W materiałach inspirowanych Tools and Weapons właśnie ta metafora zostaje przeniesiona na chmurę. Współczesne centra danych tworzą coś, co można nazwać rozproszoną Biblioteką Aleksandryjską XXI wieku. Różnica polega na tym, że dzisiejsze archiwum nie przechowuje wyłącznie dzieł uznanych za godne zachowania – magazynuje również codzienność: e-mail napisany w pośpiechu, fotografię dziecka, wyniki badań lekarskich, projekt mostu, księgi przedsiębiorstwa, zapisy rozmów, lokalizację samochodu, historię transakcji, dokumentację sądu, mapy wojskowe, kod programu, dane z eksperymentu naukowego czy kopię filmu oglądanego wieczorem. Granica pomiędzy biblioteką, archiwum, sejfem, pamiętnikiem i magazynem danych zaczyna się zacierać.

Chmura stanowi jakościowo nowy etap eksternalizacji pamięci. Dawne archiwa przechowywały bowiem jedynie wybrane reprezentacje życia.

Od pasywnego archiwum do aktywnej maszyny predykcyjnej

Cyfrowa infrastruktura jest w stanie zachować nieprzerwany strumień ludzkiej aktywności. Im więcej czynności zostaje zapośredniczonych przez systemy informatyczne, tym mniej z nich znika bez śladu. Płacimy kartą, wyszukujemy informacje, przemieszczamy się ze smartfonem, rejestrujemy ruch zegarkiem, prowadzimy korespondencję, zapisujemy dokumenty, uczestniczymy w wideokonferencjach czy korzystamy z e-administracji. Każda z tych operacji generuje metadane, logi, identyfikatory i kopie. Cywilizacja cyfrowa nie tylko pamięta więcej – ona coraz częściej pamięta automatycznie.

Właściwość ta odróżnia pamięć cyfrową od tradycyjnego archiwum również w wymiarze epistemologicznym. Dokument papierowy zazwyczaj musiano świadomie stworzyć, nazwać i umieścić w teczce, by później go odnaleźć. System cyfrowy zapisuje dane bez istotnego udziału osoby, której zachowania dotyczą. Człowiek staje się zatem jednocześnie autorem informacji i jej źródłem. Część danych przekazuje intencjonalnie, część wytwarza jako produkt uboczny korzystania z infrastruktury, a jeszcze część zostaje wywnioskowana na podstawie innych obserwacji. Archiwum przestaje być wyłącznie miejscem, do którego wkładamy dokumenty; staje się środowiskiem, które rejestruje zdarzenia.

Tu pojawia się pierwsza zasadnicza różnica między dawną kartoteką a chmurą. Kartoteka przechowywała informację w formie względnie statycznej. Chmura umożliwia natomiast jednoczesne przechowywanie, kopiowanie, indeksowanie, porównywanie i analizowanie danych. Informacja nie tylko „leży” – jest przetwarzana. Z punktu widzenia teorii władzy zmiana ta jest fundamentalna. Biblioteka z milionem książek nie wie automatycznie, które zdania są do siebie podobne; system obliczeniowy potrafi dokonać takiego porównania na gigantyczną skalę.

Archiwum cyfrowe zaczyna więc nie tylko pamiętać przeszłość, ale wytwarzać nową wiedzę o tym, co przechowuje. To przejście można opisać jako ewolucję od pamięci do analityki, a następnie od analityki do predykcji. Zgromadzenie faktów pozwala rekonstruować przeszłość, analiza korelacji umożliwia rozpoznawanie wzorców, natomiast modele predykcyjne pozwalają szacować przyszłe zachowania. W konsekwencji archiwum zyskuje właściwość, której tradycyjna kartoteka prawie nie posiadała: może stać się maszyną przewidywania. Historia zakupów pozwala przewidzieć kolejny produkt, historia spłat kredytu – oszacować ryzyko, dokumentacja kliniczna – ocenić prawdopodobieństwo choroby, a sekwencja zachowań użytkownika – określić treść, która najprawdopodobniej zatrzyma jego uwagę.

Pamięć zostaje włączona w mechanizm podejmowania decyzji. Dlatego tak istotna jest metafora „światowej szafy kartotecznej” obecna w materiale źródłowym. Szafa ta wydaje się przedmiotem banalnym, lecz reprezentuje kluczowy moment w historii zarządzania informacją: przejście od zwykłego przechowywania dokumentu do jego systematycznego porządkowania w celu szybkiego odnajdywania. W tym kontekście przywołany zostaje Edwin Seibel i pionowa kartoteka z końca XIX wieku jako symbol odpowiedzi epoki przemysłowej na narastający nadmiar informacji. Niezależnie od szczegółów technicznych poszczególnych konstrukcji, intuicja pozostaje trafna: rewolucja informacyjna nie zaczyna się w momencie powstania większej ilości danych, lecz wtedy, gdy pojawiają się systemy pozwalające skutecznie nimi zarządzać. Każda epoka produkująca więcej wiedzy niż poprzednia musi wynaleźć własną technologię zapominania i odnajdywania.

Jest to paradoks archiwum: nie sposób korzystać z pamięci totalnej bez mechanizmów selekcji. Biblioteka pozbawiona katalogu staje się magazynem papieru; Internet bez wyszukiwarki byłby oceanem dokumentów pozbawionym nawigacji; ogromny zbiór danych bez indeksowania i algorytmów analitycznych może posiadać wysoką wartość potencjalną, lecz niską wartość operacyjną. Przyrost informacji zwiększa zatem znaczenie tych, którzy kontrolują sposób jej klasyfikowania. Prowadzi to do problemu powracającego: klasyfikacja nie jest neutralna. Każdy katalog przyjmuje określone kategorie, każdy system wyszukiwania ustala kryterium trafności, a każdy model analityczny definiuje zmienne uznane za istotne. Michel Foucault, badając historię wiedzy, wielokrotnie wskazywał, że systemy klasyfikowania rzeczywistości wpływają na sposób jej postrzegania. W epoce algorytmicznej ta intuicja nabiera nowego znaczenia. Kto organizuje archiwum, ten nie tylko porządkuje przeszłość, lecz w części decyduje, jaka przeszłość będzie dostępna i jakie wnioski można z niej wydobyć.

Materialna natura chmury warunkuje suwerenność danych

Słowo „chmura” wykonuje niezwykle skuteczną pracę retoryczną. Sugestia lekkości i bezcielesności skutecznie przesłania materialny charakter całego systemu. Dane zdają się unosić ponad urządzeniem, podczas gdy w rzeczywistości istnieją dzięki bardzo ziemskim składnikom: krzemowi, miedzi, światłowodom, stali, betonowi oraz energii elektrycznej i ludziom utrzymującym infrastrukturę. Kliknięcie ikony obłoku uruchamia procesy zachodzące w budynkach, które częściej przypominają elektrownie lub instalacje przemysłowe niż jakikolwiek obiekt meteorologiczny. Ta demitologizacja ma kluczowe znaczenie polityczne.

Gdyby chmura była rzeczywiście bezmiejscowa, można by uznać, że problem terytorium przestał istnieć. Tymczasem centrum danych zawsze gdzieś stoi. Korzysta z konkretnej sieci energetycznej, podlega prawu określonego państwa, jest chronione przez lokalne służby i znajduje się w zasięgu kompetencji organów publicznych. Informacja może być logicznie globalna, lecz jej infrastruktura pozostaje geograficzna. Świat cyfrowy nie unieważnił terytorium; uczynił jedynie relację między terytorium a informacją znacznie bardziej skomplikowaną.

Studium centrum danych w Quincy w stanie Waszyngton dobrze obrazuje sprzeczność między wizualną prostotą interfejsu a przemysłową złożonością zaplecza. Opis obejmuje potężne źródła zasilania, systemy redundancji oraz wielopoziomowe zabezpieczenia fizyczne: od kontroli biometrycznej po procedury niszczenia zużytych nośników. Dysk, będący dla użytkownika abstrakcyjnym miejscem przechowywania pliku, pod koniec swojego życia może zostać fizycznie unicestwiony, aby informacja nie przetrwała na materialnym nośniku w sposób niekontrolowany. W tej scenie kryje się filozoficzny paradoks cyfrowości: informacja wydaje się niematerialna, ale jej bezpieczeństwo zależy od materii. Prywatność może wymagać kuloodpornych drzwi.

Ciągłość działania aplikacji zależy od generatora, a suwerenność danych od lokalizacji budynku. Cyberbezpieczeństwo zaczyna się nie tylko od kryptografii, lecz również od tego, kto ma dostęp do pomieszczenia z serwerami. Najbardziej abstrakcyjny zasób współczesnej gospodarki opiera się na jednej z najbardziej materialnych infrastruktur, jakie kiedykolwiek zbudowano. Centrum danych jest jednocześnie biblioteką, fabryką i twierdzą. Biblioteką, bo przechowuje pamięć; fabryką, bo nieprzerwanie przetwarza informacje; twierdzą, bo musi bronić zawartości. Do tej triady należy dodać elektrownię jako figurę funkcjonalną, gdyż ciągłość pamięci cyfrowej wymaga ciągłości energii. Pergamin można czytać po tysiącu lat bez dostarczania napięcia, podczas gdy serwer przestaje działać w momencie odcięcia zasilania. Cyfrowa pamięć jest zatem znacznie bardziej zależna od nieprzerwanej pracy infrastruktury niż pamięć papierowa. Ta zależność ma daleko idące konsekwencje dla bezpieczeństwa państwa.

Redundancja jako architektura odporności i rozproszenia

Jeżeli administracja, bankowość, opieka zdrowotna, logistyka, telekomunikacja i przedsiębiorstwa przechowują kluczowe zasoby w systemach cyfrowych, centrum danych staje się elementem infrastruktury krytycznej – niezależnie od tego, czy formalnie należy do państwa, czy do prywatnej korporacji. Granica między infrastrukturą gospodarczą a bezpieczeństwa zaciera się. Awaria serwera przestaje być jedynie problemem firmy, gdy od jego działania zależy możliwość

przeprowadzenia operacji medycznej, wykonania płatności lub komunikacji służb ratunkowych. Stąd kluczowe znaczenie redundancji; w języku technicznym brzmi ona niepozornie, lecz w rzeczywistości stanowi filozofię odporności. Redundancja zakłada, że element systemu ulegnie awarii. Nie próbuje stworzyć urządzenia nieśmiertelnego, lecz buduje architekturę zdolną przeżyć śmierć części. Dane są kopiowane, ścieżki komunikacyjne dublowane, źródła zasilania zabezpieczane, a centra rozmieszczane tak, by lokalna katastrofa nie oznaczała utraty całego zasobu. To technologiczna wersja starej zasady instytucjonalnej: nie ufaj jednemu punktowi, od którego zależy wszystko.

Istnieje tu analogia między redundancją techniczną a konstytucyjnym podziałem władz. W obu przypadkach system projektuje się w przekonaniu, że pojedynczy element może zawieść. Demokracja nie zakłada doskonałości każdego rządzącego; dlatego tworzy mechanizmy kontroli, sądy, procedury odwoławcze i ograniczenia kompetencji. Architektura odpornego centrum danych również nie opiera się na wierze w niezawodność pojedynczego dysku, generatora czy połączenia. W jednym przypadku chodzi o odporność polityczną, w drugim o informacyjną, lecz logika pozostaje ta sama: dojrzały system nie ufa własnej bezbłędności.

Ta zasada wykracza poza technikę. Cyfrowe społeczeństwo powinno nauczyć się projektować również redundancję epistemiczną. Gdy jedna platforma staje się podstawowym kanałem informacji, jeden dostawca kontroluje dominującą warstwę infrastruktury, jeden algorytm decyduje o widoczności lub jedna baza staje się źródłem krytycznych decyzji – powstaje odpowiednik single point of failure. Awaria może być wtedy techniczna, ekonomiczna, polityczna lub poznawcza. Monokultura technologiczna bywa wygodna aż do chwili, gdy przestaje działać.

Metafora chmury jako jednej „światowej szafy kartotecznej” wymaga zatem korekty. Nie istnieje jedna szafa. Istnieje globalny archipelag centrów danych połączonych kablami, protokołami i umowami, zarządzanych przez podmioty prywatne i publiczne oraz rozmieszczonych w różnych systemach prawnych. Logiczna jedność chmury współistnieje z geograficznym i prawnym rozproszeniem. To właśnie owo rozdarcie między jednym cyfrowym środowiskiem a wieloma jurysdykcjami stanie się źródłem sporów o suwerenność danych, dostęp organów ścigania i transgraniczną ochronę prywatności. Zanim przejdziemy do prawa, należy jednak zrozumieć jeszcze jedną zmianę pojęciową: odrzucenie popularnego porównania danych do ropy naftowej na rzecz metafory powietrza.

Dane jako środowisko i problem powiernictwa

To nie jest wyłącznie efektowny bon mot. Metafory ekonomiczne niosą za sobą konkretne konsekwencje, gdyż sugerują określony sposób zarządzania zasobem. Jeśli dane są ropą, naturalnym pytaniem staje się: kto je posiada, wydobywa, rafinuje i sprzedaje? Jeśli zaś są powietrzem cyfrowej cywilizacji, punkt ciężkości przesuwa się ku jakości środowiska, dostępności oraz odpowiedzialności podmiotów kontrolujących warunki korzystania z niego.

Żadna z tych metafor nie jest doskonała. Dane – w przeciwieństwie do powietrza – można kopiować bez utraty oryginału, odcinać od nich dostęp, a ich wartość zmienia się zależnie od kontekstu; mogą one ujawniać informacje o osobach, które nigdy świadomie ich nie przekazały. Niemniej obraz powietrza obnaża kluczową właściwość cyfrowej gospodarki: współczesne instytucje coraz trudniej funkcjonują bez przepływu informacji. Dane stają się elementem środowiska działania, podobnie jak elektryczność, transport czy telekomunikacja. Ich brak może oznaczać nie tylko utratę produktu, ale ograniczenie zdolności uczestnictwa w społeczeństwie. Tu pojawia się paradoks obfitości.

Dane mogą być technicznie reprodukowalne niemal bez granic, lecz kontrola nad dostępem do nich pozostaje silnie skoncentrowana. Cywilizacja może wytwarzać więcej informacji niż kiedykolwiek wcześniej, a jednocześnie tworzyć największe w historii asymetrie informacyjne. Korporacja może wiedzieć o zachowaniach milionów użytkowników znacznie więcej, niż pojedynczy człowiek wie o logice działania tej korporacji. Państwo może dysponować możliwościami korelowania rejestrów, których obywatel nie jest w stanie nawet odtworzyć. Platforma zna regułę rekomendacji, podczas gdy odbiorca widzi jedynie jej rezultat. To sprawia, że centralnym problemem chmury przestaje być samo przechowywanie danych.

Kwestią kluczową staje się powiernictwo. Kto posiada techniczną możliwość dostępu do cudzej pamięci, wchodzi w relację podobną do depozytariusza. W tradycyjnym sejfie bankowym klient powierza instytucji ochronę rzeczy, a nie prawo do dowolnego korzystania z ich zawartości. Podobna intuicja stoi za rozwijaną przez Microsoft koncepcją data stewardship: dostawca infrastruktury ma zarządzać środowiskiem przechowywania, nie przejmując moralnej własności informacji klienta. W materiale źródłowym ta ewolucja zostaje ujęta w sposób znamienny: chmura przestaje być tylko produktem, a staje się zobowiązaniem do ochrony zasobów, które do dostawcy nie należą. Taka konstrukcja jest jednak łatwiejsza do wypowiedzenia niż do zastosowania. Powiernik techniczny musi bowiem odpowiadać na pytania, których tradycyjny magazyn nie znał: czy może analizować przechowywane dane dla poprawy własnej usługi? Czy może wykorzystywać

metadane? Kiedy powinien ulec żądaniu organu państwowego, a kiedy może odmówić, uznając je za nadmierne?

Czy prawo państwa, w którym mieści się siedziba przedsiębiorstwa, może sięgać po dane przechowywane w innym kraju? Czy klient może żądać całkowitego usunięcia informacji, jeśli istnieją jej kopie zapasowe? Kto odpowiada, gdy algorytm działający na cudzych danych wytworzy nową informację, której wcześniej w zbiorze explicite nie było?

Archiwum nieuchronnie prowadzi do prawa. Ten moment jest historycznie logiczny. Gdy człowiek powierzał list poczcie, prawo musiało odpowiedzieć na pytanie, czy utrata fizycznego posiadania koperty oznacza utratę prywatności. Gdy dokumenty przeniesiono do szaf bankowych, konieczne stało się określenie warunków dostępu. Gdy pamięć została umieszczona w globalnej chmurze, stary konflikt powrócił na skalę nieporównywalnie większą: czy przekazanie informacji pośrednikowi oznacza oddanie mu prawa do decydowania o jej losie? To pytanie otwiera jednocześnie mroczniejszy rozdział historii archiwum. Pamięć może chronić przed arbitralnością władzy, gdyż dokument pozwala wykazać, co rzeczywiście się wydarzyło. Może jednak służyć władzy do coraz dokładniejszego katalogowania ludzi. Archiwum wyzwala od zapomnienia, ale może też odbierać prawo do bycia zapomnianym. Ułatwia dochodzenie sprawiedliwości i umożliwia prześladowanie; pozwala ocalić tożsamość i stworzyć dossier. Biblioteka Aleksandryjska oraz kartoteka policji politycznej są odległymi instytucjami, lecz obie ujawniają tę samą właściwość zorganizowanej pamięci: jej moralna wartość zależy od celu, praw dostępu i struktury władzy.

Kolejnym problemem nie może być zatem pytanie o to, ile informacji potrafimy przechować. Znacznie ważniejsze jest to, kto może otworzyć szufladę. W epoce chmury szuflada nie posiada drewnianego uchwytu. Ma klucz kryptograficzny, procedurę autoryzacji, regulamin, umowę, przepisy państwa i – czasami – nakaz sądowy. Za każdym z tych elementów kryje się spór o granicę pomiędzy bezpieczeństwem a wolnością. Światowa szafa kartoteczna staje się w tym miejscu areną konfliktu pomiędzy archiwum a panoptikonem. Dane jako powietrze.

Dane nie są ropą, lecz reprezentacją kształtowaną przez władzę

Nowa ontologia zasobu. Chmura jest największym archiwum, jakie zbudowała ludzkość, a dane są jego tworzywem. Jednak język, którym go opisujemy, wciąż zdradza poznawcze przyzwyczajenia epoki przemysłowej. Próbujemy ująć informację w kategoriach wypracowanych dla świata rzeczy: mówimy o posiadaniu danych, ich magazynowaniu, wydobywaniu, przenoszeniu, kradzieży czy

sprzedaży. Najpopularniejsza metafora głosi, że dane są nową ropą naftową. Jest ona efektowna, gdyż wskazuje na znaczenie gospodarcze zasobu, konieczność jego przetwarzania oraz możliwość koncentracji bogactwa w rękach podmiotów kontrolujących dostęp do strategicznych złóż. Pozostaje jednak niebezpiecznie nieprecyzyjna.

Ropa znika po spaleniu; jej baryłka może znajdować się zasadniczo tylko w jednym miejscu, a wykorzystanie jej przez jednego konsumenta wyklucza równoczesne użycie przez drugiego. Informacja zachowuje się inaczej. Można ją skopiować, nie odbierając jej posiadaczowi; może być wykorzystywana wielokrotnie i w różnych kontekstach, a po połączeniu z innymi zbiorami ujawnić wiedzę, której wcześniej nie zawierał żaden pojedynczy rekord.

W tym miejscu pojawia się inna metafora: dane jako powietrze cyfrowej cywilizacji. Nie chodzi tu o poetycką zamianę jednego sloganu na drugi, lecz o zmianę perspektywy ekonomicznej i politycznej. Jeśli dane przypominają ropę, przedsiębiorstwo jawi się jako wydobywca, właściciel złoża i rafineria. Jeśli zaś przypominają powietrze, dostawca infrastruktury staje się administratorem środowiska, od którego jakości zależy funkcjonowanie całego ekosystemu. W tej koncepcji dane są zasobem odnawialnym, wszechobecnym i niezbędnym, a podmioty technologiczne ewoluują z roli zwykłych dostawców usług w stronę regulatorów jakości cyfrowego otoczenia.

Również metafora powietrza wymaga jednak krytycznego namysłu. Powietrze jest dobrem naturalnym, podczas gdy ogromna część danych powstaje w wyniku zaprojektowanych procesów technicznych i społecznych. Platforma decyduje, jakie zdarzenia rejestruje; urządzenie wybiera parametry pomiaru; państwo określa, jakie informacje obywatel ma przekazać do rejestru; przedsiębiorstwo projektuje formularz, który wyznacza kategorie przyszłej bazy danych.

Dane nie są więc odkrywaną substancją zalegającą w naturze, lecz rezultatem wcześniejszej decyzji o tym, co warto mierzyć. Zanim powstanie baza, ktoś konstruuje aparat obserwacji. Dane nie są rzeczywistością samą w sobie, lecz jej reprezentacją uzyskaną według określonych reguł. Temperatura zapisana przez sensor jest reprezentacją zdarzenia fizycznego; ocena kredytowa – rezultatem wyboru zmiennych i modelu.

Liczba kliknięć opisuje zachowanie użytkownika tylko w granicach interfejsu, który umożliwił określone czynności. Dane medyczne są selektywną reprezentacją organizmu uzyskaną przez dostępne badania. Każdy zbiór posiada zatem swą prehistorię: decyzje o pomiarze, definicjach, kategoriach, czasie obserwacji i sposobie zapisu. Można powiedzieć, że pierwszym aktem władzy nad danymi nie jest ich analiza, lecz ustalenie, co stanie się daną. To twierdzenie wykracza poza klasyczną krytykę statystyki. Kategoria bezrobotnego, użytkownika aktywnego, pacjenta wysokiego ryzyka czy treści angażującej nie spada z nieba jako oczywisty fakt – musi zostać zdefiniowana. Gdy

definicja zostaje osadzona w systemie informatycznym, uzyskuje niezwykłą trwałość i skalę. Kod zamienia decyzję pojęciową w rutynową operację wykonywaną miliony razy bez ponownego zadawania pytania o jej sens.

Dane mają ponadto charakter relacyjny. Informacja o człowieku często nabiera znaczenia dopiero w zestawieniu z innymi danymi. Sama lokalizacja telefonu w konkretnym punkcie może niewiele mówić, lecz powtarzalność tego punktu codziennie o podobnej porze wskazuje miejsce pracy, a regularne przebywanie nocą w jednym miejscu pozwala wnioskować o miejscu zamieszkania. Dane jako powietrze stają się zatem nie tylko tłem, ale i narzędziem definiowania naszej cyfrowej egzystencji.

Synergia danych i iluzja świadomej zgody

Połączenie lokalizacji z kalendarzem, historią zakupów, wyszukiwaniem czy siecią kontaktów pozwala stworzyć profil niewspółmiernie bogatszy od każdego z pierwotnych rekordów. Wartość analityczna danych rośnie zatem nie tyle dzięki ich nagromadzeniu, co możliwości zestawiania ich ze sobą.

Dwie bazy danych połączone mogą być warte więcej niż suma ich poszczególnych wartości. Ekonomia przemysłowa zna efekt synergii, jednak w gospodarce informacyjnej przybiera on szczególnie intensywną postać. Zbiór danych transportowych może być umiarkowanie użyteczny, podobnie jak zbiór meteorologiczny; ich połączenie pozwala natomiast przewidywać opóźnienia. Dane kliniczne zestawione z genetycznymi mogą prowadzić do zupełnie nowych hipotez badawczych.

Informacje o zużyciu energii połączone z pogodą i charakterystyką budynków usprawniają zarządzanie siecią. Z kolei korelacja danych behawioralnych, demograficznych i społecznych może tworzyć instrumenty manipulacji znacznie skuteczniejsze niż każda baza osobno. Oznacza to, że wartość danych jest w dużej mierze kontekstowa i potencjalna – informacja dziś bezwartościowa może stać się niezwykle cenna po wynalezieniu nowej metody analitycznej.

Fotografie publikowane przez miliony użytkowników powstawały jako wspomnienia lub komunikaty społeczne, zanim stały się materiałem do rozwoju systemów rozpoznawania obrazu. Wielkie zbiory tekstu były biblioteką ludzkiej komunikacji, zanim powstały modele zdolne wydobywać z nich statystyczne regularności języka. Archiwum nabiera więc nowej wartości nie dlatego, że zmieniła się jego zawartość, lecz że zmieniło się narzędzie interpretacji. To jeden z powodów, dla których klasyczna zgoda na przetwarzanie informacji jest konceptualnie trudniejsza,

niż sugeruje formularz z przyciskiem „akceptuję”. Człowiek może rozumieć dzisiejszy cel wykorzystania danych, lecz nie sposób oczekiwać, by przewidział wszystkie przyszłe metody analizy i wnioski możliwe do wyciągnięcia za dekadę. Problem nie polega więc jedynie na tym, czy rekord został zebrany legalnie, ale czy późniejsza zdolność poznawcza wobec tego rekordu pozostaje zgodna z pierwotnym kontekstem jego pozyskania. Materiał źródłowy ujmuje ten konflikt poprzez zasadę ograniczenia celu: pytanie o to, czy dane zgromadzone dla jednego zadania mogą następnie służyć innym operacjom analitycznym.

W świecie materialnym własność pomaga rozwiązać wiele problemów alokacji. Posiadając rzecz, możemy decydować o jej użyciu i wykluczać innych. W przypadku danych sprawa jest bardziej złożona. Informacja może dotyczyć mnie, zostać zarejestrowana przez urządzenie należące do przedsiębiorstwa, być przechowywana przez jednego dostawcę, przetwarzana przez podwykonawcę i wykorzystywana do decyzji podejmowanej przez jeszcze inną instytucję. Pytanie „czyje są dane?” okazuje się zbyt proste, ponieważ nakłada na jeden zasób kilka odmiennych relacji: pochodzenie, kontrolę, dostęp, odpowiedzialność, interes ekonomiczny oraz prawa osoby, której informacja dotyczy. To właśnie tę komplikację próbuje uporządkować doktryna powiernictwa.

Od technicznej możliwości do moralnego uprawnienia: model powiernictwa danych

Dostawca chmury powinien zarządzać infrastrukturą i chronić powierzony zasób, nie uznając samego faktu technicznego przechowywania za tytuł do swobodnego dysponowania treścią. Proponowany model rozdziela funkcję steward/processor od funkcji owner/controller: pierwszy odpowiada przede wszystkim za bezpieczeństwo kontenera i zgodność infrastruktury, drugi zaś określa cel oraz zakres wykorzystania informacji. Jest to podejście atrakcyjne, ponieważ przeciwstawia możliwość techniczną uprawnieniu moralnemu: fakt, że administrator potrafi coś zrobić z danymi, nie oznacza, iż wolno mu to zrobić.

Powiernictwo wprowadza do gospodarki cyfrowej kategorię dobrze znaną starszym instytucjom zaufania. Lekarz ma dostęp do informacji, których nie może dowolnie rozpowszechniać. Bank przechowuje aktywa, lecz nie staje się ich właścicielem przez sam fakt posiadania infrastruktury. Adwokat zna sekrety klienta, jednak ciąży na nim zobowiązanie wykraczające poza zwykłą umowę handlową. W każdym z tych przypadków asymetria wiedzy rodzi szczególną odpowiedzialność. Im bardziej gospodarka cyfrowa opiera się na powierzaniu informacji wyspecjalizowanym pośrednikom, tym silniej potrzebuje podobnej kultury obowiązku.

Nie oznacza to jednak, że analogia jest pełna. Dostawca chmury działa w modelu przemysłowym o skali nieporównywalnej z tradycyjnym stosunkiem powierniczym. Ponadto system informatyczny może automatycznie wykonywać operacje, których żaden człowiek nie obserwuje jednostkowo. Odpowiedzialność musi być zatem projektowana na poziomie architektury. Nie wystarczy moralne zobowiązanie administratora siedzącego przed ekranem; niezbędne są uprawnienia dostępu, szyfrowanie, rejestrowanie operacji, separacja funkcji, polityki retencji, kontrola podwykonawców i procedury reagowania na żądania władz. Etyka zostaje przetłumaczona na techniczną organizację systemu.

Tutaj ujawnia się kolejna specyfika danych: możliwość oddzielenia posiadania informacji od dostępu do jej znaczenia. Kryptografia, prywatność różnicowa, systemy query-only czy techniki analizy na zaszyfrowanych danych próbują zerwać z historycznym założeniem, że aby analizować informację, trzeba ją najpierw ujawnić analitykowi w czytelnej postaci. Koncepcja "zamkniętego kontenera" rozwija tę ideę: algorytm może otrzymać możliwość wykonania określonej operacji bez przekazywania użytkownikowi całej zawartości zbioru. Jest to zmiana doniosła, gdyż przez większość historii ochrona tajemnicy polegała na ograniczaniu dostępu – drzwi archiwum były zamknięte, dokument opieczętowany, a list ukryty w kopercie.

Współczesna informatyka poszukuje rozwiązania bardziej subtelnego: nie tylko binarnego wyboru między "wolno wejść" a "nie wolno wejść", lecz możliwości zadania określonego pytania bez otrzymywania całej bazy. Kontrola może zatem dotyczyć nie samego dostępu do informacji, ale rodzaju dopuszczalnej operacji. Pozwala to sformułować ważną zasadę: w gospodarce danych prawo do analizy może być czymś innym niż prawo do posiadania kopii. Rozróżnienie to będzie szczególnie istotne w badaniach naukowych i ochronie zdrowia, gdzie społeczna wartość analityki bywa ogromna, a ryzyko związane z ujawnieniem danych równie wysokie. Tradycyjny wybór między pełnym zamknięciem zbioru a jego przekazaniem może zostać zastąpiony architekturą, w której wiedza powstaje bez niekontrolowanego przemieszczania surowej informacji. Formuła "Visit the Data" ujmuje tę zmianę niemal aforystycznie: zamiast zabierać dane do algorytmu, można wysłać algorytm do danych.

Model federacyjny zachowuje informacje u pierwotnego dysponenta, umożliwiając wspólne analizy przy ograniczeniu potrzeby centralizacji zasobów. Mechanizm ten stanie się przedmiotem osobnej analizy w dalszej części artykułu, gdyż prowadzi do nowego rozumienia suwerenności informacyjnej: współpraca nie musi oznaczać transferu własności ani fizycznego przeniesienia całego zbioru.

Na tym etapie pojawia się paradoks koncentracji. Dane mogą być technicznie łatwe do kopiowania, a mimo to gospodarka danych sprzyja koncentracji rynkowej. Powodem nie jest materialna

rzadkość informacji, lecz koszt budowy infrastruktury, dostęp do ogromnych strumieni nowych danych, efekty sieciowe, zasoby obliczeniowe i kompetencje analityczne oraz przewaga wynikająca z uczenia modeli na kolejnych interakcjach. Podmiot posiadający wielu użytkowników generuje więcej danych; dzięki temu doskonali usługę, co z kolei przyciąga kolejnych użytkowników.

W ten sposób obfitość informacji paradoksalnie współistnieje z koncentracją kontroli. W ekonomii dóbr materialnych przewaga często wynikała z kontroli nad rzadkim złożem, portem albo linią produkcyjną. W gospodarce cyfrowej przewagę tworzy kontrola nad przepływem. Nie trzeba posiadać każdej informacji na świecie, aby być potężnym; wystarczy znajdować się w punkcie, przez który przechodzą ogromne ilości danych i decyzji. Przykładem jest wyszukiwarka, która organizuje relację człowieka z zasobami internetu.

Władza jako kontrola nad infrastrukturą pośrednictwa

System operacyjny pośredniczy między użytkownikiem a urządzeniem, chmura – między organizacją a mocą obliczeniową, platforma społecznościowa – między nadawcą a publicznością, a brama płatnicza – między transakcją a jej wykonaniem. Władza informacyjna często nie opiera się już na klasycznym posiadaniu, lecz na byciu koniecznym pośrednikiem. Z tego powodu kategoria infrastruktury okazuje się bardziej użyteczna niż kategoria produktu; produkt można bowiem kupić lub odrzucić.

Infrastruktura organizuje środowisko wyborów i może stać się warunkiem uczestnictwa w innych sferach życia. Im bardziej dane przypominają powietrze, tym bardziej problem wykluczenia z infrastruktury zaczyna przypominać kwestię dostępu do podstawowej usługi. Nie oznacza to, że każda baza danych powinna być publiczna czy każda platforma stanowić dobro publiczne. Oznacza natomiast, że społeczne znaczenie kontroli nad informacją może przeważać nad formalnym statusem prywatnej własności przedsiębiorstwa.

Ta obserwacja ujawnia konflikt pomiędzy prywatnością a użytecznością. Im więcej danych można łączyć, tym większa jest ich potencjalna wartość poznawcza i szersze możliwości innowacji. Jednocześnie każde rozszerzenie analizy zwiększa ryzyko identyfikacji, profilowania lub wykorzystania informacji poza pierwotnym kontekstem. Nie istnieje zatem prosta oś, na której po jednej stronie znajduje się „postęp”, a po drugiej „ochrona danych”. Dojrzała polityka informacyjna musi poszukiwać architektur pozwalających czerpać korzyści poznawcze przy jednoczesnej minimalizacji niepotrzebnego ujawnienia danych.

Szczególnie interesujący jest przypadek danych medycznych. Dla jednostki informacja o chorobie jest jednym z najbardziej intymnych elementów prywatności, podczas gdy dla badacza milion podobnych rekordów staje się zasobem umożliwiającym odkrycie prawidłowości ratującej życie. Ten sam element posiada więc jednocześnie charakter osobisty i społeczny.

Dane jako surowiec epistemiczny a ryzyko redukcjonizmu cyfrowego

Zbyt łatwy dostęp do danych może naruszać godność, zbyt radykalne zamknięcie – ograniczać rozwój wiedzy. Konfliktu tego nie da się rozwiązać sloganami o „więcej prywatności" czy „większej ilości danych". Wymaga on architektury zgodnego wykorzystania, ścisłego określenia celu, technik zabezpieczeń oraz instytucji godnych zaufania. Przykład współpracy analitycznej w badaniach nad nowotworami ma pokazać, że wartość społeczna może wynikać z wtórnego wykorzystania danych, o ile zachowany zostanie odpowiedni związek między pierwotnym kontekstem a nowym celem oraz mechanizmy ochrony.

Z punktu widzenia filozofii informacji kluczowe jest jednak coś innego: dane przestają być traktowane jako bierne resztki przeszłości. Stają się surowcem epistemicznym, z którego konstruuje się nowe hipotezy. Nie ma przy tym gwarancji, że duża ilość danych przekłada się na dużą ilość prawdy – to jedna z najbardziej zwodniczych intuicji ery cyfrowej. Zbiór może być ogromny, a jednocześnie systematycznie stronniczy. Pomiar może być precyzyjny, lecz dotyczyć niewłaściwej zmiennej. Korelacja bywa stabilna, choć pozbawiona związku przyczynowego. Dane historyczne mogą wiernie odtwarzać dawną niesprawiedliwość i właśnie dlatego stać się fatalnym materiałem do automatyzacji przyszłych decyzji. Ilość informacji nie znosi problemów epistemologii; przeciwnie – zwiększa koszt błędnej interpretacji, gdyż błąd zyskuje możliwość skalowania.

Warto zatem rozszerzyć metaforę powietrza o pojęcie jakości danych. Tak jak powietrze może być czyste lub skażone, tak system informacyjny może być zasilany danymi aktualnymi i reprezentatywnymi albo błędnymi i historycznie obciążonymi. W pierwotnym ujęciu podmiot technologiczny ma dbać o „czystość" cyfrowego środowiska, rozumianą jako dokładność i bezpieczeństwo. W epoce AI należy dodać do tej listy reprezentatywność, dokumentowalność pochodzenia oraz możliwość oceny, czy dane w ogóle odpowiadają problemowi, który model ma rozwiązać.

Błąd danych ma charakter szczególny, ponieważ często udaje fakt. Literówkę w tekście łatwo dostrzec; rekord zapisany w bazie z odpowiednim identyfikatorem i datą nabiera pozoru urzędowej

pewności. Jeśli zostanie skopiowany do kolejnych systemów, zaczyna własne życie instytucjonalne. Osoba błędnie sklasyfikowana jako dłużnik, podejrzany czy pacjent określonej kategorii ryzyka może trafić w sytuację, w której kolejne automatyczne decyzje jedynie wzmacniają pierwotny błąd. Informacja fałszywa, lecz interoperacyjna, bywa bardziej niebezpieczna niż prawda zamknięta w pojedynczym segregatorze. W tym kontekście „prawo do korekty" informacji ma wymiar głębszy niż administracyjna poprawka wpisu – jest ochroną jednostki przed instytucjonalizacją błędnej tożsamości.

Cyfrowy profil staje się rodzajem cienia człowieka: modelem wykorzystywanym przez systemy, które nigdy nie spotykają osoby bezpośrednio. Bank widzi punktację, platforma sygnały behawioralne, ubezpieczyciel kategorię ryzyka, pracodawca wynik selekcji, a administracja rekordy w rejestrach. Im więcej decyzji zapada na podstawie reprezentacji informacyjnych, tym ważniejsze staje się pytanie, czy ta reprezentacja rzeczywiście odpowiada osobie. Pojawia się nowy paradoks antropologiczny: cyfrowa gospodarka dąży do coraz dokładniejszego modelowania człowieka, ale model nigdy nie jest człowiekiem.

Dane są śladem życia, a nie jego pełnią. Ryzyko redukcjonizmu pojawia się wtedy, gdy skuteczność predykcyjną mylimy z prawdą o osobie. Algorytm może trafnie przewidzieć prawdopodobieństwo zachowania w danym kontekście, lecz nie oznacza to, że odkrył istotę jednostki. Człowiek pozostaje bowiem zdolny do zmiany, sprzeczności i przekraczania statystycznych oczekiwań.

Dane jako potencjał przyszłej władzy

Ma to fundamentalne znaczenie dla demokracji i prawa. Państwo liberalne oparto na przekonaniu, że człowiek nie może zostać całkowicie zredukowany do kategorii nadanej mu przez władzę. Ma on prawo odpowiadać na zarzuty, zmieniać poglądy, rehabilitować się, kwestionować decyzje i być oceniany w ramach przejrzystej procedury. Jeśli infrastruktura cyfrowa zaczyna podejmować decyzje w oparciu o profil, zasady te muszą zostać przełożone na nowy język. Przejrzystość, możliwość zakwestionowania wyniku, kontrola jakości danych oraz odpowiedzialność za model stają się tym samym cyfrowymi odpowiednikami proceduralnej sprawiedliwości.

„Dane jako powietrze" są metaforą użyteczną przede wszystkim wtedy, gdy przypominają, że informacja przestała być marginalnym produktem ubocznym gospodarki, a stała się środowiskiem, w którym funkcjonują instytucje. Nie oznacza to jednak, że należy traktować je jak zasób bez właściciela czy otwierać do nich powszechny dostęp. Podczas gdy metafora powietrza podkreśla powszechność i niezbędność danych, koncepcja powiernictwa przypomina, że informacja może być

przekazana komuś w konkretnym celu, bez nadawania mu nieograniczonego prawa do jej eksploatacji.

Z tej syntezy wyłania się precyzyjna ontologia. Dane są jednocześnie reprezentacją, zasobem, relacją i możliwością: reprezentacją, gdyż opisują fragment rzeczywistości według określonego systemu pomiaru; zasobem, ponieważ służą do wytwarzania wiedzy i wartości ekonomicznej; relacją, gdyż często dotyczą wielu osób i nabierają znaczenia w powiązaniu z innymi informacjami; oraz możliwością, ponieważ ich przyszła wartość zależy od narzędzi analitycznych, których dziś możemy jeszcze nie posiadać.

Ta ostatnia właściwość jest kluczowa. Magazyn danych jest magazynem potencjalnych przyszłych pytań. Zachowanie informacji oznacza zachowanie możliwości jej ponownej interpretacji, dlatego gromadzenie danych „na wszelki wypadek" nie jest epistemicznie neutralne. Powiększa ono przyszłe pole działania administratora, państwa, badacza, korporacji czy napastnika. To, co zebrano dziś, może zostać kiedyś wykorzystane przez podmiot, którego obecny zbierający nawet nie przewiduje. Minimalizacja danych nie jest zatem jedynie metodą oszczędzania miejsca czy kwestią zgodności proceduralnej – ona ogranicza przyszłą powierzchnię władzy.

Można sformułować kolejną maksymę niniejszej analizy: każda zachowana informacja jest jednocześnie zachowaną możliwością przyszłego działania. Może służyć leczeniu, badaniom, innowacjom, rozliczaniu władzy lub ochronie przed oszustwem, ale może również służyć dyskryminacji, inwigilacji, szantażowi, manipulacji bądź represji.

Nie sposób z góry rozstrzygnąć wszystkich przyszłych zastosowań. Można jednak projektować instytucje tak, aby zminimalizować ryzyko wykorzystania danych w sposób sprzeczny z prawami jednostki i społecznym celem ich gromadzenia. W tym punkcie ontologia danych ponownie spotyka się z metaforą Tools and Weapons. Dane same w sobie nie są bronią w sensie fizycznym, jak karabin; są raczej zdolnością poznawczą, która w połączeniu z algorytmem, infrastrukturą i władzą wykonawczą może stać się narzędziem ingerencji. Sama lista nazwisk nie więzi człowieka, lecz połączona z aparatem bezpieczeństwa może wyznaczać cele represji. Historia zdrowia sama w sobie nie dyskryminuje – czyni to system decyzji wykorzystujący ją w niewłaściwym celu.

Prywatność jako instytucja rozdzielająca wiedzę od władzy

Sama lokalizacja telefonu nie prześladuje obywatela. Robi to jednak instytucja zdolna zamienić strumień współrzędnych w mapę kontaktów.

W tym kontekście pytanie o bezpieczne przechowywanie danych nie wystarcza. Można bowiem doskonale zabezpieczyć system, który realizuje niemoralny cel. Najbardziej szczelna baza danych państwa autorytarnego pozostaje narzędziem opresji, jeśli służy totalnej klasyfikacji obywateli. Cyberbezpieczeństwo odpowiada na pytanie, czy system działa zgodnie z wolą uprawnionego operatora; etyka i prawo muszą natomiast zapytać, czy sama wola operatora jest dopuszczalna. Bez tego można stworzyć perfekcyjnie bezpieczny panoptikon.

Czas skierować uwagę nie na techniczną jakość danych, lecz na granicę władzy nad informacją. Historia Johna Wilkesa, general warrants, Czwartej Poprawki, Stasi, Snowdena i PRISM pokazuje, że spór o prywatność jest znacznie starszy od Internetu. Zmieniło się jednak coś zasadniczego: dawniej państwo musiało wejść do domu, przejąć list albo otworzyć szafę. W epoce cyfrowej ogromna część ludzkiej pamięci znajduje się już poza domem, w infrastrukturze zarządzanej przez pośredników. Konflikt o prywatność staje się zatem pytaniem o to, czy przeniesienie pamięci do chmury oznacza jednoczesne przeniesienie władzy nad nią.

Jeśli dane są powietrzem cyfrowej cywilizacji, prywatność jest jednym z warunków, aby tym powietrzem dało się oddychać bez poczucia, że każdy oddech jest rejestrowany przez kogoś, kto może go kiedyś wykorzystać jako dowód. Doszliśmy do wniosku, że każda zachowana informacja jest zarazem zachowaną możliwością przyszłego działania. Wynika z tego konsekwencja, która zmienia sens pojęcia prywatności: nie może być ona rozumiana jedynie jako prawo do ukrywania tego, czego człowiek się wstydzi, ani jako luksus samotności przysługujący temu, kto chce „mieć święty spokój”. W społeczeństwie informacyjnym jest ona instytucją rozdzielającą wiedzę od władzy. Określa, kto może wiedzieć o człowieku, co może wiedzieć, w jakim celu, przez jak długo, na podstawie jakiego upoważnienia i z jakimi konsekwencjami. Jej przeciwieństwem nie jest publiczność, lecz sytuacja, w której jednostka traci kontrolę nad społecznym kontekstem własnych informacji.

Historia problemu rozpoczęła się na długo przed wynalezieniem komputera. Jednym z najważniejszych źródeł zachodniej tradycji ochrony prywatności był sprzeciw wobec arbitralnego przeszukania. Angielska maksyma o domu jako zamku nie ustanawiała absolutnej nietykalności przestrzeni prywatnej, lecz wyrażała zasadę o ogromnej doniosłości politycznej: nawet władza publiczna nie powinna móc wejść wszędzie tylko dlatego, że jest władzą. W XVII- i XVIII-wiecznej Anglii, a następnie w koloniach amerykańskich, konflikt ten koncentrował się wokół general warrants i writs of assistance – nakazów pozwalających urzędnikom przeszukiwać domy bez precyzyjnego wskazania poszukiwanej rzeczy, miejsca czy osoby. Sprawy związane z Johnem Wilkesem, a zwłaszcza uznawana za konstytucyjny punkt odniesienia sprawa Entick v. Carrington,

stały się częścią genealogii przekonania, że państwo nie może otrzymywać otwartej licencji na poszukiwanie informacji o obywatelu.

Po drugiej stronie Atlantyku James Otis atakował w 1761 roku writs of assistance używane przez brytyjską administrację celną. Nie chodziło wyłącznie o ochronę drewnianych drzwi i papierowych dokumentów; rodziła się zasada, według której przeszukanie powinno być ograniczone celem, oparte na podstawie prawnej i poddane kontroli kogoś innego niż sam zainteresowany funkcjonariusz. Jest coś niezwykle współczesnego w tej XVIII-wiecznej intuicji: general warrant był niebezpieczny właśnie dlatego, że nie ograniczał dostatecznie pola poszukiwania.

Dzisiejsza technologia odtwarza podobny problem w skali, której Otis nie byłby w stanie sobie wyobrazić. Dawny urzędnik wchodził do domu i otwierał szuflady; współczesny aparat analityczny może przeszukiwać korespondencję, historię lokalizacji, powiązania komunikacyjne, metadane, fotografie, dokumenty i zachowania transakcyjne bez fizycznego wejścia do mieszkania. Zmienia się mechanizm, lecz pytanie konstytucyjne pozostaje: jak szeroko wolno władzy szukać, zanim poszukiwanie samo stanie się formą arbitralnej dominacji?

Pytanie to nabiera dodatkowego znaczenia, ponieważ współczesny człowiek wyniósł znaczną część swojego życia poza fizyczny dom. Dokumenty znajdują się w chmurze, listy stały się wiadomościami elektronicznymi, fotografie trafiły na serwery, książka adresowa została zsynchronizowana, kalendarz przechowuje plan życia, aplikacje rejestrują ruch, a telefon komórkowy stał się jednocześnie mapą, portfelem, aparatem, pamiętnikiem, biblioteką, terminalem komunikacyjnym i urządzeniem identyfikacyjnym. Gdy zmienia się miejsce przechowywania życia prywatnego, prawo stojące na straży prywatności musi podążać za funkcją informacji, a nie pozostawać przywiązane do fizycznej formy pojemnika.

Ta zmiana wyjaśnia doniosłość współczesnego orzecznictwa dotyczącego urządzeń cyfrowych. Amerykański Sąd Najwyższy w sprawach takich jak Riley v. California i później Carpenter v. United States musiał skonfrontować dawną doktrynę przeszukania z faktem, że cyfrowy ślad człowieka różni się jakościowo od tradycyjnego przedmiotu. Telefon nie jest kieszonkowym notesem tylko dlatego, że mieści się w kieszeni. Historia lokalizacji nie staje się informacją banalną tylko dlatego, że technicznie przechowuje ją operator telekomunikacyjny. Wieloletni zapis poruszania się człowieka może odtworzyć niezwykle szczegółową mapę jego życia: domu, pracy, relacji, religii, zdrowia, przyzwyczajeń i spotkań.

Ochrona danych jako gwarant autonomii politycznej

W erze cyfrowej poziom ochrony informacji nie może być ustalany wyłącznie na podstawie miejsca, w którym znajduje się zapis. Gdyby prawo chroniło dziennik leżący na biurku, lecz traciło zainteresowanie tym samym dokumentem po zsynchronizowaniu go z serwerem, techniczna modernizacja prowadziłaby do regresu praw człowieka. Im więcej życia przenosilibyśmy do środowiska cyfrowego, tym mniej praw zachowywalibyśmy. Byłby to paradoks cywilizacyjny: technologia zwiększałaby funkcjonalność obywatela wprost proporcjonalnie do zmniejszania jego konstytucyjnej osłony.

Z tego ducha wyrasta obecna w materiale źródłowym doktryna digital neutrality. Informacja powinna korzystać z odpowiedniej ochrony ze względu na swój charakter i funkcję, a nie dlatego, że zapisano ją na konkretnym rodzaju nośnika albo w konkretnym pomieszczeniu. Obywatel nie powinien tracić prywatności w momencie, gdy dokument opuszcza dysk komputera i przekracza granicę państwa wewnątrz światłowodu. Neutralność cyfrowa jest więc próbą uwolnienia praw podstawowych od przypadkowości architektury technicznej.

Podobna ewolucja dokonała się w europejskiej kulturze prawnej, choć przyjęła bardziej bezpośrednią postać. Europejska konstrukcja praw podstawowych nie sprowadza ochrony danych wyłącznie do tajemnicy domu lub korespondencji. W Karcie praw podstawowych Unii Europejskiej obok prawa do poszanowania życia prywatnego, domu i komunikowania się wyodrębniono autonomiczne prawo do ochrony danych osobowych.

Prywatność chroni określone sfery życia przed nadmierną ingerencją; ochrona danych wprowadza natomiast reguły dotyczące samego procesu przetwarzania informacji – również wtedy, gdy nie przypomina on klasycznego "wtargnięcia" do prywatnego pokoju. Europejskie myślenie o danych nie zatrzymuje się więc na pytaniu, czy ktoś poznał tajemnicę. Pyta także, czy informacja została zebrana uczciwie, dla określonego celu i na prawidłowej podstawie, czy człowiek ma możliwość uzyskania do niej dostępu oraz jej skorygowania, a także czy istnieje niezależny organ zdolny kontrolować administratora. Wolność informacyjna zostaje tu przetłumaczona na procedury. Nie jest to triumf biurokracji nad filozofią; przeciwnie, to próba zamienienia abstrakcyjnej godności człowieka w technicznie egzekwowalne ograniczenia władzy.

Szczególnie ważnym etapem tej ewolucji był niemiecki wyrok konstytucyjny dotyczący spisu ludności z 1983 roku. Federalny Trybunał Konstytucyjny rozwinął w nim pojęcie informacyjnego samostanowienia. Istota tej konstrukcji sięga głębiej niż prawo własności do danych: jednostka powinna co do zasady zachowywać możliwość współdecydowania o ujawnianiu i wykorzystywaniu informacji dotyczących jej osoby.

Trybunał dostrzegł przy tym zjawisko, które ponad czterdzieści lat później brzmi niemal jak opis współczesnej analityki Big Data: znaczenia pojedynczej informacji nie da się oceniać w izolacji, ponieważ pozornie banalny rekord może uzyskać zupełnie nową wagę po połączeniu z innymi danymi. Nie istnieje bowiem absolutna kategoria "niewinnego fragmentu danych".

Kod pocztowy może być administracyjną drobnostką, dopóki nie zostanie połączony ze statystyką dochodów, ryzykiem kredytowym i modelem ubezpieczeniowym. Historia lokalizacji może wyglądać jak informacja techniczna, dopóki nie pozwoli odtworzyć uczestnictwa w zgromadzeniu politycznym, wizyty w klinice, miejscu kultu religijnego czy siedzibie związku zawodowego. Sieć kontaktów może być zwykłą listą numerów, dopóki algorytm nie wykorzysta jej do rekonstrukcji relacji społecznych. Wartość informacyjna rekordu nie jest więc jego naturalną właściwością – powstaje ona w środowisku analitycznym. Z tego powodu informacyjne samostanowienie pozostaje czymś więcej niż prawem do sekretu; chroni ono warunki autonomicznego życia.

Człowiek, który nie wie, kto dysponuje informacjami na jego temat, jakie dane zgromadzono i do czego mogą zostać użyte, zaczyna zachowywać się inaczej jeszcze zanim ktokolwiek zastosuje wobec niego sankcję. Niepewność co do bycia obserwowanym może wywoływać autocenzurę. Jednostka może zrezygnować z udziału w legalnym zgromadzeniu, z poszukiwania kontrowersyjnej książki, kontaktu z określoną organizacją albo wypowiedzenia niepopularnej opinii – nie dlatego, że czynność jest zakazana, lecz dlatego, że nie wie, jaki ślad po sobie pozostawi.

W tym miejscu prywatność łączy się z teorią demokracji. Wolność słowa potrzebuje nie tylko prawa do wypowiedzenia zdania, ale również przestrzeni, w której myśl może powstać. Autonomia polityczna wymaga możliwości czytania, szukania, spotykania się, zmieniania poglądów, popełniania błędów i prowadzenia rozmów bez przekonania, że każde zachowanie zostanie trwale przypisane do tożsamości i kiedyś wydobyte z archiwum. Demokracja potrzebuje obywatela widzialnego w przestrzeni publicznej, lecz nie całkowicie przezroczystego dla władzy.

Hannah Arendt rozróżniała sferę publiczną i prywatną nie po to, aby uczynić z prywatności kult odosobnienia, lecz by pokazać, że człowiek potrzebuje różnych przestrzeni istnienia. Bycie obywatelem wymaga pojawiania się przed innymi, ale możliwość publicznego działania zależy od istnienia zaplecza, w którym jednostka nie jest stale wystawiona na wspólnotowy osąd. Totalna widzialność może być równie opresyjna jak całkowite wykluczenie z publiczności. Społeczeństwo demokratyczne potrzebuje więc zarówno agory, jak i drzwi, które można zamknąć.

Cyfrowy panoptikon i pułapka retrospektywnego nadzoru

Michel Foucault opisał najbardziej znaną figurę odwrócenia porządku: panoptikon. W więzieniu zaprojektowanym przez Jeremy'ego Benthama osadzony nie musi wiedzieć, czy w danej chwili jest obserwowany. Wystarczy sama świadomość tej możliwości, aby nadzór zaczął oddziaływać na zachowanie obserwowanego. Największa efektywność panoptikonu nie wynika z liczby spojrzeń strażnika, lecz z przekształcenie niepewności w samodyscyplinę. Jednostka przejmuje perspektywę obserwatora i zaczyna kontrolować samą siebie. Oczywiście cyfrowy świat nie jest jednym globalnym panoptikonem, a traktowanie każdej analityki danych jako odpowiednika więzienia byłoby nadużyciem. Analogia ta pozostaje jednak heurystycznie cenna.

Współczesne systemy nadzoru potrafią działać bez nieustannej, aktywnej obserwacji człowieka przez człowieka. Kamery, sensory, logi systemowe i dane komunikacyjne zapisywane są automatycznie; analityk może do nich powrócić w dowolnym momencie. Nadzór przestaje wymagać jednoczesności. Możliwość rekonstrukcji przeszłości zaczyna pełnić funkcję obserwacji teraźniejszości – to jedna z fundamentalnych zmian, jakie przyniosło cyfrowe archiwum. Tradycyjny policjant musiał podążać za człowiekiem w czasie jego przemieszczania się; system cyfrowy pozwala odtworzyć trasę po fakcie.

Dawny podsłuch należało uruchomić przed rozmową. W środowisku, w którym komunikacja jest zapisywana domyślnie, zainteresowanie organów może pojawić się znacznie później. Władza nad archiwum tworzy swoistą możliwość cofania czasu: to, czego nie obserwowano jako wydarzenia, można zrekonstruować jako dane. Problem ten dostrzegł Amerykański Sąd Najwyższy w sprawie Carpenter.

Długotrwała historia danych lokalizacyjnych przechowywanych przez operatora komórkowego pozwalała odtworzyć ruchy człowieka z precyzją i łatwością nieosiągalną dla tradycyjnej obserwacji. Kluczowe stało się podważenie założenia, że przekazanie danych osobie trzeciej automatycznie znosi uzasadnione oczekiwanie prywatności. W cyfrowym społeczeństwie człowiek nie ma bowiem realnej możliwości funkcjonowania bez ciągłego pozostawiania śladów u pośredników. Stara reguła prawna przestaje chronić wolność, jeśli warunkiem jej zachowania jest faktyczne wycofanie się ze współczesnego życia. Do podobnej konkluzji prowadzi europejska zasada proporcjonalności. Nie każde naruszenie prywatności jest zakazane, tak jak nie każde przeszukanie jest niedopuszczalne. Państwo ma legalny interes w ściganiu przestępstw, przeciwdziałaniu terroryzmowi czy zapewnianiu bezpieczeństwa narodowego. Problemem nie jest sama możliwość ingerencji, lecz jej granice: konieczność posiadania podstawy prawnej, określonego celu, proporcjonalności oraz

procedur ograniczających nadużycia. Prywatność w państwie prawa nie oznacza zatem, że policja ma nie wiedzieć niczego. Oznacza, że nie może ona wiedzieć wszystkiego tylko dlatego, iż technologia umożliwiła taką wiedzę. To rozróżnienie jest kluczowe dla interpretacji historii Edwarda Snowdena.

Prywatność jako fundament bezpieczeństwa i zaufania

Ujawnienia z 2013 roku nie stworzyły konfliktu między państwem a gigantami technologicznymi; one go jedynie odsłoniły i gwałtownie zaostrzyły. Programy nadzoru prowadzone przez amerykańskie służby i ich sojuszników, w tym PRISM oraz inne mechanizmy pozyskiwania informacji, wywołały globalną dyskusję o skali dostępu państw do infrastruktury cyfrowej. Dla dostawców chmury problem stał się egzystencjalny: klienci na całym świecie zaczęli pytać, czy amerykańska technologia nie jest w rzeczywistości kanałem amerykańskiej inwigilacji. Nie należy jednak upraszczać tej historii, widząc w firmach technologicznych niewinne ofiary, a w państwie jednolity aparat szpiegowski. Relacja ta jest znacznie bardziej złożona.

Służby bezpieczeństwa potrzebują danych przechowywanych przez firmy; firmy z kolei podlegają nakazom prawnym i obowiązkowi współpracy, a sądy autoryzują dostęp do informacji. Jednocześnie tajność tych procedur utrudnia społeczną kontrolę nad ich skalą. Korporacje technologiczne stają się tym samym pośrednikami między konstytucyjnym państwem a prywatnością milionów ludzi. Ich serwery to miejsce, w którym interes bezpieczeństwa publicznego zderza się z prawami jednostki. Materiał źródłowy opisuje ten moment jako przejście od roli zwykłego dostawcy kodu do powiernika globalnego zaufania.

Po ujawnieniach Snowdena Microsoft musiał przekonywać klientów, że nie istnieje mechanizm nieograniczonych „tylnych drzwi". Spory o jawność żądań państwowych skłoniły firmę i innych graczy rynkowych do walki o prawo publikowania szerszych informacji na temat dostępu służb. Niezależnie od motywów biznesowych, lekcja pozostaje istotna: zaufanie do chmury wymaga, aby użytkownik znał nie tylko zabezpieczenia przed przestępcą, ale i reguły dostępu państwa.

Tu pojawia się paradoks bezpieczeństwa. Ten sam system szyfrowania, który chroni dysydenta przed represjami czy pacjenta przed kradzieżą danych, może utrudnić organom ścigania dostęp do komunikacji sprawcy ciężkiego przestępstwa. Infrastruktura zapewniająca prywatność miliardom ludzi może zostać wykorzystana przez terrorystę, a mechanizmy retencji pomagające odtworzyć przebieg zbrodni mogą stać się narzędziem masowej obserwacji niewinnych obywateli.

Nie istnieje rozwiązanie, w którym bezpieczeństwo i prywatność zawsze rosną równocześnie. Błędem byłoby jednak traktowanie tego napięcia jako prostej gry o sumie zerowej. Prywatność jest bowiem elementem samego bezpieczeństwa. System posiadający uniwersalny mechanizm obejścia szyfrowania dla „dobrych" funkcjonariuszy musi rozwiązać problem ochrony tego przejścia przed „złymi" użytkownikami, obcymi służbami czy przestępcami. Centralizacja ogromnych zbiorów danych tworzy atrakcyjny cel ataku; państwo gromadzące informacje ponad konieczność zwiększa koszt ewentualnego wycieku. Ochrona prywatności może więc być rozumiana nie jako przeszkoda, lecz jako jedna z warstw bezpieczeństwa.

Dobrze oddaje tę logikę zasada minimalizacji. Informacji, której nie zgromadzono, nie można ukraść z bazy. Danych usuniętych zgodnie z prawem nie można wykorzystać w nowym celu. Klucza, którego administrator nie posiada, nie można od niego zażądać. System z rozdzielonymi uprawnieniami jest trudniejszy do przejęcia w jednym punkcie. Privacy by design nie jest zatem wyłącznie programem ochrony abstrakcyjnego prawa podmiotowego; bywa także strategią ograniczania powierzchni ataku.

Prywatność i bezpieczeństwo łączy głębsza relacja: oba pojęcia opierają się na zaufaniu instytucjonalnym. Obywatel przekazuje państwu dane podatkowe czy medyczne, bo spodziewa się ich wykorzystania zgodnie z określonym celem. Klient powierza dane bankowi w nadziei na zachowanie tajemnicy, a pacjent mówi lekarzowi o sprawach intymnych, gdyż poufność jest fundamentem relacji terapeutycznej.

Jeżeli instytucja zaczyna wykorzystywać zasoby w nieprzewidzianych celach, szkoda wykracza poza pojedyncze naruszenie – osłabia gotowość społeczeństwa do dalszej współpracy. Niemiecki Federalny Trybunał Konstytucyjny wcześnie dostrzegł tę zależność w kontekście statystyki publicznej: jeśli obywatel nie ufa, że informacje przekazane dla celów statystycznych pozostaną chronione i nie zostaną wykorzystane administracyjnie przeciwko niemu, może unikać szczerych odpowiedzi. Prywatność staje się wtedy warunkiem jakości samego państwowego poznania. Paradoksalnie aparat publiczny, który chce wiedzieć zbyt wiele bez dostatecznych gwarancji, może ostatecznie otrzymywać gorsze informacje. Prowadzi to do kluczowej maksymy: państwo buduje zdolność poznawczą nie tylko przez gromadzenie danych, ale przede wszystkim przez wzbudzanie zaufania, dzięki któremu ludzie chcą te dane przekazywać. Totalna obserwacja może zwiększyć liczbę zapisów, lecz jednocześnie zmienia zachowanie obserwowanych i zniekształca badaną rzeczywistość. Nadzór nie jest neutralnym oknem. Może stać się czynnikiem wpływającym na to, co próbuje mierzyć.

Cyfrowa inwigilacja znosi bariery techniczne kontroli

Najbardziej dramatyczną ilustrację tego mechanizmu dostarcza historia systemów totalitarnych. Przykład Stasi służy tu jako ostrzeżenie przed sytuacją, w której archiwum przestaje być narzędziem pamięci państwa, a staje się aparatem systematycznego poznawania obywatela. Niemieckie Archiwum Akt Stasi przechowuje dziś ponad 111 kilometrów dokumentacji pozostawionej przez Ministerstwo Bezpieczeństwa Państwowego NRD. Sama ta fizyczna skala jest lekcją polityczną: aparat kontroli wymagał niewyobrażalnej pracy ludzi, papieru, kartotek, informatorów i procedur.

Stasi potrzebowała kilometrów półek, maszynopisów i armii tajnych współpracowników, by osiągnąć poziom obserwacji, który współczesne systemy cyfrowe mogą radykalnie przekroczyć przy znacznie niższym koszcie krańcowym. Nie oznacza to, że demokratyczne platformy czy dostawcy chmury są współczesną Stasi – takie porównanie byłoby historycznie i moralnie nieuczciwe. Oznacza ono jednak, że bariera techniczna, która niegdyś ograniczała skalę inwigilacji, dramatycznie się obniżyła, co w konsekwencji zwiększa wagę barier prawnych i etycznych.

Los Hansa-Jochena Scheidlera stanowi mikrohistorię pokazującą, jak państwo może potraktować akt komunikacji jako przedmiot represyjnego zainteresowania. Dziś wysłanie informacji trwa ułamek sekundy, lecz właśnie dlatego jej kontrola może odbywać się w zupełnie innej skali; władza nie musi już otwierać każdej koperty.

Zamiast tego może analizować wzorce komunikacji, sieci relacji i cechy zachowania. Technologia przesuwa zatem centrum ciężkości z przechwytywania pojedynczej wiadomości na analizę struktury społecznej. Szczególnie pouczające są tutaj metadane. Potoczna intuicja sugeruje, że brak dostępu do treści rozmowy gwarantuje prywatność. Tymczasem wiedza o tym, kto z kim rozmawia, kiedy, jak często i skąd, pozwala stworzyć niezwykle bogaty obraz życia jednostki. W odpowiednio dużym zbiorze „dane o danych” stają się pełnowartościową informacją o człowieku. Potwierdza to tezę niemieckiego orzeczenia spisowego: nie istnieje z góry nieważny rekord, jeśli nowoczesna analityka potrafi zmienić jego znaczenie poprzez kontekst.

W tym ujęciu cyfrową prywatność można rozpatrywać na trzech poziomach. Pierwszy dotyczy treści: tego, co człowiek powiedział, napisał lub sfotografował. Drugi odnosi się do zachowania: kiedy i w jaki sposób dokonał określonej czynności. Trzeci zaś dotyczy inferencji: tego, czego system może o nim wywnioskować na podstawie danych pierwotnych. To właśnie ten trzeci poziom jest najbardziej charakterystyczny dla epoki AI.

Prywatność jako ochrona integralności kontekstowej

Można bowiem nie posiadać bezpośredniej informacji o określonej cesze jednostki, a mimo to oszacować ją z wysokim prawdopodobieństwem.

Tradycyjna doktryna „niczego nie ukrywam, więc nie potrzebuję prywatności" jest poznawczo wadliwa. Człowiek może nie mieć żadnego sekretu, a nadal posiadać interes w tym, aby nie zostać permanentnie sklasyfikowanym, przewidzianym i ocenionym poza kontekstem. Prywatność nie chroni winy.

Chroni zdolność do bycia czymś więcej niż suma cudzych obserwacji. Pozwala utrzymywać różne role społeczne, eksperymentować z poglądami, zmieniać decyzje i oddzielać poszczególne sfery życia. Helen Nissenbaum opisywała prywatność właśnie poprzez „integralność kontekstową": informacja właściwa w jednym kontekście nie musi być właściwa w drugim. Człowiek mówi lekarzowi coś, czego nie powierza pracodawcy; przekazuje bankowi dane, których nie ujawnia sąsiadowi i prowadzi rozmowę z przyjacielem w sposób odmienny od wystąpienia publicznego. Problemem cyfrowym jest zatem nie tylko wyciek tajemnicy, ale zerwanie granic pomiędzy kontekstami. Dane zgromadzone dla jednego celu mogą zostać przeniesione do drugiego, gdzie całkowicie zmienia się ich społeczne znaczenie.

Zasada ograniczenia celu zyskuje tu nie tylko prawne, ale i antropologiczne uzasadnienie. Chroni ona człowieka przed sytuacją, w której jedno zdarzenie zaczyna nieograniczenie podążać za nim przez wszystkie przestrzenie życia. Świat bez granic kontekstowych byłby światem, w którym rozmowa z lekarzem może automatycznie wpłynąć na proces zatrudnienia, aktywność konsumencka na decyzję polityczną, szkolny błąd na ocenę kredytową, a młodzieńcza wypowiedź na dorosłą tożsamość zawodową.

Cyfrowa pamięć absolutna mogłaby okazać się wrogiem ludzkiej zdolności do zmiany. Prywatność ma bowiem także wymiar temporalny. Człowiek potrzebuje nie tylko przestrzeni poza obserwacją, lecz również możliwości oddalenia się od własnej przeszłości. Społeczeństwa tradycyjne posiadały naturalne mechanizmy zapominania: dokument ginął, fotografia blakła, gazeta znikała z kiosku, a lokalna kompromitacja traciła publiczność wraz z upływem czasu. Internet i tanie magazynowanie danych osłabiły tę naturalną entropię informacji. Przeszłość stała się wyszukiwalna, kopiowalna i natychmiast zestawialna z teraźniejszością.

Nie należy jednak romantyzować zapomnienia. Archiwum pozwala ścigać zbrodnie, dokumentować represje i rozliczać władzę. Właśnie dzięki zachowanym aktom Stasi można dziś rekonstruować mechanizmy dyktatury i pozwolić poszkodowanym poznawać własne historie. To piękny paradoks

archiwum: dokument stworzony jako narzędzie kontroli może po upadku reżimu stać się dowodem przeciwko kontrolującemu. Pamięć państwa może zostać odwrócona przeciwko państwu.

Problem nie polega zatem na wyborze pomiędzy pamięcią a zapomnieniem, lecz na władzy określania warunków obu tych procesów. Demokratyczne archiwum musi pamiętać władzę wystarczająco długo, aby można ją było rozliczyć, ale nie powinno pamiętać obywatela bez ograniczeń tylko dlatego, że przechowywanie danych stało się tanie. Przejrzystość państwa i prywatność jednostki są wartościami asymetrycznymi. W demokracji to władza powinna być bardziej przejrzysta dla obywatela niż obywatel dla władzy. Ta asymetria jest jednym z najważniejszych fundamentów ustrojowych społeczeństwa informacyjnego.

Totalitaryzm dąży do sytuacji odwrotnej: państwo wie wszystko o obywatelu, podczas gdy obywatel wie mało o państwie. Demokracja powinna dążyć do odwrócenia tych proporcji: publiczne decyzje wymagają kontroli, podczas gdy prywatne życie jednostki korzysta z domniemania ochrony. Nie chodzi o absolutną niewidzialność obywatela ani absolutną jawność państwa, lecz o kierunek ciężaru dowodu.

Nadzór niezależnego sądu, wymóg konkretnego nakazu, niezależny organ ochrony danych, raportowanie żądań państwowych, procedury odwoławcze i obowiązki transparentności nie są zatem technicznymi dodatkami do systemu.

Rola dostawcy chmury jako cyfrowego bezpiecznika między państwem a obywatelem

Stanowią cyfrowy odpowiednik zamka w drzwiach i sędziego stojącego pomiędzy policjantem a domem. W tradycji amerykańskiej nakaz sądowy wprowadza niezależnego arbitra między aparat ścigania a prywatność jednostki; w europejskiej zaś podobną funkcję rozdzielania władzy pełnią sądy oraz niezależne organy nadzorcze, kontrolujące legalność ingerencji.

W świecie cyfrowym tę logikę należy rozciągnąć na administratora infrastruktury. Dostawca chmury nie może być traktowany jak zupełnie bierna ściana magazynu, skoro to właśnie do niego kierowane są żądania wydania informacji. Jednocześnie nie powinien on stać się prywatnym trybunałem, który samodzielnie definiowałby zakres legalnych kompetencji państwa. Tworzy to złożoną relację trójstronną: obywatel posiada prawa, państwo określone kompetencje, a pośrednik technologiczny – dysponując techniczną kontrolą nad zasobem – znajduje się pomiędzy nimi. W tym układzie szczególnie niebezpieczne są nakazy połączone z długotrwałym zakazem informowania użytkownika. Materiał źródłowy przywołuje w tym kontekście konflikt Microsoftu z

amerykańskim Departamentem Sprawiedliwości wokół tzw. gag orders i praktyki określanej retorycznie jako „Secrecy Forever".

Problem ten ma wymiar ustrojowy: obywatel, który nigdy nie dowiaduje się o ingerencji, traci realną możliwość jej zakwestionowania. Tajność niezbędna na etapie śledztwa może, po utracie funkcjonalnego uzasadnienia, przestać być instrumentem ochrony dochodzenia, a stać się narzędziem uniemożliwiającym kontrolę władzy. Nie oznacza to, że każdy dostęp państwa powinien być natychmiast jawny – ostrzeżenie podejrzanego przed przeszukaniem mogłoby przecież zniweczyć skuteczność postępowania. Właśnie dlatego właściwą kategorią nie jest absolutna jawność, lecz proporcjonalność czasowa: tajność powinna trwać tak długo, jak istnieje konkretna potrzeba jej utrzymania, zamiast stawać się domyślną cechą relacji państwa z cyfrowym archiwum.

Tutaj powraca maksyma Smitha o gotowości, by raczej ponieść porażkę, niż utracić wiarygodność. W ujęciu źródłowym spór z własnym państwem jest przedstawiany jako inwestycja w globalne zaufanie klientów. Narrację tę należy odczytywać jednocześnie normatywnie i ekonomicznie. Obrona prywatności może wynikać z przekonania o niezbywalnych prawach człowieka, lecz dla globalnego dostawcy chmury jest ona również warunkiem pozostania wiarygodnym przedsiębiorstwem na rynkach Niemiec, Francji, Brazylii, Japonii czy Indii. Prywatność staje się zatem elementem kapitału instytucjonalnego firmy.

Nie jest to argument przeciwko takim działaniom. Przeciwnie – ukazuje on mechanizm, w którym interes komercyjny może współgrać z wartością publiczną. Globalna firma może sprzeciwiać się nadmiernej inwigilacji własnego państwa właśnie dlatego, że koszt utraty międzynarodowego zaufania byłby dla niej wyższy niż korzyść z politycznej uległości. Rynek nie gwarantuje ochrony praw człowieka, ale odpowiednio skonstruowane bodźce mogą czasem wzmacniać prawo. Warunkiem jest jednak możliwość wyboru dostawcy, reputacyjna wrażliwość przedsiębiorstwa oraz istnienie norm, według których klienci potrafią tę reputację oceniać.

Współczesny spór o prywatność nie daje się zatem zamknąć w prostej opozycji „obywatel kontra państwo". Mamy do czynienia z co najmniej czterema ośrodkami interesów: jednostką, państwem, przedsiębiorstwem technologicznym oraz zbiorowością korzystającą z bezpieczeństwa i wiedzy wytwarzanej dzięki analizie danych. W określonych sytuacjach interesy te mogą się pokrywać, w innych pozostają w głębokim konflikcie.

Prywatność jako system rozdzielania uprawnień do wiedzy

Pacjent pragnie prywatności, nauka potrzebuje danych, szpital dba o bezpieczeństwo, państwo może wymagać informacji w postępowaniu karnym, a dostawca chmury musi chronić infrastrukturę i respektować prawo. Dojrzały system nie może absolutyzować żadnej z tych perspektyw.

Prywatność powinna być zatem postrzegana jako system rozdzielania uprawnień do wiedzy, podobnie jak konstytucja rozdziela uprawnienia do wykonywania władzy. Nie każdy ma wiedzieć wszystko.

Lekarz powinien wiedzieć to, co niezbędne do leczenia; fiskus – to, co konieczne do zastosowania prawa podatkowego; policja – tego, czego legalnie wymaga konkretne postępowanie; a dostawca infrastruktury tyle, ile wymaga techniczne utrzymanie systemu. Sednem ochrony danych nie jest stworzenie społeczeństwa niewiedzy, lecz takiego, w którym wiedza instytucjonalna ma ściśle określony zakres. Stąd można wyprowadzić kolejną maksymę artykułu: wolność w społeczeństwie informacyjnym zależy nie od tego, czy istnieją dane, lecz od tego, czy istnieją granice pomiędzy tymi, którzy mogą z nich korzystać. W epoce papieru granice te często miały charakter fizyczny: zamknięta szafa, oddzielny urząd, lokalne archiwum czy brak technicznej możliwości szybkiego połączenia rejestrów. Cyfryzacja usuwa większość tych naturalnych barier.

Dlatego ich miejsce muszą zająć bariery celowo zaprojektowane: prawne, organizacyjne, kryptograficzne i proceduralne.

W tym świetle można zrozumieć, dlaczego prywatność jest częścią demokracji, a nie jedynie regulacją rynku danych. Człowiek całkowicie przezroczysty wobec instytucji traci zdolność negocjowania z nimi swojej pozycji. Asymetria informacyjna staje się asymetrią władzy. Jeżeli pracodawca, ubezpieczyciel, bank, platforma albo państwo zna szczegółowo zachowania jednostki, podczas gdy ona sama nie zna reguł modelu, który ją ocenia, formalna swoboda kontraktu lub procedury może maskować głęboką nierównowagę poznawczą. Władza cyfrowa ma szczególną właściwość: często nie wydaje rozkazu. Klasyczna władza mówiła „musisz”.

Władza algorytmiczna może powiedzieć „nie kwalifikujesz się”, „nie jesteś widoczny”, „nie uzyskałeś odpowiedniego wyniku”, „system ocenił ryzyko” albo po prostu nigdy nie pokazać człowiekowi określonej możliwości. Dlatego ochrona prywatności zaczyna łączyć się z transparentnością, prawem do wyjaśnienia, kontrolą jakości danych i możliwością

zakwestionowania automatycznego wyniku. Granica między archiwum a panoptikonem nie przebiega więc pomiędzy przechowywaniem a nieprzechowywaniem informacji. Przebiega pomiędzy dwoma modelami instytucjonalnymi.

Archiwum demokratyczne pamięta według reguł, ogranicza dostęp, respektuje cel, pozwala skorygować błąd i poddaje administratora kontroli. Panoptikon dąży do maksymalizacji widzialności obserwowanego przy minimalizacji widzialności obserwatora. Pierwszy model buduje zaufanie przez ograniczenie własnej władzy; drugi buduje posłuszeństwo przez niepewność co do granic obserwacji. Współczesna technologia potrafi obsługiwać oba modele. To samo centrum danych może być archiwum demokratycznego państwa prawa albo repozytorium systemu represji.

To samo rozpoznawanie twarzy może pomóc osobie z niepełnosprawnością lub zbudować automatyczny system śledzenia przeciwników politycznych. Ten sam system analityczny może wykrywać epidemię albo tworzyć profile obywateli służące represji. Ponownie wracamy więc do Tools and Weapons: nie urządzenie rozstrzyga o moralnej naturze systemu, lecz połączenie celu, uprawnień, danych, kontroli i możliwości odwołania. Prywatność okazuje się w rezultacie nie przeszkodą stojącą na drodze nowoczesności, lecz jednym z warunków, dzięki którym nowoczesność może pozostać zgodna z wolnością. Gdy społeczeństwo potrafi gromadzić niemal nieograniczone ilości informacji, jego dojrzałość przejawia się nie w zdolności dowiedzenia się wszystkiego, lecz w umiejętności powstrzymania się od wiedzy, której nie potrzebuje. Władza technologiczna osiąga polityczną dojrzałość wtedy, gdy potrafi powiedzieć nie tylko „możemy to wiedzieć", lecz również „nie mamy prawa tego wiedzieć". Tym samym „dom jako zamek" nie znika w epoce chmury. Zmienia architekturę. Jego mury tworzą dziś kryptografia, ograniczenie celu, minimalizacja danych, niezależna kontrola, konkretność nakazu, transparentność, prawo dostępu, prawo korekty oraz możliwość zakwestionowania ingerencji. Zamek obywatela nie stoi już tylko przy ulicy. Część jego ścian znajduje się w centrum danych tysiące kilometrów dalej. To jednak rodzi następne pytanie, jeszcze trudniejsze.

Od własności rzeczowej do funkcjonalnego powiernictwa danych

Skoro dane znajdują się w infrastrukturze przedsiębiorstwa, kto w świetle prawa może decydować o ich wykorzystaniu? Czy dostawca chmury jest właścicielem, powiernikiem, procesorem, strażnikiem, czy jedynie technicznym wykonawcą poleceń klienta? Kto odpowiada za wtórną analizę, kto ustala cel i kto ponosi konsekwencje, gdy legalnie zebrane informacje zostają

wykorzystane w nowej operacji analitycznej? Granica pomiędzy prywatnością a panoptikonem prowadzi nas zatem bezpośrednio do problemu własności, kontroli i powiernictwa danych.

Pytanie „czyje są dane?" wydaje się proste tylko dopóty, dopóki traktujemy informację jak rzecz. Gdy książka leży na stole, samochód stoi w garażu, a pieniądze znajdują się na rachunku, język własności dostarcza intuicyjnej odpowiedzi na pytanie o uprawnienia. Możemy wskazać właściciela, określić zakres jego władztwa i ustalić moment naruszenia cudzego prawa. Dane komplikują tę konstrukcję niemal natychmiast.

Informacja może dotyczyć jednej osoby, zostać zebrana przez drugą, znajdować się na serwerze trzeciej, być analizowana przez czwartą i służyć decyzji podejmowanej przez piątą. Każdy z tych podmiotów pozostaje w realnej relacji z tym samym zasobem, lecz żadna z nich nie musi być klasyczną własnością.

W tym miejscu język popularny zaczyna rozchodzić się z językiem prawa. W narracji Tools and Weapons oraz w materiale źródłowym powraca atrakcyjna i komunikacyjnie skuteczna maksyma: dane należą do klienta. Jest to deklaracja o wielkiej wartości normatywnej, ponieważ przeciwstawia się pokusie uznania, że przedsiębiorstwo posiadające techniczną kontrolę nad serwerem automatycznie uzyskuje moralne prawo do jego zawartości. Materiał ujmuje tę zmianę jako przejście od modelu dostawcy infrastruktury do modelu stewardship – powiernictwa, w którym korporacja chroni zasób powierzony przez klienta, zamiast traktować go jak własny surowiec. Wymaga to jednak wprowadzenia korekty teoretycznej, która paradoksalnie wzmacnia tę ideę.

W europejskim prawie ochrony danych osobowych podstawowym pojęciem nie jest własność. RODO nie buduje ochrony informacji poprzez stworzenie prostego prawa rzeczowego do danych. Posługuje się inną architekturą: prawami osoby, której dane dotyczą, obowiązkami administratora, rolą podmiotu przetwarzającego oraz zasadami legalności, ograniczenia celu, minimalizacji, rozliczalności i bezpieczeństwa. Pytanie „kto jest właścicielem?" zostaje zatem zastąpione pytaniami bardziej precyzyjnymi: kto ustala cel przetwarzania, kto określa zasadnicze środki, kto wykonuje operacje na czyje polecenie, kto ponosi odpowiedzialność i jakie prawa zachowuje osoba, której informacja dotyczy?

To rozróżnienie ma ogromne znaczenie. Własność sugeruje jednolite i wyłączne władztwo; ochrona danych tworzy natomiast wiązkę uprawnień i obowiązków rozdzielonych między wielu uczestników. Pacjent może posiadać prawo dostępu do dotyczących go danych medycznych, lecz dokumentacja nie staje się przez to przedmiotem, który można po prostu zabrać ze szpitala jak własną walizkę. Bank może być administratorem danych transakcyjnych, lecz nie uzyskuje przez to dowolności ich wykorzystania. Dostawca infrastruktury może przechowywać dane klientów na

tysiącach serwerów, ale samo techniczne posiadanie nośnika nie daje mu prawa do określania nowych celów użycia informacji.

Europejskie pojęcie administratora jest funkcjonalne. Administratorem nie jest ten, kto posiada najwięcej serwerów, ani ten, kogo umowa ceremonialnie nazwie „właścicielem danych". Jest nim podmiot, który rzeczywiście określa cele i zasadnicze sposoby przetwarzania. Jeżeli przedsiębiorstwo decyduje, po co dane są gromadzone, jakie kategorie informacji będą używane, wobec kogo, przez jaki czas i w ramach jakiej logiki operacyjnej – wchodzi w rolę administratora niezależnie od tego, czy fizycznie przechowuje bajty na własnym sprzęcie. Podmiot przetwarzający znajduje się natomiast w pozycji odmiennej: wykonuje operacje na danych w imieniu administratora i zasadniczo według jego udokumentowanych instrukcji. Nie jest jednak jedynie mechanicznym przedłużeniem kabla.

Odpowiedzialność wynika z realnej władzy decyzyjnej

RODO nakłada na procesora konkretne obowiązki, dotyczące m.in. bezpieczeństwa, poufności, angażowania dalszych podmiotów przetwarzających czy współpracy przy realizacji praw osób. Granica pomiędzy administratorem a procesorem jest więc granicą funkcji, nie prestiżu. Można dysponować największą chmurą obliczeniową świata i w danym procesie pozostać procesorem; można być niewielką instytucją bez własnego centrum danych i nadal pełnić rolę administratora, gdyż to ten podmiot określa cel przetwarzania.

Pozwala to lepiej zrozumieć intuicję źródłowego "kontenera". W tej relacji klient decyduje, co znajduje się w kontenerze i w jakim celu ma być analizowane, podczas gdy dostawca odpowiada za bezpieczeństwo i sprawność infrastruktury. Obraz ten jest użyteczny, o ile nie potraktujemy go jako absolutnego opisu każdej usługi chmurowej. W rzeczywistości zakres odpowiedzialności zależy od architektury konkretnej usługi, umowy, faktycznych decyzji oraz tego, czy dostawca rzeczywiście pozostaje wyłącznie wykonawcą instrukcji.

W tym miejscu wyłania się kluczowa zasada odpowiedzialności cyfrowej: rola prawna nie wynika z etykiety, lecz z rzeczywistej władzy decyzyjnej. Umowa może nazwać przedsiębiorstwo procesorem, lecz jeśli zacznie ono samodzielnie określać nowe cele wykorzystania danych, w odniesieniu do tych operacji może stać się administratorem. Prawo ochrony danych nie powinno pozwalać na ucieczkę od odpowiedzialności za pomocą słownika kontraktowego; instytucjonalna rzeczywistość jest ważniejsza od nagłówka dokumentu.

Ta zasada ma głębokie uzasadnienie polityczne. Władza zawsze próbowała przedstawiać się jako techniczna konieczność. Urzędnik "tylko wykonuje procedurę", platforma "tylko pokazuje wyniki", algorytm "tylko liczy", a dostawca infrastruktury "tylko przechowuje". Czasem opis ten jest prawdziwy, jednak słowo "tylko" często ukrywa istotny wybór. Jeśli podmiot wyznacza kryteria, ustala parametry, wybiera dane wejściowe lub definiuje nowy cel przetwarzania, uczestniczy w kształtowaniu rzeczywistości normatywnej i nie powinien korzystać z moralnej anonimowości maszyny.

Należy zatem powrócić do rozróżnienia pomiędzy własnością a kontrolą. W gospodarce cyfrowej bardziej użyteczne niż pytanie "kto posiada informację?" bywa pytanie "kto posiada zdolność uruchomienia wobec niej operacji?". Kontrola może być rozproszona: jeden podmiot posiada klucze szyfrujące, drugi określa instrukcje, trzeci żąda danych na podstawie prawa, a czwarty zachowuje prawo do dostępu lub usunięcia określonych informacji. Informacja znajduje się w centrum skrzyżowania kompetencji.

Można tę sytuację porównać do wielopiętrowej konstrukcji zamka. Osoba, której dane dotyczą, nie musi być właścicielem budynku, aby posiadać prawa do tego, co znajduje się w środku. Administrator nie musi posiadać fizycznych serwerów, aby ponosić zasadniczą odpowiedzialność za legalność celu. Dostawca chmury nie musi ustalać celu analitycznego, aby odpowiadać za bezpieczeństwo techniczne. Państwo nie staje się właścicielem informacji tylko dlatego, że uzyskuje do niej dostęp na podstawie normy prawnej.

Każda warstwa otrzymuje inną kombinację praw i obowiązków. Taka architektura może wydawać się bardziej skomplikowana niż prosta własność, ale właśnie ta komplikacja odpowiada naturze informacji. Dane są kopiowalne i relacyjne; mogą dotyczyć kilku osób równocześnie, być niezbędne do realizacji obowiązku prawnego lub posiadać znaczenie publiczne i prywatne zarazem. Próba zamknięcia problemu w formule "moje dane, moja własność" brzmi atrakcyjnie, lecz szybko prowadzi do paradoksów. Czy pojedynczy człowiek miałby prawo usunąć z rejestru publicznego każdą informację dotyczącą własnej działalności? Czy jedna osoba mogłaby "posiadać" treść rozmowy prowadzonej z drugą? Czy pacjent mógłby zakazać szpitalowi przechowywania dokumentacji wymaganej prawem? A czy sprawca przestępstwa byłby właścicielem zapisu własnego czynu?

W tym kontekście adekwatną kategorią jest uprawniona kontrola kontekstowa. Człowiek nie musi mieć absolutnej własności każdej informacji dotyczącej siebie, aby posiadać realne prawa wobec jej przetwarzania. Podobnie instytucja nie musi być właścicielem danych, aby móc legalnie wykonywać na nich określone operacje.

Ograniczenie celu jako bariera przed dowolną eksploatacją danych

Kluczowe stają się cel, podstawa, zakres, czas oraz odpowiedzialność. W tej konstrukcji zasada ograniczenia celu pełni funkcję przypominającą konstytucyjny zakaz nadużycia kompetencji. Informacja zebrana dla jednego zadania nie powinna automatycznie stawać się uniwersalnym zasobem dla wszystkich przyszłych ambicji administratora. RODO nakazuje zbierać dane w konkretnych, wyraźnych i prawnie uzasadnionych celach oraz – co do zasady – nie wykorzystywać ich później w sposób z tymi celami niezgodny. Materiał źródłowy trafnie wskazuje właśnie to zagadnienie jako główny problem analityki chmurowej: czy informację pozyskaną w jednym celu można następnie uruchomić w zupełnie innym kontekście. Znaczenie ograniczenia celu rośnie wraz ze wzrostem mocy obliczeniowej. W świecie papierowym bariery techniczne same w sobie utrudniały wtórne wykorzystanie danych; konieczne było odnalezienie teczki, przepisanie rekordu, połączenie archiwów i zatrudnienie ludzi do analizy. W chmurze koszt korelacji może spaść dramatycznie.

Z tego powodu to, co dawniej ograniczała fizyczna niewygoda, dziś musi ograniczać prawo i architektura systemu. Pojawia się tu istotny paradoks. Nowoczesna analityka osiąga największą wartość właśnie wtedy, gdy potrafi wykorzystać dane w sposób, którego pierwotnie nie przewidziano. Nauka rozwija się dzięki stawianiu nowych pytań starym obserwacjom; sztuczna inteligencja może dostrzec wzorzec niewidoczny dla osoby zbierającej dane. Dane kliniczne zgromadzone w celu leczenia konkretnych pacjentów mogą dostarczyć wiedzy kluczowej dla przyszłych terapii. Gdyby ograniczenie celu potraktować mechanicznie i absolutnie, mogłoby to zahamować innowację poznawczą. Jeśli jednak zostałoby całkowicie porzucone, każda baza stałaby się magazynem do dowolnej eksploatacji.

Prawo próbuje rozwiązać ten konflikt poprzez pojęcie zgodności dalszego przetwarzania, szczególne zasady dla badań oraz środki ochronne. Nie każde nowe wykorzystanie musi być traktowane jak zdrada pierwotnego celu, ale nie każda korzyść poznawcza legitymizuje wszystko. Należy ocenić między innymi związek między celami, kontekst zebrania danych, charakter informacji, możliwe konsekwencje dla osoby oraz zastosowane zabezpieczenia. Widać tu charakterystyczną dla nowoczesnego prawa zmianę: zamiast prostego zakazu otrzymujemy procedurę oceny proporcjonalności.

Przykład badań onkologicznych doskonale ilustruje to napięcie. Współpraca analityczna może przekształcić rozproszone zbiory informacji w wiedzę służącą diagnostyce i terapii. Materiał traktuje wykorzystanie danych w badaniach nad nowotworami jako sytuację, w której wtórna

analiza pozostaje bliska pierwotnemu dobru pacjenta i celowi medycznemu. Nie należy jednak wyciągać z tego wniosku, że każde „badanie naukowe” automatycznie legalizuje dowolne wykorzystanie danych. Właśnie dlatego współczesne prawo rozwija szczególne gwarancje dla nauki, zamiast tworzyć dla niej obszar całkowitego wyłączenia. W 2026 roku dyskusja ta jest szczególnie aktualna; Europejska Rada Ochrony Danych przedstawiła w kwietniu tego roku projekt wytycznych dotyczących przetwarzania danych osobowych do celów badań naukowych. Sam fakt powstania tych wytycznych pokazuje, że napięcie pomiędzy swobodą badań, użytecznością danych a ochroną osoby nie zostało rozwiązane prostą formułą. Im potężniejsze stają się techniki analityczne, tym bardziej nauka potrzebuje nie tylko danych, lecz także infrastruktury zaufania. Można powiedzieć, że ograniczenie celu nie jest zakazem uczenia się z informacji. Jest zakazem uznania, że skoro informację raz legalnie uzyskano, przestaje istnieć moralna granica jej przyszłego wykorzystania. To różnica subtelna, lecz kluczowa.

Powiernictwo jako architektura zaufania i odpowiedzialności

Archiwum nie staje się bezpańskim terytorium tylko dlatego, że zgromadzono w nim wiele cennych rekordów. To właśnie tutaj koncepcja stewardship nabiera pełniejszego znaczenia. Powiernik nie jest właścicielem celu, lecz strażnikiem warunków działania infrastruktury. Jego odpowiedzialność wykracza poza zapewnienie dostępności serwera; musi on dbać o to, by techniczna konstrukcja systemu umożliwiała realizację zobowiązań prawnych administratora. Obejmuje to między innymi odpowiednie zabezpieczenia, zarządzanie uprawnieniami, możliwość wykonywania konkretnych operacji na danych, rejestrowanie dostępu, retencję i usuwanie, reagowanie na incydenty oraz kontrolę łańcucha dalszych podmiotów przetwarzających. Należy jednak unikać romantyzowania pojęcia „powiernik”.

Stewardship jest jednocześnie etyką, modelem zarządzania i strategią biznesową. Pozycjonowanie przedsiębiorstwa jako zarządcy, a nie właściciela danych, może stać się architekturą zaufania i realną przewagą rynkową, co w języku ekonomii instytucjonalnej jest całkowicie racjonalne. Klient przenosi do chmury zasób, którego utrata, ujawnienie lub niewłaściwe wykorzystanie mogą spowodować ogromne szkody. Dostawca, który przekonuje rynek, że nie zamierza wykorzystywać asymetrii technicznej przeciwko klientowi, obniża koszt zaufania i zwiększa atrakcyjność swojej usługi.

Zaufanie nie powinno jednak opierać się wyłącznie na reputacji. Im ważniejsza infrastruktura, tym mniej rozsądne jest uzależnianie bezpieczeństwa od charakteru aktualnego zarządu firmy. Dobre

instytucje powstają właśnie po to, aby cnota jednostki nie była jedynym zabezpieczeniem systemu. Powiernictwo musi zostać zakotwiczone w umowie, prawie, audycie i architekturze technicznej, a także w realnej możliwości egzekwowania zobowiązań. Model Czterech Zobowiązań Chmurowych można zatem odczytać jako próbę zamiany abstrakcyjnego zaufania w cztery kategorie odpowiedzialności: prywatność, bezpieczeństwo, zgodność i przejrzystość. Ich znaczenie wykracza poza korporacyjny kodeks wartości, jeśli potraktujemy je jako prototyp konstytucji infrastruktury informacyjnej. Prywatność odpowiada na pytanie, czy cudzy zasób nie zostanie wykorzystany poza uprawnionym kontekstem. Bezpieczeństwo pyta, czy nie uzyska do niego dostępu podmiot nieuprawniony. Zgodność weryfikuje, czy operacje mieszczą się w granicach prawa, a przejrzystość pozwala użytkownikowi i instytucjom kontrolnym dowiedzieć się, jakie reguły faktycznie obowiązują.

Te cztery kategorie nie są niezależnymi ozdobnikami; brak jednej osłabia pozostałe. Bezpieczeństwo bez prywatności może stworzyć perfekcyjnie zabezpieczony system nadzoru. Prywatność bez bezpieczeństwa pozostaje jedynie deklaracją, którą pierwszy skuteczny napastnik może unicestwić. Zgodność bez przejrzystości może zamienić się w nieweryfikowalne zapewnienie, że „wszystko jest zgodne", natomiast przejrzystość bez realnej odpowiedzialności ograniczy się do publikowania dokumentów, których nikt nie zdoła wykorzystać do zakwestionowania działania systemu. Najciekawsza relacja zachodzi jednak między bezpieczeństwem a kontrolą. Dostawca chmury może nie decydować o celu przetwarzania, ale jego wybory techniczne drastycznie wpływają na ryzyko. Rodzaj szyfrowania, zarządzanie kluczami, segmentacja sieci, system uprawnień, sposób tworzenia kopii zapasowych, konfiguracja logów czy model aktualizacji oprogramowania to środki techniczne, które niosą za sobą normatywne konsekwencje. Procesor nie jest więc prawodawcą celu, lecz może być architektem możliwości. To kolejny powód, dla którego prosta analogia magazynu jest niewystarczająca – magazynier może przecież nie wiedzieć, co znajduje się w szczelnie zamkniętej skrzyni.

Rozróżnienie władzy infrastrukturalnej od semantycznej jako fundament rozliczalności

Operator chmury projektuje środowisko, w którym tysiące klientów wykonują operacje na danych. Nawet jeśli nie powinien wykorzystywać treści dla własnych celów, to właśnie jego infrastruktura determinuje możliwe poziomy izolacji, kontroli i odporności. Władza nad architekturą nie jest tym samym co władza nad treścią, lecz pozostaje realną władzą. Pozwala to na rozróżnienie między władzą semantyczną a infrastrukturalną. Administrator dysponuje władzą semantyczną, określając

cel przetwarzania danych i znaczenie wyników operacji. Dostawca infrastruktury posiada natomiast władzę infrastrukturalną, gdyż decyduje o technologicznych warunkach wykonania zadania. Odpowiedzialność obu podmiotów powinna zatem odpowiadać rodzajowi sprawowanej przez nie kontroli.

W praktyce granica ta jest płynna. W prostym modelu infrastruktury klient sam konfiguruje znaczną część środowiska, jednak w usługach wyższego poziomu dostawca oferuje gotowe mechanizmy analityczne, modele AI, systemy klasyfikacji czy zarządzane bazy danych. Im bardziej usługa ewoluuje od wynajmu mocy obliczeniowej ku aktywnemu kształtowaniu operacji na danych, tym kluczowsze staje się pytanie o rzeczywisty zakres decyzji dostawcy.

W tym miejscu prawo spotyka się z ekonomią platformową. Przedsiębiorstwa technologiczne rzadko są dziś wyłącznie pasywnymi wykonawcami cudzej logiki; oferują gotowe systemy decyzyjne, modele, API oraz narzędzia bezpieczeństwa i integracji. Często to one tworzą standardy, według których później funkcjonuje cały sektor. Powiernictwo nie może więc sprowadzać się do wygodnego stwierdzenia: „nie odpowiadamy, bo to klient zdecydował". Należy każdorazowo badać, kto realnie posiadał możliwość dokonania danego wyboru. Europejska Rada Ochrony Danych podkreśla zresztą funkcjonalny charakter ról administratora i procesora – liczy się faktyczny wpływ na cele i zasadnicze środki przetwarzania, a nie jedynie kontraktowa nazwa funkcji.

Zasada rozliczalności wymaga dodatkowo, aby administrator nie tylko przestrzegał prawa, lecz potrafił to udowodnić. W cyfrowym państwie prawa odpowiedzialność bez dokumentowalności jest bowiem odpowiedzialnością deklaratywną. Rozliczalność stanowi jedno z największych osiągnięć współczesnego governance danych, przesuwając ciężar z reakcji na naruszenie w stronę projektowania systemu zdolnego wyjaśnić własne działanie.

Organizacja musi wiedzieć, jakie dane posiada, w jakim celu i na jakiej podstawie, jak długo je przechowuje, komu udostępnia, jakie środki bezpieczeństwa stosuje i kto odpowiada za konkretny proces. Innymi słowy: instytucja powinna posiadać mapę własnej pamięci. To pozornie administracyjny wymóg, lecz jego sens jest głęboko filozoficzny. Władza, która nie wie, jakie informacje posiada i jak je wykorzystuje, staje się władzą niezdolną do odpowiedzialności. Można wymagać od niej dobrej woli, ale nie można skutecznie kontrolować jej działania. Cyfrowa rozliczalność jest zatem instytucjonalnym odpowiednikiem samoświadomości: system musi umieć opowiedzieć własną historię przetwarzania.

Odpowiedzialność kaskadowa i prawo do wyjścia

W chmurze problem komplikuje łańcuch podmiotów. Dostawca korzysta z kolejnych podwykonawców, infrastruktura może obejmować różne regiony, a usługa integrować wiele komponentów. Pojawia się zjawisko odpowiedzialności kaskadowej. Administrator pozostaje odpowiedzialny za wybór i nadzorowanie procesora w zakresie wymaganym prawem, procesor odpowiada za własne obowiązki, a dalszy podmiot przetwarzający nie powinien być niewidzialnym ogniwem poza systemem odpowiedzialności. EDPB w opinii z 2024 roku dotyczącej korzystania z procesorów i subprocesorów podkreśliła znaczenie wiedzy administratora o łańcuchu przetwarzania oraz odpowiedzialności za ocenę jego zgodności. Jest to szczególnie istotne w gospodarce chmurowej, gdzie klient może odnieść techniczne wrażenie korzystania z jednej usługi, podczas gdy za ekranem działa rozbudowany ekosystem dostawców. Można tu dostrzec analogię do nowoczesnego łańcucha dostaw w przemyśle: producent samochodu nie może wiarygodnie zapewniać o jakości całości, jeżeli nie kontroluje kluczowych komponentów dostarczanych przez podwykonawców.

Podobnie administrator danych nie powinien traktować outsourcingu jako outsourcingu odpowiedzialności. Można przekazać wykonanie czynności, ale nie można automatycznie przenieść całej odpowiedzialności za wybór systemu, w którym ta czynność będzie realizowana. Zasada ta jest kluczowa z punktu widzenia cyberbezpieczeństwa. Im więcej ogniw znajduje się w łańcuchu, tym więcej potencjalnych punktów słabości. Atakujący nie musi przełamywać najsilniejszego elementu systemu, jeśli może wejść przez najmniej dojrzałego podwykonawcę. Zaufanie w chmurze jest więc zaufaniem kaskadowym. Każdy nowy uczestnik może zwiększyć funkcjonalność, ale jednocześnie powiększa powierzchnię ryzyka.

Powiernictwo nie kończy się na deklaracji, że "dane należą do klienta". Prawdziwa doktryna stewardship musi odpowiedzieć na bardziej niewygodne pytanie: czy klient może rzeczywiście odejść? Jeżeli dostawca formalnie nie rości sobie praw do danych, lecz technicznie utrudnia ich przeniesienie, uzależnia aplikacje od własnych formatów albo narzuca wysokie koszty wyjścia, powstaje subtelniejsza forma kontroli. To nie własność, lecz zależność staje się źródłem władzy.

Rozwój prawa unijnego wyraźnie wykracza już poza klasyczne RODO. Data Act, stosowany od września 2025 roku, wprowadza między innymi reguły mające ułatwiać klientom zmianę dostawcy usług przetwarzania danych, w tym usług chmurowych i edge. Komisja Europejska interpretuje te przepisy jako instrument usuwania barier takich jak wysokie koszty wyjścia, utrudnione procedury oraz brak interoperacyjności. Jest to kluczowe dla filozofii powiernictwa. Jeżeli klient naprawdę

pozostaje gospodarzem swojego zasobu, powinien mieć praktyczną możliwość przeniesienia go wraz z istotnymi elementami własnego środowiska do innego dostawcy.

Wolność bez możliwości wyjścia jest wolnością ograniczoną. Albert Hirschman opisywał relację pomiędzy exit i voice: uczestnik organizacji może próbować wpływać na jej działanie albo ją opuścić. W gospodarce chmurowej techniczna możliwość exit staje się jednym z warunków równowagi między klientem a dostawcą. Pozwala to rozszerzyć Cztery Zobowiązania Chmurowe o piąty element, który wynika nie tyle ze źródłowego katalogu, ile ze współczesnej ewolucji europejskiego prawa: przenoszalność instytucjonalną. Powiernik, który rzeczywiście nie rości sobie suwerenności nad cudzym zasobem, powinien projektować system tak, aby klient mógł racjonalnie zmienić powiernika. Brak technicznej zakładniczości jest cyfrowym odpowiednikiem prawa zabrania dokumentów z jednego bankowego sejfu do innego. Nie oznacza to oczywiście, że migracja wielkiej infrastruktury musi być całkowicie bezkosztowa albo banalna.

Powiernictwo jako architektura rozproszonej władzy informacyjnej

Systemy różnią się architekturą, funkcjami i warstwami własności intelektualnej. Prawo nie może magicznie uczynić wszystkich technologii identycznymi, może jednak ograniczać praktyki, których ekonomicznym celem jest utrudnienie wyjścia, oraz promować interoperacyjność tam, gdzie jest ona technicznie uzasadniona.

W tym miejscu ujawnia się różnica między własnością formalną a suwerennością operacyjną. Można formalnie "mieć swoje dane", lecz pozostawać głęboko zależnym od infrastruktury, bez której stają się one praktycznie bezużyteczne. Plik w egzotycznym formacie może być własnością klienta, ale jeśli tylko jeden system potrafi go odczytać i wykorzystać, formalne prawo nie gwarantuje realnej autonomii. Wolność danych wymaga zatem nie tylko prawa do kopii, lecz także rzeczywistej możliwości ich ponownego użycia. Ekonomia cyfrowa przesuwa pojęcie własności z rzeczy ku zdolności działania – i nie jest to pierwszy raz w historii.

W prawie własności intelektualnej od dawna ważniejsze od fizycznego nośnika są prawa do określonych sposobów eksploatacji. W usługach finansowych klient nie "posiada" konkretnych banknotów w sejfie banku, lecz roszczenie i możliwość dysponowania środkami. Podobnie w przypadku danych rośnie znaczenie kontroli funkcjonalnej: dostępu, przeniesienia, wykorzystania, ograniczenia, usunięcia, sprzeciwu oraz możliwości kwestionowania decyzji.

Źródłowe zdanie "dane należą do klientów" należy zatem zachować, lecz interpretować je jako maksymę stewardship, a nie dogmatyczną definicję prawa własności. Jej siła tkwi w moralnym ograniczeniu dostawcy: infrastruktura nie powinna automatycznie przejmować praw do sensu cudzej informacji. Jest to deklaracja lojalności wobec klienta, a nie próba rozwiązania całej teorii praw do danych jednym sloganem. Właściwa architektura prawna jest bogatsza. Osoba, której dane dotyczą, zachowuje prawa podstawowe; administrator odpowiada za cel i zgodność; procesor działa zasadniczo na instrukcję i ponosi własne obowiązki, natomiast dostawca infrastruktury odpowiada za tę część bezpieczeństwa i działania, nad którą faktycznie sprawuje kontrolę. Państwo może ingerować jedynie w granicach kompetencji i procedur.

Prawo konkurencji oraz Data Act mogą dodatkowo chronić możliwość zmiany dostawcy i ograniczać uzależnienie infrastrukturalne. Nie istnieje jeden właściciel całego problemu – istnieje konstytucja relacji. Model ten jest intelektualnie mniej elegancki niż prosta własność, ale politycznie dojrzalszy. Wielkie systemy społeczne rzadko dają się bezpiecznie organizować poprzez przyznanie jednemu podmiotowi absolutnej władzy. Państwo konstytucyjne dzieli kompetencje, spółka rozdziela funkcje zarządzania i kontroli, a rynek tworzy kontrahentów o przeciwstawnych uprawnieniach. Ochrona danych robi coś podobnego z informacją: rozdziela zdolność do działania tak, aby żadna pojedyncza rola nie mogła bez ograniczeń przejąć całego zasobu. Powiernictwo staje się w ten sposób kategorią ustrojową.

Dostawca chmury nie jest suwerenem danych, lecz zarządcą określonej warstwy środowiska. Administrator nie jest właścicielem człowieka, którego profil posiada, lecz podmiotem korzystającym z informacji w prawnie określonym celu. Państwo zaś nie posiada danych obywatela tylko dlatego, że może legalnie ich zażądać.

Każdy z uczestników powinien posiadać tyle władzy, ile jest niezbędne do wykonania jego funkcji – i nie więcej. Można tę zasadę nazwać minimalizacją władzy informacyjnej. Jest ona odpowiednikiem minimalizacji danych: skoro nie należy gromadzić więcej informacji niż potrzeba, nie należy także przyznawać podmiotowi większej kontroli nad nimi, niż wymaga realizacja jego zadań. Programista nie musi widzieć danych produkcyjnych, jeśli może pracować na testowych. Analityk nie potrzebuje znać tożsamości, jeśli wystarcza mu agregat. Dostawca infrastruktury nie musi swobodnie używać treści, jeśli jego zadaniem jest zapewnienie mocy obliczeniowej. Państwo nie potrzebuje historii całego życia obywatela, jeśli konkretne postępowanie wymaga jedynie wąskiego zbioru informacji.

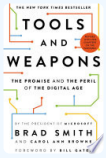
Zasada ta prowadzi ku kolejnemu etapowi rozwoju technologii ochrony prywatności. Jeżeli problemem jest nadmierna koncentracja zarówno danych, jak i uprawnień, można projektować systemy, w których informacja pozostaje u pierwotnego dysponenta, a do niej kierowane jest

jedynie określone zapytanie lub model. Można oddzielić wynik analizy od dostępu do surowego rekordu, dodać kontrolowany szum statystyczny, ograniczyć możliwość odtworzenia jednostki, wykonywać obliczenia bez ujawniania pełnej treści albo federować proces uczenia.

Wtedy powiernictwo przestaje być jedynie relacją prawną i zaczyna być architekturą obliczeniową. Stare archiwum stawiało problem w sposób zero-jedynkowy: albo ktoś otrzymał klucz do drzwi, albo pozostawał na zewnątrz. Współczesna kryptografia i analityka pozwalają zadać pytanie bardziej wyrafinowane: czy można uzyskać wiedzę z danych, nie uzyskując jednocześnie pełnej władzy nad danymi? Jeśli odpowiedź brzmi choć częściowo „tak", otwiera się możliwość nowego kompromisu pomiędzy prywatnością a postępem poznawczym. Algorytm nie musi już zabierać archiwum ze sobą; może – zgodnie ze źródłową maksymą – odwiedzić dane. Zapraszamy do kolejnego artykułu Fundacji Dobre Państwo.

> Prawdziwa dojrzałość polityczna cywilizacji informacyjnej nie objawi się w tym, ile potrafimy dowiedzieć się o sobie nawzajem, lecz w odwadze powiedzenia: „możemy to wiedzieć, ale nie mamy prawa tego wiedzieć". W świecie, gdzie mury domu zostały zastąpione przez kryptografię i protokoły dostępu, wolność przestaje być brakiem nadzoru, a staje się sztuką projektowania granic. Czy potrafimy zatem zbudować system, w którym techniczna wszechmoc nie oznacza moralnego przyzwolenia na totalną przejrzystość człowieka?

Inspiracje

[1] 

"Tools and Weapons" Brad Smith

2019 | Penguin Press | ISBN: 978-1984877710

Bradford Lee Smith (ur. 17 stycznia 1959 r.) to amerykański prawnik i dyrektor biznesowy, wiceprezes i prezes Microsoftu. Dołączył do firmy w 1993 r. i odegrał kluczową rolę w jej sprawach prawnych i korporacyjnych, w tym w prowadzeniu ważnych sporów antymonopolowych. Smith jest powszechnie uznawany za lidera w kluczowych kwestiach na styku technologii i społeczeństwa, takich jak cyberbezpieczeństwo, sztuczna inteligencja, prywatność, prawa człowieka i zrównoważony rozwój środowiska. Często określany jako ambasador branży technologicznej, często zeznaje przed rządami na całym świecie. Uzyskał tytuł licencjata (Bachelor of Arts) na Uniwersytecie Princeton oraz tytuł doktora prawa (Juris Doctor) na Wydziale Prawa Uniwersytetu Columbia. W 2019 r. był współautorem książki „Tools and Weapons", która analizuje odpowiedzialność sektora technologicznego w stawianiu czoła globalnym wyzwaniom stawianym przez postęp cyfrowy.

Bradford Lee Smith (born January 17, 1959) is an American attorney and business executive who serves as the vice chair and president of Microsoft. He joined the company in 1993 and has played a pivotal role in its legal and corporate affairs, including navigating major antitrust litigation. Smith is widely recognized for his leadership on critical issues at the intersection of technology and society, such as cybersecurity, artificial intelligence, privacy, human rights, and environmental sustainability. Often described as a de facto ambassador for the technology industry, he frequently testifies before governments worldwide. He holds a Bachelor of Arts from Princeton University and a Juris Doctor from Columbia Law School. In 2019, he co-authored the book Tools and Weapons, which examines the responsibilities of the tech sector in addressing the global challenges posed by digital advancement.

Microsoft

Literatura uzupełniająca

Książki

Autorzy przywoływani w artykule:

[1] "Crow's Landing"

Brad Smith

2012 | Simon and Schuster | ISBN: 9781439197530

[2] "The Return of Kid Cooper"

Brad Smith

2018 | Simon and Schuster | ISBN: 9781628728729

[3] "Shoot the Dog"

Brad Smith

2013 | Simon and Schuster | ISBN: 9781439197585

[4] "Minnesota logging utilization factors, 1975-1976"

James E. Blyth, W. Brad Smith

1980

[5] "Indiana Forest Statistics, 1986"

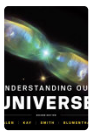
W. Brad Smith

1988

[6] "All Hat"

Brad Smith

2013 | Henry Holt and Company | ISBN: 9781466855557



[7] "Understanding Our Universe"

Stacy Palen, Laura Kay, Brad Smith, George Ray Blumenthal

2015 | W. W. Norton | ISBN: 9780393936315

[8] "Copperhead Road"

Brad Smith

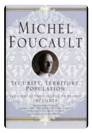
2022 | At Bay Press | ISBN: 9781988168708

Literatura pokrewna (Google Scholar):

[9] "The Essence of Human Freedom"

Martin Heidegger

2002 | Burns & Oates



[10] "Security, Territory, Population"

Michel Foucault

2007 | Palgrave MacMillan | ISBN: 9781403986528

[11] "Mortality and Morality"

Hans Jonas

1996 | Northwestern University Press | ISBN: 9780810112858

[12] "The rational and social Foundations of music"

Max Weber

ISBN: 9780758136602

[13] "Obfuscation"

Helen Nissenbaum

MIT Press | ISBN: 9780262331326

[14] "The question concerning technology and other essays"

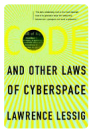
Martin Heidegger

Facsimiles-Garl

[15] "Schelling's Treatise on the Essence of Human Freedom"

Martin Heidegger

1985 | ISBN: 9780821406908



[16] "Code and Other Laws of Cyberspace"

Lawrence Lessig

Basic Books | ISBN: 9780465039135

[17] "The Future of Ideas"

Lawrence Lessig

Vintage | ISBN: 9781400033317

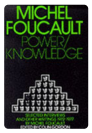
[18] "Michel Foucault, an Interview : Sex, Power and the Politics of Identity"

Michel Foucault

[19] "Power"

Michel Foucault

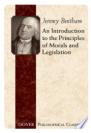
2019 | Penguin UK | ISBN: 9780141991375



[20] "Power/knowledge"

Michel Foucault

1980 | Longman | ISBN: 9780710800718



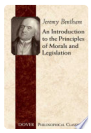
[21] "Introduction to the Principles of Morals and Legislation"

Jeremy Bentham

Courier Corporation | ISBN: 9780486120423

[22] "A Protest against Law-Taxes"

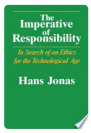
Jeremy Bentham



[23] "An Introduction to the Principles of Morals and Legislation"

Jeremy Bentham

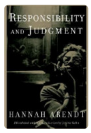
Courier Corporation | ISBN: 9780486120423



[24] "The Imperative of Responsibility"

Hans Jonas

1984 | University of Chicago Press | ISBN: 9780226405971



[25] "Responsibility and Judgment"

Hannah Arendt

2003 | Schocken

[26] "The Human Condition"

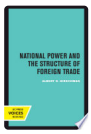
Hannah Arendt

1958 | Wattpad | ISBN: 9780226586748

[27] "Condition de l'homme moderne - Nouvelle édition 2018"

Hannah Arendt

2018 | Calmann-Lévy | ISBN: 9782702167212



[28] "National Power and the Structure of Foreign Trade"

Albert Hirschman

2024 | Univ of California Press | ISBN: 9780520378179

[29] "Linear Algebra for Data Science with Python"

Divya Kumar

2026 | Educohack Press | ISBN: 9789361529870

Artykuły naukowe

Autorzy przywoływani:

[1] "KNOWLEDGE AND POLITICS IN INTERNATIONAL LAW"

David Kennedy, F. Bacon

2018

Google Scholar

[2] "Tools and Weapons"

Brad Smith, Carol Ann Browne

2019

Google Scholar

[3] "Making sense of big business"

John Browne

2006 | Business Strategy Review | DOI: 10.1111/j.0955-6419.2006.00419.x

Google Scholar

[4] "Book review: Meaning, Subjectivity, Society – Making Sense of Modernity"

Craig Browne

2013 | Thesis Eleven | DOI: 10.1177/0725513612459939

Google Scholar

[5] "ESSAYS OR COUNSELS CIVIL AND MORAL"

Francis Bacon

2011 | Cambridge University Press eBooks | DOI: 10.1017/cbo9781139149594.021

Google Scholar

[6] "Fuel cells, past, present and future"

Francis Bacon

1969 | Electrochimica Acta | DOI: 10.1016/0013-4686(69)87042-8

Google Scholar

[7] "gion, knowledge, and power in the England of his day and to encourage his ideals of natural philosophy and governance.1 In the late eighteenth century, the British social reformer and philosopher"

F. Bacon, J. Bentham, Robert L. Fishman, Le Corbusier

2017

Google Scholar

[8] **"The finite future: Martin Heidegger"**

Martin Heidegger

2011 | Time and Philosophy | DOI: 10.1017/upo9781844652778.008

Google Scholar

[9] **"Code and Other Laws of Cyberspace"**

Lawrence Lessig

1999 | Medical Entomology and Zoology

Google Scholar

[10] **"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

Google Scholar

[11] **"Remix: making art and commerce thrive in the hybrid economy"**

Lawrence Lessig

2009 | Choice Reviews Online | DOI: 10.5860/choice.46-5102

Google Scholar

[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

Google Scholar

[13] **"Power/Knowledge: Selected Interviews and Other Writings 1972-1977"**

Michel Foucault, Colin Gordon

1980

Google Scholar

[14] **"The Order of Things: An Archaeology of the Human Sciences."**

Francesca Moore, Michel Foucault

1971 | Man | DOI: 10.2307/2799252

Google Scholar

[15] **"The Subject and Power"**

Michel Foucault

1982 | Critical Inquiry | DOI: 10.1086/448181

Google Scholar

[16] **"Archaeology of Knowledge"**

Michel Foucault

1970 | Social Science Information | DOI: 10.1177/053901847000900108

Google Scholar

[17] **"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

Google Scholar

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

Hans Jonas

1985 | DigitalGeorgetown (Georgetown University Library)

Google Scholar

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

Daniel Sommer Robinson, Hans Jonas

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

Google Scholar

[20] **"Philosophical Reflections on Experimenting with Human Subjects"**

Hans Jonas

1979 | DOI: 10.1007/978-1-4615-6561-1_16

Google Scholar

[21] **"The Rational and Social Foundations of Music"**

Robert W. Lundin, Max Weber, Don Martindale, Johannes Riedel, Gertrude Neuwirth

1960 | Journal of Music Theory | DOI: 10.2307/843058

Google Scholar

[22] **"CHARISMATIC POLITICS AND THE SYMBOLIC FOUNDATIONS OF POWER"**

Max Weber

2008 | Democracy and the Politics of the Extraordinary | DOI: 10.1017/cbo9780511755842.002

Google Scholar

[23] "The Technical Fix: Education, Computers and Industry"

John Wilkes, Keith Robins, Frank Webster

1990 | British Journal of Educational Studies | DOI: 10.2307/3121208

Google Scholar

[24] "An analytic behavior model for disk drives with readahead caches and request reordering"

Elizabeth Shriver, Arif Merchant, John Wilkes

1998 | ACM SIGMETRICS Performance Evaluation Review | DOI: 10.1145/277858.277906

Google Scholar

[25] "The HP AutoRAID hierarchical storage system"

John Wilkes, Richard A. Golding, Carl Staelin, T. J. Sullivan

1995 | ACM SIGOPS Operating Systems Review | DOI: 10.1145/224057.224065

Google Scholar

[26] "Against the Law: Countering Lawful Abuses of Digital Surveillance"

Edward Snowden, bunnie Huang

2016 | PubPub | DOI: 10.21428/12268

Google Scholar

[27] "Look away: The revelations of Edward Snowden have confirmed just how much surveillance the state undertakes"

Edward Snowden

2014 | Australian rationalist

Google Scholar

[28] "Continental Illinois National Bank v. Washington: does the contract clause mandate the completion of nuclear power plants at all costs"

Edward Snowden

1984 | OSTI OAI (U.S. Department of Energy Office of Scientific and Technical Information)

Google Scholar

[29] "The Human Condition"

Hannah Arendt, Margaret Canovan, Danielle Allen

1998 | DOI: 10.7208/chicago/9780226586748.001.0001

Google Scholar

[30] **"Between past and future eight exercises in political thought"**

Hannah Arendt

1987

Google Scholar

[31] **"Lectures on Kant's Political Philosophy"**

Hannah Arendt, Ronald S. Beiner

1982 | DOI: 10.7208/chicago/9780226231785.001.0001

Google Scholar

[32] **"Between Past and Future."**

Judith N. Shklar, Hannah Arendt

1963 | History and Theory | DOI: 10.2307/2504107

Google Scholar

Artykuły pokrewne (Google Scholar):

[33] **"CMS Innovation Center at 10 Years — Progress and Lessons Learned"**

Brad Smith

2021 | New England Journal of Medicine | DOI: 10.1056/nejmsb2031138

Google Scholar

[34] **"Implications of Integrity Management Regulations on a Provincially Regulated Pipeline Operator"**

Brad Smith

2006 | Volume 1: Project Management; Design and Construction; Environmental Issues; GIS/Database Development; Innovative Projects and Emerging Issues; Operations and Maintenance; Pipelining in Northern Environments; Standards and Regulations | DOI: 10.1115/ipc2006-10183

Google Scholar

[35] **"Stemming the rising tide of anger in the workplace: how to build emotion control among employees before anger spills out"**

Brad Smith

2022 | Strategic HR Review | DOI: 10.1108/shr-01-2022-0001

Google Scholar

[36] **"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

Google Scholar

[37] "The protective power of hope and belonging in the workplace"

Brad Smith

2024 | Strategic HR Review | DOI: 10.1108/shr-07-2024-0054

Google Scholar

[38] "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

Google Scholar

[39] "Letters to the editor"

Brad Smith

1972 | ACM SIGMIS Database: the DATABASE for Advances in Information Systems | DOI: 10.1145/2579434.2579438

Google Scholar

[40] "ARM and Intel Battle over the Mobile Chip's Future"

Brad Smith

2008 | Computer | DOI: 10.1109/mc.2008.142

Google Scholar

[41] "Using and Evaluating Resampling Simulations in SPSS and Excel"

Brad Smith

2003 | Teaching Sociology | DOI: 10.2307/3211325

Google Scholar

[42] "U.S. forest resource facts and historical trends"

W. Brad Smith, David R. Darr

2004

Google Scholar

[43] "Forest Resources of the United States, 2002"

W. Brad Smith, Patrick D. Miles, John S. Vissage, Scott A. Pugh

2004 | DOI: 10.2737/nc-gtr-241

Google Scholar

[44] **"Forest Resources of the United States, 2017: a technical document supporting the Forest Service 2020 RPA Assessment"**

Sonja N. Oswalt, W. Brad Smith, Patrick D. Miles, Scott A. Pugh

2019 | DOI: 10.2737/wo-gtr-97

Google Scholar

[45] **"Forest inventory and analysis: a national inventory and monitoring program"**

W. Brad Smith

2002 | Environmental Pollution | DOI: 10.1016/s0269-7491(01)00255-x

Google Scholar

[46] **"Forest Resources of the United States, 2012: a technical document supporting the Forest Service 2010 update of the RPA Assessment"**

Sonja N. Oswalt, W. Brad Smith, Patrick D. Miles, Scott A. Pugh

2014 | DOI: 10.2737/wo-gtr-91

Google Scholar

[47] **"Forest Resources of the United States, 2007"**

W. Brad Smith, Patrick D. Miles, Charles H. Perry, Scott A. Pugh

2017 | DOI: 10.2737/wo-gtr-78

Google Scholar

[48] **"Forest Resources of the United States, 1997"**

W. Brad Smith, John S. Vissage, David R. Darr, Raymond M. Sheffield

2001 | DOI: 10.2737/nc-gtr-219

Google Scholar

[49] **"Allometric Biomass Equations for 98 Species of Herbs, Shrubs, and Small Trees"**

W. Brad Smith, Gary J. Brand

1983 | DOI: 10.2737/nc-rn-299

Google Scholar

Treść tworzy Fundacja Dobre Państwo.
Redaguje i publikuje APA ONE, autorski system redakcyjny Fundacji oparty na AI.
APA ONE Publishing System

Article ID: 239526cd-8e22-4277-8b40-670dcd8b98ec