NIE CZEKAJMY NA DOWODY, AŻ BĘDZIE ZA PÓŹNO.

Anatomia systemu, który może odebrać nam wolność

Kiedy roczne dziecko bawi się obok kominka, którego szyba ma 300 stopni, odpowiedzialny rodzic nie czeka na „dowód", że dziecko się poparzy. Widzi zagrożenie, przewiduje możliwy skutek i stawia zabezpieczenie. Dlaczego więc w przypadku państwa, technologii, danych i naszej wolności mielibyśmy zachowywać się inaczej?

To jest zasadniczy błąd współczesnej debaty.

Słyszymy:

„Nie ma dowodów, że system zostanie wykorzystany przeciwko ludziom".

Ale kiedy taki dowód się pojawi, może już nie być czego chronić.

Dane będą zgromadzone.

Systemy połączone.

Gotówka zmarginalizowana.

Tożsamość zdigitalizowana.

Firmy uzależnione od infrastruktury.

Obywatele sprofilowani.

Mechanizmy kontroli gotowe.

Prawo dostosowane.

I wtedy dyskusja o tym, czy należało wcześniej postawić zabezpieczenie, będzie miała wartość podobną do dyskusji prowadzonej po pożarze o tym, czy warto było kupić czujnik dymu.

Nie twierdzę: „wiem, że tak będzie"

Stawiam inne pytanie:

skoro technologia umożliwia stworzenie systemu kontroli, infrastruktura do niego powstaje, dane są gromadzone, a zakres cyfrowego nadzoru rośnie — czy

rozsądne jest zakładanie, że nigdy nie zostanie on wykorzystany przeciwko obywatelowi?

To nie jest pytanie spiskowe.

To jest **analiza ryzyka**.

W cyberbezpieczeństwie dokładnie tak przecież działamy.

Nie pytamy:

„Czy mamy dowód, że jutro zostaniemy zaatakowani?”.

Pytamy:

„Co się stanie, jeśli zostaniemy zaatakowani i czy jesteśmy na to przygotowani?”.

Tworzymy backup.

Segmentujemy sieć.

Wprowadzamy MFA.

Budujemy disaster recovery.

Nie dlatego, że znamy datę ataku.

Dlatego, że znamy **możliwość ataku oraz jego konsekwencje**.

Dlaczego wobec wolności całego społeczeństwa mielibyśmy stosować niższy standard bezpieczeństwa?

Biblia również nie mówi: czekajcie, aż zobaczycie dowód

Dla człowieka wierzącego istnieje jeszcze jeden wymiar tego problemu.

Chrześcijaństwo nie przedstawia historii świata jako procesu zmierzającego wyłącznie do coraz większej wygody, pokoju i technologicznego dobrobytu.

Chrystus ostrzega przed okresem wielkiego ucisku.

W Ewangelii Mateusza 24 znajdujemy zapowiedź ucisku o wyjątkowej skali oraz słowa mówiące, że gdyby ten czas nie został skrócony, zagrożone byłoby przetrwanie człowieka.

Apokalipsa przedstawia natomiast wizję systemu, w którym możliwość uczestniczenia w obrocie gospodarczym — **kupowania i sprzedawania** — zostaje powiązana z podporządkowaniem się określonemu porządkowi.

Przez dwa tysiące lat ludzie mogli pytać:

jak technicznie można byłoby kontrolować możliwość kupowania i sprzedawania milionów ludzi?

Dzisiaj pierwszy raz w historii odpowiedź nie wymaga właściwie żadnej fantazji.

Cyfrowa tożsamość.

Cyfrowe płatności.

Centralne rejestry.

AI.

Biometria.

Automatyczny scoring.

Analiza transakcji.

Algorytmiczna ocena ryzyka.

Systemy natychmiastowej wymiany informacji.

Technologia pozwalająca połączyć to wszystko w czasie rzeczywistym.

Nie oznacza to automatycznie, że każdy z tych systemów jest realizacją proroctwa.

Oznacza coś innego: po raz pierwszy istnieje technologiczna infrastruktura, dzięki której opisany w Biblii poziom kontroli ekonomicznej stał się technicznie możliwy.

I właśnie dlatego trzeba patrzeć kilka ruchów do przodu.

Jak może narodzić się ucisk?

Nie musi rozpocząć się od dyktatora.

Może rozpocząć się od czegoś znacznie bardziej przekonującego:

bezpieczeństwa.

Każdy kolejny element systemu będzie można racjonalnie uzasadnić.

Cyfrowa identyfikacja?

Żeby ograniczyć oszustwa.

Kontrola transakcji?

Żeby walczyć z praniem pieniędzy.

Ograniczenie anonimowych płatności?

Żeby walczyć z przestępczością.

Więcej danych o firmach?

Żeby ograniczyć wyłudzenia podatkowe.

Monitoring internetu?

Żeby chronić przed dezinformacją.

Profilowanie?

Żeby wykrywać zagrożenia.

AI analizująca zachowania?

Żeby administracja działała skuteczniej.

Każdy pojedynczy krok może wyglądać rozsądnie.

Niebezpieczeństwo ujawnia się dopiero wtedy, kiedy złożymy wszystkie elementy w jeden system.

To jak puzzle.

Jeden fragment niczego nie pokazuje.

Dopiero po ułożeniu kilkudziesięciu zaczynamy widzieć obraz.

ETAP 1. Oddajemy dane

To już się wydarzyło.

Przez dwadzieścia lat oddawaliśmy prywatność w zamian za:

wygodę,

szybkość,

darmowe usługi,

media społecznościowe,

mapy,

wyszukiwarki,

chmurę,

telefony,

płatności mobilne,

personalizację.

Powstała cyfrowa mapa człowieka.

System może wiedzieć nie tylko, kim jesteś.

Może wiedzieć:

gdzie byłeś,

co kupiłeś,

czego szukałeś,

z kim się kontaktowałeś,

jakie masz zainteresowania,

jakie problemy,

jakie poglądy,

jak wygląda twoja sytuacja ekonomiczna,

a coraz częściej również przewidywać, co prawdopodobnie zrobisz.

Dawna władza musiała człowieka obserwować.

Dzisiejszy człowiek sam nosi urządzenie obserwacyjne w kieszeni.

ETAP 2. Uzależniamy państwo od infrastruktury, której nie kontrolujemy

Tutaj pojawia się problem cyfrowej suwerenności.

Państwo może być formalnie niezależne, posiadać własny parlament, rząd, wojsko i granice, a jednocześnie być technologicznie zależne od systemów, których nie potrafi zastąpić.

Jeżeli administracja przez kilkanaście lat buduje swoje procesy wokół technologii kilku globalnych dostawców, powstaje **vendor lock-in**.

Przejście do konkurencji staje się:

droższe,

trudniejsze,

ryzykowne,

czasochłonne,

czasami praktycznie niewykonalne.

I wtedy nie trzeba nikomu kraść danych.

Wystarczy kontrolować technologię, bez której właściciel danych nie potrafi funkcjonować.

To subtelniejsza forma zależności.

I potencjalnie znacznie skuteczniejsza.

ETAP 3. Likwidujemy anonimowość ekonomiczną

Gotówka posiada jedną cechę, której system cyfrowy zasadniczo nie posiada.

Można kupić bochenek chleba bez stworzenia rekordu opisującego:

kto,

gdzie,

kiedy,

za ile,

od kogo.

Cyfrowa gospodarka tworzy ślad.

Im więcej gospodarki zostaje zdigitalizowane, tym dokładniejszy obraz aktywności ekonomicznej człowieka może powstać.

I ponownie:

sama cyfrowa płatność nie jest uciskiem.

Ale infrastruktura pozwalająca identyfikować, analizować, klasyfikować i potencjalnie ograniczać transakcje jest warunkiem stworzenia systemu ekonomicznej kontroli.

Kominek jeszcze nie poparzył dziecka.

Ale szyba jest już gorąca.

ETAP 4. Prawo staje się coraz trudniejsze do spełnienia

Tutaj pojawia się drugi mechanizm.

Nie trzeba uczynić człowieka przestępcą poprzez zakazanie jego istnienia.

Można stworzyć taki poziom regulacji, aby praktycznie każdy człowiek i każda firma znajdowali się nieustannie w ryzyku niezgodności.

Podatki.

RODO.

AML.

Cybersecurity.

AI.

Raportowanie.

Regulacje sektorowe.

ESG.

Prawo pracy.

Ochrona konsumenta.

Obowiązki dokumentacyjne.

Każdy przepis może mieć racjonalne uzasadnienie.

Ale suma regulacji powoduje coś, czego nie wolno ignorować.

Koszt pozostania „idealnie zgodnym” staje się coraz wyższy.

Globalna korporacja zatrudni:

prawników,

doradców podatkowych,

compliance officerów,

specjalistów bezpieczeństwa,

audytorów,

zespoły regulatory affairs.

Mała firma nie ma takich zasobów.

Co robi?

Popełnia błędy.

Nie nadąża.

Rezygnuje.

Wchodzi w szarą strefę.

Albo zostaje przejęta przez większego gracza.

W efekcie regulacje, nawet stworzone z dobrymi intencjami, mogą prowadzić do **koncentracji rynku**.

ETAP 5. Każdy ma coś na sumieniu

I tutaj system osiąga niezwykle niebezpieczny punkt.

Im więcej obowiązków, regulacji i cyfrowych śladów, tym większe prawdopodobieństwo, że prawie każdy gdzieś popełnił błąd.

Nieprawidłowa deklaracja.

Spóźniony dokument.

Błędnie zakwalifikowana transakcja.

Nieświadome naruszenie procedury.

Nieaktualna polityka.

Błąd pracownika.

Nieprawidłowo przetworzone dane.

A jeżeli system potrafi analizować wszystko automatycznie?

Wtedy teoretycznie można znaleźć naruszenie niemal u każdego.

I to właśnie jest potencjalny „bat”.

Najpotężniejszy system kontroli nie polega na karaniu wszystkich.

Polega na tym, że **wszystkich można ukarać**.

Władza zaczyna się wtedy od selekcji:

kogo sprawdzamy,

kogo nie,

komu odpuszczamy,

a przeciwko komu wykorzystujemy pełną moc regulacji.

ETAP 6. Powstają obywatele różnych kategorii

Kiedy mamy dane oraz AI, naturalną konsekwencją jest scoring.

Już dzisiaj scoring istnieje w ogromnej części gospodarki.

Banki oceniają ryzyko.

Ubezpieczyciele oceniają ryzyko.

Platformy wykrywają fraud.

Instytucje finansowe analizują transakcje.

Firmy analizują klientów.

Państwo również wykorzystuje algorytmy do selekcji przypadków wymagających kontroli.

Następny krok technologiczny jest oczywisty:

coraz dokładniejsza, automatyczna klasyfikacja człowieka.

Nie musi nazywać się:

„dobry obywatel” i „zły obywatel”.

To byłoby zbyt prymitywne.

Może nazywać się:

niski poziom ryzyka,

podwyższone ryzyko,

brak weryfikacji,

transakcja nietypowa,

konto wymagające dodatkowej kontroli,

podmiot wysokiego ryzyka,

treść potencjalnie szkodliwa.

Język będzie techniczny.

Neutralny.

Profesjonalny.

A konsekwencje mogą być jak najbardziej realne.

ETAP 7. Wolność zostaje zastąpiona dostępem warunkowym

To może być najważniejsza zmiana.

Dawny system mówił:

„Nie wolno ci”.

Nowoczesny system może powiedzieć:

„Nie spełniasz warunków”.

Różnica językowa ogromna.

Praktyczny skutek ten sam.

Nie musisz skonfiskować firmy.

Możesz odebrać jej możliwość uczestniczenia w określonym systemie.

Nie musisz zabraniać człowiekowi podróżowania.

Wystarczy, że nie przejdzie procedury.

Nie musisz zabraniać transakcji.

System może ją automatycznie odrzucić.

Nie potrzebujesz cenzora.

Algorytm może ograniczyć zasięg treści.

Nie potrzebujesz funkcjonariusza przed drzwiami.

Potrzebujesz systemu, który nie da autoryzacji.

I właśnie tak może wyglądać ucisk XXI wieku.

Po co miałby powstać taki system?

Nie trzeba zakładać jednego tajnego centrum dowodzenia.

Wystarczy zrozumieć interesy poszczególnych uczestników.

Państwo chce kontroli

Im więcej wie o gospodarce i obywatelu, tym skuteczniej może:

ściągać podatki,

egzekwować prawo,

walczyć z oszustwami,

przewidywać ryzyka,

zarządzać społeczeństwem.

Administracja chce danych

Bo dane dają mierzalność.

To, czego nie można zmierzyć, trudno kontrolować.

BigTech chce danych i uzależnienia

Dane są paliwem współczesnej gospodarki.

Im więcej klient ma usług jednego dostawcy, tym trudniej mu odejść.

Wielkie korporacje korzystają ze skomplikowanych regulacji

Ponieważ mają pieniądze na compliance.

Ich mniejsi konkurenci często nie mają.

Politycy chcą bezpieczeństwa

A społeczeństwo w sytuacji zagrożenia jest gotowe oddać część wolności w zamian za obietnicę bezpieczeństwa.

I tutaj znajduje się historycznie jeden z najbardziej niebezpiecznych mechanizmów:

rozwiązania wyjątkowe bardzo łatwo stają się rozwiązaniami permanentnymi.

A teraz wyobraźmy sobie kryzys

Wojna.

Pandemia.

Gigantyczny cyberatak.

Krach finansowy.

Seria zamachów.

Masowe zamieszki.

Poważne zagrożenie terrorystyczne.

Upadek systemu finansowego.

Nie wiemy, które z tych wydarzeń nastąpi.

Ale historia mówi nam, że kryzysy następują.

I wtedy państwo posiadające rozbudowaną infrastrukturę cyfrowej kontroli może usłyszeć:

„Musimy czasowo rozszerzyć jej zastosowanie”.

Dla bezpieczeństwa.

Na trzy miesiące.

Tylko na czas kryzysu.

Tylko wobec niebezpiecznych osób.

Tylko w szczególnych przypadkach.

I właśnie wtedy okaże się, czy wcześniej zbudowaliśmy bezpieczniki.

Bo technologia nie posiada sumienia.

Jeżeli można czegoś użyć do ochrony obywatela, często można wykorzystać tę samą infrastrukturę do jego kontroli.

I dlatego nie chcę czekać na dowód

Ktoś powie:

„To teoria spiskowa”.

Dobrze.

Potraktujmy ją więc jako **stress test demokracji**.

Załóżmy na chwilę najbardziej niebezpieczny scenariusz.

Wyobraźmy sobie, że za dziesięć lat władzę obejmuje człowiek, któremu absolutnie nie ufamy.

Co będzie miał do dyspozycji?

Jakie bazy danych?

Jaką wiedzę o obywatelach?

Jaką kontrolę nad płatnościami?

Jaką możliwość profilowania?

Jak bardzo scentralizowaną infrastrukturę?

Jak skuteczną AI?

Jak dużo informacji historycznych?

Jak łatwo będzie mógł połączyć wszystkie te systemy?

Demokracji nie projektuje się przecież dla dobrego władcy.

Projektuje się ją tak, aby również **zły władca nie dostał do ręki zbyt wielkiej mocy**.

To jest sedno sprawy.

W perspektywie biblijnej pytanie staje się jeszcze poważniejsze

Jeżeli Biblia rzeczywiście zapowiada okres wyjątkowego ucisku oraz system, w którym uczestnictwo gospodarcze może zostać uzależnione od podporządkowania, człowiek wierzący nie powinien pytać wyłącznie:

„Czy to już jest to?”.

Powinien zapytać:

„Czy budujemy właśnie infrastrukturę, która kiedyś pozwoli coś takiego zrobić?”

To ogromna różnica.

Nie twierdzimy, że:

cyfrowy dokument = znamię,

cyfrowe pieniądze = Apokalipsa,

AI = Antychryst,

konkretna instytucja = realizator proroctwa.

Takie uproszczenia byłyby nieuczciwe.

Pytamy natomiast:

czy po raz pierwszy w historii człowiek stworzył techniczne narzędzia umożliwiające globalną identyfikację, profilowanie i potencjalne kontrolowanie uczestnictwa w gospodarce?

Odpowiedź brzmi:

technologicznie — tak, jest to możliwe.

I to wystarczy, żeby wymagać zabezpieczeń **dzisiaj**, a nie wtedy, gdy ktoś już użyje tej infrastruktury przeciwko nam.

Co więc powinniśmy zrobić?

Nie niszczyć technologii.

Nie wracać do papieru.

Nie odrzucać AI.

Nie demonizować cyfryzacji.

Zrobić coś znacznie mądrzejszego:

budować technologię tak, aby nigdy nie mogła stać się narzędziem totalnej kontroli.

Potrzebujemy:

prawa do gotówki,

prawa do funkcjonowania offline w podstawowych sprawach,

minimalizacji zbieranych danych,

zakazu tworzenia uniwersalnego scoringu obywatela,

realnej kontroli człowieka nad automatycznymi decyzjami,

prawa do odwołania od decyzji algorytmu,

rozproszonej infrastruktury,

suwerenności technologicznej państwa,

możliwości zmiany dostawcy,

ochrony przed vendor lock-in,

transparentności algorytmów administracji,

silnego rozdzielenia baz danych,

zasady, że informacji zebranych w jednym celu nie wolno automatycznie używać w innym,

oraz systemu hamulców, którego żadna przyszła władza nie będzie mogła łatwo wyłączyć.

Bo pytanie nie brzmi:

„Czy ktoś już nas uciska?”

Pytanie brzmi:

„Czy tworzymy system, dzięki któremu kiedyś będzie można uciskać ludzi na skalę, której wcześniejsze pokolenia technologicznie nie były w stanie osiągnąć?”

I właśnie w tym miejscu powinna zapalić się czerwona lampka.

Nie wtedy, gdy zobaczymy pierwszy niepodważalny dowód nadużycia.

Nie wtedy, gdy komuś zostanie wyłączone konto.

Nie wtedy, gdy ktoś zostanie odcięty od systemu.

Nie wtedy, gdy algorytm zdecyduje, że jesteśmy niewłaściwymi obywatelami.

Wtedy może być już za późno.

Kominek zabezpiecza się **przed** tragedią.

System demokratyczny również.

Bo prawdziwa wolność nie polega na wierze, że obecna władza nigdy nie wykorzysta swoich narzędzi przeciwko człowiekowi.

Prawdziwa wolność polega na stworzeniu takiego systemu, żeby żadna przyszła władza nie miała takiej możliwości.

I o to właśnie trzeba walczyć teraz.

Nie ze strachu.

Z przezorności.