

O korzyściach i zagrożeniach z zastosowania nowych technologii w publicznych i obywatelskich inicjatywach antykorupcyjnych (część 2)

GRZEGORZ MAKOWSKI

Collegium Civitas

g_makowski@outlook.com

Promises and risks of using new technologies in public and civic anti-corruption initiatives (part 2)

DOI: 10.26368/17332265-048-4-2019-3

SŁOWA KLUCZOWE

korupcja, polityka
antykorupcyjna,
organizacje strażnicze,
nowe technologie

ABSTRAKT

W ostatnich kilku dekadach pole badań zarówno nad korupcją i polityką antykorupcyjną, jak i nad nowymi technologiami znacznie się rozszerzyło. Współcześnie korupcja to nie tylko łapówkarstwo czy w ogóle rodzaj przestępstwa, ale splot instytucji i innych czynników społecznych, który powoduje, że o dostępie do różnego rodzaju dóbr publicznych decydują partykularystyczne przesłanki (na przykład przynależność partyjna czy klanowa). Z drugiej strony nowe technologie informacyjne są coraz bardziej obecne w życiu publicznym. Istnieje wiele przesłanek, które pozwalają postawić hipotezę, że rozwój nowych technologii pomaga w ograniczeniu ryzyka korupcji. Jednocześnie to nowe technologie tworzą także nowe zagrożenia i nowe ryzyka, także nowe formy korupcji. W drugiej części artykułu przedstawiono przykłady konkretnych rozwiązań technologicznych – ich jasne i ciemne strony.

KEYWORDS

corruption,
anti-corruption
policy, watchdog
organisations,
new technologies

ABSTRACT

The past few decades have brought new depth and breadth of research in corruption/anti-corruption policy and in new technologies alike. As perceived today, corruption is not limited to simple bribery (or, for that matter, to a simple criminal offence), but also encompasses a conjunction of institutional and societal factors contributing to a state of affairs where access to sundry public resources is predicated upon party affiliation, clan membership etc. In an independent phenomenon, new technologies continue to permeate public life. There is much to support the hypothesis that technological development reduces the risk of corruption. On the other hand, new technologies themselves give rise to new risks, also by enabling new forms of corruption. This second part of the article presents examples of specific technological solutions, discussing their benefits and uses as well as their more ominous aspects.

W pierwszej części artykułu zakresiliśmy pole analizy i przedstawiliśmy hipotezy o tym, że – ogólnie rzecz biorąc – rozwój nowych technologii sprzyja ograniczeniu ryzyka korupcji i zaangażowaniu w inicjatywy antykorupcyjne. W drugiej części zaprezentujemy przykłady konkretnych rozwiązań technologicznych, które poddamy krytycznej analizie ich potencjału antykorupcyjnego.

Sztuczna inteligencja

Pod względem stopnia wykorzystania cyfrowych usług publicznych i e-administracji jako pozytywny przykład państwa – jednocześnie zaś społeczeństwa, które jest świadome posiadanych możliwości i aktywnie ich używa – wskazuje się Estonię. W kraju tym zasięg cyfryzacji funkcji państwa i wszelkiego rodzaju usług publicznych jest już legendarny. Estonia zdigitalizowała niemal wszystkie usługi publiczne, począwszy od tych najprostszych, jak podstawowe działania administracji państwowej (aplikowanie i wydawanie dokumentów), przez administrację podatkową, zarządzanie katastrzem, głosowanie w wyborach i referendach, kończąc na dostępie do szeroko rozumianej służby zdrowia (od e-recept czy elektronicznych zwolnień lekarskich po organizację pracy szpitali i innych placówek ochrony zdrowia). Konsekwentna digitalizacja funkcji państwa i otwieranie zasobów danych dla obywateli dały Estończykom ogromne możliwości bezpośredniego kontrolowania wszelkiego rodzaju aktywności instytucji publicznych, urzędników i polityków (Lember, Kattel, Tõnurist 2018).

Estonia nie uniknęła przy tym problemów, czego najlepszym przykładem był w 2007 roku atak DDOS (*distributed denial of service*) na estońskie serwery, przeprowadzony prawdopodobnie przez Rosję (Lesk 2007). Zdarzały się także wycieki danych osobowych z publicznych rejestrów. Jak dotąd trudności w tym zakresie nie były jednak na tyle poważne, żeby Estonia zrezygnowała z dalszej digitalizacji. Wprost przeciwnie – Estończycy nieustannie robią na tym polu postępy, rozwijając między innymi systemy bezpieczeństwa elektronicznego i instrumenty obrony, również przed atakami, które mogłyby stworzyć szeroko pojęte ryzyko korupcyjne (na przykład umożliwić wprowadzenie nielegalnych środków do systemu bankowego czy zakłócić proces wyborczy).

Jedną z najnowszych innowacji, której wprowadzenie rozważa estoński rząd, jest projekt sędziego robota (*robot-judge*) (Niiler 2019). O pracach nad tym systemem po raz pierwszy opowiedział magazynowi „Wired” Ott Velsberg, szef departamentu danych w estońskim Ministerstwie Gospodarki. Sędzia robot ma być algorytmem (sztuczną inteligencją) zdolnym do wydawania wyroków w nieskomplikowanych, typowych – jak na estońskie warunki – sprawach, w których wartość szkody nie przekracza 7 tysięcy euro. Analizowałby on i porównywał akta spraw, a następnie podejmował decyzje, które mogłyby być ewentualnie kontrolowane przez zwykłych sędziów. Estoński rząd liczy, że wprowadzenie systemu odciąży sądownictwo i pozwoli sędziom ludziom bardziej wydajnie zajmować się sprawami, z którymi sztuczna inteligencja póki co nie byłaby w stanie sobie poradzić.

Na kanwie estońskiego przykładu warto od razu zwrócić uwagę na wyzwanie, które pojawia się dla państwa obywateli. Wspomniane rozwiązanie teoretycznie może pomóc usprawnić funkcjonowanie sądownictwa, może również spowodować, że system będzie mniej narażony na korupcję, bardziej

transparentny i racjonalny. Być może obywatele zyskają dzięki temu łatwiejszy dostęp do wymiaru sprawiedliwości, a państwo zaoszczędzi miliony euro. Jednocześnie uruchomienie takiego systemu jak sędzia robot to nie tylko wyzwanie technologiczne, ale także ideologiczne i etyczne. Nie ma bowiem systemu technologicznego bez wartości.

Powstaje zatem na przykład pytanie o to, czy system taki będzie działać zgodnie z zasadami demokratycznego państwa prawa, które gwarantuje każdemu równość wobec prawa i prawo do sprawiedliwego sądu. Być może bowiem taki system okaże się dyskryminujący, ograniczający dostęp do sprawiedliwego wyroku, a zatem bardziej partykularystyczny i przez to podatny na korupcję. To zresztą pytanie, które można sformułować w nawiązaniu zarówno do sędziego robota, jak i do wszelkich innych zautomatyzowanych rozwiązań, które pojawiają się w relacjach państwo – obywatel. Czy takie systemy można zaprojektować tak, żeby zbliżały nas do uniwersalistycznego postulatu równości w dostępie do różnego rodzaju dóbr i usług publicznych, a więc takiego działania państwa, które będzie sprzyjało ograniczaniu pola korupcji? Czy takie systemy można ochronić przed manipulacją? Czy jesteśmy w stanie dostarczać takim systemom danych wystarczająco dobrej jakości, żeby mogły wydawać decyzje zgodne ze standardami demokratycznego państwa prawa, uczyć się, rozwijać i budować zaufanie do instytucji publicznych?

Na konferencji Banku Światowego w Ankarze, obradującej 11 i 12 czerwca 2019 roku pod hasłem „Europe and Central Asia Regional Conference Building Effective, Accountable, and Inclusive Institutions”, przedstawiciel estońskiego rządu opisywał między innymi sędziego robota. W ramach panelu wywiązała się interesująca dyskusja, w której także miałem okazję uczestniczyć. Jeden z uczestników debaty, profesor Alan R. Shark, zwrócił uwagę na jakość danych wejściowych do systemów opierających się na sztucznej inteligencji jako niezbędnego warunku ich poprawnego funkcjonowania. Dane bowiem, czyli w tym wypadku na przykład zgłoszenia o popełnieniu przestępstwa, protokoły przesłuchań, decyzje o kwalifikacji czynów, są – i jeszcze długo będą – tworzone przez ludzi, ci zaś są podani na typowo ludzkie błędy i pokusy, na przykład korupcyjne (przyjęcie korzyści w zamian za lepszą kwalifikację czynu). Jeśli dane wprowadzane do systemu będą wadliwe, to wadliwe będą nie tylko konkretne wyroki, ale także – jeśli tego rodzaju danych będzie więcej – cały system może być „zatruty” błędnymi danymi. To z kolei oznaczałoby poważny kryzys z punktu widzenia standardów państwa prawa i obniżenie zdolności do przeciwdziałania korupcji.

Żeby lepiej zobrazować ryzyko, profesor Alan R. Shark wspomniał historię projektu „Watson for oncology”, który niegdyś uruchomił IBM (Froomkin, Kerr, Pineau 2018). Postanowiłem bliżej przyjrzeć się temu przedsięwzięciu. Celem projektu było stworzenie samouczącego się algorytmu, który mógłby

wesprzeć, a może nawet zastąpić, radiologów przy diagnostyce raka. Po kilku latach okazało się jednak, że system diagnozował raka niewłaściwie, a główną przyczyną była właśnie zła jakość danych wejściowych. Algorytm nie był w stanie wykrywać ludzkich błędów i samemu nauczyć się ich nie popełniać. Koncern IBM nigdy oficjalnie nie przyznał się do porażki (Chorey 2019), ale środowiska medyczne po opisaniu wad w funkcjonowaniu projektu są do niego zdystansowane, tym bardziej że zdarzyły się zgony po kontrowersyjnych diagnozach stawianych przez system.

Podobnie „skorumpowane” mogą się okazać algorytmy stosowane w sektorze publicznym. Z jednej strony mogą usprawnić działanie państwa, sprawić, że będzie ono bardziej transparentne i odporne na różne formy korupcji. Albo takie będziemy odnosić wrażenie. Z drugiej jednak strony ich uruchomienie nie powinno usypiać czujności obywatelskiej. Mogą one bowiem być jednocześnie narzędziem w ręku obywateli, którym zależy na poprawie jakości życia publicznego, jak i czymś, co będzie wymagało monitoringu i reagowania, gdyby się okazało, że działają wadliwie.

Kończąc ten wątek, warto wspomnieć, że koncern IBM nie bardzo chciał się podzielić danymi o wadliwym funkcjonowaniu projektu „Watson for oncology”. Niewygodne fakty wyszły na jaw, gdy anonimowy sygnalista ujawnił tajne raporty ukazujące błędy w działaniu algorytmu (Palmer 2018). Historia ta pokazuje więc, że rozwiązania technologiczne – tak w medycynie, jak i w życiu publicznym – nie rozwiążą „dylematu strażnika”. Ktoś musi pilnować pilnującego, nawet jeśli ten jest robotem (a może nawet tym bardziej). Ostateczną instancją wciąż pozostanie aktywny, zainteresowany obywatel.

Mimo wszystko przykład Estonii jest inspirujący, choćby dlatego, że jest to jedyny kraj z grona państw byłego bloku wschodniego, który zbliżył się pod względem percepcji korupcji do zachodnich krajów wysoko rozwiniętych. W edycji indeksu percepcji korupcji Transparency International za 2018 rok Estonia zajęła osiemnaste miejsce, jako jedyne państwo byłego bloku sowieckiego zbliżając się do najlepiej ocenianych państw zachodnich (www.transparency.org).

Pozostając w kręgu rozważań o e-usługach, e-administracji i sztucznej inteligencji jako czynnikach, przynajmniej potencjalnie, pozytywnie wpływających na możliwości przeciwdziałania korupcji i mobilizowania do tego obywateli, zatrzymajmy się jeszcze na chwilę przy sztucznej inteligencji właśnie. Rozwój e-usług i e-administracji jako elementów skutecznej polityki antykorupcyjnej jest dość dobrze opisany (jak na ogólnie skromny zasób badań z tego zakresu i literatury przedmiotu). Z kolei rozważania o tym, w jakim stopniu sztuczna inteligencja może być takim czynnikiem, są już nieco bardziej teoretyczne lub opierają się na dość wycinkowych analizach i studiach przypadku. Żeby jednak nie pozostawiać czytelników wyłącznie z budzącą

pewne kontrowersje historią estońskich sędziów robotów, wspomnijmy, że istnieją także ciekawe przykłady zastosowania sztucznej inteligencji w polityce antykorupcyjnej.

Na hiszpańskim uniwersytecie w Valladolid opracowano algorytm tłumaczący i pozwalający przewidywać ryzyko wystąpienia korupcji w zależności od zmian w podatkach od nieruchomości, cen nieruchomości, poziomu wzrostu gospodarczego w poszczególnych prowincjach, poziomu oszczędności firm prywatnych i okresu sprawowania władzy przez dane stronnictwa polityczne. W ten sposób powstała dynamiczna mapa korupcji w Hiszpanii, która może być narzędziem mobilizującym obywateli do czujniejszego patrzenia lokalnym władzom na ręce (López-Iturriaga, Sanz 2017). Póki co jednak badania nad zastosowaniem sztucznej inteligencji w polityce antykorupcyjnej są w powijkach.

Blockchain

Nieco więcej z punktu widzenia przeciwdziałania korupcji wiemy o innej technologii, jaką jest blockchain. Ujmując rzecz w wielkim skrócie, blockchain to rodzaj rozproszonej bazy danych działającej na podobnej zasadzie jak sieci wymiany plików *peer-to-peer*, w której każdy użytkownik jest w posiadaniu pełnej kopii danych. Wszystkie informacje (na przykład o transakcjach) są przekazywane, weryfikowane i zapisywane w blokach danych u każdego użytkownika. Dzięki temu nie ma możliwości ich niepostrzeżonej zmiany, nielegalnego przejęcia czy usunięcia, tak jak to się dzieje w tradycyjnych, scentralizowanych bazach danych, które są umieszczane na konkretnym komputerze. Teoretycznie więc nie istnieje możliwość unicestwienia bazy danych opierającej się na technologii blockchain. Tradycyjne bazy danych można z kolei zaatakować, włamując się do centralnego komputera, zmieniając informacje lub je niszczyć, podobnie jak nieliczne kopie danych przechowywane na innych komputerach (Natarajan, Krause, Gradstein 2017; Williams-Elegbe 2018; Aliyev, Safarov 2019; de Souza, Luciano, Wiedenhöft 2018). Jaki to wszystko ma jednak związek korupcją i polityką antykorupcyjną?

Na początek dobre wiadomości. Z punktu widzenia problematyki, którą się tu zajmujemy, główną zaletą technologii blockchain jest to, że przynajmniej potencjalnie opierające się na niej rozwiązania gwarantują dużą transparentność i dostępność dla obywatela. Na przykład w administracji publicznej pojawia się coraz więcej rozwiązań opartych na systemach blockchain, jak elektroniczny obieg dokumentów, systemy monitorowania transakcji i wydatków publicznych, rejestry podmiotów gospodarczych i ich działalności, a nawet katastry, platformy przetargowe czy systemy głosowania elektronicznego (Kshetri 2017). Przykładów zastosowania tej technologii w celu poprawy zarządzania różnego rodzaju procesami w szeroko pojętej sferze publicznej można by podać

bez liku. Poprzestanę na jednym, który jest o tyle interesujący, że łączy wiele współczesnych problemów – od migracji przez korupcję aż po kwestię zarządzania publicznymi zasobami.

W 2017 roku World Food Program uruchomił system dystrybucji voucherów na żywność w jordańskich obozach dla uchodźców z Syrii. Uczyniono tak dlatego, że tradycyjne sposoby rozdziału żywności szybko były korumpowane przez kliki tworzące się w przeludnionych obozach. System opiera się na wykorzystaniu biometrycznych danych uchodźców – skanów siatkówki oka. Dzięki temu bez żadnego dokumentu czy gotówki mogą oni otrzymać dzienny przydział żywności. W ten sposób w niespełna rok World Food Program rozdyskrybuował blisko półtora miliona voucherów w społeczności liczącej ponad 10 tysięcy uchodźców. Obniżono znacznie koszty administracyjne przy jednoczesnym ograniczeniu nadużyć związanych z przejmowaniem przydziałów żywności przez obozowe mafie. W 2018 roku system rozszerzono na populację ponad 100 tysięcy uchodźców (Wong 2017). Po tym doświadczeniu Organizacja Narodów Zjednoczonych rozważa zastosowanie podobnych technologii do dystrybucji wszelkiego rodzaju pomocy rzeczowej przekazywanej państwom i grupom potrzebującym. Szacuje się bowiem, że blisko jedna trzecia zasobów redystrybuowanych przez Organizację Narodów Zjednoczonych jest tracona w wyniku korupcji i malwersacji (<https://breakermag.com>).

Przykład zastosowania technologii blockchain przez Organizację Narodów Zjednoczonych w programach pomocowych jest o tyle interesujący, że mógłby się okazać inspiracją dla wielu organizacji pozarządowych realizujących podobne działania. Liczne podmioty o zasięgu globalnym, takie jak Oxfam czy Czerwony Krzyż, dysponują ogromnymi środkami zarówno publicznymi, jak i pochodzącymi od prywatnych darczyńców. Niejednokrotnie także dotyczyły je skandale korupcyjne związane z malwersacjami pieniędzy i zasobów rzeczowych przeznaczanych na projekty pomocowe (www.lawliberty.org). Stosując podobne rozwiązania jak testowane przez Organizację Narodów Zjednoczonych, z pewnością można by obniżyć ryzyko kolejnych nadużyć i skandali. Przykład ten pokazuje więc, że nowe technologie mogą być nie tylko narzędziem w rękach zarówno instytucji publicznych, jak i organizacji społecznych służącym do kontrolowania władzy i przeciwdziałania korupcji, ale także same organizacje społeczne, które również są narażone na nadużycia, mogą i powinny zastanowić się nad wykorzystaniem ich w celu poprawy własnego funkcjonowania.

Blockchain nie jest jednak pozbawiony wad. Ciemna strona tej technologii wiąże się przede wszystkim z rozwojem kryptowalut, dla których jest ona podstawą. Kryptowaluty są już problemem całkiem dobrze rozpoznanym w literaturze i badaniach (Dodd 2017). Same w sobie nie są kontrowersyjne, a przez wielu są nawet postrzegane jako nowy bastion swobód obywatelskich

i rynkowych. Jednocześnie istnieje już wiele przesłanek, wskazujących, że kryptowaluty są bardzo umiejętnie wykorzystywane do ukrywania środków pochodzących z przestępstw i prania brudnych pieniędzy (Campbell-Verduyn 2018). Praktyki te są zaś współcześnie kwalifikowane jako korupcja. Przy czym kontrolowanie przepływu środków pochodzących z przestępstw przez kryptowaluty paradoksalnie nie jest wcale łatwe, mimo że opierają się one przecież na technologii blockchain, która ma gwarantować transparentność (interesujący raport na ten temat zamówił w 2018 roku Parlament Europejski: *Cryptocurrencies and blockchain* – por. www.europarl.europa.eu). Dlatego coraz więcej państw decyduje się na jakąś formę regulacji i kontroli obrotu kryptowalutą.

Jednocześnie jest wciąż niewiele organizacji społecznych, które mają potencjał pozwalający na monitorowanie, analizowanie i rekomendowanie działań zapobiegających wykorzystywaniu kryptowalut w celach przestępczych. Jedną z takich organizacji o światowym zasięgu jest Global Financial Integrity działająca w Stanach Zjednoczonych. Od niedawna zajmuje się ona także problematyką kryptowalut (Iorio 2019). Jest to jednak działanie wymagające nie tylko sporych zasobów, ale także wysokich kompetencji i współpracy między specjalistami z zakresu technologii, finansów i korupcji. Jeśli jednak antykorupcyjne działania obywatelskie miałyby się rozwijać i podejmować wyzwania związane z pojawieniem się nowych technologii, to jest to z pewnością jeden z najważniejszych obszarów, jakimi należałoby się zająć.

Big data, crowdsourcing i sygnaliści

Zmierzając ku końcowi przeglądu technologicznych innowacji, które z jednej strony tworzą nowe możliwości przeciwdziałania korupcji, z drugiej zaś strony same generują nowe zagrożenia i wyzwania, wspomnę o mniej kontrowersyjnych rozwiązaniach, które stają się coraz bardziej popularne. Są one tworzone nie tylko przez instytucje publiczne (czasem przez podmioty prywatne), żeby poprawić zarządzanie oraz ograniczyć ryzyka nadużyć i usprawnić zarządzanie, ale także przez organizacje społeczne, a nawet indywidualnych obywateli (na przykład w ramach hackatonów), i czasem skutecznie wykorzystywane do monitorowania czy przeciwdziałania korupcji oraz przenoszenia problemu korupcji do debaty publicznej.

Oprócz różnego rodzaju rozwiązań, które mieszczą się w szerokim pojęciu e-administracji czy e-usług publicznych, w ostatnich latach coraz więcej innowacji w zakresie przeciwdziałania korupcji i mobilizowania obywateli do zaangażowania na tym polu wykorzystuje duże zbiory danych (*big data*), platformy crowdsourcingowe i systemy dla sygnalistów.

Zwłaszcza duże zbiory danych cieszą się coraz większą i rosnącą popularnością. Jest to naturalna konsekwencja rozwoju Internetu i digitalizacji funkcji

państwa – od administracji publicznej po usługi społeczne. Z jednej strony państwo gromadzi coraz więcej danych o obywatelach i osobach prawnych. Z drugiej strony następuje szybki rozwój kultury dostępu do informacji publicznej i nowych rozwiązań w zakresie udostępniania danych. Chodzi przede wszystkim o tak zwane otwarte formaty danych, których prosta i jednolita forma umożliwiła szybką, maszynową analizę ogromnych zbiorów. A programy do wykonywania takich analiz mogą przygotować nie tylko agendy państwowe czy firmy prywatne, ale także sami obywatele.

Mamy więc do czynienia z rosnącym zasobem informacji, który pozostaje w dużym stopniu w gestii państwa, ale który jest jednocześnie coraz bardziej dostępny obywatelom. Dlatego od lat obserwujemy rozwój rządowych systemów takich jak ARACHNE. To specjalna platforma stworzona przez Komisję Europejską, gromadząca ogromne ilości danych o wydatkowaniu funduszy unijnych oraz powiązaniach gospodarczych i personalnych osób i firm korzystających z finansowania unijnego lub starających się o projekty unijne. Jest ona dostępna wyłącznie rządowi państw członkowskich i służy szacowaniu ryzyka nadużyć przy wydatkowaniu funduszy strukturalnych (Makowski 2017). Z kolei ze strony obywatelskiej warto wspomnieć o europejskim projekcie DIGIWHIST (<http://digiwhist.eu>). To interesujące przedsięwzięcie, dzięki któremu opracowano narzędzia *online* pozwalające na monitorowanie informacji o zamówieniach publicznych we wszystkich państwach członkowskich Unii Europejskiej oraz w kilku państwach stowarzyszonych. Choć realizacja projektu zakończyła się w 2018 roku, jego dorobek jest dostępny i możliwy do wykorzystania na zasadzie otwartych licencji. Na bazie doświadczeń DIGIWHIST powstał na przykład Barometr Ryzyka Nadużyć w zamówieniach publicznych (<http://barometrryzyka.pl>), wspólny projekt Fundacji im. Stefana Batorego i serwisu Zamówienia 2.0. Jest to narzędzie *online*, które na bieżąco ocenia rozstrzygnięcia przetargów i ogłoszenia o przetargach, wskazując miejsca, które mogą być źródłem nieprawidłowości (na przykład zbyt krótkie terminy podjęcia decyzji o wyborze wykonawcy). Za jego pomocą można także zbiorczo analizować zachowania konkretnych zamawiających i wykonawców w blisko dziesięcioletniej perspektywie (baza zawiera ponad 7 milionów rekordów z lat 2010–2019). Dlatego Barometr Ryzyka Nadużyć może służyć nie tylko obywatelom, organizacjom społecznym czy mediom jako narzędzie monitorowania konkretnych przetargów, ale także jako instrument pozwalający na analizę procedur przetargowych dla konkretnych instytucji, dostarczając informacje pozwalające na reformę i poprawę przejrzystości oraz efektywności przetargów (Makowski 2018).

Oczywiście masowa analiza różnego rodzaju danych dostępnych w coraz większej skali daje wiele innych możliwości, na przykład śledzenia korupcji wyborczej, analizowania oświadczeń majątkowych czy wykrywania procederu

prania brudnych pieniędzy (www.oecd-forum.org). Trudno byłoby w tym miejscu omówić je choćby skrótowo. Dość powiedzieć, że *big data* zapewnia nie tylko rządowi, ale przede wszystkim obywatelom ogromne możliwości włączania się w działania antykorupcyjne. Dalej jednak jest potrzebny człowiek (obywatel) i pomysł na to, co i jak zrobić – dane same z siebie nie pomogą ograniczyć korupcji (przegląd wielu interesujących inicjatyw obywatelskich – por. <https://transparencee.org>).

Warto wspomnieć jeszcze o dwóch typach innowacji technologicznych znajdujących zastosowanie w działaniach antykorupcyjnych. Pierwsza to tak zwane platformy crowdsourcingowe, które co do idei działają podobnie jak narzędzia crowdfundingowe, tyle że zamiast do gromadzenia pieniędzy od indywidualnych darczyńców służą do gromadzenia informacji od indywidualnych informatorów. Są to rozwiązania służące przede wszystkim do zgłaszania drobnej korupcji, uświadamiania problemu i mobilizowania społeczeństwa do działań antykorupcyjnych na szerszą skalę. Najlepiej znaną tego rodzaju platformą jest *I Paid A Bribe* uruchomiona w Indiach (<http://www.ipaidabribe.com>). Ta prosta aplikacja internetowa pozwala każdemu anonimowo zgłosić sytuację choćby oczekiwania łapówki ze strony funkcjonariusza publicznego. W samych Indiach od momentu uruchomienia pierwszej wersji aplikacji w 2010 roku zgłoszono blisko 185 tysięcy przypadków korupcji. Aplikacja pozwala także poinformować, że obywatel został dobrze i uczciwie potraktowany przez funkcjonariusza publicznego. Dane gromadzone dzięki *I Paid A Bribe* pozwalają szacować, w jakim regionie, jakiej miejscowości czy instytucji publicznej ryzyko korupcji jest największe. Nawet jeśli nie wszystkie zgłaszane zdarzenia się potwierdzają, jest to ważna informacja, która może być punktem wyjścia reform. Podobne systemy z inicjatywy organizacji społecznych czy instytucji państwowych działają dziś w ponad dwudziestu państwach. Rozwiązania crowdsourcingowe pomagające w walce z korupcją są również uruchamiane specyficznie dla konkretnych sektorów życia publicznego. W Ugandzie na przykład istniała niegdyś specjalna platforma *Not In My Country*, stworzona specjalnie do informowania o korupcji na uczelniach wyższych (niestety, po kilku latach funkcjonowania została zamknięta).

E-narzędzia sygnalizowania są w zasadzie podobne do platform crowdsourcingowych, tyle że są budowane najczęściej na potrzeby konkretnych organizacji czy instytucji. Zwykle są również częścią całych systemów zarządzania etycznego w organizacjach i służą zdobywaniu informacji o poważniejszych przejawach korupcji. Dane z takich narzędzi są później wykorzystywane w organizacjach do zmian w systemach zarządzania i ograniczaniu ryzyka w przyszłości. Jest to także rynek, który współcześnie jest mocno skomercjalizowany. Istnieje wiele specjalnych, często licencjonowanych pakietów oprogramowania (na przykład *GlobalLeaks* czy *BKMS*), które firmy lub instytucje publiczne

mogą wykupić i samodzielnie dostosować do swoich potrzeb. Często oprogramowanie pozwalające na anonimowe zgłoszenia przejawów korupcji w organizacjach, komunikację z sygnalistami i zarządzanie informacjami jest jedynie interfejsem, za których stoją całe zespoły prawników i specjalistów od zarządzania ryzykiem. Jest to interesujący przykład innowacji, którego źródłem są inicjatywy obywatelskie, a który został jakby zapomniany i w dużym stopniu urynkowiony.

Odnosząc się do tego skrótowego przeglądu innowacji technologicznych, które mogą wspomóc państwo i obywatele w działaniach antykorupcyjnych, w podsumowaniu warto wskazać kilka kwestii. Przede wszystkim, z czysto akademickiego punktu widzenia, w wypadku związku między rozwojem technologii informacyjnych i korupcją (jej skalą i zdolnością społeczeństw oraz państw do przeciwstawiania się temu zjawisku) mamy do czynienia z polem badawczym, które wciąż jeszcze jest słabo zagospodarowane. Dysponujemy ogólnymi, ale dość wycinkowymi i powierzchownymi analizami, pozwalającymi ocenić, że rozwój technologii informacyjno-komunikacyjnych sprzyja ograniczaniu korupcji. Dzięki nim możemy także potwierdzić dość oczywistą intuicję, że sama infrastruktura (rozwiązania technologiczne) nie powoduje, że zagrożenie korupcją jest mniejsze czy że zdolności do reagowania i zapobiegania temu problemowi są większe. Obywatele muszą wiedzieć o tych technologiach, muszą umieć i chcieć ich używać. Krótko mówiąc – infrastruktura technologiczna nie pomoże w walce z korupcją bez informacji i edukacji. Obszar ten jednak wymaga się zainteresowania badaczy. Potrzeba nam więcej danych empirycznych, przede wszystkim badań ilościowych, pozwalających ocenić wpływ rozwiązań technologicznych na jakość życia publicznego. Nie zawsze bowiem wpływ ten jest jednoznaczny. Żeby ocenić, czy dane rozwiązania rzeczywiście mają potencjał antykorupcyjny, warto na nie spojrzeć z perspektywy dychotomii uniwersalizm – partykularyzm i sprawdzić, czy biorąc pod uwagę wszystkie ich wady i zalety, można uznać, że przyczyniają się one do równiejszego dostępu do różnych dóbr publicznych, czy przeciwnie – mogą się okazać narzędziem realizacji partykularystycznych interesów.

Mamy jednak już wystarczająco dużo wiedzy o tym, jak działają innowacje technologiczne, żeby stwierdzić, że nie są one złotym środkiem na korupcję i że same także tworzą nowe problemy, jak technologia blockchain czy sztuczna inteligencja. To oznacza także nowe wyzwania – dla państwa i dla organizacji społecznych. Wyzwaniem nie jest tylko tworzenie nowych rozwiązań pomagających w walce z korupcją, informowanie o nich i uczenie, jak ich używać. Pojawia się także potrzeba uczenia się, jak radzić sobie z nowymi problemami, takim jak wykorzystywanie nowych technologii do popełniania

starych przestępstw (ukrywania majątków pochodzących z nielegalnych źródeł czy prania brudnych pieniędzy). Nie lada wyzwaniem dla obywateli jest monitorowanie tego, jak nowe technologie tworzone z myślą o poprawie życia publicznego i przeciwdziałania korupcji powstają i jak są wykorzystywane. Na tej płaszczyźnie bowiem paradoksalnie pojawia się nowe pole do nadużyć – przede wszystkim ze strony państwa wobec obywateli. „Dobre”, antykorupcyjne technologie łatwo zmienić w „złe” rozwiązania, służące na przykład inwigilacji. Co być może ważniejsze – nowe technologie mogą wywoływać nowe nierówności (na przykład w dostępie do usług publicznych czy w dostępie do określonych dóbr, choćby wymiaru sprawiedliwości). Mogą one powstawać intencjonalnie, ponieważ systemy będą tworzone tak, żeby automatycznie dyskryminować tę czy inną grupę społeczną, lub w wyniku błędów i nadmiernego optymizmu co do technologicznych możliwości rozwiązywania problemów społecznych. Nierówności zaś to podglebie partykularyzmów i korupcji. Zadaniem przede wszystkim organizacji społecznych jest więc monitorowanie tego, jak są tworzone i wdrażane innowacje.

Nowe technologie informacyjne nie są złotym środkiem na korupcję, ale z pewnością tworzą nowe możliwości. Parafrazując angielskie powiedzenie – *there are no silver bullets, but windows of opportunities*. Czy państwo i obywatele zdołają je wykorzystać z pożytkiem dla jakości życia publicznego? To zależy od tego, czy będziemy wiedzieć, jak tych technologii używać i jak bardzo będziemy chętni, żeby to robić. Aktywności obywatelskiej nie zastąpi póki co żadna nowa technologia.

BIBLIOGRAFIA

- Adam, Isabelle, Fazekas, Mihály. 2018. Are emerging technologies helping win the fight against corruption in developing countries?. *P4PCommission Background Paper*, 21.
- Aliyev, Ziya, Safarov, Igbal. 2019. *Logos, Mythos And Ethos Of Blockchain: An Integrated Framework For Anti-Corruption*. 2019 OECD Global Anti-Corruption Conference, 20–21 marca 2019 roku, Paryż.
- Andersen, Thomas B. 2009. E-government as an anti-corruption strategy. *Information Economics and Policy*, 21(3): 201–210.
- Campbell-Verduyn, Malcom. 2018. Bitcoin, crypto-coins, and global anti-money laundering governance. *Crime Law and Social Change*, 69(2): 283–305.
- de Souza, Rodrigo C., Luciano, Edimara M., Wiedenhöft Guilherme C. 2018. *The uses of the Blockchain Smart Contracts to reduce the levels of corruption: Some preliminary thoughts*. Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age, art. 110.
- Dodd, Nigel. 2017. The social life of Bitcoin. *Theory, Culture & Society*, 35(3): 35–56.
- Froomkin, Michael A., Kerr Ian R., Pineau Joelle. 2019. When AIs Outperform Doctors: The dangers of a tort-induced over-reliance on machine learning and what (not) to do about it. *University of Miami Legal Studies Research Paper*, 18–3.
- Huntington, Samuel P. 1968. *Modernization and corruption. Political order in Changing Societies*, [w:] Arnold J. Heidenheimer, Michael Johnston, Victor T. LeVine (red.), *Political Corruption. A Handbook*. New Haven: Yale University Press
- Klitgaard, Robert. 1988. *Controlling Corruption*, Berkley: University of California Press.

- Krastev, Ivan. 2004. The Anti-American Century?. *Journal of Democracy*, 15(2): 5–17.
- Kshetri, Nir. 2017 Will blockchain emerge as a tool to break the poverty chain in the Global South?. *Third World Quarterly*, 38(8): 1710–1732.
- LaFree, Gary, Morris, Nancy. 2003. *Corruption as a Global Social Problem*, [w:] George Ritzer, *Handbook of Social Problems. A Comparative International Perspective*. London: Sage, s. 600–618
- Leff, Nathaniel. 1964. Economic Development Through Bureaucratic Corruption. *American Behavioral Scientist* 8(3): 8–14.
- Lember, Veiko, Kattel, Rainer, Tõnurist, Piret. 2018. Technological capacity in the public sector: the case of Estonia. *International Review of Administrative Sciences*, 84(2): 214–230.
- Lesk, Mihael. 2007. The new front line: Estonia under cyber assault. *IEEE Security & Privacy*, 5(4): 76–79.
- Lui, Francis T. 1996. Three Aspects of Corruption. *Contemporary Economic Policy*, 14(3): 26–29.
- Makowski, Grzegorz. 2008. *Korupcja jako problem społeczny*. Warszawa: Trio.
- Makowski, Grzegorz. 2017. *From Weber to the Web... Can ICT Reduce Bureaucratic Corruption?*, [w:] Alois A. Paulin, Leonidas G. Anthopoulos, Christopher G. Reddick, *Beyond Bureaucracy. Towards Sustainable Governance Informatisation*. Cham: Springer.
- Makowski, Grzegorz. 2018. Postępowania jędoofertowe jako wskaźnik ryzyka korupcji w zamówieniach publicznych, *Zarządzanie Publiczne*, 4(40): 525–550.
- Mungiu-Pippidi, Alina. 2013. The Good, the Bad and the Ugly: Controlling Corruption in the European Union. *European Research Centre for Anti-corruption and State-building Working Paper*, 35.
- Mungiu-Pippidi, Alina (red.). 2011. *Contextual Choices in Fighting Corruption: Lesson Learned*. Berlin: Hertie School of Governance.
- Pavarala, Vinod. 1996. *Interpreting Corruption: Elite Perspectives in India*. London: Sage.

ŹRÓDŁA INTERNETOWE

- Chorev, Michal. 2019. *AI Models Predict Breast Cancer with Radiologist-Level Accuracy*, <https://www.ibm.com/blogs/research/2019/06/ai-models-radiologist-level-accuracy> [dostęp: 23 czerwca 2019 roku].
- Iorio, Ben. 2019. *Cryptocurrency and the rise of new illicit financial flows*, <https://gfintegrity.org/cryptocurrency-and-the-rise-of-new-illicit-financial-flows> [dostęp: 23 czerwca 2019 roku].
- Kossow, Niklas, Dykes, Victoria. 2018. *Embracing Digitalisation: How to use ICT to strengthen Anti-Corruption*, <https://www.giz.de/de/downloads/giz2018-eng ICT-to-strengthen-Anti-Corruption.pdf> [dostęp: 23 czerwca 2019 roku].
- Lopez-Iturriaga, Felix J., Pastor-Sanz, Iván. 2017, *Predicting Public Corruption with Neural Networks: An Analysis of Spanish Provinces*. Social Indicators Research, <http://dx.doi.org/10.2139/ssrn.3075828> [dostęp: 23 czerwca 2019 roku].
- Natarajan, Harish, Krause, Solvej Karla, Gradstein, Helen Luskin. 2017. *Distributed Ledger Technology (DLT) and Blockchain Acknowledgments*, <http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf> [dostęp: 23 czerwca 2019 roku].
- Niiler, Eric. 2019. *Can AI be a fair judge in court? Estonia thinks so*, <https://arstechnica.com/tech-policy/2019/03/can-ai-be-a-fair-judge-in-court-estonia-thinks-so/?comments=1&post=37107331> [dostęp: 23 czerwca 2019 roku].
- Palmer, Annie. 2018. *IBM's Watson AI suggested 'often inaccurate' and 'unsafe' treatment recommendations for cancer patients, internal documents show*, <https://www.dailymail.co.uk/sciencetech/article-6001141/IBMs-Watson-suggested-inaccurate-unsafe-treatment-recommendations-cancer-patients.html> [dostęp: 23 czerwca 2019 roku].
- Williams-Elegbe, Sope. 2018. *Public Procurement, Corruption and Blockchain Technology: A Preliminary (Legal) Inquiry*. Wykład inauguracyjny 25 października 2018 roku, Department of Mercantile Law Faculty of Law, Stellenbosch University, <https://www.youtube.com/watch?v=GU39i05WB4U> [dostęp: 23 czerwc 2019 roku].

Wong, Joon I. 2017. *The UN is Using Ethereum's Technology to Fund Food for Thousands of Refugees*, <https://qz.com/1118743/world-food-programmes-ethereum-based-blockchain-for-syrian-refugees-in-jordan> [dostęp: 23 czerwca 2019 roku].