

## MATERIAŁY, INFORMACJE, ROZMOWY

Dominika Janus

### **Między siłą a informacją. Zarządzanie Internetem, cyberbezpieczeństwo i nowe technologie w Chinach po XIX zjeździe KPCh**

Niniejszy artykuł jest poświęcony wybranym aspektom obecnej cyberpolityki Chin i chińskiej innowacji technologicznej. Jest to próba scharakteryzowania ewolucji chińskiego podejścia do zarządzania Internetem i informacją w kontekście XIX zjazdu Komunistycznej Partii Chin oraz reform cyberbezpieczeństwa do 2018 r. W artykule podjęta zostanie również próba nakreślenia implikacji nowej polityki cyfrowej i informacyjnej dla odbioru Chin na świecie.

Do 2017 r. działania w cyberprzestrzeni pozwalały władzom Chińskiej Republiki Ludowej osiągnąć dwa cele: wewnętrzny, czyli kontrolę przepływu informacji w Internecie w celu ochrony interesu politycznego, i zewnętrzny, czyli realizację interesów gospodarczych. Xi Jinping sformułował dwa „cele na stulecie”: pierwszy, do 1 lipca 2021 r., jest związany ze stuleciem istnienia KPCh, natomiast drugi odnosi się do stulecia powstania ChRL – 1 października 2049 r., kiedy to Chiny mają osiągnąć *zhonghua minzu weida fuxing*, czyli „wielki renesans narodu chińskiego”. Pierwszym kamieniem milowym miało być stworzenie społeczeństwa umiarkowanego dobrobytu, *xiaokang shehui*. Zgodnie z tą koncepcją motorem napędowym chińskiej gospodarki byłyby silna klasa średnia i rozbudowany rynek wewnętrzny, co doprowadziłoby do zmiany charakteru chińskiej gospodarki: z produktów niskiej jakości na nowoczesne technologie.

24 października 2017 KPCh zakończyła XIX zjazd – w czasie trwającej tydzień sesji Xi Jinping potwierdził swoje przywództwo i skonsolidował władzę. Zjazd rzucił światło na podejście kierownictwa partii do gospodarki cyfrowej i budowania cyberpotęgi Chin. Pekin planował nie tylko wprowadzenie wysublimowanego zarządzania informacją – ambicje objęły rozwój obszaru AI (sztucznej inteligencji)

i doktryny wojskowej. Deklaracje polityczne, które padły na XIX zjeździe, jasno wskazały, że rozwój technologii informacyjno-komunikacyjnych znajduje się wśród nowych priorytetów na kolejną kadencję Xi Jinpinga, a osiągnięcie statusu globalnego lidera innowacji do 2035 r. jest strategicznym celem Chin.

### **Zarządzanie Internetem w Chinach**

Od lat 90. XX w. Internet był postrzegany jako samorządna przestrzeń bez granic, w dużej mierze poza władzą państwa. Jego gwałtowna ekspansja wywołała liczne kontrowersje, skłaniając polityków do rozpoczęcia debaty na temat zarządzania Internetem „z chińską charakterystyką”. Chińscy przywódcy nadal zmagają się z formułowaniem i reformowaniem ram prawnych dla cyberbezpieczeństwa. Do najistotniejszych kwestii należą: zdefiniowanie krytycznej infrastruktury informacyjnej, regulacja przepływu i zarządzanie „transgranicznymi” danymi oraz ustalenie relacji między chińskimi i międzynarodowymi standardami.

Chińska konceptualizacja prawa w cyberprzestrzeni jest jednym z najgorętszych zagadnień polityki i stosunków międzynarodowych w ostatnich latach, podobnie jak dyplomacja cyfrowa między Waszyngtonem i Pekinem – reprezentującymi diametralnie różne modele zarządzania. Chiny są powszechnie postrzegane jako mające ograniczoną zdolność do zapewniania alternatywnych norm w globalnej cyberprzestrzeni. Zmieniający się kształt chińskiej polityki internetowej, której idee często nie są klarowne dla zachodnich obserwatorów, powoduje brak zaufania do nowych koncepcji (takich jak wspomniana suwerenność Internetu). Co więcej, chińska administracja jest znana z prób wdrażania kontrowersyjnych – z zachodniego punktu widzenia – aspektów prawa dotyczącego przepływu danych. ChRL wykorzystuje bowiem cyberprzestrzeń do globalnej promocji swojej koncepcji suwerenności, stanowczo sprzeciwiając się „cyfrowej hegemonii”, czyli dominacji Stanów Zjednoczonych w zarządzaniu siecią, sankcjonuje prawo państw do kontroli przepływu treści w Internecie.

### **XIX zjazd partii: rezultaty**

Podczas XIX Zjazdu podkreślano, że cyberbezpieczeństwo jest integralną częścią bezpieczeństwa narodowego, a bez informatyzacji nie będzie szans na modernizację chińskiego społeczeństwa – zagrożenia, jak również możliwości zapoczątkowane w cyberprzestrzeni coraz częściej przenikały do obszarów polityki, gospodarki, kultury i życia społecznego. Konsolidacja władzy (w osobie Xi

Jinpinga) miała zdecydowanie przyspieszyć wdrażanie zmian do polityki cyfrowej i sfinalizowanie niedokończonych projektów, takich jak zabezpieczenie krytycznej infrastruktury informacyjnej.

Technologia stała się kluczową częścią wizji Xi Jinpinga na jego drugą kadencję. Po raz pierwszy przemówienie otwierające zjazd identyfikowało specyficzne terminy, takie jak sztuczna inteligencja (AI) i cyfrowe Chiny jako priorytety w planach rozwoju kraju. Po XIX zjeździe, praca partii i służby cywilnej miała się skupić na następujących czterech obszarach:

1. Ulepszenia i innowacje w obszarze pozytywnej propagandy online,
2. Wzmocnienie fundamentów w cyberbezpieczeństwie,
3. Wzmocnienie ochrony bezpieczeństwa krytycznej infrastruktury informacyjnej
4. Promowanie pogłębienia rozwoju integracji wojskowej i cywilnej na rzecz bezpieczeństwa cybernetycznego i informatyzacji.

Nowa perspektywa na chińską dominację technologiczną nakreślona przez Xi Jinpinga zakładała między innymi, że zależność świata online i offline może być pokazana jako koncentryczne kręgi. Dzięki takiej konceptualizacji kierownictwo KPCh będzie mogło dotrzeć również do globalnej społeczności i wypromować chińskie rozwiązania technologiczne. Idea ta początkowo odniosła spektakularne rezultaty (dominacja Huawei na rynku 5G, DJI wśród firm produkujących UAVs, czy TikTok pośród aplikacji).

## 2017: nowe regulacje

Należy pamiętać, że mimo różnic kulturowych, w Chinach cyberbezpieczeństwo postrzegane jest nie inaczej niż w innych regionach: jako ochrona Internetu przed szkodliwymi działaniami, które mogą wpłynąć na interesy handlowe i społeczne. Jest to niewątpliwie jeden z powodów, dla których rząd chiński jest bardziej skłonny do szybkich reakcji i bezzwłocznego wprowadzania nowych standardów prawnych – również dla firm operujących tylko w Internecie lub korzystających z wyłącznie z nowych technologii<sup>1</sup>.

Cyberbezpieczeństwo jest postrzegane jako problem ponadnarodowy ze względu na anonimowość, multidyscyplinarność i multiagencyjność, współlistnienie sprzętu i oprogramowania. Mając na uwadze potencjalne spowolnienie lub paraliż infrastruktury cybernetycznej, rozpowszechnianie informacji (w tym obrazów)

<sup>1</sup> Catherine Su, *China Doubles Down on Real-name Registration Laws, Forbidding Anonymous Online Posts*, 27 sierpnia 2018, <https://techcrunch.com/2017/08/27/china-doubles-down-on-real-name-registration-laws-forbidding-anonymous-online-posts/> [dostęp 25 maja 2018].

szkodliwych dla zachowania obecnego kształtu ustroju, społeczeństwa lub gospodarki, zarządzanie Internetem w 2017 wykroczyło poza tradycyjne wyzwania legislacyjne. Dodatkowo, KPCh musiała myśleć o utrzymaniu planowanego tempa rozwoju, przyspieszeniu innowacyjności względem konkurujących państw, zagadnieniach związanych z prywatnością, jak również o współpracy polityków z sektorem informatycznym i inżynierami.

XIX zjazd nakreślił nowe zagrożenia bezpieczeństwa kraju: cyberprzestępczość (*cyber-enabled crime*) i *hacking*, propagandę internetową oraz luki w systemach wojskowych. Aby skuteczniej szerzyć ideę „suwerenności internetowej”, jak również swoją wizję Internetu i cyberbezpieczeństwa, w narracji związanej z regulacjami z 2017 r. Pekin skorzystał na kontrowersjach wokół roli fałszywych wiadomości rozpowszechnianych w mediach społecznościowych (dezinformacji) w czasie wyborów prezydenckich w Stanach Zjednoczonych<sup>2</sup>. W obliczu negatywnego wizerunku zachodnich rozwiązań dotyczących bezpieczeństwa cyfrowego, w marcu 2017 r. Pekin zaproponował „chińskie rozwiązanie” dla globalnego zarządzania danymi. To rozwiązanie zostało nakreślone w pierwszym dokumencie strategicznym opisującym wizję sieci, w której poszczególne kraje kontrolują informacje przepływające przez ich granice<sup>3</sup>. W 2018 r. koncepcja ta była już w fazie operacyjnej – promowanie „suwerenności Internetu” było rozumiane jako normatywna pozycja Chin w cyberprzestrzeni. XIX zjazd reprezentował więc chińskie podejście do ewolucji do cyberpotęgi, wskazując na dążenie do (przynajmniej) dorównania Stanom Zjednoczonym.

## Prawne aspekty cyberbezpieczeństwa

W czerwcu 2017 r. rozpoczęto wprowadzanie wielopoziomowego systemu ochrony sieci<sup>4</sup>. Nowe ramy prawne połączyły trzy obszary: cyberbezpieczeństwo *per se*, gospodarkę cyfrową i *big data*, jak również moderowanie treści online w sposób, którego żaden inny kraj nie chciał lub nie był w stanie do tej pory zaimplementować. Nowy system prawny był kompleksowy i dotyczył wszystkich

<sup>2</sup> Patrick Greenfield, *The Cambridge Analytica Files: The Story So Far*, 26 marca 2018, <https://www.theguardian.com/news/2018/mar/26/the-cambridge-analytica-files-the-story-so-far> [dostęp 25 maja 2018].

<sup>3</sup> Jack Wagner, *China's Cybersecurity Law: What You Need to Know*, „The Diplomat”, 1 czerwca 2017, <https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/> [dostęp 25 maja 2018].

<sup>4</sup> Davis Wright Tremaine, *The Chinese Government Issues Draft Cybersecurity Regulations to Protect Critical Information Infrastructure*, <https://www.lexology.com/library/detail.aspx?g=d36a5919-cb3a-4bad-bbec-1686b04eae27> [dostęp 25 maja 2018].

dostępnych interakcji online: od forów przez czaty po komentarze. Przepisy wprowadzone w 2017 wymagały między innymi rejestracji tożsamości online pod prawdziwym imieniem. Internauci mogli w dalszym ciągu wybrać nazwę ekranową lub wyglądać anonimowo, ale ich prawdziwe dane osobowe zaczęły być przechowywane w Ministerstwie Bezpieczeństwa Publicznego. Zwolennicy nowych ram prawnych twierdzili jednocześnie, że dane są bezpieczniejsze w ministerstwie niż na platformach prywatnych firm<sup>5</sup>.

Chińskie władze są niezwykle efektywne we wprowadzaniu rozwiązań dotyczących prywatności i przechowywania danych w sieci. Jest to związane zarówno z wydarzeniami dotyczącymi bezprawnego udostępniania danych na Zachodzie<sup>6</sup> oraz z faktem, że Chiny starają się pokazać spektakularny postęp w zakresie nowego prawa, odwracając uwagę Chińczyków od bardziej złożonych, kontrowersyjnych kwestii, takich jak zabezpieczenie krytycznej infrastruktury informacyjnej<sup>7</sup>. Działania te do 2018 r. były częścią wysiłków podejmowanych przez administrację Xi Jinpinga w celu wzmocnienia istniejącego systemu cyberbezpieczeństwa i rozszerzenia ram prawnych w obszarze kontroli danych, sieci i treści. Model zarządzania Internetem forsowany przez KPCh spowodował, że przestrzeń anonimowości w Internecie ulega erozji, a dane zebrane z „cyfrowych tożsamości” zasilają rozległy rządowy system punktowy, tzw. System Wiarygodności Społecznej (*shehui xinyong xitong*).

Xi Jinping nie pojawił się na Światowej Konferencji Internetu<sup>8</sup>, która odbyła się w Wuzhen 3–5 grudnia 2017 r., a więc już po XIX zjeździe, co nie dziwi, patrząc na status, jaki osiągnął w czasie zjazdu. Wydał jednak list, w którym znajdują się stwierdzenia podkreślające, że ChRL nie ma zamiaru odcinać się od światowego Internetu. Zapewnił również, że „rozwój cyberprzestrzeni w ChRL wchodzi na przyspieszoną ścieżkę [...]. Chińskie drzwi będą się otwierać coraz bardziej”<sup>9</sup>, ale kluczem pozostaje kwestia suwerenności. Rząd uważnie obserwuje podejście innych krajów do prywatności w sieci. Niemniej jednak konieczność zachowania pełnej kontroli nad Internetem przez władze pozostaje priorytetem. Chodzi zarówno o moderację wypowiedzi chińskich internautów, jak i reglamentację dostawców

<sup>5</sup> J. Wagner, *China's Cybersecurity Law...*

<sup>6</sup> P. Greenfield, *The Cambridge Analytica...*

<sup>7</sup> Jing de Jong-Chen, Bobby O'Brien, *A Comparative Study: The Approach to Critical Infrastructure Protection in the U.S., E.U., and China*, 14 listopada 2017, <https://www.wilsoncenter.org/publication/comparative-study-the-approach-to-critical-infrastructure-protection-the-us-eu-and-china> [dostęp 25 maja 2018].

<sup>8</sup> <http://www.wuzhenwic.org/>.

<sup>9</sup> Lam Yan Liang, *China Continues to Push for its Vision of the Internet*, 3 grudnia 2017, <https://www.straitstimes.com/asia/east-asia/xi-jinping-says-china-will-not-close-door-to-global-internet-but-insists-on-cyber> [dostęp 31 sierpnia 2020].

wszelkich usług internetowych oraz rolę Internetu w masowym programie kontroli behawioralnej obywateli – wspomnianym Systemie Wiarygodności Społecznej. Należy dodać że Czwarta Światowa Konferencja Internetu była istotna z komercyjnej perspektywy: zachęciła do przyjazdu do Wuzhen nie tylko szefów największych spółek internetowych ChRL – Alibaby, Tencent czy Baidu, ale przede wszystkim reprezentantów gigantów technologicznych z Zachodu reprezentujących Apple, Google czy Wikipedię, mimo że większość zachodnich serwisów była w ChRL zablokowana, co niewątpliwie wskazywało na to, jak ważnym rynkiem stały się Chiny.

### **Wewnętrzna regulacja Internetu**

Wracając do kwestii regulacji z 2017 r., co porusza Zachód najbardziej w kontekście cyberbezpieczeństwa w Chinach, to oczywiście cenzura. Podczas gdy Chiny są domem dla największej liczby użytkowników Internetu na świecie, raport amerykańskiego think tanku Freedom House z 2015 r. wskazał, że mają one najbardziej restrykcyjne strategie korzystania z Internetu spośród 65 badanych krajów<sup>10</sup>.

Różne formy cenzury internetowej, zwane łącznie The Great Firewall (wielką zaporą ogniową, *fanghuo changcheng*), to w rzeczywistości system kontroli reprezentowany przez dwa główne filary – „Wielką Zaporę” i „Złotą Tarczę”. Powstawały one stopniowo przez wiele lat, a wiara w ich skuteczność jest w dużej mierze zakorzeniona w obawach, że niekontrolowane dyskusje online dotyczące drażliwych tematów mogą przekształcić się w powszechne niezadowolenie, w końcu zaś w zagrożenie dla porządku publicznego poza siecią. Chiny oczywiście nie są odosobnione we wprowadzaniu takich rozwiązań, jednak efektywność i kompleksowość chińskich rozwiązań jest gigantyczna.

W obliczu zmagania wielu państw z problemem dezinformacji propaganda internetowa w kontekście dostępu obywateli do treści propagowanych przez kraje zachodnie, które mają wprowadzać ich w stan niewiedzy, wydaje się nabierać nieco innego niż dotychczas znaczenia. Kontrola Internetu w Chinach przechodzi trzy fazy: automatycznego i ręcznego blokowania treści, filtrowania treści znajdujących się w sieciach Chin na podstawie międzynarodowych umów z operatorami i dostawcami Internetu oraz model, który łączy w sobie oba poprzednie rozwiązania z samocenzurą obywateli, którzy są nagradzani za ujawnianie nielegalnych treści w Internecie. Strony www, które zostały skonstruowane, aby omijać zautomatyzowane formy filtrowania, są wyszukiwane przez „cyberpolicję”, czyli – w 2018 r.

<sup>10</sup> Sanja Kelly, Madeline Earp, Laura Reed, Adrian Shahbaz, Mai Truong, *Freedom on the Net. Privatizing Censorship, Eroding Privacy*, Freedom House, październik 2015, [https://freedomhouse.org/sites/default/files/FH\\_FOTN\\_2015Report.pdf](https://freedomhouse.org/sites/default/files/FH_FOTN_2015Report.pdf) [dostęp 8 maja 2018].

– około 30 tys. zatrudnionych przez Ministerstwo Bezpieczeństwa Publicznego pracowników, którzy ręcznie przeczesują sieć w poszukiwaniu nielegalnych treści.

Osiągnięcie pełnej kontroli nad siecią w ten sposób nigdy nie będzie możliwe, co wynika między innymi z różnorodnych postaw reprezentowanych przez obywateli. Problem z fałszywymi wiadomościami, które rozpowszechniają się w sieci, jest jednak bardzo poważny i realny. Centrum Przeciwko Zagranicznym Fałszywym Pogłoskom (*fan haiwai yaoyan zhongxin*) ujawniło kolekcje wyedytowanych zdjęć, których używano do ilustracji nieprawdziwych informacji w tzw. *self-media* (*zi me-iti*)<sup>11</sup>. Termin ten odnosi się do niezależnie zarządzanych kont mediów społecznościowych – na platformach takich jak WeChat czy Weibo – i zwykle uruchamianych przez indywidualnych użytkowników. Nie są to jednak kanały informacyjne.

### System wiarygodności społecznej

Rząd centralny, wprowadzając pilotażowy System Wiarygodności Społecznej, promował go jako odpowiednik zachodnich systemów wiarygodności kredytowej. Miał on za zadanie przyznawać obywatelom punkty za odpowiednią postawę i zachowanie, co miało wpływać też na faktyczną zdolność kredytową. Narracja partii na 2018 r. była wątpliwa: dłużnicy stanowili ledwie 10% osób na czarnej liście SWS. Faktycznie natomiast osoby, które dokonały drobnych wykroczeń lub wdały się w spór z lokalną administracją, miały ograniczone możliwości wyjazdów zagranicznych czy kupna krajowych biletów kolejowych 1. klasy. SWS wpływał również na stopień dopasowania w aplikacjach randkowych. Punkty były odejmowane za publikowanie w mediach społecznościowych negatywnych komentarzy dotyczących władzy. Warto zauważyć, że SWS objął także przedsiębiorstwa, gdzie władze wykorzystywały początkowo ponad 30 różnych projektów śledzących informacje podatkowe, raporty bezpieczeństwa pracy, poziom zaangażowania w ochronę środowiska czy wyniki inspekcji sanitarnych.

System Wiarygodności Społecznej od początku został okrzyknięty sukcesem, choć władze były świadome, że wprowadzone rozwiązania nie są bez wad: w związku z ogromną ilością danych przechowywanych w jednym miejscu udany cyberatak lub nieuczciwy pracownik rządowej agencji mogą pograżyć najlepsze nawet przedsiębiorstwo. Co więcej, atrakcyjność systemu punktowego może zachęcić przestępców do ogłaszania na czarnym rynku usług zwiększających ranking SWS.

---

<sup>11</sup> Ivy Yu, *How 'Self-media' in China has Become a Hub for Misinformation*, [online] SupChina, 27 marca 2018, <https://supchina.com/2018/03/27/how-self-media-in-china-has-become-a-hub-for-misinformation/> [dostęp 25 sierpnia 2018].

## Blockchain, kryptowaluty i sztuczna inteligencja

XIX zjazd, jak również osobny plan rozwoju nowej generacji sztucznej inteligencji, wprowadzony w lipcu 2017 r. przez Radę Państwa, jasno pokazują że Pekin ma ambicje „przewodzenia świata” w obszarze zastosowań AI do 2030 r. Chiny szybko nabierają rozmachu: w nowym modelu innowacji wykorzystują zarówno wsparcie państwa, jak i dynamikę prywatnych przedsiębiorstw.

Sztuczna inteligencja dopiero niedawno dołączyła do chińskich priorytetów pod egidą programu przekształcenia Chin w „państwo innowacji”. W sierpniu 2016 r. w 13. pięcioletnim krajowym planie innowacji w zakresie nauki i technologii wezwano do zajęcia czołowych pozycji w międzynarodowym rozwoju naukowym, uruchamiając serię 15 „megaprojektów i innowacji w dziedzinie nauki i technologii 2030”<sup>12</sup>, w których uwzględniono zarówno inteligentną produkcję, *big data*, jak i robotykę. Sztuczna inteligencja nie została w 2016 r. uwzględniona jako priorytet, choć wspomniano o tym koncepcie również we wcześniejszych planach, takich jak trzyletni plan wdrażania działań AI „Internet Plus” z maja 2016 r. Dopiero w maju 2017 r. Ministerstwo Nauki i Technologii ogłosiło decyzję o dodaniu „AI 2.0” do pierwszego składu jako 16. megaprojekt. W listopadzie 2017 r. Ministerstwo Nauki i Technologii (MNiT) zwołało posiedzenie wysokiego szczebla, które oficjalnie uruchomiło Biuro Promocji Rozwoju Nowej Generacji AI: przedsięwzięcie całego rządu angażujące nie mniej niż 15 różnych podmiotów, z udziałem MNiT, Komisję Narodowego Rozwoju i Reform oraz Ministerstwa Przemysłu i Technologii Informatycznych (MPiTI). Ponadto oficjalne zaangażowanie Centralnego Biura Komisji Rozwoju Fuzji Wojskowo-Cywilnej, Naukowo-Technicznej Centralnej Komisji Wojskowej i Departamentu Rozwoju Sprzętu Centralnej Komisji Wojskowej potwierdza włączenie sztucznej inteligencji do wojskowych zastosowań i rozszerzenie zakresu program krajowego.

W grudniu 2017 r. Ministerstwo Przemysłu i Technologii Informatycznych opublikowało trzyletni plan działania na rzecz rozwoju sztucznej inteligencji nowej generacji jako branży (w latach 2018–2020). Ten nowy plan wezwał Chiny do osiągnięcia „przełomu w produkcji związanej ze sztuczną inteligencją” i „stworzenia międzynarodowej przewagi” do 2020 r. Plan ten został niemal zrealizowany, a technologie, takie jak mechanizm rozpoznawania twarzy, są rutynowo stosowane w Chinach w czasie wykonywania tak podstawowych zadań, jak zakupy, uzyskiwanie dostępu do niektórych usług publicznych itd. Systemy rozpoznawania twarzy Baidu na przykład potwierdzają tożsamość pasażerów na niektórych bramkach lotniska. Ostatnie postępy w zakresie sztucznej inteligencji umożliwiły

<sup>12</sup> <http://chinainnovationfunding.eu/national-st-megaprojects/>.



identyfikację osób nie tylko na zdjęciach z bliska, ale także w wideo, co było pilotażowo wdrożone w prowincji Xinjiang<sup>13</sup> i w Kantonie<sup>14</sup>.

Należy pamiętać, że to chińskie firmy technologiczne pozostaną integralnymi graczami w innowacyjnych przedsięwzięciach, takich jak te wymienione powyżej – kilka wiodących chińskich firm AI, działających jako „drużyna narodowa”, podjęło się opracowania nowych „otwartych platform innowacji”. I tak Baidu jest odpowiedzialne za autonomiczne pojazdy, Alibaba Cloud (Aliyun) za inteligentne miasta, Tencent za obrazowanie medyczne, a iFlytek za inteligentny głos. Utworzenie krajowych laboratoriów sztucznej inteligencji na poziomie korporacyjnym jest bezprecedensowe i ilustruje ważny trend: wzmocnienie, ale także sterowania prywatnymi firmami internetowymi przez Pekin. Rozwój technologii w Chinach i odpowiadających im ram prawnych postępuje równocześnie. Tak jak ropa naftowa podsycała epokę przemysłową, dane – głównie pochodzące z systemów takich jak SWS – napędzają rozwój sztucznej inteligencji, a Chiny, jak to ujął „The Economist”, to „Arabia Saudyjska danych”<sup>15</sup>. Za każdym razem, gdy ktoś wprowadza zapytanie do Baidu, płaci kartą z portfelem WeChat, korzysta z Taobao (chiński Amazon) lub jedzie na przejażdżkę z Didi (chiński Uber) – dane mogą być ponownie wykorzystane przez algorytmy, aby poprawić ich dokładność. Ich skala jest ponadprzeciętna: China Network Information Centre informowało w 2018 r., że w Chinach jest około 751 mln unikatowych użytkowników serwisów online, a ponad 95% z nich korzysta z Internetu za pomocą urządzeń mobilnych<sup>16</sup>. W 2016 r. chińskie transakcje z płatności mobilnych wyniosły 5,5 bln dol., czyli około 50 razy więcej niż w Stanach Zjednoczonych w tym samym roku (szacunek IResearch, firmy konsultingowej z Szanghaju).

Rozważając sferę finansową, Chiny są również istotne z perspektywy rozwoju kryptowalut. W 2017 i 2018 r. ponad połowa 406 patentów światowych związanych z blockchainami pochodziła z Chin<sup>17</sup>. Mimo wdrożenia wielu zakazów dotyczących kryptowalut – we wrześniu 2017 r. władze zakazały obrotu wirtualną walutą

<sup>13</sup> Elsa B. Kania, *Technological Entanglement: Cooperation, Competition and the Dual-use Dilemma in Artificial Intelligence*, 28 czerwca 2018, <https://apo.org.au/node/180151> [dostęp 31 sierpnia 2020].

<sup>14</sup> *S.China City Subway Adopts Facial Recognition*, 10 września 2019, [http://www.xinhuanet.com/english/2019-09/10/c\\_138381309.htm](http://www.xinhuanet.com/english/2019-09/10/c_138381309.htm) [dostęp 31 sierpnia 2020].

<sup>15</sup> *The Algorithm Kingdom. China May Match or Beat America in AI*, 15 lipca 2017, <https://www.economist.com/business/2017/07/15/china-may-match-or-beat-america-in-ai> [dostęp 28 maja 2018].

<sup>16</sup> *Statistical Report on Internet Development in China*, styczeń 2018 [online], <https://cnnic.com.cn/IDR/ReportDownloads/201807/P020180711391069195909.pdf> [dostęp 25 maja 2018].

<sup>17</sup> Stephanie Nebehay, *‘Driving Force’ China Accounts for Nearly Half Global Patent Filings: U.N.*, 16 października 2019, <https://www.reuters.com/article/us-global-economy-innovations/driving-force-china-accounts-for-nearly-half-global-patent-filings-u-n-idUSKBN1WU2XR> [dostęp 30 sierpnia 2020].

– Pekin zaczyna być bardziej otwarty na rozwój technologii blockchain. Chce więc wyeliminować bitcoina, ale zachować „kopalnie”, ponieważ celem władz może być wprowadzenie wirtualnego RMB wzorowanego na bitcoinie. Wirtualny pieniądz kontrolowany przez władze jest logicznym uzupełnieniem budowanego Systemu Wiarygodności. Dodatkowo Chińskie Ministerstwo Przemysłu i Technologii Informacyjnych opublikowało listę celów, które mają zachęcić do rozwoju i standaryzacji sektora technologii blockchain<sup>18</sup>. Cele te będą rekomendować standardy „w specyfikacji formatu danych, interoperacyjności i inteligentnych kontraktach”<sup>19</sup>.

## Perspektywy

Do 2018 Pekin skutecznie równoważył gospodarkę cyfrową z celami wytyczonymi dla stabilności politycznej. Bezpośredni udział prywatnych firm w krajowych inicjatywach, które mogą tworzyć technologie i aplikacje podwójnego zastosowania, odzwierciedla uwikłanie przedsiębiorstw w ogólną agendę państwa: „kompleks partyjno-korporacyjny”. Wysoki poziom inwestycji i rosnące kwoty finansowania rządowego, a także priorytyzacja cyberbezpieczeństwa po XIX zjeździe są w dalszym ciągu korzystne dla długoterminowego wspierania badań i rozwoju technologii. Jednocześnie istnieją obawy, że w wyniku takiego procesu i nacisku na jeden sektor w Chinach może powstać bańka technologiczna.

Chiny koncentrują się na wzmocnieniu kontroli Internetu w kraju oraz w zaprzyjaźnionych reżimach. Powstaje w ten sposób infrastruktura i technologie, które mogą być na życzenie poszczególnych rządów implementowane w kolejnych krajach. Istotnym pytaniem jest, czy nowe pomysły legislacyjne, przede wszystkim te związane z Systemem Wiarygodności Społecznej, mogą zagrażać rządowym inicjatywom mającym na celu wspieranie bardziej innowacyjnej chińskiej gospodarki. W dalszym ciągu nie ma pewności, czy chińska wizja suwerenności cybernetycznej jest – jak zakładano – odtwarzalna w innych miejscach, szczególnie w krajach rozwijających się. Pekin niewątpliwie używa inwestycji zagranicznych w rozwiązaniach dotyczących bezpieczeństwa i kontroli w sieci do powiększania istniejących stref wpływu, licząc, że wraz z ich rozszerzaniem chińskie standardy będą brane pod uwagę również przez większych graczy.

<sup>18</sup> Aaron Wood, *China: IT Ministry To Create Committee For Blockchain Standards, Domestic And International*, 24 marca 2018, <https://cointelegraph.com/news/china-it-ministry-to-create-committee-for-blockchain-standards-domestic-and-international> [dostęp 30 sierpnia 2020]

<sup>19</sup> Zhou Yanyan, *国家发改委直属协会将设区块链投资发展中心, 拟推出行业标准*, 13 marca 2018, [https://www.thepaper.cn/newsDetail\\_forward\\_2028742](https://www.thepaper.cn/newsDetail_forward_2028742) [dostęp 15 marca 2018].

Oczywiste jest, że Chiny stoją na czele globalnej rewolucji w zakresie innowacji technologicznej, choć jej przyszła trajektoria i dalsza realizacja chińskich ambicji pozostaje niepewna. Niewątpliwie trudne jest oddzielenie priorytetów Chińskiej Partii Komunistycznej i prób zapewnienia bezpieczeństwa państwa poprzez wzmocnienie zdolności kontroli społecznej. W ostatnich miesiącach do takich niewiadomych dołączyły relacje ze Stanami Zjednoczonymi i przede wszystkim długoterminowe skutki pandemii.

## Bibliografia

1. Greenfield P., *The Cambridge Analytica Files: The Story So Far*, 26 marca 2018, <https://www.theguardian.com/news/2018/mar/26/the-cambridge-analytica-files-the-story-so-far>.
2. Ivy Yu, *How 'Self-media' in China has Become a Hub for Misinformation*, 27 marca 2018, <https://supchina.com/2018/03/27/how-self-media-in-china-has-become-a-hub-for-misinformation/>.
3. Jing de Jong-Chen, Bobby O'Brien, *A Comparative Study: The Approach to Critical Infrastructure Protection in the U.S., E.U., and China*, 14 listopada 2017, <https://www.wilsoncenter.org/publication/comparative-study-the-approach-to-critical-infrastructure-protection-the-us-eu-and-china>.
4. Kania E.B., *Technological Entanglement: Cooperation, Competition and the Dual-use Dilemma in Artificial Intelligence*, 28 czerwca 2018, <https://apo.org.au/node/180151>.
5. Kelly S., Earp M., Reed L., Shahbaz A., Truong M., *Freedom on the Net. Privatizing Censorship, Eroding Privacy*, Freedom House, październik 2015, [https://freedomhouse.org/sites/default/files/FH\\_FOTN\\_2015Report.pdf](https://freedomhouse.org/sites/default/files/FH_FOTN_2015Report.pdf).
6. Lam Yan Liang, *China Continues to Push for its Vision of the Internet*, 3 grudnia 2017, <https://www.straitstimes.com/asia/east-asia/xi-jinping-says-china-will-not-close-door-to-global-internet-but-insists-on-cyber>.
7. Nebehay S., *'Driving Force' China Accounts for Nearly Half Global Patent Filings: U.N.*, 16 października 2019, <https://www.reuters.com/article/us-global-economy-innovations/driving-force-china-accounts-for-nearly-half-global-patent-filings-u-n-idUSKBN1WU2XR>.
8. *S. China City Subway Adopts Facial Recognition*, 10 września 2019, [http://www.xinhuanet.com/english/2019-09/10/c\\_138381309.htm](http://www.xinhuanet.com/english/2019-09/10/c_138381309.htm).
9. *Statistical Report on Internet Development in China*, styczeń 2018, <https://cnnic.com.cn/IDR/ReportDownloads/201807/P020180711391069195909.pdf>.

10. Su C., *China Doubles Down on Real-name Registration Laws, Forbidding Anonymous Online Posts*, 27 sierpnia 2018, <https://techcrunch.com/2017/08/27/china-doubles-down-on-real-name-registration-laws-forbidding-anonymous-online-posts/>.
11. *The Algorithm Kingdom. China May Match or Beat America in AI*, 15 lipca 2017, <https://www.economist.com/business/2017/07/15/china-may-match-or-beat-america-in-ai>.
12. Tremaine D.W., *The Chinese Government Issues Draft Cybersecurity Regulations to Protect Critical Information Infrastructure*, <https://www.lexology.com/library/detail.aspx?g=d36a5919-cb3a-4bad-bbec-1686b04eae27>.
13. Wagner J., *China's Cybersecurity Law: What You Need to Know*, „The Diplomat”, 1 czerwca 2017, <https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/>.
14. Wood A., *China: IT Ministry To Create Committee For Blockchain Standards, Domestic And International*, 24 marca 2018, <https://cointelegraph.com/news/china-it-ministry-to-create-committee-for-blockchain-standards-domestic-and-international>.
15. Zhou Yanyan, *国家发改委直属协会将设区块链投资发展中心, 拟推出行业标准*, 13 marca 2018, <https://www.thepaper.cn/newsDetail>.