

Tomasz Wójtowicz  
Uniwersytet Pedagogiczny im. KEN w Krakowie  
tomasz.wojtowicz2@up.krakow.pl  
<https://orcid.org/00000-0001-6468-8973>

## Social Credit System w Chińskiej Republice Ludowej

**Abstrakt:** Jednym z największych zagrożeń i wyzwań dla współczesnych państw jest funkcjonowanie programów masowej inwigilacji i wpływ nowych technologii informacyjnych na ograniczenie prywatności. Celem niniejszego artykułu jest przedstawienie genezy, wizji funkcjonowania oraz krytyki programu Social Credit System (SCS), który powstaje w Chińskiej Republice Ludowej. Głównym problemem badawczym wynikającym z założonego celu była odpowiedź na pytania: czym jest SCS w Chińskiej Republice Ludowej, jaka jest geneza jego powstania oraz na czym polega jego funkcjonowanie? Do rozwiązania problemów badawczych zastosowane zostały następujące metody badawcze: metoda monograficzna, metoda badania dokumentów, metoda analizy i krytyki piśmiennictwa oraz metoda analizy i syntezy. Biorąc pod uwagę wstępnie przeprowadzone badania, autor postawił następującą hipotezę badawczą: SCS należy traktować znacznie szerzej niż tylko program mający na celu masowy nadzór nad chińskim społeczeństwem i powstrzymywanie zagrożeń związanych z separatyzmem, terroryzmem i buntem społecznym (kolorowymi rewolucjami). Jest on jednym z narzędzi budowania społeczeństwa opartego na tradycyjnych chińskich wartościach i tożsamości narodowej: lojalności, harmonii, prawości i uczciwości. Społeczeństwa zdyscyplinowanego, które obok silnej i innowacyjnej gospodarki umożliwi Chinom uzyskanie statusu globalnego mocarstwa, podważając tym samym jednobiegunowy „amerykański porządek międzynarodowy”. Pomimo iż Chiny nie są państwem demokratycznym, powodzenie systemu może przyczynić się do wdrożenia podobnych rozwiązań w innych krajach Azji. Tym samym zasadne wydaje się prowadzenie badań nad SCS.

**Słowa kluczowe:** Chińska Republika Ludowa, system zaufania społecznego, bezpieczeństwo wewnętrzne, masowy nadzór.

## Social Credit System in the People's Republic of China

**Abstract:** Mass surveillance programmes and the impact of new information technologies on privacy restriction are among the greatest threats and challenges faced by modern countries. This article aims to present the origins and functional vision of, and some critical remarks on, the Social Credit System (SCS) under development in the People's Republic of China. The underlying research issue arising from the assumed objective was to respond to the following questions: What

is the SCS developed in the People's Republic of China? What are its origins? How exactly does it function? The following research methods were used to solve the research queries: the monograph method, the document analysis method, the literature analysis and critique method, and the analysis and synthesis methods. In view of the preliminary investigation, the author formulated the following research hypothesis: the SCS should be viewed in a broader sense than merely as a programme aimed at conducting mass supervision of the Chinese society and preventing threats of separatism, terrorism, and social riot (colour revolutions). It is one of the tools to shape a society based on traditional Chinese values and national identity: loyalty, harmony, integrity, and fairness – a disciplined society which, along with a strong and innovative economy, will enable China to attain the status of global power, thus questioning the American “unipolar world order”. Although China is not a democratic country, the system's success can contribute to implementing similar solutions in other Asian countries. Therefore, it appears justified to conduct studies focused on the SCS.

**Keywords:** People's Republic of China, social credit system, internal security, mass surveillance

## Wstęp

Rozwój technologii informacyjnych oraz technologii związanych z Big Data umożliwił poszczególnym państwom zbudowanie systemów masowego nadzoru (*mass surveillance*). Systemów definiowanych jako praktyka szpiegowania części lub całej populacji. Szpiegowanie może odbywać się za pomocą różnych metod, m.in.: użycia kamer CCTV, przechwytywania wiadomości e-mail, czy włamywania się do komputerów (*hacking*). Masowy nadzór prowadzony jest przez państwa lub przez prywatne korporacje, które realizują go na zlecenie rządów bądź z własnej inicjatywy. Programy wykorzystywane przez rządy służą zapewnieniu bezpieczeństwa wewnętrznego przed zagrożeniami terroryzmu i ekstremizmu lub mają na celu tworzyć „zaporę” przed informacyjnymi wpływami innych krajów (kultur). Problem masowego nadzoru społecznego nie dotyczy wyłącznie Chińskiej Republiki Ludowej. W ciągu ostatnich kilkunastu lat na świecie doszło do powstania wielu tego rodzaju rozwiązań w państwach zarówno demokratycznych, jak i autorytarnych. W Stanach Zjednoczonych powstały m.in. Echelon i PRISM, w Rosji SORM, Iran z kolei miał uzyskać dostęp do oprogramowania NetEnforcer (York, 2011).

Pomimo że termin pełnego wykorzystania SCS w stosunku do wszystkich obywateli i podmiotów gospodarczych wyznaczony został na rok 2020, wszystko wskazuje na to, iż pełna aktywacja nie nastąpi przed końcem roku. Z jednej strony większość obywateli ChRL korzysta z komercyjnych systemów oceny społecznej, takich jak Sesame Credit czy Tencent Credit, z drugiej jednak niewielki procent

objęty jest lokalnymi państwowymi pilotażowymi systemami (ok. 8% w 2019 roku). SCS należy traktować jako kolejny program masowego nadzoru, powstający w ChRL obok Wielkiej Zapory Ogniowej i projektu Złotej Tarczy. Różnica między nim a innymi systemami polega na tym, że obok technologii nadzoru zastosowane zostaną w nim również metody oceny zaufania obywateli, zbliżone do metod wykorzystywanych przez instytucje finansowe, zajmujące się oceną zdolności kredytowych. Pierwsze oficjalne informacje na temat Social Credit System pochodzą z 2007 roku, kiedy Generalne Biuro Rady Państwa zwróciło się do wszystkich instytucji rządowych oraz władz prowincji z opinią na temat budowy SCS (The Central People's Government of the People's Republic of China, 2007). Następnie w 2014 roku opublikowany został rządowy dokument, przedstawiający czym jest SCS oraz prezentujący proces jego wdrażania – *State Council Notice concerning Issuance of the Planning Outline for the Construction of a Social Credit System (2014–2020)* (China Copyright and Media, 2014). Obok oficjalnych dokumentów rządowych, przedstawiających punkt widzenia Pekinu, w pracy wykorzystane zostały artykuły, które ukazały się na łamach czasopism: „Wired”, „Global Times”, „Newsweek”, „Economist”, „Times”, „Businessinsider”, „Forbes”, a ponadto opracowania Stockholm International Peace Research Institute, Ośrodka Studiów Wschodnich i Polskiego Instytutu Spraw Międzynarodowych (PISM). Spośród polskich badaczy na SCS uwagę zwrócili m.in. Marcin Przychodniak z PISM oraz Agnieszka Konopka, Konstanty Kowalewski czy Adrian Zwoliński z Centrum Studiów Polska – Azja (Zwoliński, 2017).

Całość pracy składa się ze wstępu, trzech części merytorycznych oraz zakończenia. Pierwsza część merytoryczna dotyczy chińskich programów nadzoru i masowej inwigilacji obywateli. Druga część skupia się na samym Social Credit System, w trzeciej natomiast poddano go krytycznej analizie odnosząc się do zagrożeń, jakie może generować – likwidacji prywatności, łamania praw człowieka, korupcji urzędniczej, walk wewnętrznych w ramach KPCh, czy budowy państwa totalitarnego.

### **Chińskie programy masowej inwigilacji obywateli**

Nowoczesne programy masowej inwigilacji oparte na wykorzystaniu technologii informacyjnych i Internecie pojawiły się w Chinach drugiej połowie lat 90. XX wieku. Nie były one jednak pierwszymi tego rodzaju metodami wykorzystywanymi przez instytucje państwa do kontroli obywateli. Jeden z historycznych przykładów

to system Baojiu, który stosowano w Mandżukuo będącym pod kontrolą Japonii w latach 1932–1945. Baojiu był mechanizmem kontroli społecznej na terenach wiejskich za pomocą takich aktywności państwa, jak rejestracja ludności przez policję, organizowanie lokalnych oddziałów samoobrony oraz powstanie nowych metod poboru podatków (Tian, 2016). Od czasu pojawienia się Internetu w Chińskiej Republice Ludowej w roku 1994 służby specjalne tego państwa opracowały szereg programów, mających na celu kontrolę dostępu do Internetu, blokadę Internetu oraz masową inwigilację obywateli (China.org.cn, 2014). Jednym z nich był projekt Złotej Tarczy (*Golden Shield Project*). Złota Tarcza była jednym z 12 tzw. „złotych projektów” realizowanych przez rząd celem budowy e-administracji w Chinach<sup>1</sup>. Sam projekt Złotej Tarczy przedstawiany był jako przyjęcie zaawansowanych technologii informacyjno-telekomunikacyjnych w celu wzmocnienia możliwości zapewnienia bezpieczeństwa publicznego przez służby policyjne (Liang, 2006, s. 5). Korzenie projektu sięgają początku lat 80. XX wieku i wiążą się ze słynnymi słowami wypowiedzianymi przez Deng Xiaopinga na temat zagrożeń związanych z „polityką otwarcia na świat”, realizowanej przez ChRL od 1979 roku. Zdaniem Xiaopinga, „jeśli otwiera się okno na świeże powietrze, należy spodziewać się, że do środka dostaną się muchy” (Torfox Stanford Project, 2011). „Muchy” były metaforą zagrożeń związanych z zachodnimi ideologiami, które mogły dotrzeć do społeczeństwa chińskiego za pomocą Internetu. Ich skutkiem mogły być stopniowa demokratyzacja społeczeństwa, niepokoje społeczne, a w ostateczności upadek ustroju socjalistycznego. Z drugiej strony, skok cywilizacyjny, na jaki zdecydowały się Chiny, nie był możliwy bez wykorzystania Internetu i technologii informacyjnych. Mając na uwadze powyższe zagrożenia, Ministerstwo Bezpieczeństwa Publicznego rozpoczęło prace nad projektem dotyczącym kontroli zawartości informacji w Internecie. Prace trwały ponad

<sup>1</sup> Oprócz projektu Złotej Tarczy realizowane były równoległe projekty: Administrative Resources System (System Rezerw Administracyjnych), Golden Macro Project (projekt zarządzania informacją rządową w obszarze makroekonomii), Golden Tax Project (projekt uszczelnienia systemu podatkowego), Golden Customs Project (projekt modernizacji systemu handlu i transakcji), Golden Finance Project (projekt integracji systemu finansowego), Golden Card Project (projekt promujący walutę elektroniczną), Golden Audit Project (projekt ustanowienia scentralizowanego audytu elektronicznego), Golden Social Security Project (projekt stworzenia jednolitego krajowego systemu informacyjnego w zakresie ochrony pracy, zabezpieczenia społecznego oraz monitorowania zmian na rynku pracy), Golden Quality Project (projekt zwiększenia przejrzystości i jakości wśród dostawców usług publicznych), Golden Agriculture Project (projekt promujący wykorzystanie technologii informacyjnych w rolnictwie), Golden Water Conservancy Project (projekt, mający na celu efektywne wykorzystanie i zarządzanie informacją z obszaru hydrologii – poziomu wód, zagrożenia powodziowego, nadzoru nad glebami).

osiem lat i kosztowały 700 mln USD, a sam program zaczął funkcjonować w 2003 roku (August, 2007). Złota Tarcza nazywana jest także Chińską Zaporą Ogniową (*Great Firewall of China*), nazwy te nie są jednak w pełni tożsame, jako że Chińska Zapora Ogniowa powstała wcześniej. Jej uruchomienie datowane jest na rok 1997, kiedy zablokowana została strona Voice of America<sup>2</sup>. Zapora Ogniowa koncentruje się na kontrolowaniu i blokowaniu zachodnich stron internetowych, natomiast Złota Tarcza – na chińskich stronach internetowych. Różni są również twórcy programów. Przyjmuje się, że ojcem założycielem Chińskiej Zapory Ogniowej jest Fang Bimxing z Uniwersytetu Pekńskiego, natomiast Złotej Tarczy Shen Changxiang (Sina English, 2011). Chińska Zapora Ogniowa składa się z dwóch części: sprzętu (*hardware*) i oprogramowania (*software*). Sprzęt stanowią głównie urządzenia internetowe firmy CISCO, rozlokowane w kilkudziesięciu miejscach na terenie całego kraju. Obecnie bardzo trudno wskazać ich precyzyjne położenie ze względu na fakt, że jest to pilnie strzeżona tajemnica państwowa. Według przypuszczeń, jakie można znaleźć w powszechnie dostępnych źródłach, jest to wiele miejsc w centralnych i wschodnich Chinach. Oprogramowanie z kolei pochodzi z chińskich uczelni technicznych. Sam system, od swojego powstania, ewoluował i był sukcesywnie udoskonalany. W pierwszych latach działalności służył głównie do blokowania stron internetowych za pomocą słów kluczowych. Od 1994 roku liczba użytkowników Internetu w Chinach zaczęła jednak dynamicznie rosnąć – w 2009 roku z sieci korzystało już ponad 28,8% obywateli (Torfox Stanford Project, 2011). W związku z rosnącą liczbą użytkowników sieci, obecnie Zapora Ogniowa ma zdolność cenzurowania połączeń, blokowania połączeń, kontrolę nad przepływami sieciowymi w popularnie zabezpieczonych połączeniach, takich jak tunele VPN i SSH. Zdaniem niektórych specjalistów jest również w stanie zlokalizować i zablokować mosty komunikacyjne użyte w projekcie Tor. Cenzurą może zostać objęta każda informacja znajdująca się w Internecie, jednak Ministerstwo Bezpieczeństwa Publicznego interesują najbardziej takie kwestie, jak treść generowana przez użytkowników na chińskich odpowiednikach serwisów społecznościowych: Twitter, Facebook, Blogspot czy Youtube (Sina Weibo, Youku, Tudou), informacje związane z opiniami na temat chińskiego rządu i przywództwa politycznego czy tematyka związana z szeroko

<sup>2</sup> Po zablokowaniu strony Voice of America, w kolejnych latach doszło do blokad innych stron, takich jak: Google (2002), Wikipedia (2004), Wordpress (2006), The New York Times (2008), YouTube (2008), Facebook (2009), Twitter (2009), WikiLeaks (2010), BBC (2010), LinkedIn (2011). Zob. więcej: Giang, 2011.

pojętym bezpieczeństwem narodowym (Bu, 2018).

Dynamiczny rozwój chińskiej Zapory Ogniowej i projektu Złotej Tarczy spowodował, że ich funkcjonowanie zwróciło uwagę zachodnich agencji wywiadowczych, szczególnie amerykańskich. W 2008 roku ukazał się dokument opracowany przez majora sił powietrznych USA Michaela D. Whitinga, zatytułowany *The Great Firewall of China a Critical Analysis*. Autor podzielił w nim techniki cenzurowania Internetu w ChRL na kilka grup, takich jak: techniki stosowane przez instytucje państwowe, techniki stosowane w biznesie, techniki stosowane przez dostawców Internetu, techniki stosowane w kafejkach internetowych, ograniczenia dotyczące każdej osoby korzystającej z Internetu, kontrola korespondencji e-mail, kontrola słów kluczowych, filtrowanie nazw domen i adresów URL, blokowanie adresów IP oraz blokowanie stron internetowych (Whiting, 2008). W obszarze instytucji państwowych zwrócił uwagę na rosnącą liczbę organów rządowych, w których kompetencjach znajduje się kontrola zawartości Internetu. Zaliczają się do nich m.in. Centralny Wydział Propagandy Komunistycznej Partii Chin (KPCh) czy Biuro Informacyjne Rady Państwa. W 2014 roku, również w strukturach Komunistycznej Partii Chin, powołana została Grupa Kierownicza ds. Bezpieczeństwa Internetowego i Informacji (GKBII). Jej pracami kierują bezpośrednio członkowie Stałego Komitetu Biura Politycznego KPCh, a decyzje realizuje Urząd ds. Cyberprzestrzeni (Przychodniak, 2017). Równoległe do ekspansji instytucji państwa pojawiły się także nowe akty prawne regulujące kwestie dostępności Internetu oraz cyberprzestępczości. Zalicza się do nich m.in. Computer Information Network and Internet Security, Protection and Management Regulations, zatwierdzone przez Radę Państwa 11 grudnia 1997 roku i opublikowane 30 grudnia 1997 roku czy nowe przepisy kodeksu karnego. W nim to cyberprzestępczość została opisana w artykułach 285, 286 i 287 (Cybercrimelaw.net, 2019). W obszarze biznesowym techniki cenzurowania dotyczą wymagań stawianych przez władze zachodnim korporacjom funkcjonującym na rynku chińskim, takim jak Cisco System, Nortel Network, Sun Microsystems, 3COM, Google, Yahoo, Microsoft czy IBM. Yahoo i Google zgodziły się zmodyfikować swoje wyszukiwarki zgodnie z chińskimi praktykami filtrowania danych. Firma Cisco z kolei zaprojektowała routery zgodnie ze wskazówkami urzędników. Szczególna odpowiedzialność spoczywa również na dostawcach Internetu. Dostawcy zobligowani są archiwizować numery telefonów swoich klientów, ich adresy IP oraz śledzić ruch

w sieci internetowej, monitorując, jakie strony są odwiedzane. Systemy używane przez dostawców muszą umożliwiać także weryfikację tożsamości użytkowników. Niewywiązywanie się z powyższych obowiązków grozi utratą licencji oraz odpowiedzialnością karną osób decyzyjnych. W kafejkach internetowych prowadzone są dzienniki z danymi osób, które korzystały z usług danej kafejki; dokumenty te muszą być archiwizowane do 60 dni. Osobom, które korzystają z zabronionych treści, administratorzy kafejki zobowiązani są blokować dostęp do informacji i zgłaszać incydent w formie raportu do odpowiednich organów państwa (Whiting, 2008).

Skalę programów inwigilacyjnych w Chińskiej Republice Ludowej podkreślają zarówno liczba zaangażowanych w nie osób w administracji rządowej, jak i ilość środków przeznaczanych na ten cel. Według Amnesty International (2008) „policja internetowa” zatrudnia od 30 do 50 tys. funkcjonariuszy. Całkowite wydatki na bezpieczeństwo wewnętrzne trudno precyzyjnie oszacować, ponieważ dane podawane przez oficjalne ośrodki rządowe uważa się za zaniżone. Zdaniem ekspertów sztokholmskiego Instytutu Badań nad Pokojem chińskie wydatki wojskowe w 2017 roku wzrosły o 5,6% i wyniosły 228 mld USD. Daje to Chinom drugą pozycję pod względem wydatków wojskowych w skali całego świata (SIPRI, 2018). Znacznie szybciej niż wydatki na cele wojskowe wzrastają wydatki na bezpieczeństwo wewnętrzne. Według powszechnie dostępnych informacji mogą one rosnąć nawet w skali 20% rocznie (Wang, 2018). Czytelna zmiana w podziale wydatków rządowych na bezpieczeństwo wewnętrzne i bezpieczeństwo militarne nastąpiła w 2010 roku. Wówczas po raz pierwszy wydatki na bezpieczeństwo wewnętrzne przewyższyły wydatki na cele wojskowe, wynosząc odpowiednio 551,770 mln juanów i 553,337 mln juanów. Tendencja ta umacnia się w ciągu ostatnich kilku lat w czasie rządów Xi Jipinga (od 2013 roku). Wydatki na bezpieczeństwo wewnętrzne wzrastają znacznie szybciej niż wydatki rządowe ogółem (wzrost o 34%), przeciwnie niż miało to miejsce w okresie rządów Hu Jintao, kiedy wydatki rządowe ogółem rosły o 51% szybciej niż środki przeznaczone na na bezpieczeństwo wewnętrzne (Zenz, 2018).

### **Idea Social Credit System**

Social Credit System, tłumaczony na język polski jako System Zaufania Społecznego lub System Wiarygodności Społecznej, jest jednym z najnowszych programów będących w trakcie realizacji w Chińskiej Republice Ludowej, który

może służyć jako narzędzie do masowej inwigilacji społeczeństwa. Według oficjalnych definicji jest on przedstawiany jako ważny elementem socjalistycznej gospodarki rynkowej oraz system zarządzania społecznego (Kopka, 2018). Pierwszym obszernym dokumentem rządowym ChRL opisującym SCS był *State Council Notice concerning Issuance of the Planning Outline for the Construction of a Social Credit System (2014–2020)*, opublikowany w czerwcu 2014 roku. Znajdują się w nim m.in. informacje o przyczynach powołania do życia SCS i obszarach jego zastosowania. Jako przyczyny podane zostały: gospodarka rynkowa, budowa harmonijnego społeczeństwa socjalistycznego oraz konieczność budowy „kultury zaufania”. Zdaniem autorów dokumentu Chiny stoją obecnie przed możliwością przyspieszenia transformacji gospodarczej. Wprowadzenie systemów zaufania społecznego ma pomóc w procesie optymalizacji alokacji dóbr, zwiększeniu popytu wewnętrznego, a także w postępie naukowym. Sam system ma funkcjonować z kolei w czterech obszarach, w których ma przyczynić się do podniesienia poziomu zaufania: obszarze funkcjonowania administracji rządowej, obszarze relacji biznesowych, obszarze relacji społecznych (socjalnych), obszarze działalności wymiaru sprawiedliwości (China Copyright and Media, 2014). Podniesienie zaufania w funkcjonowaniu administracji rządowej ma polegać m.in. na efektywnej i uczciwej pracy urzędników służby cywilnej czy budowie przejrzystych zasad prowadzenia działalności gospodarczej i wymiany handlowej. Praca urzędników ma być poddawana cyklicznej kontroli poprzez zastosowanie w stosunku do nich osobistych systemów zaufania społecznego. Mają zostać tym samym wyeliminowane wszelakie praktyki nadużywania uprawnień administracyjnych lub działań protekcyjnych, uniemożliwiających funkcjonowanie przejrzystego i wolnego rynku. Podniesienie zaufania w obszarze relacji biznesowych ma polegać na wprowadzeniu regulacji i baz danych, które wpłyną na skuteczną walkę z monopolami, na identyfikacji przedsiębiorców niewywiązujących się z umów w ramach realizacji zamówień publicznych, na zachęcaniu przedsiębiorców do wywiązywania się ze spłaty zobowiązań kredytowych itp. Podnoszenie zaufania w obszarze relacji społecznych (socjalnych) ma skupiać się na funkcjonowaniu służby zdrowia, opieki nad osobami starszymi, pomocy ofiarom klęsk żywiołowych, funkcjonowaniu sektora edukacji i oświaty, sportu, turystyki i rekreacji. W tym celu mają powstać systemy oceny kredytowej, dotyczące pracowników służby zdrowia i edukacji. Szczególnie chroniona ma być własność intelektualna, a jej kradzież surowo karana. Podnoszenie



zaufania w obszarze wymiaru sprawiedliwości ma skupiać się z kolei na budowie wiarygodności sądów powszechnych poprzez m.in. system ocen pracowników, zbieranie danych (Big Data) na tematy związane z poziomem przestępczości, bezpieczeństwem ruchu drogowego itp. (China Copyright and Media, 2014).

Oficjalne dokumenty rządowe nie udzielają precyzyjnej odpowiedzi na pytanie, jak dokładnie będzie funkcjonował Social Credit System oraz jakie zagrożenia są z nim związane. Uwagę badaczy przykuwa jednak kilka chińskich przedsiębiorstw zarządzających systemami oceny kredytowej, które mogą być punktem odniesienia dla SCS. Jednym z nich jest Alibaba Group Holding, przedsiębiorstwo założone w 1999 roku przez Chung Tsai i Yun Ma i zajmujące się mobilnymi systemami sprzedaży i handlem elektronicznym. W 2017 roku wartość rynkowa Alibaba Group Holding wyniosła 472,4 mld USD, wyprzedzając tym samym firmę Amazon o wartości 470 mld USD (Shidong, 2017). Z kolei w lipcu 2018 roku wartość rynkowa Alibaby wyniosła ponad 500 mld USD (Forbes, 2018). Grupa nadzoruje szereg innych przedsiębiorstw, z których najistotniejszą – z punktu widzenia zarządzania systemami oceny kredytowej – jest Ant Financial Services Group, funkcjonująca wcześniej pod nazwą Alipay. Jedną z kluczowych usług świadczonych przez Ant Financial Services Group dla Alibaba Group jest system oceny kredytowej Sesame Credit. System zbiera informacje z różnych źródeł dostępnych w ramach Alibaba Group, takich jak portale społecznościowe czy zakupy robione przez Internet, aby przyporządkować ostatecznie klientowi liczbę punktów, która będzie wskazywała jego zdolność kredytową. Liczba punktów waha się między 350 a 950. Ant Financial nie ujawnia zasad działania algorytmu, lecz wskazuje na kilka czynników, jakie brane są pod uwagę w jego obliczaniu. Są nimi: historia kredytowa (regulowanie zobowiązań kredytowych i podpisanych na czas umów), zdolność klienta do wypełniania zobowiązań umowy na czas, trzeci czynnik dotyczy weryfikacji danych podawanych przez klienta (dane osobowe, numer telefonu, adres), natomiast czwarty i piąty dotyczą zachowania klienta i relacji interpersonalnych. Zdaniem osób odpowiedzialnych za zarządzanie systemem zebrane informacje pozwalają ocenić stosunek klienta do pracy, obowiązków zawodowych, jego odpowiedzialność i sposób spędzania wolnego czasu. Jeśli ktoś na przykład spędza kilkanaście godzin dziennie grając w gry komputerowe, uznawany jest za osobę marnującą swój czas i bezproduktywną. Jeśli ktoś często kupuje pieluchy dla niemowląt przez Internet, uznawany jest za osobę posiadającą dzieci i odpowiedzialną. Zwyczaże konsumenckie i zachowanie

na portalach społecznościowych przekładają się następnie na poziom uzyskanych punktów. Jeśli wyniesie on 600, klient może skorzystać z pożyczki Just Justend do 5000 juanów (około 565 funtów brytyjskich). Poziom 650 punktów umożliwia wynajęcie samochodu bez pozostawiania depozytu lub szybszą odprawę w hotelach i na lotniskach. Osoby posiadające 666 punktów mogą skorzystać z pożyczki gotówkowej w wysokości 50000 juanów (5700 funtów brytyjskich), natomiast 750 punktów otwiera drogę do uzyskania wizego do strefy Schengen. W przypadku Social Credit System konsekwencje uzyskania określonej liczby punktów mogą być podobne. Obywatele, którzy uzyskają mniejszą liczbę punktów, nie będą mogli liczyć na prestiżową pracę w służbie cywilnej, prasie czy telewizji. Pierwszeństwo w zapisaniu swoich dzieci do prywatnych przedszkoli, szybkiej odprawy na lotnisku czy wypoczynku w atrakcyjnych miejscach będą miały osoby z wysokim poziomem punktów (Botsman, 2017). Prawdopodobieństwo, że SCS będzie funkcjonował na podobnych zasadach jak Sesame Credit, podkreśla fakt, że w 2015 roku Ludowy Bank Chin udzielił licencji ośmiu firmom na uruchomienie próbnych systemów oceny zaufania społecznego. Wśród nich znalazły się m.in.: Sesame Credit Management Co., Ltd, Tencent Credit Co., Ltd. czy China Chengxin Credit Co., Ltd. (The State Council of the People's Republic of China, 2015). Oprócz firm chińskich Social Credit System będzie obejmował wszystkie korporacje działające na terenie Państwa Środka, w tym także zachodnie. Jak wynika z raportu Izby Handlowej Unii Europejskiej *The Digital Hand: How China's Corporate Social Credit System Conditions Market Actors*, opublikowanym w sierpniu 2019 roku, europejskie firmy nie są gotowe na sprostanie wymaganiom administracyjnym związanym z jego funkcjonowaniem. Konsekwencje błędów lub niedopełnienia obowiązków przez menedżerów mogą mieć z kolei bardzo poważne konsekwencje, takie jak nałożenie sankcji bądź wpisanie na tzw. „czarną listę”. Wiążą się one nie tylko z nałożeniem kar finansowych i wyrokach sądowych za nieprzestrzeganie przepisów prawa, ale także z większą liczbą kontroli, negatywną decyzją administracyjną dotyczącą zgody na inwestycje, prawa do użytkowania gruntów, ograniczeniem partycypowania w zamówieniach publicznych, czy likwidacją ulg podatkowych. Łącznie zagraniczne korporacje będą podlegały ponad 300 ocenom i ratingom, które będą decydować o ilości otrzymanych punktów (European Union Chamber of Commerce in China, 2019).

Pomimo założenia, że Social Credit System ma zacząć działać do 2020 roku i objąć wszystkich obywateli Państwa Środka, niektóre jego elementy już są

testowane i stosowane. Jak poinformowała agencja China News Service, w 2016 roku, w wyniku działania systemu, 4,9 mln obywateli Chin dostało zakaz lotów samolotami, a 1,65 mln nie może kupić biletu na pociąg (Turek i Nguyen, 2016). W poszczególnych regionach Chin wdrażanych jest coraz więcej technologii komunikacyjnych, które w przyszłości mają stanowić elementy SCS. Liczba kamer monitorujących w 2016 roku przekroczyła 176 mln, a do 2020 roku ich liczba ma wzrosnąć do 626 mln (Hersey, 2017). Oprócz kamer, rozwijanych jest również wiele innych technologii inwigilacyjnych. Alexandra Ma z redakcji „Business Insider” przedstawiła 10 technologii (sposobów), jakie mogą wykorzystać władze Chin w ramach funkcjonowania Social Credit System. Są to: technologia rozpoznawania twarzy w dużym tłumie ludzi, obserwowanie i identyfikowanie użytkowników forów i czatów grupowych, zmuszanie obywateli do pobierania aplikacji, które pozwalają odpowiednim służbom mieć dostęp do danych znajdujących się na telefonie, analiza zwyczajów zakupowych konsumentów w Internecie, wyposażenie funkcjonariuszy policji i służb bezpieczeństwa w okulary służące do identyfikacji twarzy w zatłoczonych miejscach, instalowanie „policyjnych robotów” w miejscach użyteczności publicznej, których zadaniem jest rozpoznawanie twarzy, instalowanie w okolicach przejść dla pieszych kamer, mających na celu identyfikację „jaywalkersów” – osób przekraczających jezdnię w niedozwolonym miejscu, umożliwienie pod względem prawnym zatrzymywanie obywateli do rutynowej kontroli osobistej i sprawdzanie telefonów lub laptopów pod kątem posiadania dokumentów, programów, plików uznanych za groźne według Komunistycznej Partii Chin, śledzenie użytkowników mediów społecznościowych i analiza ich postów pod kątem treści niepoprawnych politycznie, budowa oprogramowań, mających na celu zbieranie dostępnych danych o obywatelach (Big Data), a następnie analizowanie i profilowanie ich pod kątem potencjalnego zagrożenia dla ustroju państwa (Ma, 2018). Na ostatnią metodę zwróciła uwagę organizacja Human Right Watch, która poinformowała, że władze Chin opracowały program pod nazwą *Integrated Joint Operation Platform* (Połączona Platforma Operacji Wspólnych). Program wykorzystywany ma być obecnie przede wszystkim w takich regionach, jak Sinciang w Zachodnich Chinach, gdzie ponad 45% społeczeństwa stanowią Ujgurzy. Wykorzystuje on informacje na temat mieszkańców, pochodzące z kamer rozpoznających twarze, raportów policyjnych, informacji bankowych, informacji zgromadzonych przez administrację publiczną, jednostki służby zdrowia itp. Funkcjonariusze

bezpieczeństwa zwracają uwagę na takie kwestie, jak „nienaturalny” zakup dużych ilości żywności przez obywatela czy nagłe przerwanie nauki przez dzieci, co według władz może świadczyć nawet o działalności w organizacjach terrorystycznych. Program ma więc charakter prewencyjny i umożliwia policji zatrzymywanie osób, które nie popełniły przestępstwa lub wykroczenia, lecz mogą to zrobić w przyszłości. Osoby takie kierowane są do specjalnych obozów – centrów edukacji politycznej, gdzie mają przebywać bez wyroku sądów (Human Rights Watch, 2018).

### **Krytyka Social Credit System**

Krytyka powstającego w Chinach Social Credit System, jaka pojawiła się w państwach zachodnich, dotyczy głównie problemu praw człowieka, masowej inwigilacji i ingerencji rządu w prywatne życie obywateli. Świadczą o tym tytuły prasowe popularnych opiniotwórczych czasopism. Na łamach „New York Times” ukazał się artykuł *‘1984’ algorithm to control life in China* (Ash, 2017), w „Newsweeku” *‘Black Mirror’ in China? 1.4 Billion Citizens to be Monitored Through Social Credit System* (Zhao, 2018), „Economist” opublikował zaś tekst pt. *China invents the digital totalitarian state* (The Economist, 2016). Z drugiej strony przedstawiciele chińskiej administracji rządowej oraz chińskie autorytety z obszaru nauki nie podejmują polemiki z krytycznymi głosami pochodzącymi z Zachodu. Jedną z przyczyn takiego podejścia może być wysoka akceptacja społeczna SCS. Według badań przeprowadzonych przez Genia Kostka z Freie Universität w Berlinie przy wsparciu niemieckich firm informatycznych świadczących usługi w Chinach, wynika, iż 80% społeczeństwa chińskiego częściowo lub w pełni akceptuje funkcjonowanie SCS, 17% traktuje go w kategoriach neutralnych, a tylko 1% wskazuje, że jest on zagrożeniem (Kostka, 2019).

Biorąc pod uwagę szerokie zastosowanie SCS zarówno w celach gospodarczych, społecznych, jak i w celu zapewnienia bezpieczeństwa wewnętrznego, krytyka skupiona wyłącznie na kwestii praw człowieka jest niewystarczająca. Chiny, podobnie jak Rosja, ze szczególnym niepokojem przyglądały się kolorowym rewolucjom, do jakich doszło głównie na obszarze byłego Związku Radzieckiego, a także w Iraku, Libanie, Iranie czy w Tunezji. Profesor Igor Panarin z Akademii Dyplomatycznej MSZ Federacji Rosyjskiej podkreślił, że wszystkie kolorowe rewolucje na obszarze Wspólnoty Niepodległych Państw oraz tzw. arabska wiosna były produktem technologii sterowania społecznego i agresji informacyjnej

Stanów Zjednoczonych (Darczewska, 2014). Podobnego zdania jest strona chińska. Na łamach „Global Times”, chińskiego czasopisma przedstawiającego problemy międzynarodowe z punktu widzenia Pekinu, ukazał się artykuł *US split on future relations with China*. Zdaniem jego autora kolorowe rewolucje są narzędziem polityki powstrzymywania w rękach Stanów Zjednoczonych. Wybuch kolorowej rewolucji na terytorium Chin miałyby doprowadzić do korekty ustroju politycznego i jego zmiany w kierunku liberalnej demokracji (Manning, 2016). To, jak poważnie rząd ChRL traktuje tego rodzaju zagrożenia, potwierdza reakcja na tzw. „jaśminową rewolucję”, do której doszło w 2011 roku. Zakończyła się ona nie tylko aresztowaniem kilkudziesięciu aktywistów, ale także dodatkową cenzurą Internetu. Poszukiwanie w sieci takich pojęć, jak „jaśminowa rewolucja”, kończyło się wyświetleniem komunikatu rządowego, który ostrzegał przed publikowaniem nieodpowiednich treści politycznych (Kan, 2011).

Obok zagrożeń w postaci masowej inwigilacji i wpływania na codzienne decyzje obywateli, SCS generuje kilka dodatkowych zagrożeń. Jednym z nich jest korupcja. Według niektórych informacji, jakie pojawiły się na temat systemu, może być on wyposażony w opcję oceny wzajemnej przez obywateli. Będzie to stanowiło okazję dla osób dysponujących odpowiednim kapitałem do „kupowania” wysokich ocen. Gdyby jednak okazało się, że SCS nie będzie posiadał powyższej funkcji, nie jest wykluczone, że poprawę oceny będą „oferowały” grupy hakerskie, dążące do uzyskania nielegalnego dostępu do zarządzania oceną zaufania obywateli (Michalek, 2017). Innym zagrożeniem jest wykorzystanie tego systemu jako narzędzia do wzajemnego zwalczania się przez poszczególne frakcje w ramach Komunistycznej Partii Chin. Od 2012 roku w ramach KPCh ma miejsce proces konsolidacji władzy przez Xi Jinpinga i jego grupę polityczną (HuffPost, 2018). Wcześniej wpływy w partii równoważyły się między frakcją populistyczną, nazywaną też frakcją Komunistycznej Ligii Młodzieżowej, a frakcją elitarną, nazywaną też frakcją szanghajską. Frakcja populistyczna skupia głównie działaczy pochodzących z uboższych zachodnich regionów Chin, których kariera nie byłaby możliwa, gdyby nie działalność w młodzieżowych organizacjach politycznych. Do frakcji tej zaliczał się m.in. były prezydent Hu Jintao i premier Li Keqiang. Frakcja elitarna z kolei składa się z działaczy takich jak Jiang Zemin, pochodzących z zamożnych, wschodnich wybrzeży Chin (BBC News, 2012). Zaburzenie równowagi w ramach partii i nagła utrata wpływów przez poszczególne grupy może doprowadzić w przyszłości do podważania

aktualnej władzy i niepokojów społecznych. Reakcją grupy Xi Jinpinga może być wykorzystanie Social Credit System do eliminacji niewygodnych członków partii, podobnie jak miało to miejsce w czasie rewolucji kulturalnej zorganizowanej w latach 60. XX wieku przez Mao Zedonga, kiedy ruch społeczno-polityczny wykorzystany został do eliminacji przeciwników politycznych.

### Zakończenie

Według oficjalnych rządowych informacji Social Credit System w Chińskiej Republice Ludowej powstaje w celu budowy „kultury zaufania” między obywatelami i instytucjami państwowymi, utrzymania tempa modernizacji gospodarczej oraz jedności społeczeństwa. Biorąc pod uwagę funkcjonowanie dotychczasowych systemów masowego nadzoru oraz możliwości technologiczne, SCS może także służyć jako „zapora” przed wpływem informacyjnym Stanów Zjednoczonych i groźbą wybuchu kolejnych kolorowych rewolucji. Wizja jego funkcjonowania skłania do analogii z rewolucją kulturową w Chinach, przeprowadzoną w latach 60. XX wieku. Podczas gdy rewolucja kulturowa prowadzona była brutalnymi metodami i pochłonęła tysiące ofiar, do zmian społecznych, jakie nastąpią w wyniku zastosowania SCS, dojdzie za pomocą zupełnie innych metod. Jednym z licznych przykładów może być wykorzystanie aplikacji i gier komputerowych, takich jak *Excellent Speech: Clap for Xi Jiping* firmy Tencent, polegająca na jak najszybszym, w ciągu 18 sekund, dotknięciu ekranu smartfonu w celu oklaskiwania przemówienia prezydenta Xi Jipinga (Peake, 2017). SCS z pewnością będzie nagradzała instalowanie tego rodzaju aplikacji na telefonach, podobnie jak inne zachowania podkreślające lojalność obywatela względem państwa. Odpowiedź na pytanie, czym jest Social Credit System, skłania do zadania kolejnych pytań: czy SCS wzmocni fundamenty państwa totalitarnego i zablokuje jakiegokolwiek przemiany demokratyczne? Czy Chiny są obecnie państwem totalitarnym? Jak SCS wpłynie na pozycję międzynarodową Chin? Zdaniem autora niniejszego artykułu odpowiedź na te pytania nie jest jednoznaczna. Biorąc pod uwagę sześć cech charakterystycznych państwa totalitarnego, jakie wskazał Zbigniew Brzeziński, Chiny mają ich pięć. Są to: oficjalna ideologia, władza sprawowana przez jedną partię polityczną typu wodzowskiego, funkcjonowanie rozbudowanego aparatu tajnej policji, kontrola środków masowego przekazu przez partię oraz kontrola wojska przez partię. Państwo Środka nie posiada natomiast gospodarki centralnie planowanej (Lee, 2020). Swoją pozycję międzynarodową zbudowało

m.in. dzięki swobodzie wolnego handlu, uczestnictwu w organizacjach międzynarodowych, liberalizacji zasad rejestracji i prowadzenia działalności gospodarczej, czy wspieraniu przez państwo innowacyjnej gospodarki w postaci funduszy *venture capital* i sieci startupów. Social Credit System zdecydowanie wzmocni fundamenty państwa totalitarnego w Chinach, jednak jego rolę należy postrzegać znacznie szerzej niż tylko kontrolę społeczną i blokowanie wpływów informacyjnych Stanów Zjednoczonych. Jest on jednym z narzędzi budowania społeczeństwa opartego na tradycyjnych chińskich wartościach, takich jak: lojalność, harmonia, prawość i uczciwość. Społeczeństwa zdyscyplinowanego, którego ciężka praca w połączeniu z silną innowacyjną gospodarką umożliwi Chinom uzyskanie statusu globalnego mocarstwa. Treść niniejszego artykułu nie wyczerpuje problemów związanych z wprowadzaniem w życie Social Credit System. Może być on jednak punktem wyjściowym do kolejnych badań i prób odpowiedzi na pytania, takie jak: czy istnieją inne metody niż SCS wykorzystania Big Data przez ChRL do masowego nadzoru, czy planowane jest wykorzystanie sztucznej inteligencji w ramach programów, takich jak SCS, oraz jakie metody zabezpieczenia programu przewidują władze w Chinach celem zabezpieczenia go przed atakami hakerskimi?

### Bibliografia

- Amnesty International. (2008, 28 marca). *What is internet censorship?* Dostęp: <https://web.archive.org/web/20150427065800/http://www.amnesty.org.au/china/comments/10926/> [9.07.2019].
- Ash, A. (2017, 11 czerwca). '1984' algorithm to control life in China. *The Times*. Dostęp: <https://www.thetimes.co.uk/article/china-introduces-social-credit-system-to-rate-citizen-behaviour-bksgrgzh> [16.07.2019].
- August, O. (2007, 23 października). The Great Firewall: China's Misguided – and Futile – Attempt to Control What Happens Online. *Wired.com*. Dostęp: <https://www.wired.com/2007/10/ff-chinafirewall/> [7.07.2019].
- BBC News. (2012, 6 listopada). *Viewpoint: The powerful factions among China's rulers*. Dostęp: <https://www.bbc.com/news/world-asia-china-20203937> [17.07.2019].
- Botsman, R. (2017, 21 października). Big data meets Big Brother as China moves to rate its citizens. *Wired.com*. Dostęp: <http://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion> [16.07.2019].
- Bu, R. (2018). *The Great Firewall of China*. Dostęp: <http://campus.murraystate.edu/academic/faculty/wlyle/540/2013/Bu.pdf> [7.07.2019].
- China Copyright and Media. (2014, 25 kwietnia). *Planning Outline for the Construction of a Social Credit System (2014–2020)*. Dostęp: <https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/> [11.07.2019].
- China.org.cn. (2014, 20 kwietnia). *20 years of the Internet in China*. Dostęp: [http://www.china.org.cn/business/2014-04/20/content\\_32150035.htm](http://www.china.org.cn/business/2014-04/20/content_32150035.htm) [3.07.2019].

- Cybercrimelaw.net. (2019). *Cyber Crime Law, People's Republic of China*. Dostęp: <http://www.cybercrimelaw.net/China.html> [9.07.2019].
- Darczewska, J. (2014). *Anatomia rosyjskiej wojny informacyjnej. Operacja krymska – studium przypadku* (Punkt Widzenia nr 42). Warszawa: Ośrodek Studiów Wschodnich. Dostęp: [https://www.osw.waw.pl/sites/default/files/anatomia\\_rosyjskiej\\_wojny\\_informacyjnej.pdf](https://www.osw.waw.pl/sites/default/files/anatomia_rosyjskiej_wojny_informacyjnej.pdf) [16.07.2019].
- European Union Chamber of Commerce in China. (2019). *The Digital Hand: How China's Corporate Social Credit System Conditions Market Actors*. Dostęp: <https://www.europeanchamber.com.cn/en/publications-corporate-social-credit-system> [20.11.2020].
- Forbes. (2018). *Alibaba Group*. Dostęp: <https://www.forbes.com/companies/alibaba/> [16.07.2019].
- Giang, V. (2011, 16 lipca). The Long List of Websites That Have Once Been Blocked or Censored in China. *Business Insider*. Dostęp: <http://www.businessinsider.com/web-sites-behind-the-great-firewall-of-china-2011-7?IR=T> [9.07.2019].
- Hersey, F. (2017, 22 listopada). China to have 626 million surveillance cameras within 3 years. *Technode.com*. Dostęp: <https://technode.com/2017/11/22/china-to-have-626-million-surveillance-cameras-within-3-years/> [10.07.2019].
- HuffPost. (2018, 18 stycznia). China's Political Factions to be Unified Under Xi's Control. *The Huffington Post*. Dostęp: [https://www.huffingtonpost.com/asiatoday/chinas-political-factions\\_b\\_14239974.html?guccounter=1](https://www.huffingtonpost.com/asiatoday/chinas-political-factions_b_14239974.html?guccounter=1) [17.07.2019].
- Human Rights Watch. (2018, 26 lutego). *China: Big Data Fuels Crackdown in Minority Region*. Dostęp: <https://www.hrw.org/news/2018/02/26/china-big-data-fuels-crackdown-minority-region> [11.07.2019].
- Kan, M. (2011, 20 lutego). China Blocks Microblogs for 'Jasmine Revolution'. *PCWorld.com*. Dostęp: <https://www.pcworld.com/article/220206/article.html> [17.07.2019].
- Kopka, A. (2018, 17 maja). *Azjatycki wielki brat, czyli Social Credit System*. Centrum Studiów Polska – Azja. Dostęp: <http://www.polska-azja.pl/a-kopka-azjatycki-wielki-brat-czyli-social-credit-system/> [11.07.2019].
- Kostka, G. (2019). China's Social Credit Systems and Public Opinion: Explaining High Levels of Approval. *New Media & Society*, 21(7), 1573–1575. DOI: <https://doi.org/10.1177/1461444819826402>
- Lee, E. (2020, 26 lutego). *Is China Totalitarian?* Dostęp: <https://www.heritage.org/asia/commentary/china-totalitarian> [20.11.2020].
- Liang, G. (2006). Under The „Golden Shine”: China's Efforts to Bridge Government and Citizens. *Regional Development Dialogue*, 27(2), 20–29. Dostęp: <http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan040605.pdf> [11.07.2019].
- Ma, A. (2018, 29 kwietnia). China is bulding a vast civilian surveillance network – here are 10 ways it could be feeding is creepy 'social credit system'. *Businessinsider.com*. Dostęp: <http://www.businessinsider.com/how-china-is-watching-its-citizens-in-a-modern-surveillance-state-2018-4?IR=T> [11.07.2019].
- Manning, R.A. (2016). US split on future relations with China. *Global Times*. Dostęp: <http://www.globaltimes.cn/content/981952.shtml> [17.07.2019].
- Michałek, M. (2017). *SCS staje się faktem. Ten system zmieni wszystko*. Magazyn TVN24. Dostęp: <https://www.tvn24.pl/magazyn-tvn24/scs-staje-sie-faktem-ten-system-zmieni-wszystko,128,2284> [17.06.2019].
- Peake, E. (2017, 20 października). China's new viral app could be straight out of Black Mirror. *Wired.com*. Dostęp: <http://www.wired.co.uk/article/china-app-clap-tencent> [17.07.2019].
- Przychodniak, M. (2017). Internet jako narzędzie polityki Chińskiej Republiki Ludowej. *Biuletyn PISM*, 75(1517). Dostęp: [https://www.pism.pl/files/?id\\_plik=23421](https://www.pism.pl/files/?id_plik=23421) [9.07.2019].
- Shidong, Z. (2017, 11 października). Alibaba's value tops US\$470 billion, briefly passing Amazon as world's most valuable merchant. *South China Morning Post*. Dostęp: <https://www.scmp.com/business/china-business/article/2114832/alibaba-briefly-overtakes-amazon-worlds-most-valuable-e> [16.07.2018].



- Sina English. (2011, 18 lutego). *Great Firewall father speaks out*. Dostęp: <https://web.archive.org/web/20110225205053/http://english.sina.com/china/p/2011/0217/360409.html> [9.07.2019].
- Stockholm International Peace Research Institute [SIPRI]. (2018, 2 maja). *Global military spending remains high at \$1.7 trillion*. Dostęp: <https://www.sipri.org/media/press-release/2018/global-military-spending-remains-high-17-trillion> [9.07.2018].
- The Central People's Government of the People's Republic of China. (2007, 2 kwietnia). *Guówùyüàn bàngōng tīng guānyú shèhuì xīnyòng tìxì jiànshè de ruò gàn yìjiàn guó bàn fā 2007, 17 hào* (ang. *Several Opinions of the General Office of the State Council on the Establishment of a Social Credit System*). Dostęp: [http://www.gov.cn/zwggk/2007-04/02/content\\_569314.htm](http://www.gov.cn/zwggk/2007-04/02/content_569314.htm) [20.11.2020].
- The Economist. (2016, 17 grudnia). *China invents the digital totalitarian state*. Dostęp: <https://www.economist.com/briefing/2016/12/17/china-invents-the-digital-totalitarian-state> [16.07.2019].
- The State Council of the People's Republic of China. (2015, 5 stycznia). *Rénmíng yínháng yīnfā "guānyú zuò hǎo gèrén zhēng xīn yèwù zhìnbèi gōngzuò de tōngzhī"* (ang. *The People's Bank of China issued the "Notice on Preparing for Personal Credit Investigation"*). Dostęp: [http://www.gov.cn/xinwen/2015-01/05/content\\_2800381.htm](http://www.gov.cn/xinwen/2015-01/05/content_2800381.htm) [16.07.2019].
- Tian, M. (2016). The Baojia System as Institutional Control in Manchukuo under Japanese Rule (1932–45). *Journal of the Economic and Social History of the Orient*, 59(4), 531–554. DOI: <https://doi.org/10.1163/15685209-12341407>
- Torfox Stanford Project. (2011, 1 czerwca). *The Great Firewall of China: Background*. Dostęp: <https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/the-great-firewall-of-china-background/index.html> [7.07.2019].
- Turek, A. i Nguyen C. (2016). Chiny oceniają swoich obywateli – blisko 5 mln osób ma za niską ocenę, by kupić bilet na samolot. *Businessinsider.com*. Dostęp: <https://businessinsider.com.pl/polityka/chiny-system-ocen-obywateli/b3qd1sc> [10.07.2018].
- Wang, B. (2018). *China defense budget increases by 8.1% but police state budget is still 20% more*. Dostęp: <https://www.nextbigfuture.com/2018/03/china-defense-budget-increases-by-8-1-but-police-state-budget-is-still-20-more.html> [9.07.2019].
- Whiting, M. D. (2008). *The Great Firewall of China: a Critical Analysis*. Dostęp: [https://www.researchgate.net/publication/235035190\\_The\\_Great\\_Firewall\\_of\\_China\\_A\\_Critical\\_Analysis](https://www.researchgate.net/publication/235035190_The_Great_Firewall_of_China_A_Critical_Analysis) [10.11.2020].
- York, J.C. (2011, 23 grudnia). *Israeli Firm Allot Communications Ltd Under Fire for Selling Spyware to Iran*. Electronic Frontier Foundation. Dostęp: <https://www.eff.org/pl/deeplinks/2011/12/israeli-firm-under-fire-selling-spyware-iran> [17.07.2019].
- Zenz, A. (2018). China's Domestic Security Spending: An Analysis of Available Data. *China Brief*, 18(4), 5–11. Dostęp: [https://jamestown.org/wp-content/uploads/2018/03/CB\\_18\\_4-2.pdf?x38211](https://jamestown.org/wp-content/uploads/2018/03/CB_18_4-2.pdf?x38211) [9.07.2018].
- Zhao, Ch. (2018, 5 stycznia). Black Mirror' in China? 1.4 Billion Citizens to be Monitored Through Social Credit System. *Newsweek*. Dostęp: <https://www.newsweek.com/china-social-credit-system-906865> [16.07.2019].
- Zwoliński, A. (2017). *System kredytu społecznego (SCS) a biznes w Chinach*. Dostęp: <http://www.polska-azja.pl/a-zwolski-system-kredytu-spoolecznego-scs-a-biznes-w-chinach/> [17.07.2019].