CATALLAXY
Volume 2 Issue 1 June 2017
e-ISSN 2544-090X
www.catallaxy.pl

Oryginalny artykuł naukowy
otrzymano: 13.05.2017 / zaakceptowano: 28.06.2017 / opublikowano *online*: 30.062017

Wiśniewski, P. (2017). E-gospodarka: problem regulacji. *Catallaxy*, 2(1): 27–35. doi:10.24136/cxyv2i1.3.

E-gospodarka: problem regulacji

PIOTR WIŚNIEWSKI

Katedra Ekonomii, Wydział Nauk Ekonomicznych i Zarządzania, Uniwersytet Mikołaja Kopernika w Toruniu, ul. Gagarina 13a, 87-100 Toruń, Polska
psw@doktorant.umk.pl
orcid.org/0000-0002-2263-4851

Abstrakt

Motywacja: Dynamiczny rozwój technologii telekomunikacyjnych i związana z tym zmiana społeczna, tworzą nowe warunki dla funkcjonowania gospodarki. Wiążą się one ze zmianą roli państwa i jego możliwości regulacyjnych. E-gospodarka jest globalnym zjawiskiem, które regulowane jest lokalnie. Z punktu widzenia nauk ekonomicznych, zrozumienie obecnie istniejących zasad jej funkcjonowania, zarówno w kontekście szans, jak i zagrożeń, stanowi podstawę do prowadzenia skutecznych badań i modelowania. Pozwala także zweryfikować dotychczasowe teorie ekonomiczne w nowych warunkach. Jest to punkt wyjścia do badań nad nową rzeczywistością gospodarczą.
Cel: Celem artykułu jest przegląd teorii dotyczących regulacji e-gospodarki, a także istniejących obecnie rozwiązań problemu regulacji tego globalnego zjawiska. Na podstawie zebranego materiału podjęto próbę określenia kierunku rozwoju e-gospodarki i możliwości jej regulacji.
Wyniki: Obecne rozwiązania w zakresie regulacji e-gospodarki mogą być uznane za niewystarczające. Na podstawie przypadku bitcoina można stwierdzić, że brak jest jednolitego podejścia do e-gospodarki w skali globalnej. Brak jest również jednolitego podejścia do regulacji nowych zjawisk gospodarczych w ogóle. Biorąc pod uwagę dynamiczny rozwój techniki i wysokie prawdopodobieństwo tworzenia kolejnych innowacji rynkowych, koniecznym wydaje się poszukiwanie elastycznych rozwiązań i teorii specyficznych dla e-gospodarki.

Słowa kluczowe: *regulacja; e-gospodarka; cyberprzestępczość; e-biznes; bitcoin*
JEL: *E40; B52; O19*

1. Wprowadzenie

Relacja między państwem a gospodarką jest jednym z wiodących zagadnień ekonomii. Przedstawiciele tej dyscypliny niemal od samego początku zadawali sobie pytanie o zasadność podejmowania i stopień interwencjonizmu państwowego. Zmiany w technice i związane z nimi przemiany społeczne sprawiają, że należy ponownie podjąć ten temat, uwzględniając nowe warunki. W ramach ekonomii, problemem regulacji zajmowały się przede wszystkim Szkoła Chicagowska i Instytucjonalizm. Ich dorobek naukowy można połączyć z badaniami nad e-gospodarką. Ta z kolei ma być, według J. Rifkina (2014, s. 26), wynikiem „trzeciej rewolucji przemysłowej", która obejmować ma: trójwymiarowy druk, Internet rzeczy (*Internet of things*), *Web 2.0* i ogólny rozwój Internetu. Warto ponownie podkreślić, że e-gospodarka, oprócz wymiaru technicznego, posiada również aspekt społeczny. Zależność tę, polegającą

na wzajemnym determinizmie, zaprezentowano na schemacie 1.

Niniejszy artykuł stanowi przegląd dotychczasowych teorii i rozwiązań z zakresu regulowania e-gospodarki. Jego celem jest wskazanie, w oparciu o dostępne informacje, trudności związanych z oddziaływaniem państwa na nowy typ gospodarki oraz kierunku, w którym proces ten będzie zmierzał.

W Sekcji 2. dokonano przeglądu literatury z zakresu e-gospodarki i teorii regulacji. Wskazano również organizacje mające istotne znaczenie w rozwoju badań i regulacji e-gospodarki. W Sekcji 3. przedstawiono polskie i międzynarodowe rozwiązania regulacyjne. W Sekcji 4. ukazano zastosowane metody wykorzystane w tym artykule. W Sekcji 5. zaprezentowano przypadek walut wirtualnych w celu przedstawienia różnicy w podejściu do tego zagadnienia przyjętego przez różne państwa. W Sekcji 6. zawarto główne wnioski.

2. Przegląd literatury

Tematyka dotycząca e-gospodarki, w szczególności zakresu jej regulacji, podejmowana jest w opracowaniach przygotowywanych przez międzynarodowe organizacje. Przez Organizację Współpracy Gospodarczej i Rozwoju (*Organisation for Economic Co-operation and Development* — OECD, 2015b, s. 16), zostały wyróżnione obszary e-gospodarki, na które składają się: sprzedaż detaliczna (e-biznes), transport (zautomatyzowane pojazdy), edukacja (*Open Online Courses*), zdrowie (rejestry elektroniczne i spersonalizowane leczenie), interakcje społeczne i relacje osobiste (media społecznościowe) (OECD, 2015b, s. 16). Argumentami ekonomicznymi przemawiającymi za wprowadzeniem regulacji, które są prezentowane w literaturze przedmiotu, są przykładowo: działania grup interesu, ochrona danego przemysłu, chęć zdobycia poparcia wyborców przy następnych wyborach. Ostanie uzasadnienie jest wyjaśniane przez Szkołę Chicagowską, jako popyt na regulacje (Stingler, 1971, s. 3). Często przywoływanym terminem, w dyskusji nad regulacjami, jest zawodność rynku. R. Baldwin i in. (2013, s. 15), uzasadniają interwencjonizm faktem, że niekontrolowany rynek zawodzi w zakresie wytwarzania rezultatów i zachowań, które są zgodne z dobrem publicznym. W przypadku e-gospodarki, bardzo znaczącą zawodnością rynku jest asymetria informacji. Konkurencyjne rynki, mogą funkcjonować poprawnie, jeśli konsumenci są wystarczająco poinformowani, aby podjąć racjonalne decyzje i maksymalizować swoją użyteczność. Rynek może zawodzić w dostarczeniu adekwatnych informacji z wielu powodów. Przykładowo, informacja może być kosztowna (koszt przeprowadzenia badań), producent informacji może nie być nagradzany przez użytkowników informacji (brak motywacji, aby dostarczać informacje na rynek). Ponadto, mogą także istnieć powody, aby informację zafałszować (Baldwin i in., 2013, s. 18). W publikacjach Organizacji Traktatu Północnoatlantyckiego (*North Atlantic Treaty Organization* — NATO), zwraca się uwagę na brak wartościowych informacji (Zimmermann, 2014, s. 3). Istnieją oczywiście szacunki dotyczące strefy e-biznesu, jednak brak jest wartościowych ocen dla sfery cyberprzestępczości (Guerra, 2009). Ponadto, znacząca część badań jest przeprowadzana przez prywatne organizacje, często związane ze sferą cyberbezpieczeństwa. Zasadnym jest wiec podchodzenie z dystansem do prezentowanych przez nie wyników. Dodatkowo, pomiar zjawiska jest utrudniony przez dynamiczny wzrost znaczenia Internetu i cyberprzestrzeni. Prognozuje się, że w 2019 roku, przepływ danych w Internecie będzie sześćdziesiąt cztery razy większy, niż w 2005 roku. Warto nadmienić, że w 2012 roku obieg informacji w Internecie był dwanaście razy większy, niż w 2005 roku. Istotne przy tym jest, że rozwój e-gospodarki wpływa na wszystkie elementy krajowego rynku, nie tylko na przedsiębiorstwa o charakterze technologicznym. Oszacowano, że 75% korzyści wynikających z Internetu, jest przejmowane przez przedsiębiorstwa niezwiązane z technologią (Pepper i in., 2016, ss. 39–40). Analizując regulacje, należy również rozważyć, jaki jest ich cel i skuteczność. Zgodnie z przedstawionymi, ekonomicznymi motywami wprowadzania regulacji, powinny one służyć przede

wszystkim usuwaniu negatywnych efektów zewnętrznych i zapewnieniu efektywnej wymiany rynkowej. W kontekście niniejszego artykułu, będą to przede wszystkim trzy cele:

- wspieranie kontaktów,
- ochrona wrażliwych danych,
- ochrona własności intelektualnej.

Zapewnienie sprawnej realizacji umów w wymianie handlowej jest istotne z punktu widzenia życia gospodarczego i teorii ekonomii (Hadfield, 2008, s. 175). W niniejszym artykule ograniczono się jedynie do problemu realizacji kontaktów, który jest w centrum zainteresowania Nowej Ekonomii Instytucjonalnej. Na potrzeby analizy regulacji, wykorzystano teorię kosztów transakcyjnych O. Williamsona (1998, s. 32). Teoretycznych podstaw, w zakresie ochrony wrażliwych danych i własności intelektualnej, dostarcza ekonomika cyberbezpieczeństwa lub ekonomika ochrony informacji (Anderson i Moore, 2006, s. 24). Dorobek ten można łączyć z teorią transakcji, jednak częściej wiąże się go z negatywnymi efektami zewnętrznymi. Jego wkład do teorii ekonomii jest istotny, gdyż brak bezpieczeństwa wskazanych rodzajów danych i formy własności, powoduje negatywne efekty zewnętrzne (CCDCOE, 2015, s. 10). Analizując dotychczasowe rozwiązania w tym zakresie, należy zwrócić uwagę na dokumenty prawne oraz międzynarodowe wytyczne i porozumienia. Są one podstawą regulowania e-gospodarki, zawierają szczegółowe przepisy i wskazują kierunki rozwoju regulacji. W dalszej części Sekcji 2. przedstawiono poszczególne rozwiązania.

Organizacją, mającą znaczący wpływ na badanie cyberprzestrzeni i e-gospodarki, jest NATO. Najistotniejszą publikacją, przygotowaną we współpracy z tą organizacją, jest pozycja autorstwa M. Schmitt (2013). Pomimo, że jej tematyka skupiona jest przede wszystkim na zagadnieniu cyberprzestrzeni w odniesieniu do wojskowości, zawarte zostały również liczne zagadnienia, istotne również dla rynkowych aspektów jej wykorzystania. Jednym z nich jest kwestia jurysdykcji cyberprzestrzeni. Łączy się to z problemem regulowania globalnego zjawiska na stopniu państwowym. Obecnie, przyjmuje się, że jurysdykcja w kwestii cyberprzestrzeni, dzieli się na trzy obszary (Schmitt, 2013, s. 18):

- jurysdykcja nad osobami zaangażowanymi w działalność przestępczą, w tym także osobami prawnymi;
- jurysdykcja nad infrastrukturą zlokalizowaną w danym państwie;
- jurysdykcja wynikająca z międzynarodowego prawa.

Należy zwrócić uwagę na problem natury technicznej wynikający ze wskazanych obszarów. Wiele usług w cyberprzestrzeni opartych jest na technologii chmury lub innych rozwiązaniach, które wykraczają poza zasięg terytorialny jednego państwa (Schmitt, 2013, s. 19). Przykładem trudności związanej z jurysdykcją, są działania podjęte przeciwko grupie przestępczej, znanej jako *DarkMarket*, przez Federalne Biuro Śledcze (*Federal Bureau of Investigation* — FBI). Czynności te, zostały przeprowadzone na terytorium Wielkiej Brytanii, Niemiec i Turcji. Sięgały więc poza granice narodowe. Ponadto, strona internetowa *DarkMarket* znajdowała się na licznych serwerach, zlokalizowanych w różnych państwach (Glenn, 2013, s. 134). W Stanach Zjednoczonych coraz częściej zwraca się uwagę na globalne konsekwencje państwowych regulacji. W 2007 roku, Transatlantycka Rada Gospodarcza (*Transatlantic Economic Council* — TEC), postawiła następujące cele: zwiększenie wymiany informacji na temat działalności regulacyjnej, szacowanie ryzyka i koordynacja poszczególnych sektorów gospodarki. Podobne porozumienia zostały nawiązane przez Stany Zjednoczone m.in. z Kanadą i Meksykiem, zaś w ramach agencji *Administrative Conference of the United States*, promowano dalsze działania w celu promowania: transparentności, wzajemnego zaufania, wymiany informacji i międzynarodowej koordynacji (Dudley i Britto, 2012, s. 107).

Istnieją liczne trudności, związane z tworzeniem efektywnych regulacji. Jedną z nich jest konieczność posiadania wszechstronnej wiedzy, bądź ścisłej współpracy specjalistów z różnych dziedzin. Regulacje powinny być oparte na dogłębnej znajomości: rozwiązań

technicznych, zasad funkcjonowaniu walut wirtualnych, wpływu e-gospodarki na całą gospodarkę, jak również teorii regulacji. W Sekcji 3. przedstawiono studium przypadku bitcoina, które prezentuje braki w tej wiedzy.

Istnieją również liczne argumenty przemawiające za nieregulowaniem e-gospodarki. Pierwszy dotyczy dostępu do baz danych prywatnych organizacji. Największe na świecie banki danych osobowych, znajdują się w posiadaniu przedsiębiorstw *Facebook* i *Google*. Fakt, że wielozadaniowa wszechobecność *Google* stanowi pogwałcenie regulacji antytrustowych, może być kwestią sporną. Jednak dzięki temu, że rząd amerykański nie blokuje działań tej firmy w zakresie danych osobowych, ma on do nich dostęp. Daje mu to więc strategiczną przewagę w stosunku do innych państw (Glenn, 2013, s. 12). Poza tym, wiele organizacji działających w e-gospodarce, może, w dużo prostszy sposób, przenieść swoją działalność między państwami, niż podobnej wielkości przedsiębiorstwa działające na tradycyjnym rynku.

Kolejny argument dotyczy dostępu do kapitału za pomocą cyberprzestępczości. Słabiej rozwinięte państwa mogą nie oferować opcji związanych z dostępem do pożyczek, dofinansowań i kredytów, które pozwoliłby na rozwój przedsiębiorstw. Poza tym, państwa te mają zazwyczaj mniejszy dostęp do innowacyjnych rozwiązań. Braki te, można skutecznie zniwelować ograniczając regulacje w zakresie ochrony własności intelektualnej i cyberprzestępczości, bądź zmniejszając skuteczność tych regulacji (Glenn, 2013, s. 63). Często podawanym przykładem w tym zakresie jest Ukraina w latach 90. XX wieku, czy Rosja i Chiny (Ablon i in., 2014, s. 6). W państwach tych, cyberprzestępczość jest często wykorzystywana przez władzę, a więc istnieje dodatkowa motywacja, aby jej nie zwalczać, o ile nie szkodzi ona wewnętrznemu rynkowi.

Ostatni argument przeciwko regulacji e-gospodarki, wiąże się z teorią wyboru publicznego, a także podejściem do regulacji, reprezentowanym przez Szkołę Chicagowską. Według G. Stigler (1971, s. 3), niedostateczny jest popyt na regulacje, wskazuje on także na ich brak. Współczesny rozwój społeczeństwa i techniki, a także wspomniany w Sekcji 1. ich wzajemny determinizm, wykształciły kulturę szybkiego dostępu do informacji, co więcej, dostępu taniego. W niektórych kwestiach, związanych z piractwem, czy własnością intelektualną, może występować silny opór społeczeństwa przed regulacjami. Ustalenie dokładnych wartości piractwa jest bardzo trudne. Według szacunków *McAfee* (2014, s. 11), piractwo komputerowe w 2013 roku było warte od 1 do 16 mld USD, co stanowiło od 0,008% do 0,02% ówczesnego, światowego PKB. Według *Business Software Alliance* (2009, ss. 6–7), w 2009 roku, w skali całego świata, aż 41% oprogramowania zainstalowanego na komputerach było wersją piracką, co kosztowało przemysł oprogramowania około 53 mld USD. Przekłada się to w sposób oczywisty na bardzo dużą grupę wyborców, którzy mogą poczuć się zagrożeni przez wprowadzenie skutecznych regulacji zwalczających różne wersje cyberprzestępczości. Logicznym jest więc fakt, że zgodnie z teorią wyboru publicznego, istnieje silna motywacja do tego, by nadać priorytet kwestiom, które sprzyjają pozyskaniu głosów wyborców, natomiast pomijać te, które mogą zmniejszyć szansę wygranej w kolejnych wyborach.

3. Polskie i zagraniczne rozwiązania regulacyjne dotyczące e-gospodarki

W Sekcji 3. uwzględniono dwie grupy regulacji. Pierwszą stanowią te, wprowadzone w Polsce, natomiast drugą, normy międzynarodowe.

W Polsce, podstawowym aktem prawnym, na którym opiera się zwalczanie cyberprzestępczości, jest ustawa *Kodeks karny* (1997), a w szczególności:

- art. 190a § 2 — podszywanie się pod inną osobę, fałszywe profile;
- art. 202 — publikowanie treści pedofilskich;
- art. 256 — szerzenie ekstremizmu politycznego, treści faszystowskich;
- art. 267 § 1 — nieuprawnione uzyskanie informacji (tzw. *hacking*);

- art. 267 § 2 — stosowanie podsłuchu komputerowego (tzw. *sniffing*);
- art. 268 § 2 — udaremnienie uzyskania informacji;
- art. 268a — udaremnienie dostępu do danych informatycznych;
- art. 269 § 1 i 2 — stosowanie sabotażu komputerowego;
- art. 269a — rozpowszechnianie złośliwych programów oraz tzw. *cracking*;
- art. 269b — stosowanie tzw. „narzędzi hackerskich";
- art. 271 — handlowanie fikcyjnymi kosztami;
- art. 286 — popełnianie oszustw za pośrednictwem Internetu;
- art. 287 — popełnianie oszustw komputerowych.

Podstawowym aktem prawnym, na którym opiera się ochrona prawa autorskiego i praw pokrewnych w Polsce, jest *Ustawa o prawie autorskim i prawach pokrewnych* (1994). Prawa autorskie i pokrewne, w ramach zwalczania przestępczości gospodarczej, zaliczane są do szeroko rozumianej przestępczości komputerowej. Pozostałe regulacje mające charakter pomocniczy, to przede wszystkim:

- ustawa *Kodeks postępowania cywilnego* (1964);
- *Ustawa o zwalczaniu nieuczciwej konkurencji* (1993);
- ustawa *Kodeks karny* (1997);
- *Ustawa o ochronie baz danych* (2001);
- *Ustawa o świadczeniu usług drogą elektroniczną* (2002a);
- *Ustawia o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym* (2002b).

W polskim prawie istnieje wiele regulacji, które mają służyć wpływaniu na e-gospodarkę. Należy zwrócić uwagę, że wśród tych przepisów istnieją tylko trzy ustawy, które odnoszą się w sposób bezpośredni do problemów związanych z nowym rodzajem gospodarki.

W skali międzynarodowej, propozycję regulacji przedstawiło wiele znaczących organizacji międzynarodowych. Unia Europejska przedstawiła *Decyzję ramową w sprawie zwalczania terroryzmu* (2002) oraz *Dyrektywę dotyczącą ataków na systemy informatyczne* (2013). Warto zwrócić uwagę, że obie regulacje mają raczej charakter wojskowy, niż gospodarczy.

Zupełnie inne podejście prezentuje NATO. Priorytetem jest w tym przypadku utworzenie organizacji mających zwalczać cyberzagrożenia i prowadzenie działań informacyjnych. W ramach pierwszego celu, powstały dwie organizacje: *Cyber Defence Management Board* (CDMB) i *Cooperative Cyber Defence Centre of Excellence* (CCDCOE). Drugi cel obejmował wydanie wielu istotnych publikacji odnoszących się do cyberzagrożeń i cyberprzestrzeni ogółem. OECD (2015a, ss. 7–8), ograniczyła się do utworzenia pewnych wskazówek dotyczących systemów informacyjnych. Organizacja ta, zajmuje się również publikowaniem wyników licznych badań i opinii dotyczących e-gospodarki. Najbliższe lata będą kluczowe w kwestii ukierunkowania regulacji e-gospodarki. Staje się ona coraz istotniejsza wśród międzynarodowej społeczności, a przez to również dla rządów poszczególnych państw. Przejawia się to w zwiększaniu znaczenia niezależnych organizacji takich, jak np. *Internet Assigned Numbers Authority* (IANA). Jednym z inicjatorów zmian jest Organizacja Narodów Zjednoczonych (ONZ), która stawia sobie za cel budowanie globalnej e-gospodarki. W jej planach zwraca się uwagę na znaczenie państw rozwijających się, które do tej pory charakteryzowały się wysoką aktywnością cyberprzestępczości. Wskazuje się również na fundamentalne znaczenie wolnego dostępu do Internetu, jako otwartej platformy dla biznesu, obywateli i rządów. Zakłada się, że współpraca między tymi trzema grupami, będzie prowadzić do rozwoju innowacyjności w e-gospodarce. Pojawiają się jednak obawy związane ze zdecentralizowaną architekturą Internetu i wolnego, nieograniczonego granicami państw przepływu informacji (OECD, 2015b, s. 20). Prezentowane podejście do kwestii e-gospodarki, różni się więc od postrzegania innych obszarów gospodarki. Rząd nie jest traktowany jako byt nadrzędny, a jako je-

den z uczestników e-gospodarki, który bierze udział w tworzeniu innowacji i ich obrocie.

4. Metody

Analizując problem regulacji e-gospodarki, odniesiono się do aktów prawnych i literatury z zakresu e-gospodarki i regulacji. Uwzględniono również prognozy na temat rozwoju trendów w prawie międzynarodowym i sposobie rozwoju e-gospodarki. Informacje te, wykorzystano m.in. do analizy walut wirtualnych i możliwości regulacyjnych e-gospodarki w przyszłości, a zatem również pewnego kształtu wymiany rynkowej.

5. Przypadek walut wirtualnych

Przykład kryptowalut, na wiele sposobów, odzwierciedla trudności związane z regulacją e-gospodarki, ale także wskazuje na konieczność jej wprowadzenia. Bitcoin, i jemu podobne waluty, są często wykorzystywane do aktywności przestępczej. Stanowią one również problem przy opodatkowaniu, a kwestią dyskusyjną jest nie tylko to, jak je regulować, ale też, czy w ogóle powinny być zalegalizowane, czy też całkowicie zakazane. Od 2013 roku firmy, które zajmują się transferem walut wirtualnych w Stanach Zjednoczonych, zobligowane są do posiadania odpowiedniej licencji, wystawianej przez agencję *Financial Crimes Enforcement Network* (FinCEN). Wymaga się od nich również zbierania informacji na temat transakcji. Agencja ta, przedstawiła projekt regulacji wymuszającej rejestrację użytkowników bitcoina posiadających go do celów komercyjnych. Słabością tej regulacji jest fakt, że nie obejmuje ona firm i jednostek, które: „kopią" bitcoin dla wewnętrznych celów, tworzą lub sprzedają oprogramowanie do transakcji na walutach wirtualnych, kupują lub sprzedają waluty wirtualne, jako inwestycje dla własnych celów (Wiśniewska, 2016, s. 108). Należy zwrócić uwagę na bardzo wąską regulację odnoszącą się jedynie do jednej waluty wirtualnej. Zakładając, że regulacja obejmowałaby wszystkie tego rodzaju waluty korzystające z kodu źródłowego bitcoina, nadal można wątpić w jej skuteczność. Jeśli jednak byłaby ona wysoce efektywna, to spowodowałaby tylko osłabienie pozycji tego typu walut na rynku, na korzyść innych rozwiązań. Poza tym, na podstawie przedstawionych wyjątków można przewidywać, że ta forma regulacji, będzie skutecznie omijana.

Stany Zjednoczone zostały przywołane jako przykład regulacji walut wirtualnych z racji tego, że w ich posiadaniu znajduje się największa liczba regulacji bitcoina. W przypadku innych państw, normy prawne albo nie istnieją, albo są dużo bardziej ograniczone. W państwach tych, bitcoin jest zakazany, lub po prostu uznaje się go za walutę. W przypadku Polski, bitcoin, jak i inne waluty wirtualne, są nadal nieuregulowane, przez co należy rozumieć brak przepisów bezpośrednio odnoszących się do obrotu nimi i wykorzystywania ich jako środka płatności. Jeszcze większa trudność związana jest z opodatkowaniem bitcoina i walut wirtualnych. Istnieją w tym zakresie dwa podejścia. Pierwsze, polega na traktowaniu go jako waluty i opodatkowanie transakcji z jego wykorzystaniem. Wówczas bitcoin traktuje się w podobny sposób, jak każdą, zagraniczną walutę, stosowaną na terenie danego państwa. W przypadku drugiego podejścia bitcoin uznany jest za towar. Wówczas opodatkowany jest on, jak każda, inna własność. Zapłatę bitcoinem traktuje się wówczas, jako dwie osobne transakcje w jednej, tj. wymiana bitcoina na pieniądz i transakcja płatnicza (Perez, 2017). W zależności od wspominanych w Sekcji 2. regulacji i podejścia do walut wirtualnych w danym państwie, sposób opodatkowania może być pewną kombinacją wymienionych w Sekcji 4. podejść. W przypadku, gdy bitcoin jest zakazany na terenie danego państwa, oczywiście nie podlega opodatkowaniu.

6. Zakończenie

E-gospodarka, będąca wynikiem zarówno rozwoju technicznego, jak i przemian społecznych, wymaga nowego podejścia do regulacji. Następuje pełne rozdzielenie lokalizacji

podmiotu gospodarczego i rynku, na którym on działa. Wymienione w Sekcji 2. rozwiązania techniczne, doprowadziły do sytuacji, w której nawet produkty materialne mogą być sprzedane w coraz prostszy sposób, bez kosztów transportu, lub produkowane za pomocą druku trójwymiarowego. Podobny stan rzeczy występuje w przypadku walut wirtualnych, które nie są regulowane przez żaden bank centralny. Ponadto, coraz silniej odczuwana jest asymetria informacji, która ma wpływ na rynek, ale także na możliwości regulacyjne. Jeśli przepływ danych w Internecie będzie wzrastał z taką samą szybkością, jak obserwowano w ostatnich latach, wówczas kontrola treści i egzekwowanie praw w cyberprzestrzeni stanie się nie tylko coraz bardziej kosztowne, lecz wręcz niemożliwe. Szybkość rozwoju technicznego i relacja między techniką a społeczeństwem, jest dostatecznie zaawansowana, aby niemożliwe było uregulowanie e-gospodarki w zadowalającym stopniu. Trzecia rewolucja przemysłowa stworzy konieczność zmian w metodach regulacyjnych państwa. Jak wskazano w Sekcji 2., jego rola na rynku zmienia się z bytu ustalającego zasady gry, na uczestnika, który musi współpracować z innymi podmiotami. Należy spodziewać się, że powstanie konkurencja między systemami instytucjonalnymi różnych państw, które będą oparte na włączeniu, a nie, jak dotychczas, na usunięciu części użytkowników. Możliwe, że działalność państwa zostanie skupiona na zapewnieniu bezpieczeństwa prowadzenia nowych form działalności i oferowaniu korzyści z legalnego działania. Wynikać to będzie z niemożności dogłębnej i szerokiej regulacji i łatwości, z jaką możliwe jest ukrywanie informacji i przenoszenie działalności. Oznacza to nowe wyzwania dla ekonomii. Coraz istotniejsza staje się kwestia budowania nowego porządku gospodarczego, który maksymalnie wykorzysta nowe warunki gry rynkowej.

Bibliografia

Ablon, L., Libicki, M.C., i Golay, A.A. (2014). *Markets for cybercrime tools and stolen data: Hackers' bazaar*. Pobrane 25.04.2017 z http://www.rand.org.

Anderson, R., i Moore, T. (2006). The Economics of information security. *Science*, 314(5799). doi:10.1126/science.1130992.

Baldwin, R., Cave, M., i Lodge, M. (2013). *Understanding regulation. Theory, strategy and practice*. New Jork: Oxford University Press.

Business Software Alliance. (2009). *Software piracy on the Internet: a threat to your security*. Pobrane 20.04.2017 z http://portal.bsa.org.

CCDCOE. (2015). *Economic aspects of national cyber security strategies*. Pobrane 20.04.2017 z https://ccdcoe.org.

Decyzja ramowa Rady 2002/475/WSiSW z dnia 13 czerwca 2002 r. w sprawie zwalczania terroryzmu (OJ L 164, 22.6.2002).

Dudley, S.E., i Britto, J. (2012). *Regulation: a primer*. Washington: Mercatus Center at George Mason University.

Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW (OJ L 218, 14.8.2013).

Glenn, M. (2013). *Mroczny rynek. Hakerzy i nowa mafia*. Warszawa: W.A.B.

Guerra, P. (2009). *How economics and information security affects cyber crime and what this means in the context of a global recession*. Pobrane 20.04.2017 z http://www.blackhat.com.

Hadfield, G. (2008). The many legal institutions that support contractual commitments. W: C. Menard, i M. Shirley (red.), *Handbook of New Instututional Economics*. Berlin: Springer.

McAfee. (2014). *Net losses: estimating the global cost of cybercrime. Economic impact of cybercrime*. Pobrane 20.04.2017 z https://www.mcafee.com.

OECD. (2015a). *Digital security risk management for economic and social prosperity*. Pobrane 20.04.2017 z http://www.oecd.org.

OECD. (2015b). *OECD Digital economy outlook 2015*. Pobrane 20.04.2017 z http://www.oecd.org.

Pepper, R., Garrity, J., i LaSalle, C. (2016). Cross-border data flows, digital innovation, and economic growth. W: S. Baller, S. Dutta, i B. Lanvin (red.), *The Global Information Technology Report 2016*. Pobrane 20.04.2017 z https://www.weforum.org.

Perez, W. (2017). *How Bitcoins are taxed*. Pobrane 15.04.2017 z https://www.thebalance.com.

Rifkin, J. (2014). *The zero marginal cost society: the Internet of things, the collaborative commons and the eclipse of capitalism*. New Jork: Palgrave Macmillan.

Schmitt, M. (2013). *Tallinn manual on the international law applicable to cyber warfare*. New York: Cambridge University Press.

Stigler, G. (1971). The theory of economic reguluation. *The Bell Jurnal of Economic and Management Science*, 2(1).

Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz.U. 1993 nr 47 poz. 211).

Ustawa z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (Dz.U. 1964 nr 43 poz. 296).

Ustawa z dnia 18 lipca 2002a r. o świadczeniu usług drogą elektroniczną (Dz.U. 2002 nr 144 poz. 1204).

Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (Dz.U. 2001 nr 128 poz. 1402).

Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. 1994 nr 24 poz. 83).

Ustawa z dnia 5 lipca 2002b r. o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym (Dz.U. 2002 nr 126 poz. 1068).

Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. 1997 nr 88 poz. 553).

Vannoy, S., i Palvia, P., (2010). The social influence model of technologyadoption. *Communications of the ACM*, 53(6).

Williamson, O., (1998). *Ekonomiczne instytucje kapitalizmu. Firmy, rynki, relacje kontraktowe*. Warszawa: PWN.

Wiśniewska, A. (2016). Bitcoin jako waluta wirtualna. W: I. Pietryka (red.), *Problemy Gospodarki Światowej*, tom V. Toruń: Instytut Badań Gospodarczych, Polskie Towarzystwo Ekonomiczne Oddział w Toruniu.

Zimmermann, A. (2014). International law and 'Cyber Space'. *ESIL Reflections*, 3(1).

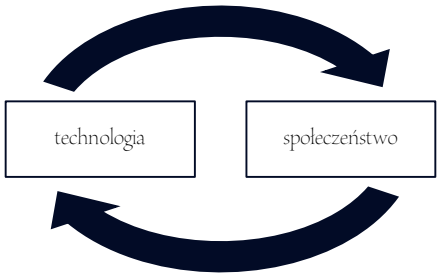
Informacje uzupełniające

Wkład autorski: autor zaakceptował ostateczną wersję artykułu.

Uwagi: wyniki badania były zaprezentowane w innej formie, tj. wystąpienia na VII Ogólnopolskiej Konferencji Naukowej *Problemy gospodarki światowej* (Toruń, 28.04.2017).

Aneks

Schemat 1.
Wzajemny determinizm technologii i społeczeństwa



Źródło: Vannoy i Palvia (2010, s. 150).

Digital economy: regulatory issues

Abstract

Motivation: The dynamic development of telecommunication technology and linked with it social change, created new conditions for economy functioning. They are related with change in the state role and its regulation ability. Digital economy is a global phenomenon that is regulated locally. From the point of view of economic sciences, understanding the currently existing principles of its functioning, both in the context of opportunities as well as threats, is the basis for effective research and modelling. This gives an opportunity for verify previous economic theories under new circumstances. This is a starting point for research on the new economic reality.
Aim: The aim of this article is to review theories of digital economy regulation as well as the existing solutions to the problem of regulation of this global phenomenon. Based on the collected material, an attempt was made to identify the direction of digital economy development and the possibility of its regulation.
Results: Currently existing solutions in terms of digital economy regulation may be considered as insufficient. Based on the Bitcoin case, it can be stated that the global approach to the digital economy is inconsistent. In general, there is also lack of coherent approach to the regulation of new economic phenomena. Considering the dynamic technology development and the high probability of further market innovations, it seems necessary to search for flexible solutions and theories specific to digital economy.

Keywords: *regulation; digital economy; cybercrime; e-commerce; bitcoin*
JEL: *E40; B52; O19*